OUT OF THE SHADOWS:
SUVERSION AND COUNTERCULTURE IN THE DIGITAL AGE

by

Christopher E. Whyte

A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Political Science

Committee:

_____ A. Trevor Thrall, Chair

_____ Edward Rhodes

_____ Eric McGlinchey

_____ Ming Wan, Program Director

_____ Mark J. Rozell, Dean

Date: _____ Summer Semester 2017
George Mason University
Fairfax, VA

Out of the Shadows: Subversion and Counterculture in the Digital Age

A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

by

Christopher Whyte
Master of Arts
George Mason University, 2012
Bachelor of Arts
College of William & Mary, 2010

Director: A. Trevor Thrall, Associate Professor
Schar School of Policy and Government

Summer Semester 2017
George Mason University
Fairfax, VA

Dedication

This dissertation project is dedicated to my wonderful wife Susan, whose unconditional love and support has been at the heart of every success I've experienced in the process of earning my doctorate.

Acknowledgements

A great number of people deserve recognition for making the process of writing my dissertation easier, more fulfilling and more likely to put me productively on the right path in the early stages of my career. Among so many others, I owe great thanks to Trevor Thrall for his many wise words as my advisor and the chair of my dissertation committee. Trevor has not only regularly gone out of his way to help me in my degree-seeking and job-finding efforts; he has masterfully tread the line between devoted mentor and friend. Under his tutelage, my scholarly efforts have qualitatively improved by several degrees of magnitude. I must now only apologize for the incredible number of words I have forced him to read over the years of my degree.

I would like to thank family for their love and support over the past several years. In particular, I would like to acknowledge the support of my parents in all things. Thank you for being there to hear my rant about inane project details and thanks for reassuring me whenever I doubted what I was doing. Likewise, I would like to thank my sister Emma for sharing her own experiences and offering feedback in a way that few siblings are equipped to do. You have been an invaluable friend and guide.

I would likewise be remiss if I did not thank my closest friends for their tireless efforts to take my mind off of issues – mundane and unusual alike – related to my degree. Colligan, Kyle, let's face it – you guys carried me.

Finally, I owe all my successes of the past few years and, at times, my sanity to my immediate family – my canine sidekick Willie and my wonderful wife Susan. Willie, you're a good boy. Susan, I love you and I like you.

Table of Contents

List of Tables

List of Figures

Abstract

Out of the Shadows: Subversion and Counterculture in the Digital Age

Christopher Whyte, Ph.D.

George Mason University, 2017

Dissertation Director: Dr. A. Trevor Thrall

Subversive groups utilize information and communications technologies (ICTs) for many activities, both legitimate and illicit. This dissertation studies the patterns and determinants of ICT usage amongst subversive groups in world politics. Specifically, this project undertakes the first comprehensive study of how extreme non-state actors utilize ICT for persuasion and why some groups use ICT antagonistically despite clear incentives not to. I demonstrate that subversive activists most often employ low-intensity digital techniques in efforts to antagonize and that agents of antagonism – hackers, script kiddies and hostile activists – are most often found among peripheral elements of subversive movements. Based on available evidence, I then theorize that greater incidence of digital antagonism emerges from the revisionist statements made by subversive leaders about aims and methods. When such statements are made, peripheral hackers are incentivized to employ shady methods when galvanizing supporters and disrupting the activities of societal opponents. When leaders move to emphasize participatory approaches to subversion, incentives to use ICT antagonistically are muted.

Chapter 1
Introduction

Christopher E. Whyte

On the 17th of December, 2011, a man called Mohamed Bouazizi stood in the middle of traffic just south of the city center of Tunis and exclaimed that, thanks to government regulation, he had no legitimate way to make a living. Then, he doused himself in gasoline and lit a match. Boazizi's self-immolation in protest of unfair government regulation, corruption and more led to mass protest of the Tunisian government in the first of the national events that would come to be known collectively as the Arab Spring. Over the course of the next two months, protesters backed by a range of civil society organizations would succeed in ousting President Zine El Abidine Ben Ali from office and forcing democratic reforms.

Over the next several years, similar protests movements would materialize across North Africa and the Middle East. However, the Tunisian Revolution remains relatively unique among the national episodes that constituted the Arab Spring in that government practices were not contested only on the streets of Tunis. Rather, dissent and antagonism that characterized protests on the street were mirrored by actions taken online. In response to government efforts to limit national access to Internet services and crack down on rampant criticism, opponents of Ben Ali took to the web to disrupt government services, to vandalize government websites and to attempt to expose specific

incidents of corruption to the public. Through February of 2012, both Tunisian activists like Slim Amamou and foreign hackers linked with various hactivist outfits undertook operations to support democratization efforts and to encourage popular support for ongoing protests via digital antagonism. These operations prominently included widespread distributed denial of service (DDoS) attacks against companies cooperating with the government and doxxing – the publication of stolen, private information – that targeted entrenched political elites.

The example of the Tunisian Revolution is illustrative of how dissidents can use the web to both mobilize and antagonize. However, it is not particularly representative of the conditions in which such activities are often found. Certainly, the use of web technologies to stimulate social or political change is common in the world today. But rarely is cyber contention so concentrated and so successful. Digital antagonism is common in recent world history; episodes in which disparate non-state actors come together to prosecute a focused, aggressive digital campaign are not. And, though recent years have certainly seen a number of national revolutions aimed at transforming the basis of political rule around the world, support for what we might think of as "shady" uses of the web technologies is almost never as broad as it was in the Tunisian case. Outside of revolutions, digital antagonism is much more often the tool of society's fringe elements than it is the focus of everyday political activists.

This dissertation project is about those fringe elements. Specifically, this dissertation is about subversion and the digital tools with which radical non-state actors

attempt to create conditions amenable to the transformation of societal norms and corresponding structures. Though often linked to political violence or the efforts of opponents in wartime, subversion is a unique phenomenon that involves uncoupling a population's loyalties from one set of symbols or institutions and transferring them to another. On the rare occasion that subversion succeeds, the result is a dramatic transformation of prevailing normative conditions that, unlike the common persuasion of lobbyists and interest groups, is characterized by a rejection of the foregoing status quo.

This project focuses on a particular aspect of the subversive enterprise – the use of information and communication technologies (ICT) by domestic dissident forces across the globe. Much as it has for sociopolitical actors of all stripes, the worldwide adoption and integration of ICT across almost all functions of global society over the past several decades has changed the landscape and tools of operation for subversive organizations. Subversive groups must not only contend with new abilities to mobilize and affect change; they must also strategize with the dynamics of a digitally augmented public sphere – essentially, new processes of information dissemination and participation – in mind. In essence, obtaining a better understanding of how subversive actors use ICT today is synonymous with the outcome of better comprehending the subversive enterprise – itself a remarkably understudied phenomenon – itself.

To clarify, this dissertation project is not about subversion as a concept or a set of macro outcomes, but rather as practice and a set of methods observed by non-state actors of many stripes. The goal of this research is twofold. First, it is the goal of this

project to shed light on the determinants of non-state actor decisions to variously utilize activist, persuasive, criminal and manipulative practices as component parts of subversive campaigns. Second, and perhaps more importantly, it is my aim in this project to present a foundational effort that describes trends in how non-state actors use ICT for a range of extreme non-violent purposes. Doing so stands to help shed light on the effects of the information revolution beyond just the context of subversive actors in world affairs and to both (1) inform theoretical work on related political phenomena, such as terrorism or state-sponsored information manipulation, and (2) outline assumptions from inference useful to the construction of deterrent and resilience-building state policies.

In the chapters that follow, I address a specific puzzle about the way in which subversive actors utilize ICT in their campaigns. In attempting to fly under the radar, ICTs provide actors abilities to hide, obfuscate and clandestinely organize in preparation for a subversive campaign. Once in the public limelight, ICTs continue to provide subversive groups new and enhanced abilities to coordinate, activate and mobilize in their attempt to affect sociopolitical transformation. In line with the move that successful subversive actors make from counterculture to mainstream voice, group usage of ICTs invariably transitions from emphasis on strategies of subterfuge to those of digital activism. This tendency is evident in a range of modern cases of attempted subversion – including, for example, with anti-Mubarak, pro-Islamist groups in Egypt in 2011 and with the Pussy Riot collective in Russia – and makes a great deal of sense.

Activist strategies are logical outgrowths of a situation in which a group suddenly finds itself relevant to mainstream popular discourse. Renouncement of techniques and strategies that might have once aided the clandestine operation of a group makes particular sense, as such activities often invite government scrutiny and threaten to link a subversive cause with a shady past in the public eye.

What's not clear about subversives' use of the Internet and other ICTs is what motivates some groups to enduringly "keep one foot in the shadows" – i.e. to continue to engage in digital antagonism that involves clandestine, sometimes illicit technologically-supported activities alongside the digital activism that characterizes the later stages of a subversive campaign. Many subversive groups gear shift towards digital activism in later phases of their campaign and abandon alternative uses of ICTs, but some do not. Given what we know of subversive organizations, this is unexpected. Once in the public limelight, continued operation "in the shadows" often threatens the integrity of the ideational platform being espoused in the eyes of the group's target audience. Moreover, use of ICTs for such activities exposes subversive groups to a range of operational challenges, from greater ease of investigation by counter-subversive entities to heightened problems of coordination amongst members. So why do some subversive groups shift gears and abandon such techniques entirely whilst operating in the public limelight, while others do not? What conditions influence or pre-determine the decision to maintain emphasis on "shady" digital practices?

In this project, I demonstrate that subversive activists most often employ low-intensity digital techniques in efforts to antagonize and that agents of antagonism – hackers, script kiddies and hostile activists – are most often found among peripheral elements of subversive movements. Based on available evidence, I then theorize that greater incidence of digital antagonism emerges from the revisionist statements made by subversive leaders about aims and methods. When such statements are made, peripheral hackers are incentivized to employ shady methods when galvanizing supporters and disrupting the activities of societal opponents. When leaders move to emphasize participatory approaches to subversion, incentives to use ICT antagonistically are muted.

In the remaining sections of this introductory chapter, I further explore the premise of this dissertation, namely that the global adoption of ICT has fundamentally altered the parameters for operation for a wide range of actors in world politics. I then outline the parameters of digital antagonism, describe the puzzle to be addressed and briefly discuss the significance of this work for both theory and policy. In short, I argue that greater understanding of subversion and subversive actors is but one positive outcome of this dissertation project, as better comprehension of how non-state actors use ICT and operate in a digitally augmented global environment informs theories of terrorism, insurgency and political activism for the modern era. I then conclude by laying out a roadmap for the dissertation.

1.1. Information Technologies and Subversion

What is "subversion?" In short, the term describes a normative transformation of contemporary society in which the resulting status quo – i.e. the "new normal," reflected in both prevailing ideas and related social and political institutions – directly rejects the legitimacy of the previous one. Subversive activities involve the detaching of popular loyalties from the guiding principles and symbols of one status quo – again, often reflective in particular policies, practices or institutions – and transferring them to those of the subversive force. Naturally, this implies a great number of different activities, from propagandizing and engaging in legitimate political debate to the manipulation of corrupt officials to sway elements of a target population.

For the layman or even the typical international relations (IR) scholar, subversion in world affairs might be said to most visibly manifest as a tool of statecraft. History is replete with examples of leaders, from Louis XIV and Ivan III to Winston Churchill and Vladimir Putin, who have authorized subversive activities abroad as an aid to foreign policy. More common than as statecraft, however, subversion regularly takes place as a homegrown effort to unseat a set of ideas or practices – often formalized in laws or political institutions – and replace them with those of the subversive force. And though such a description likely conjures images of significant and rare historical episodes like Mao's Long March and the efforts of the Việt Cộng, the fact of the matter is that dissentious campaigns to subvert a prevailing status quo are common features of world politics. One need only read the front matter of reporting and punditry today to

see that subversion – from that practiced by global Islamist organizations and extreme anti-globalization advocates to that attempted by liberal activists under repressive regimes – is present in a variety of forms across the full gamut of global social and political systems.

Subversive groups take on a variety of forms and are often constituted of decentralized entities – such as front group proxies or agents detached from a core directing body – that coordinate to achieve complex tasks. Because of the nature of the subversive enterprise as being concerned with broad-scoped normative outcomes, organization tactics inevitably pivot on assessments of three sets of variables – (1) the nature and dynamics of the public sphere (i.e. how is information made available to and framed for the target audience?), (2) the shape of obstacles to subversion (including the nature of prevailing political institutions and the power of different status quo forces), and (3) the resources and tools available to a group. Subversive groups take on a variety of forms and are often constituted of decentralized entities – such as front group proxies or agents detached from a core directing body – that coordinate to achieve complex tasks. Analysis of these variables communicates to a subversive group just how entrenched the normative status quo is and what challenges and opportunities are bound up in a potential subversive campaign.

The premise of this dissertation is a simple one – that systematic changes to the informational substrate of the global public sphere have radically changed the nature of the environment in which subversive groups must operate. This is not an uncommon

claim.[1] Much in the same way that the invention and spread of the Gutenberg movable-type printing press in the 1400s catalyzed broad-scoped changes in social and political systems across Europe over the decades that followed, the invention of network technologies and the systems that enable the maintenance of a digital information ecosystem – particularly the technologies that undergird the Internet – and the integration of information and communications technologies (ICT) across most global societal functions have fundamentally altered the dynamics of the public sphere in several respects.

First, global ICT adoption has resulted in the wholesale digitization of infrastructure. Most tasks, from financial transactions and bookkeeping to utilities' provision, have core digital elements such that related practices and processes have been completely restructured over the past two or more decades. Second, and more specifically, new technologies have transformed the landscape of information access and communications possibilities. A diverse content and connectivity environment of services and features have meant the proliferation of avenues to interface with an audience. And finally, global ICT integration has meant fundamental changes for the nature of information transmission and presentation itself. More than just the emergence of new communications systems, the networkization of information systems and various kinds of

[1] See, among others, Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press, 2012); Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: The (IR)relevant Theory?" *International Political Science Review*, Vol. 27, No. 3 (July 2006), pp. 221–244; and Mary M. Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly*, Vol. 54, No. 2 (June 2010), pp. 381–401.

media have made for new patterns of content framing. Gatekeepers of public opinion are no longer just political elites or traditional media organizations and the presentation of any single piece of information is subject to a great many more input influences than might have been the case a half century ago. In short, as others have argued,[2] the information substrate of world politics has changed so fundamentally that studying the use of ICT by a particular type of actor – in this case, one entirely concerned with the interaction of public sphere information dynamics and civil society institutions – is closely equivalent to studying that actor's strategic operation more broadly.

1.2. What is Digital Antagonism?

What does the information revolution mean for non-state actors in real terms? What tools might subversive actors – among other belligerent non-state entities – turn to in order to enhance the effectiveness of their efforts? In part, non-state actors interested in political participation and persuasion have, for more than a decade, extensively taken advantage of what Jared Diamond and others have commonly called "liberation technologies." Generally, according to Diamond, these technologies are any techniques or digital ability that allows a population or specific non-state group to throw off the chains of repression. It is worth noting, however, that Diamond's work specifically links web technologies to revolutions and to the act of resisting repression. In reality, not all advocacy organizations that use the web to enhance their operation – not

[2] See, for instance, Molly Sauter, *The Coming Swarm: DDoS Actions, Hactivism and Civil Disobedience on the Internet*, Bloomsbury: New York, 2014.

even all extremist groups that do so – are actively engaged in revolutionary efforts. Thus, it seems more reasonable to say that advocacy organizations of all stripes are able to engage in web-based activism – digital efforts to better coordinate and actualize change through the use of email, websites, media sharing services, e-governance tools and more.

At the same time, non-state actors are able to use ICT to antagonize. Regardless of whether the purpose of antagonism is to fight repression or to protest a legitimate democratic government, the fact of the matter is that non-state actors are able to use ICT to break with established laws and standards of non-criminal behavior. Specifically, the information revolution has provided non-state actors with a broad range of tools to disrupt the activities of governments and other elements of modern civil society and to undertake criminal activity in a clandestine fashion. These tools, which are described in greater detail in Chapter 3, are either broadly considered illicit or commonly thought of as useful principally for enabling criminal actions in across the globe. They include denial of service methods of cyber attack, malware, methods of physically sabotaging hardware and methods for stealing information from private networks, as well as more pedestrian spamming, phishing and encryption tools. They differ from instruments of activism in that non-state actors must knowingly violate both legal and normative standards across the board. This distinction is central to the puzzle and research design in the following chapters of this dissertation.

1.2. The Puzzle: Keeping One Foot in the Shadows

In 1934, a set of extrajudicial killings and kidnappings took place in Germany on the orders of the newly elected Chancellor, Adolf Hitler. Operation Hummingbird, colloquially better known in history as the Night of Long Knives, involved operations against several anti-Nazi politicians and activists. However, the main targets of these attacks were members of the Nazi Party itself. Specifically, Operation Hummingbird targeted both mid- and high-level members of the Sturmabteilung, the paramilitary wing of the Party better known as the "Brownshirts." The Brownshirts had been pivotal in the years-long campaign to subvert national politics and propel – both forcefully and then, later, legitimately – Hitler to the Chancellorship of Germany. Operation Humminbird, also called the "blood purge" of 1934, was an effort to expunge liabilities from the infrastructure of the NSDAP. For some months, public opinion had been turning against the thuggish actions of the Brownshirts and the media, increasingly censored, had nevertheless had some small success in linking the actions of the paramilitary wing of the Party to the ideational platform espoused by its highest office.

The Night of Long Knives was a brutal purge of an organization's membership to safeguard to integrity of the political movement and operation in the public's eye. Though brutal, however, it stands as a particularly illustrative example of actions common to political actors that subvert national politics and then move to operate as a legitimate political force. Similar activities are common across the modern history of groups that attempt radical normative transformation. Several groups in Latin America

in the 1950s and '60s, from the pseudo-Marxist populist organization that preceded Shining Path to the initial manifestation of Proseguir, undertook similar efforts to abandon links with criminal elements after successful attempts were made to integrate with the existing political system. And post-Accords elements of Sinn Fein and the Irish Republican Army lent material and political resources to British efforts to deal with the continuing militancy of, among other splinter groups, the Real IRA into the 2000s.

In recent years, a great number of organizations that have used information technologies for a range of operational purposes have abandoned tactics focused on digital subterfuge and disruption in favor of those of digital activism – of reaching out to engage the public. Indeed, as some scholars have noted (Rid, 2011 and Rid 2013, in particular), this pattern of abandonment of emphasis on some strategies in favor of others appears to be particularly pronounced subversive organizations that broadly employ ICT in their operations. Case observations of organizations like the Egyptian Muslim Brotherhood – wherein the events of the Arab Spring present as a marked inflection point between a range of criminal cyber actions undertaken by the Brotherhood since 2002 and a shift in tactics aimed at engaging the public and denouncing disruptive attacks – have demonstrated that groups that have committed to the observation and execution of a digital activist set of strategies have compelling incentives to scale back and eventually abandon the tactical use of ICTs for clandestine purposes. From the use of encryption in intra-organizational communications and financial procedures to the maintenance of anti-establishment websites, the use of ICTs

in line with circumvention and disruption strategies stand to invite the scrutiny of government and intergovernmental organizations invested in the status quo. Too, such activities, revealed to the public, might threaten the integrity of the ideas or the organizational assets involved in pushing ideational transformation. In short, maintained emphasis on such techniques poses a threat to the objective potential of a subversive movement such that they become a liability. These risks are magnified by the realities of operation in the world of digital activism, in which higher member mobility and lower degrees of organizational control expose such groups to various kinds of exogenous shocks.

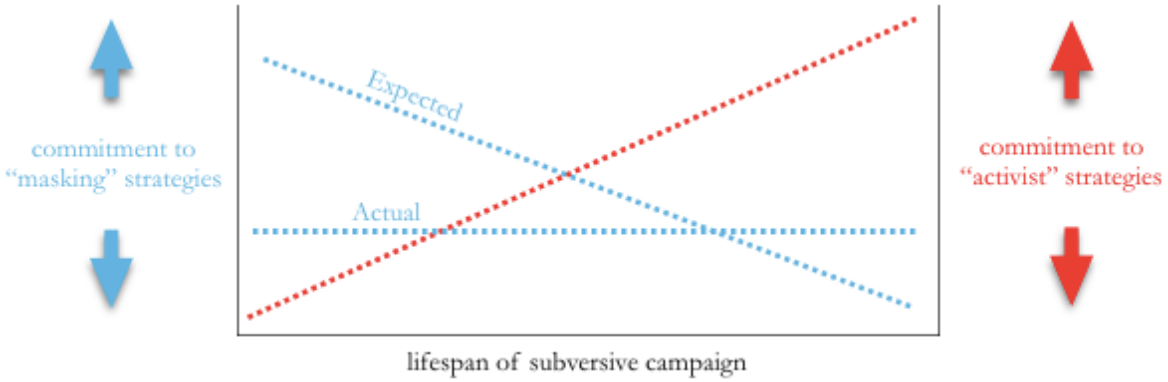

Figure 1.1. Expected vs. actual emphasis on competing strategies of ICT usage for subversive purposes across cases.

In spite of this dynamic, a significant number of groups involved in broad-scoped digital advocacy maintain emphasis on the use of ICT for circumvention and disruption, often prolifically. Case studies presented in Chapters 6 through 10 of this project

describe several such groups. With Civic Passion, for instance, pro-democracy and pro-autonomy activism in Hong Kong over the past five years has been unusually punctuated by incidence of digital antagonism wherein group members have – specifically since 2014 – been associated with website defacements and disruptive denial of service attacks on government officials. Likewise, Germany's far right National Democratic Party (NPD), a group discounted by most as extreme and with historical ties to criminal elements, has in recent decades made massive commitments to digital activism. At the time of writing, more than 5,000 far right websites focused on German politics and society are in operation. More than a third of these have clear ties to the NPD. However, while some such sites do include illicit content, the NPD's sponsorship of web activism appeared, until 2009, typically intolerant of criminality. More recently, however, the rate of incidence of publication of illegal content on far right sites has skyrocketed and NPD member affiliates have been implicated in low-level cyber crime focused on harassment of the country's left-wing political scene. What changed? More broadly, why do some subversive groups abandon while others reinforce commitment to clandestine, "shadowy" ICT usage (see Figure 1.1)? What strategic, environmental, organizational or ideational factors influence a group's decision to renounce or not?

Table 1.1. Breakdown of observed organizations by evidence of antagonistic ICT usage (or not)

	Number of Organizations	
Digital Activists	No Evidence of Antagonistic ICT Usage	Evidence of Antagonistic ICT Usage
All Observations	189	90
Top 10% Most Active	20	7
Top 25% Active	52	18

An effort to answer these questions stands to provide critical insight into the format and function of subversive groups across the globe, as does the basic effort – undertaken in this project's quantitative examination of the puzzle – to see if this tendency towards antagonism is particularly common amongst subversive activists. As Table 1.1 above shows, this is indeed the case. Of 279 organizations studied in this project's large-N investigation, almost a third have used ICT *bot* for activism and antagonism. Moreover, as Figure 1.2 below shows, variation on the dependent variable – i.e. the use of ICT by subversive actors *only* for activism or for *both* activism and antagonism – is not simply a function of commitment to web tools for group functions. Many subversive actors that use the web broadly for activism will antagonize in only a few, specific ways. Others that antagonize often will attempt to engage the public only sparingly. And yet others look to the web across the full gamut of possible actions. Again, what explains the use of ICT for criminal, disruptive purposes alongside use of the web for activism among some, but not all, subversive groups?

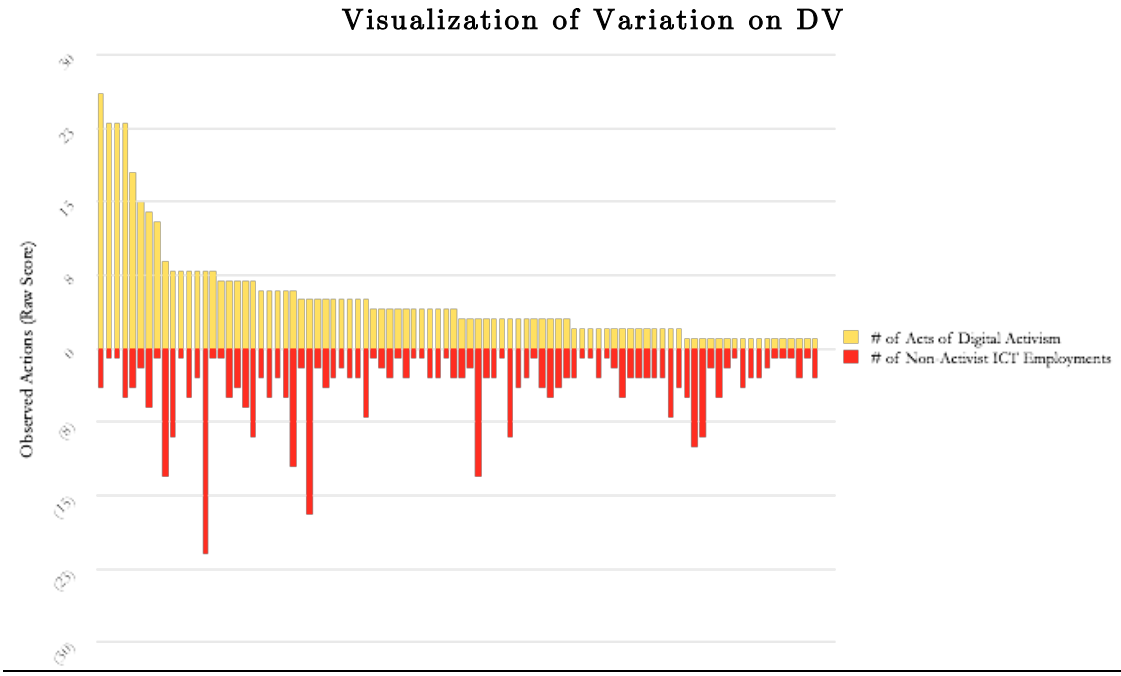

Figure 1.2. Visualization of variation on the dependent variable. This figure shows the raw scores of total uses of ICT as pertaining to digital activism or digital antagonism across the 90 deviator observations, ordered by number of activist employments.

This dissertation is an effort to answer this question through both large-N testing of relevant data on digital activists over the past 30 years and qualitative examination of competing cases in which subversive actors have exhibited divergent behavioral preferences. Below, I outline the steps involved in this task that constitute the remaining chapters of this dissertation project. As outlined above, the results of my analyses suggest several layers of nuance in that, combined, account for decisions made by subversive groups to deviate from the expectations of prior historical analysis and theoretical work.

1.3. Objectives of the Dissertation

At the functional level, this dissertation project has three main objectives. The first of these relates directly to the premise of the puzzle being investigated. The assertion that subversive groups attempting to digitally engage the public also sometimes utilize ICT for disruptive and illicit purposes against the expectations of prior theoretical work is reasonably well established. Rid (2013) outlines several cases of such a deviation and, though his selection of organizations to investigate – including Anonymous and the Earth Liberation Front (ELF) – is questionable from some theoretical perspectives, he arguably does the best job linking such behaviors to the relatively small body of work in modern history focused on the behavior of such groups.[3] However, the bulk of evidence presented in support of the basic premise of the puzzle outlined above comes in the form of several dozen case studies (or multiple case study analyses) of radical persuasive groups around the world in scholarly and non-profit research works over the past two decades. Vidino's (2010) investigation of the Western branch elements of the global Muslim Brotherhood, for instance, outlines unique cases of group ICT usage for a range of shady purposes through the 2000s whilst community-building and activist efforts were underway, particularly in the United Kingdom.[4] Karagiannis and McCauley's (2006) work describe similar trends amongst core and affiliate elements of Hizb ut-Tahrir al-

[3] See Thomas Rid, *Cyber War Will Not Take Place*, Oxford University Press, 2013.
[4] See Vidino, Lorenzo. *The new Muslim brotherhood in the West*. Columbia University Press, 2010. Also, see Vidino, Lorenzo. "The Muslim Brotherhood's Conquest of Europe." *Middle East Quarterly*, 2005.

Islami in Central Asia.[5] Likewise, various studies of civil and human rights movements operating under oppressive societal conditions, including in Russia,[6] China[7] and Iran,[8] have outlined, among other ICT employments, regular usage of websites for explicitly illicit purposes and the use of the darkweb and P2P encryption to hide organization links with outlawed entities.

Despite the relatively robust nature of the literature on this phenomenon, as well as the confirming presumptions made in recent work on the function of human rights organizations in authoritarian states regarding the disincentives to engage in criminal enterprise whilst trying to persuade a population, the fact is that no dataset exists at present to corroborate this claim of a trend. Thus, clearly, the first objective of this dissertation project is to see if there does indeed exist an empirically demonstrable trend

---

[5] See Karagiannis, Emmanuel, and Clark McCauley, "Hizb ut-Tahrir al-Islami: Evaluating the Threat Posed by a Radical Islamic Group That Remains Nonviolent," *Terrorism and Political Violence,* Vol. 18, 2006. Also see International Crisis Group (ICG), *Radical Islam in Central Asia: Responding to Hizb ut-Tahrir,* Asia Report No. 58, June 30, 2003; and Khamidov, Alisher "Countering the Call: The US, Hizb-ut-Tahrir, and Religious Extremism in Central Asia," Washington, D.C.: Saban Center for Middle East Policy, Brookings Institution, Analysis Paper No. 4, July 2003.

[6] See, for instance, McMichael, Polly. "Defining Pussy Riot musically: Performance and authenticity in new media." *Digital Icons: Studies in Russian, Eurasian and Central European New Media* 9 (2013): 99-113; and Voronina, Olga G. "Pussy Riot Steal the Stage in the Moscow Cathedral of Christ the Saviour: Punk Prayer on Trial Online and in Court." *Digital Icons: Studies in Russian, Eurasian and Central European New Media* 9 (2013): 69-85.

[7] For a macro narrative description, see Sullivan, Jonathan. "The Power of the Internet in China: Citizen Activism Online Guobin Yang New York: Columbia University Press, 2009; and Yang, Guobin. *The power of the Internet in China: Citizen activism online*. Columbia University Press, 2009. For a more recent case overview, see Xu, Beina. "Media censorship in China." Council on Foreign Relations 25, 2014; Yang, Guobin. "Internet activism & the party-state in China." *Daedalus* 143.2 (2014): 110-123; and Goldstein, Avery, and Guobin Yang. *The Internet, Social Media, and a Changing China*. University of Pennsylvania Press, 2016.

[8] For general trends and specific examples, see Rahimi, Babak. "Internet and Political Activism in Post-Revolutionary Iran." *The Handbook of Media and Mass Communication Theory* (2014): 907-928; Ricchiardi, Sherry. *Supporting Internet Freedom: The Case of Iran*. Center for International Media Assistance, 2014; and Rahimi, Babak. "Vahid Online: Post-2009 Iran and the Politics of Citizen Media Convergence." *Social Sciences* 5.4 (2016): 77.

amongst some subversive activists to deviate from the expectations of prior theory and continue involvement in shady enterprise.

Relatedly, the second objective of this dissertation project is to take a step beyond the work of Rid, Stam, Tillson and others in conceptually marking a division in what is meant by "liberation"[9] vs. other circumventive/disruptive new information technologies. A great number of projects cite digital technologies that enable social networking and effective organization of citizen groupings as broadly meaningful for protest activities and persuasive political campaigns (as well as for authoritarian governments).[10] However, the "other side of the equation" – i.e. ICT techniques and platforms that are more commonly the domain of extremist groups, intelligence organizations and militants seeking to augment organizational prospects through digital means – are less well categorized in the several literatures that touch on the subject of non-state uses of ICT, including that on protest movements, terrorism online and cyber conflict. This is unsurprising in some ways and naturally reflects one of the key challenges – that of reconciling the different terminologies of behaviors and tactics across categories of different types of actors in world affairs – facing scholars seeking to research cybersecurity issues in the social sciences. Nevertheless, there is a clear need to

[9] The term "liberation technology" first appears in Diamond, Larry. "Liberation technology." *Journal of Democracy* 21.3 (2010): 69-83. Diamond expands on his treatment of ICT in this vein in Diamond, Larry, and Marc F. Plattner. *Liberation technology: Social media and the struggle for democracy*. JHU Press, 2012.

[10] See, for instance, Deibert, Ronald, and Rafal Rohozinski. "Liberation vs. control: The future of cyberspace." *Journal of Democracy* 21.4 (2010): 43-57; Lynch, Marc. "After Egypt: The limits and promise of online challenges to the authoritarian Arab state." *Perspectives on politics* 9.02 (2011): 301-310; MacKinnon, Rebecca. "China's" networked authoritarianism"." *Journal of Democracy* 22.2 (2011): 32-46; Schedler, Andreas. *The politics of uncertainty: Sustaining and subverting electoral authoritarianism*. OUP Oxford, 2013; and Morozov, Evgeny. *The net delusion: The dark side of Internet freedom*. PublicAffairs, 2012.

define what is meant by "shady" or "circumventive" or criminal uses of ICT in the context of subversive groups and to better understand how exactly such extreme non-violent entities use digital technologies. Thus, this dissertation project, in investigating the puzzle, seeks to flesh out and empirically investigate the shape of ICT usage by subversive groups across a spectrum of contexts.

Finally, it is the objective of this dissertation project to examine factors that predict variation from the expectations of subversive group behavior theory outlined above. Again, the chapters that follow primarily aim to answer the question: why do some subversive groups abandon while others reinforce commitment to clandestine, "shadowy" ICT usage? What strategic, environmental, organizational or ideational factors influence a group's decision to renounce or not? In investigating this puzzle, I employ a wide range of independent variable data that speaks to a range of common explanations for non-state actor behavior found in the literatures on terrorism, insurgency and transnational crime found in the social sciences.

1.4. Significance of the Project for Theory and Practice

The findings of this dissertation project are meaningful for a number of reasons. These are discussed in detail in Chapter 12. Foremost among these, however, is the empirical demonstration of the fact that subversive organizations are reasonably more prone to criminality in the digital age than they might have been in eras past. Certainly, a sizable number of radical non-state groups in this vein have always maintained support for criminal elements of society or undertaken explicitly criminal acts. But that number

has remained small over time. By contrast, this project suggests that a much broader number of subversive actors have turned to criminality in the form of illicit web activities. I also demonstrate that the most common set of ICT actions taken by subversive actors in this vein are what might be thought of as low-intensity actions – those cyber attacks, obfuscations and circumventions that violate established law in the most minimal ways. This is, in many ways, unsurprising. Not only do cyber actions tend to be harder to legislate and detect, the characteristics of low-intensity acts of digital antagonism include plausible deniability for belligerents through attribution difficulties, greater opportunities for maintaining secrecy in criminal actions and lower standards of state response based on limited opportunities for non-digital disruption. Cyber antagonism, in short, helps subversive actors irritate and achieve under conditions of dramatically reduced likelihood of being caught.

1.5. Outline of the Dissertation

Chapter 2 of this dissertation project engages the topic of subversion more directly than has been done in this introductory chapter. Though this project is about subversion as a set of practices rather than an outcome, it is still necessarily to engage in a more complete conceptual discussion of what subversion means, looks like and entails for dissident non-state actors operating around the world. It is also necessary to clarify the scope of this study, which rests on non-state dissidents and *not* on either state actors or their proxies attempting to leverage propaganda and to manipulate the information environment for the purposes of foreign policy. Finally, Chapter 2 describes the premise

of the project more fully, linking the contours of the information revolution to the question of non-state subversive behavior.

Chapter 3 then describes the puzzle outlined above in greater detail and develops the theoretical framework of the dissertation. Specifically, discusses a range of possible explanations drawn from a variety of relevant literatures, derives hypotheses and discuss requirements for effective testing. From here, I then describe the project's research design and data collection for quantitative testing presented in Chapter 4. Data used to operationalize the dependent variable and provide the basis for broad-scoped testing of a range of explanations are drawn from the Global Digital Activism Dataset (GDADS), a multi-scholar project based out of the University of Washington, contains both qualitative and quantitative variables describing digital activism campaigns from around the world.[11] The GDADS has been published in two tranches and contains almost eighteen hundred entries (1,180 in the initial tranche, 426 in the second, and more than two hundred additional entries in a supplementary dataset) describing such campaigns. The dataset covers digital activism in more than 150 countries and spans three decades from 1982 to 2012. In addition to qualitative information on digital activist campaigns and basic descriptive measurements of different actions involved in the activist effort (website usage, blog usage, chat/IM coordination, email coordination, e-petition used, etc.), the GDADS also includes detailed data on the intended purposes of different campaign actions and 28 variables on environmental conditions (regime type, rule of law,

[11] For more information, see http://digital-activism.org/projects/GDADSs/.

etc.). All data is documented and freely available, all sources are catalogued and the project behind GDADS provides summary case information for every digital activist campaign covered. I add data to the original GDADS effort, taking advantage of the well-documented coding procedures of the project, in the form of almost 700 additional digital activist episodes and organizations through early 2016. This data resource then serves as a basis for testing.

From this data resource, I identify nearly 300 subversive organizations engaged in digital activist efforts, from blogging and email campaigns to e-petitions and citizen journalism. I then outline data collection undertaken on what we might call "the other side of the equation." Generically, my coding covers incidents across the range of tasks subversive organizations undertake to mobilize, to name, shame and disrupt threats to progress in the form of societal opponents, and to enhance their information environment. Specifically, I code for more than 20 types of disruptive and circumventive ICT activities, including among others, the simple use of websites for illegal and unconstitutional purposes (such as inciting protest against state laws), several categories of website blocking actions, distributed denial of service attacks, malware employments, unauthorized data collection actions, email spearphishing, website defacement and unauthorized hardware installations. The result is a dataset of episodes that allows for the first real empirical exploration of subversive group employments of information technologies. Matched with a range of independent variable information, both original

and drawn from locations such as Polity IV and World Bank indices, this dataset is useful for both broad-scoped descriptive and statistical analysis.

Chapter 4 presents a theory of subversion in the digital age based on both quantitative analysis and subsequent qualitative testing. The analysis presented shows that subversive activists most often employ low-intensity digital techniques in efforts to antagonize and that agents of antagonism – hackers, script kiddies and hostile activists – are most often found among peripheral elements of subversive movements. Based on available evidence, I then theorize that greater incidence of digital antagonism emerges from the revisionist statements made by subversive leaders about aims and methods. When such statements are made, peripheral hackers are incentivized to employ shady methods when galvanizing supporters and disrupting the activities of societal opponents. When leaders move to emphasize participatory approaches to subversion, incentives to use ICT antagonistically are muted.

Chapters 5 through 11 present case study analyses several subversive organizations in two countries that have employed information technologies as part of their campaigns. In each case, the focus is on process tracing decisions and outcomes related to the use of a diverse set of ICT in order to determine key factors relating the subversive enterprise to decisions to "keep one foot in the shadows." By focusing on two countries – Germany and China – in which various subversive groups have operated over a period of years, I am naturally able to study multiple manifestations of the phenomenon under investigation whilst also controlling for context of operation.

Chapters 6 and 7 focus on the case of subversive organizations in Germany over nearly two decades, while Chapters 8, 9 and 10 assess the case of groups in China since the late 1990s. Chapters 11 and 12 then conclude the dissertation with a discussion of findings, corroborating evidence and implications of the project for scholarship and policy.

Chapter 2
What is Subversion?

Christopher E. Whyte

This dissertation project is an effort to produce better knowledge about one critical aspect of the subversive enterprise in the 21st century – the use of information and communications technologies (ICTs) by dissident non-state actors in attempts to subvert national politics. Specifically, I ask why some groups that use ICT for activist purposes – i.e. to engage with a constituency or broader population in a participationist, persuasive fashion – also employ digital techniques for subterfuge and explicitly illicit activities, despite clear incentives not to. Answering this question is of great significance to scholars trying to better understand the behavior of subversive organizations and the use of ICTs by non-state actors more broadly because a superior comprehension of employment of digital techniques is informative of the overall subversive enterprise. The information revolution and the massive worldwide adoption of ICTs across most societal functions have produced global conditions such that understanding subversives' behavior in employing ICTs is essentially synonymous with understanding the subversive effort in general. Thus, this study stands to advance theoretical perspectives on subversion itself and to enhance empirical knowledge and expectations related to associated phenomena.

The puzzle at the heart of this dissertation project is fleshed out more fully in Chapter 3, which then details expectations for testing, research design and approach. First, however, this chapter takes on the task of providing a more complete conceptual picture of what subversion is and what particular form it takes in the digital age. Subversion is one of the most complex sociopolitical phenomena that social scientists study. It is simultaneously self-evident in a cursory examination of many real world situations and difficult to get a handle on for the purposes of testing and theorization. Moreover, the study and description of subversion is something that has gone in and out of vogue over the past several centuries, as different versions of national and international systems have grappled with subversive manifestations of political activism to greater or lesser degrees. The last major surge of interest in the subject, aside from a small number of explicitly subversion-focused examinations in the past decade, came during the early years of the Cold War, as the specter of both global communist subversion and pronounced dissident subversion in places like Libya, Northern Ireland and Indochina drove researchers to look more closely at ideational transformation across the landscape of history. As such, subversion in is understudied both as a historical and contemporary phenomena, leaving a limited foundation for new scholarly work on the subject.

In the sections below, I describe the nature of subversion and address misconceptions and conflations often bound up in a popular understanding of the phenomenon. I then offer a definition of subversion useful for the purposes of

theorization and research design, before discussing the general shape of subversive actors as they are being studied herein – actors engaged in what is called internal or dissident subversion through efforts to undermine, detach and reconstruct the loyalties of a given population to the prevailing status quo. I then revisit the notion that a greater understanding of how subversive actors use information technology equates to better comprehension of subversion as a political phenomenon more generally. Specifically, I outline the premise that links subversion to worldwide changes resulting from the information revolution, before describing new opportunities and challenges faced by non-state actors today.

2.1. What is Subversion?

The actions taken both by subversive elements of societies attempting normative transformation and by governments in trying to suppress a force seen as illegitimate or oppressive are not new features of world politics. The struggle between countercultural elements of different societies trying to achieve broad-scoped change in public perspective and the structural representatives of the status quo opposing them has featured prominently in the affairs of states for hundreds of years. Students of American history know well the episodic regularity with which elected officials have responded to perceived threats from foreign ideologies with the establishment of countersubversive entities for the assurance of continuity in "Americanism." The second President of the United States, John Adams, famously signed into law the Alien and Sedition Acts in 1798 as a response to the dual fear of coup d'etat and subversion emanating from the

ranks of foreign-born immigrants of radical persuasion.[12] In the 1930s, despite there being no law officially banning contestation in the form suggested, Congress formally recognized and enabled what would become the House Un-American Activities Committee as an investigative body with broad oversight to examine cases of disloyalty and subversion, much of which was purportedly the outcome of actions by the American Communist Party and a range of quasi-fascist oligarchic organizations.[13]

As is described below, subversion is countercultural – it is about hearts and minds. It is about normative outcomes and intentions on the part of subversive actors. But, just as terrorism is prone to sideslipping towards criminal and insurgent activities, subversive actors can themselves sideslip into what we would ultimately categorize as related forms of political advocacy or counter-establishment activities – revisionist political violence, crime or mundane activism aimed at modification, not transformation. Such a tendency is evident in innumerable episodes of subversion involving external patronage, from the 1888 "Bay of Bargas" effort to subvert Hungarian authority in service to Russian interests to the CIA-backed activities of Kuomintang Nationalists operating to persuade and incite sedition in mainland China in the 1950s.[14] Likewise, subversion has often benefited from oligarchic patronage and a *lack* of such direction towards structural overthrow. The corporatization of Spain and the subversive

[12] For a good description, see Smith, James Morton, *Freedom's Fetters: The Alien and Sedition Laws and American Civil Liberties*. Ithaca NY: Cornell University Press, 1956.; and Stone, Geoffrey R. *Perilous Times: Free Speech in Wartime from The Sedition Act of 1798 to the War on Terrorism*, W.W. Norton, 2004.

[13] See O'Reilly, Kenneth, Hoover and the Unamericans: The FBI, HUAC, and the Red Menace. Temple University Press, 1983.

[14] See Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations*, Quadrangle Books, 1964.

replacement of the authority of the "Old Kingdoms," as described in Ortega y Gasset's classic *Invertebrate Spain*,[15] illustrate well how limited interests in replacing the prevailing normative status quo so often produces subversion without the accommodation of structural transformation. Unlike concepts such as revolution or insurgency, subversion is solely defined by the effort to transform the ideational status quo to something that would be considered illegitimate by what came before. For a cause to be subversive, it demands neither structural transformation – though that development is often bound up in a specific effort – nor a totality of vision. Subversion can encompass a limited platform and set of ambitions insofar as it may address issues that characterize a society writ large but are not strictly codified or considered in law, such as social expectations regarding sexual persuasion or religion.

For scholars of world politics, subversion has consistently posed as both a compelling and somewhat inaccessible topic for study. For the same reasons that insurgency and civil warfare are popular topics of study amongst international relations (IR) and comparative politics researchers, subversion presents as an interesting phenomenon, the understanding of which would undoubtedly improve our abilities to comprehend and predict patterns of political transformation in the world. Successful subversion produces new dynamics that link clearly to the structures of state policymaking and the nature of the government-public relationship – of civic culture. At the same time, subversion is difficult to tease apart from other manifestations of political

[15] See Jose Ortega y Gasset, *Invertebrate Spain*, Howard Fertif, 1974.

advocacy and contention. Despite the normative nature of the subversive enterprise, conditions of ideational transformation often produce violent outcomes in revolutionary or insurgent activity. Likewise, subversion often succeeds in normalizing a counterculture perspective or witnesses a compromise of position between extreme bodies of thought, thus producing conditions that might be sorted into more traditional categories of political contestation, including democratic activism.

IR scholars and their predecessors in the political philosophy and historical analytic traditions have focused on subversion as a discrete political phenomenon at particular intervals in the past two centuries. The common thread among them is the link between subversive efforts in specific national situations and the manifestation of attempts to affect normative transform in a transnational format. Many of the global schisms highlighted prominently by scholars in the English School and related literatures particularly correlate with surges of scholarly and philosophical focus on subversion. A range of the earliest historical accounts and assessments of subversion, largely as encouraged by great powers interested in gaining new support abroad, date to the years following the Crimean War. This period, thought still commonly labeled by students of IR as the era of the Concert of Vienna, saw remarkable normative divisions appear across Europe in the form of broad populist influences on policymaking and agenda in France and the United Kingdom against conservative consolidation and commitment to the spirit (but not the letter) of consultation agreements with Western Europe in Russia,

the Ottoman Empire and Poland.[16] Subversive activity between 1860 and the early years of the 20th century were a common focus of political commentators describing efforts by the continental powers to affect protective insulation through the manipulation of border states. Some years later, T.E. Lawrence and others would describe the patronage of subversive efforts in the 1910s and '20s aimed at, among other things, producing favorable operating conditions for colonial powers in Africa, the Middle East and Asia.[17] Most recently, though still some decades in the past at the time of writing, IR scholars have made broad-scoped efforts to describe subversion as a discrete political phenomenon in the context of the Cold War. With only a handful of exceptions, including a range of works that broad subversion as one part of a toolkit available to separatist organizations in Ireland, India and elsewhere, the bulk of available scholarship and theoretical work on subversive behavior dates from the mid-point of the global struggle between communism and liberal capitalism and focuses on state-sponsored efforts at subversion. Kahin and Kahin's (1995) description of Eisenhower's sponsorship of a clandestine subversive campaign in Indonesia, for instance, is one of the few robust explorations of the subversive phenomenon in modern context.[18] In short, though counterculture has appeared as a compelling topic for study across at least modern history, the difficulties in separating subversion from related manifestations of political contention have

[16] For an excellent overview of great power political interactions in Europe across this period, see Talbot Imlay and Monica Duffy Toft (eds.), *The Fog of Peace and War Planning: Military and Strategic Planning under Uncertainty*, New York: Routledge 2006.
[17] See T.E. Lawrence, *Seven Pillars of Wisdom*, 1922.
[18] See Audrey Kahin and George Kahin, *Subversion as Foreign Policy: The Secret Eisenhower and Dulles Debacle in Indonesia*, New Press, 1995.

enduringly set complex challenges for scholars. By and large, only meaningful interface with state strategies and threats in the context of transnational ideological conflict has prompted a groundswell of scholarly attention to the phenomenon as different – though linked – from terrorism, insurgency and civil activism.[19] Even in such cases, however, the phenomenon often receives attention only as an adjunct tool or aim of statecraft.

Today, the IR community is faced with yet another set of broad transnational prompts to the study of subversion. Different paces of globalization continue to produce unique transnational ideational challenges for the current prevailing liberal world order. The rise of populist movements across the Western world has, if nothing else, demonstrated that unique ideational fault lines are enduringly and arguably increasingly a meaningful source of political change and contention. Extreme political advocacy is simultaneously a beast of global circumstances and enabled, through the interconnectedness of capability offered by the complexification of socioeconomic processes and global adoption of ICT (among other things), to attempt ideational manipulation in unprecedented fashion. This dissertation project is among the first of those works returning to the topic of subversion with the hope of generating meaningful theory and evidence on the operation of subversive actors in world politics. In order to

[19] For discussion of subversion or forced ideational change in what we might call the mainstream IR literature, see *inter alia* K. J. Holsti, Peace and War: *Armed Conflicts and International Order 1648-1989*, New York: Cambridge University Press, 1991; Stephen M. Walt, *Revolution and War*, Ithaca, NY: Cornell University Press, 1996; Mark N. Katz, *Revolutions and Revolutionary Waves*, New York: Palgrave Macmillan, 1999; Mark L. Haas, The Ideological Origins of Great Power Politics, 1789-1989 (Ithaca, NY: Cornell University Press, 2005; Lo, Barry Hashimoto, and Dan Reiter, "Ensuring Peace: Foreign-Imposed Regime Change and Postwar Peace Duration, 1914-2001," International Organization 62 (2008), 717-36.; and John Owen, *The Clash of Ideas in World Politics: Transnational Networks, States, and Regime Change, 1510-2010*, Princeton University Press, 2010.

better situation the precise puzzle under examination here and to set the stage for later chapters' analyses of subversion in the digital age, the remainder of this chapter will thus discuss the shape of the subversive enterprise and set definitional parameters useful for bounding both the scope and the research design of the study.

2.1.1. What Are Subversive Outcomes?

The word "subversion" describes a particular kind of outcome. In the broadest sense, subversion is the successful manipulation of expectations and sociopolitical processes such that previously taboo issues and outcomes – or those beyond reproach in contemporary society – become legitimately considerable. Subversion is about hearts and minds insofar as it describes persuasion of a population to a position radically juxtaposed to what was formerly the norm. In applying this understanding of subversion to the vignettes above, it is not difficult to grasp the general shape of the subversive enterprise. Naturally, however, these statements are relatively non-specific and as such imply a host of potential mechanical outcomes. This dynamic is reflected in past efforts to construct a defensible definition of the term.

Specifically, many past efforts to problematize and define subversion suffer somewhat from the context of their investigatory scope. Studies of subversive actors often take place as a component part of projects focused primarily on political extremism, civil militancy, terrorism and insurgency. But while it is certainly the case that there are common linkages between such phenomena and subversion, it would be inaccurate to assume that these political activities are synonymous with subversive

activities. Terrorists, for example, do attempt subversion. However, subversive behavior is relatively rare and terrorists, focused as they often are on forcing policy changes on the part of national or international authorities, must often undertake activities broadly designed to alienate – rather than persuade – elements of a population. The result of debating subversion by means of a focus on terror or insurgent violence is that studies often assume the perspective of the researchers or the intended audience in making a definition of subversion particularly relevant to the topic at hand. Favoring particular applications in this way can misstate the core set of outcomes implied by the term.

Much literature on the nature of insurgent activities in civil conflict stands as good example of the effort to label subversion in the context of closely related categories of political behavior. Kitson (1971), for instance, advocates the use of the term to describe all elements of modern warfare that involved navigating the interaction of government and social processes to achieve political goals.[20] Trinquier (1961)[21] goes even further in aligning an understanding of subversion as primarily being related to the insurgent enterprise in saying that subversion is synonymous with modern warfare, an "[...] interlocking systems of actions, political, economic, psychological and military that aims at the overthrow of established authority in a country."[22] Treatments of the specter of global communist subversion of political processes during the Cold War, while somewhat less adamant about the link between overthrow and the ideational

[20] See Frank Kitson, *Low intensity operations: subversion, insurgency, peacekeeping,* Harrisburg PA: Stackpole Books, 1971.
[21] See Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency*, Pall Mall Press, 1964.
[22] Ibid, pp. 6-24. Also referenced in Kitson (1971) on p. 5.

transformation implied by the vignettes above, also tend to cast subversive activities as entirely aimed at the destruction of extant political systems. Bezmenov (1983) broadly labels subversion as a "[...] destructive, aggressive activity aimed to destroy the country, nation, or geographical area of your enemy [...],"[23] a description remarkably reminiscent of the Department of Defense's own recent categorization of the phenomenon as any effort to lend "[...] aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of incumbent governments by force and violence [...]"[24] And yet more efforts over the past few to define the concept suffer from a limitation of perspective, such as the need to consider subversion as sedition in order to produce a meaningful legal definition.[25]

The challenge for a study attempting to study subversion is, thus, the task of stripping away the biases of work that considers the phenomenon as one component part of a broader actor toolset or the larger set of threats that states' face.[26] Though the reference to state-sponsored (i.e. external) subversion is clear, Paul Blackstock[27] offers the definition of subversion perhaps most free of such bias in arguing that it "[...] is the undermining or detachment of the loyalties of significant political and social groups within the victimized state, and their transference, under ideal conditions, to the

[23] See Yuri Bezmenov, "Soviet Subversion of Western Society," Lecture on Subversion, 1983.
[24] DoD; Joint Education and Doctrine Division, November 2010.
[25] See, for instance, Spjut, R. J. "Defining Subversion". *British Journal of Law and Society*, 1979, **6** (2): 254–261.
[26] Though his work lacks a strict attempt to define or bound the phenomenon, Beilenson's work is one of the few attempts to consider the phenomenon of subversion entirely on its ideational merits. See Beilenson, Laurence, *Power Through Subversion*, Washington, D.C.: Public Affairs Press, 1972.
[27] See Blackstock, *The Strategy of Subversion: Manipulating the* [...], 1964.

symbols and institutions of the aggressor."[28] Blackstock's definition is well articulated for a number of reasons. First, it detaches an understanding of subversion as being explicitly tied to the overthrow – violent or otherwise – of governments or sub-governmental institutions. This is important because, as noted above, subversion is not always seditious. Modern history is full of cases – from LGBT movements in culturally oppressive regimes to white supremacist movements in Central and Eastern Europe – in which subversion either occurs or is attempted without a stated ambition for structural transformation or violence. Subversion is about ideas and perspectives that are often, but not necessarily, reflected in structures. Second, in referencing the loyalties of individuals, Blackstock links ideational perspectives to a population's preferences. Again, this is critical because subversion takes place under conditions of contestation. New ideas that are tolerable given the progressive nature of a particular society or culture are not subversive, even if they are controversial. Subversive activities are inherently undertaken in an effort to affect a polar shift in the political and social preferences of a population. In short, there must be contest; otherwise, there is no struggle. Finally, Blackstock's definition does well to describe the transformation of ideational conditions and the transfer of normative loyalties to the "[...] symbols and institutions [...]" of the subversive force insofar as it describes subversive efforts as bound up in the unique sociopolitical spaces of particular cultures and nations. No subversive effort is identical to another, even when the cause and the argument is the same. Even in the over-connected world of

[28] Ibid, p. 56.

the 21st century, attempts at subversion naturally take place across different theaters of the global public sphere that boast unique characteristics and challenges.

As Blackstock's definition retains clear reference to the use of subversion as a tool of statecraft, I offer an adapted version of his definition as the basis for this dissertation's analysis and theory-building effort on the contours of subversion in the digital age:

> *Subversion is a transformation of the normative status quo among a significant community or population characterized by the detachment and transference of prevailing political and social group loyalties to the symbols and institutions of the subversive force. Though subversive actors need not consider prevailing conditions to be entirely illegitimate, successful subversion is itself characterized by the establishment of a status quo position that would previously have been considered illegitimate.*

In short, subversion describes ideational transformation via the specific – but broadly interpretable – process of preference transference reflected in loyalty to new alternative symbols or institutions. The final identifier – "the subversive force" – is phrased so as to avoid being too specific about the origins of such symbols or institutions, as subversion originates with particular sociopolitical actors but by definition presents as an ideational phenomenon that can only be understood in context. After all, ideas that take hold in the public imagination have a life of their own beyond (but potentially in line with) what is intended by the originating actor and manifest based on a range of broad societal inputs (treatment by other civil society groups, exogenous shocks, government engagement, etc.).

It is important to note the second sentence of the offered definition. This addition to the modified form of Blackstock's original definition is significant because it enables a line to be drawn between persuasive efforts that are subversive and those that are merely radically progressive. It is certainly the case that not all subversive organizations consider the prevailing status quo to be wholly illegitimate. Indeed, in many cases it is one part of ideational conditions that appears as the objectionable segment of society and the subversive effort is built around an effort to replace a single part (thus changing the characteristic of the whole). The suggested subversion of West Germany by Johannes Agnoli in the mid-20th century is an example of one such agenda, where Marxist ideology as a replacement for Western progressive liberal thought would nevertheless attempt to accommodate traditional national cultural and linguistic traits as a means of normative advancement. However, successful subversion implies a new set of prevailing norms that would by definition be considered illegitimate by the old regime. Thus, the subversive organization is interested in transformation and not addition or adaptation.

The actual form that subversive efforts take is discussed further in the subsections below. First, however, it is important to note that the above definition is articulated with a mind to setting appropriate parameters for the identification of subversive episodes and actors in world politics. In particular, the definition (1) retains Blackstock's focus on the subversive enterprise as being about ideation and not explicitly about structural overthrow and political violence. It also (2) keeps the earlier emphasis

on preference contestation as a critically important factor in differentiating subversion from the tolerated expression of uncontroversial thought in a given society or polity. Finally, it (3) broadly defines the scope of subversion as necessarily tied to social and political dynamics at the national or international level. Of course, this bounding of subversion to large-scale units is not meant to disallow consideration of efforts whose aim is subnational subversion (such as those undertaken by organizations in Balochistan, Tibet and elsewhere). Rather, the intention is to communicate the notion that subversion is the replacement of imagined community symbols and related institutions with alternative versions, and that this process naturally implies an identifiable population bound together by significant normative and/or structural constructs. These parameters will be discussed further in Chapter 4 when research design and case coding are described.

2.1.2. The Context of Subversion

Before considering more directly what the phenomenon entails in terms of actor efforts, it is first important to clarify something of its scope. Subversion takes many forms and occurs in a variety of unique contexts. Despite the fact that subversion has most commonly been attempted throughout human history by groups and movements not linked to governments – by definition, in many cases – scholarship on the phenomenon in this context is limited. By contrast, subversive efforts undertaken or directly supported by governments are actually relatively well studied by modern social scientists. Scholars who have studied government-sponsored subversion scholars –

Laurence Beilenson (1972) and Paul Blackstock (1964), for instance – break the subversive enterprise out into two broad categories (*internal* and *external*) in order to distinguish their research program on statecraft from direct consideration of subversion as it more commonly occurs.

Internal subversion involves attempts to affect the conditions necessary for subversive transformation by dissidents residing within a country,[29] while *external subversion* describes the actions of states in attempting to influence conditions abroad.[30] External subversion is a common tool of statecraft and is often used to achieve ancillary aims for states (or specific rulers) interested in affecting political change abroad through more traditional means, including conquest and the securing of favorable treaty arrangements. Louis XIV, for instance, employed subversion via the encouragement of corruption and the manipulation of cultural practices for years in advance of his military campaigns in central Europe. Centuries before, the competing leaderships of the fragmented Eastern and Western Roman Empires did much the same, extending influence into less well connected parts of the European continent in an attempt to subvert both cultural and formal political loyalties along the frontier. Ivan III would encourage sedition in Russia in the 16th century from abroad as a preparation for the internal campaign to throw off the Mongol yoke, as would the Habsburgs, the English, the British, the Nazis, the Bolsheviks and others at various times over the past several hundred years as an aid to broader strategies of domination. The logic, in each case, was

[29] See Beilenson (1972), pp. 5-6.
[30] Ibid, p. 56.

fairly simple – conquest and/or superior positions in international relations is made much easier by the acquiescence of a target's population and ruling elites. And the employment of subversive tactics by governments is not merely an artifact of the pre-modern international system. Forcible regime promotion through subversive (among other) techniques has received some recent attention by scholars[31] inspired by events in, *inter alia*, Iraq (2003), Afghanistan (in both 1979 and 2001), Panama (1989), Angola (1975), Lebanon (1975-76) and Cambodia (1970).[32] In short, and in defense of scholars who have eschewed consideration of internal subversion, external subversion is a common characteristic of the international system.

As this section is essentially a discussion of a key differentiation in how subversion is problematized for examination in scholarship on world politics, it seems impossible to avoid noting actions taken by a range of states in recent years to affect normative political outcomes abroad through influence operations. Perhaps the most visible and offensive actor in this regard is the Russian Federation, which, under the leadership of President Vladimir Putin and his administration associates, has demonstrably utilized cyber techniques and traditional intelligence methods to interfere in the regular function of political processes abroad, notably peaking with interference in the U.S. presidential campaign between 2015-2016.[33] According to the U.S. intelligence

[31] See Owen, *The Clash of Ideas in World Politics,* 2010.
[32] Ibid, pp.48-52.
[33] U.S. intelligence community reporting and analysis released to the public describes how, in summer 2015, a Russia-based entity labeled APT29 ("Advanced Persistent Threat 29") prosecuted a spearphishing campaign using directed emails that contained a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate domains, which included domains associated with U.S.

community, with corroborating reports made by British, German, French and other security services, Russia has regularly sponsored a range of sophisticated and coordinated attacks against information infrastructure in the Western world with the clear purpose of manipulating deliberative outcomes. From the theft of sensitive data from both individuals and civil society organizations like the Democratic National Committee to the release of private information, Russia has verifiably interfered in the elections of several Western countries from the late 2000s onwards. Specifically, Russian state-connected sources have been responsible for establishing disinformation outlets, setting up fake media outlets, using targeted social media doxxing for destabilization operations and disseminating information meant to alter perceptions of news media credibility.[34]

---

organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure. In spring 2016, another Russia-based entity (APT28) compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed in an effort to exert directed influence on the deliberative processes at work during the 2016 American presidential election period. For the full public release report on Russia's actions taken during the 2015-2016 American presidential election season, see Joint Analysis Report 16-20296A, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, December 29, 2016.

[34] For further coverage and discussion of how Russia has employed cyber techniques, troll/bot armies and traditional intelligence disinformation operations to achieve foreign political manipulation objectives, see Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York, NY: The Institute of Modern Russia, 2014; 'Russian trolls spread government propaganda', Al Jazeera, 11 August 2015 (http://www.aljazeera.com/news/2015/08/russian-trolls-internet-government-propaganda-150811205218686.html); 'This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists', Stopfake, 13 July 2015, (http://www.stopfake.org/en/this-is-how-pro-russia-trolls-manipulate-finns-online-check-the-list-of-forums-favored-by-propagandists/); Michael McFaul, 'What's it like to be hated by the Russian internet?', *Guardian*, 26 May 2015 (http://www.theguardian.com/world/2015/may/26/russia-internet-hated); Anton Butsenko, 'Тролли из Ольгино переехали в новый четырехэтажный офис на Савушкина' [Trolls from

Regardless, this dissertation focuses on internal subversion. To be clear, in the chapters that follow, I consider subversive actors that receive support from foreign states. In looking at the operation of subversive agents themselves, this project is interested in the relationship between subversive actors and their target audiences and is *not* primarily a study of the specific foreign policy tools and machinations of governments seeking to achieve subversive outcomes abroad. Nevertheless, it is certainly the case that this projects outputs have meaning for other studies that seek to better operationalize cyber threats from state and state-sponsored entities in the form of influence operations. This will be discussed further in my concluding chapter.

Internal subversion is a broad-scoped and multi-faceted enterprise that can occur for a number of reasons. As noted above, subversive efforts are themselves simply a form of attempt at political persuasion, albeit with distinct aims regarding national character and practice. Below, I briefly tease apart the different types of activities undertaken by subversive organizations and generalize on distinct phases of subversive campaigns. It is again, however, important to reinforce the point made above about the goals and desired outcomes of those actors that qualify for inclusion in the internal subversion category – success in subversive activities *does not always mean the structural overthrow of existing regimes and/or governing institutions*. In other words, subversion is not always seditious.

Olgino move to a new four-storey office on Savushkina Street], *Delovoy* Peterburg, 28 October 2014 (http://www.dp.ru/103iph/); Jessikka Aro, 'Yle Kioski Traces the Origins of Russian Social Media Propaganda – Never-before-seen Material from the Troll Factory', *Yle*, 20 February 2015 (http://kioski.yle.fi/omat/at-the-origins-of-russian-propaganda); and Alec Luhn, 'Game of trolls: the hip digi-kids helping Putin's fight for online supremacy', *Guardian*, 18 August 2015 (http://www.theguardian.com/world/2015/aug/18/trolls-putin-russia-savchuk).

In saying this, I depart quite radically – but, I believe, uncontroversially – from the treatments of scholars like Blackstock (1964),[35] Beisinger (2002),[36] Pike (1966),[37] Varon (2004)[38] and Selznik (1952),[39] whose inspiration for studying subversion as a political phenomenon was the threat of global communist revolution. Not only is the universe of cases of subversion in modern history less monolithic in terms of the sources of possible subversive inspiration than was that portrayed by Cold War-era studies of the phenomenon, but it is simply not the case that attempted subversion *has* to involve structural overthrow. As a variety of analysts and researchers might attest to, this clarification is critical not only because of the greater conceptual accuracy involved, but because a great number of actors that concern intelligence communities and defense officials claim normative goals and work in a participationist – if contextually objectionable – manner to achieve their goals. Normative transformation often does involve radical structural change, but often targets sentiments or practices that can be reformatted and accommodated by extant political institutions (or modified versions thereof). Without making such a clarification, we risk critical mismatch between theoretical and empirical foundations such that the scholarly production of knowledge might be incomplete.

---

[35] See Blackstock, *The Strategy of Subversion: Manipulating the* [...], 1964.

[36] See Mark R. Beissinger, *Nationalist Mobilization and the Collapse of the Soviet State* (Cambridge: Cambridge University Press, 2002.

[37] See Pike, Douglas, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam,* Cambridge, Mass., and London: MIT Press, 1966.

[38] See Varon, Jeremy, *Bringing the War Home: The Weather Underground, the Red Army Faction, and Revolutionary Violence in the Sixties and Seventies,* Berkeley, Los Angeles, and London: University of California Press, 2004.

[39] See Selznick, Philip, *The Organizational Weapon: A Study of Bolshevik Strategy and Tactics,* New York: McGraw- Hill Book Company, Inc., 1952.

2.1.3. How Does Subversion Happen?

What does subversion look like in action? If subversion is an outcome that involves a sea change in sociopolitical preferences and associated structures, what are the distinct elements of subversive efforts? A broad range of literatures, namely (1) those on the sociology of ideational transformation and (2) those that consider subversion as a tool for political advocacy and statecraft, agree that the subversive enterprise is a participationist process in which a countercultural movement attempts to persuade a population to dissolve loyalty to a particular set of preferences in favor of another. This is not to say that subversive organizations or civil society groups don't employ distinctly non-participationist practices – such as criminal logistical and financial activities – at times. But the main thrust of an effort to subvert is not characterizable by such practices. Moreover, this is not to say that persuasion is about laying a cause on the table for society to pass judgment on. In reality, it might be useful to think about the most common types of subversive effort in terms of clusters of popular preferences. A vast range of inclinations and positions, learned through habituation to sociopolitical norms and normalized under particular structures, constitute the worldview of a given population. Counterculture rarely involves radical transformation of every element of a people's worldview; rather, it is most often an exercise in replacing critical parts of a

population's clustered preference set in such a way as to produce transformation of the broader status quo.[40] This is discussed further below.

Though generally non-specific about what subversive or counterculture actors look like in terms of modes of operation, the neo-Gramscian body of work on counterhegemony in world politics does well to adapt realism[41] to describe the broad shape of efforts to fight an ideational status quo.[42] The counterhegemony body of thought is premised on the notion that different political systems pivot on particular hegemonies of thought – a status quo perspective manifested in the normative and structural outlook of the consensus that is deemed, to the exclusion of others, to be "legitimate."[43] Counterhegemony presents as an alternative normative perspective – often labeled in terms of prevailing ethical, moral or ideological tendencies – that challenges the prevailing hegemony directly (i.e. there is an implied contest because the

[40] This is a common conceptualization of worldview expressed in the literature on political communication and behavior. Generically, the idea is that worldview is constituted of a range of different preferences and predispositions woven together to form a particular attitude and decision-making paradigm for the individual. Alteration of that worldview, thus, has to do with efforts to alter the significance of different predispositions to the individual, the nature of different perspectives or the composition of the cluster as a whole. See, for instance, Matthes, Jörg, and Matthias Kohring. "The content analysis of media frames: Toward improving reliability and validity." *Journal of communication* 58.2 (2008): 258-279.

[41] With initial jumpoff points being the works of hegemonic stability theorists and the literature on systems transformation. See, for instance, Snidal, Duncan. "The limits of hegemonic stability theory." *International organization* 39.04 (1985): 579-614; Strange, Susan. "The persistent myth of lost hegemony." *International organization* 41.04 (1987): 551-574; Keohane, Robert O. *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press, 2005; and Gilpin, Robert. *The political economy of international relations*. Princeton University Press, 2016.

[42] For a good overview of this vein of thought, see Cox, Robert W. *Production, power, and world order: Social forces in the making of history*. Vol. 1. Columbia University Press, 1987; and Robert W. Cox, "Social Forces, States and World Orders" in Keohane, Robert Owen. *Neorealism and its Critics*. Columbia University Press, 1986.

[43] See Cox, Robert W., "Gramsci, Hegemony and International Relations," *Millennium Journal of International Affairs*, 12(2), 1987; and S. Gill and D. Law, "Global Hegemony and the Structural Power of Capital," *International Studies Quarterly*, 33-475, 1989.

counterhegemonic perspective cannot co-exist with the status quo).[44] Unfortunately for the purposes of this analysis, much scholarship in this vein is concerned with where such counterhegemonic movements come from and does not describe operation beyond basic terminology – propaganda, activism, persuasion, etc.[45] Indeed, much neo-Gramscian work abandons the idea that subversion is a unique phenomenon past early efforts to persuade, with a consistent theme in the counterhegemonic narrative being the transition from basic persuasion to political extremism aimed at overthrow once enough support is available. There are clearly elements of accurate historical representation in such perspectives. But, as a body of work, counterhegemonic scholarship does not perform well as a mechanically effective framework for understanding the manifestation of subversion across the universe of cases.

Work on subversion in the context of terrorism, insurgency and militant activism does better in this regard in describing some manifestations of the subversive effort. Though the focus of such efforts usually includes transformation of normative ventures to violent ones, such as is the case with Kitson's famous treatise on irregular and information warfare, Rosenau's discussion of modern sedition[46] and Rid's summation of modern hactivism,[47] the literature does well in describing the various modes of activities

---

[44] Cox, R., *Production, Power...*, p. 43.

[45] Works like Jessop's neo-Gramscian exploration of urban governance regimes do a good job outlining what is meant by propaganda and subversion in the abstract, but do remarkably little to outline techniques or offer example of parameters for implementation and success. See Jessop, Bob. "A neo-Gramscian approach to the regulation of urban regimes: accumulation strategies, hegemonic projects, and governance." *Reconstructing urban regime theory: regulating urban politics in a global economy* 5 (1997): 1-74.

[46] See William Rosenau, "Subversion and Insurgency," RAND Counterinsurgency Study, Paper 2, Santa Monica, California: RAND Corporation, 2007.

[47] See Thomas Rid, *Cyber War Will Not Take Place*, Oxford University Press, 2013.

undertaken by subversive campaigns in propagandizing, persuading and corroding the legitimacy of status quo symbols and institutions. Rosenau, in particular, takes cues from a range of past works in summarizing three different kinds of subversive activity in line with distinct categories of strategic function.[48]

First, the subversive enterprise is commonly composed of front operations.[49] Subversion is countercultural and naturally originates from a position set apart from mainstream norms and expectations of political behavior. Subversive groups require arms that appear unattached to the countercultural core in order to achieve both logistical and activist goals. In general, there are two types of front organization – (1) those knowingly linked to the subversive group and (2) those unwittingly or only informally operating as an agent of counterculture. The redirection of resources by pro-LGBT groups to religious organizations and education programs in countries like Chad, Burkino Faso, Iran and Sudan serves as good example of the latter type of front group, where broad advocacy for one position is masked in the charitable operations of other, more permissible activities. By contrast, the function of entities like the Holy Land Foundation for Relief and Development, Union of Good or North American Islamic Trust by affiliated members of branch elements of the Muslim Brotherhood movement – which, in some countries, might be characterized as subversive – provides a good

[48] See Rosenau, "Subversion and Insurgency [...]," p. 6.
[49] Ibid, p. 6. Also see Thompson, John, *Other People's Wars: A Review of Overseas Terrorism in Canada,* Toronto, Ontario, Canada: Mackenzie Institute, 2003.

example of the former type of group, in which representation of more extreme perspectives is knowingly maintained through informal and interpersonal connections.[50]

Second, subversion often involves infiltration and espionage-like activities to place sources of influence within the institutions of the prevailing status quo position.[51] This means the placement of individuals either belonging to or sympathetic to the cause of a subversive organization in either government, opposition or civil society institutions. The role of such agents is twofold. First, it is often the responsibility of such an operative to sabotage or divert organization processes that would otherwise hamper the subversive cause. Second, it is occasionally the role of the agent to affect institutional subversion in changing the shape and nature of an organization such that conflict with the subversive cause is reduced. For situations where the organization or community is not directly opposed to the function of the subversive enterprise, infiltration is often about persuasion and recruitment. This type of activity is not unique to subversion, of course, insofar as violent and legitimate political actors place operatives in locations of opportunity as commonplace practice. There exists an extensive set of cases where al Qaeda and affiliate groups have placed operatives in Muslim communities, organizations and mosques across the West in an effort to either mobilize support or to target specific recruitment needs,[52] as did the IRA, Nepal's Maoist insurgency, Aum Shinrikyo and more in decades past. Islamic State agents likewise filled the ranks of Iraqi security

[50] See Vidino, Lorenzo. *The new Muslim brotherhood in the West*. Columbia University Press, 2010.
[51] See Rosenau, "Subversion and Insurgency [...]," p. 6-7.
[52] See Lathem, Niles, "Qaeda Claim: We 'Infiltrated' UAE Government," *New York Post,* February 25 2006.

forces in limited numbers prior to the initial push against Baghdad in 2014-16[53] much as had happened in 2003-04[54] and much as did the Viet Cong in the 1960s and '70s in South Vietnam.[55]

Finally, subversive groups functionally act to frame the contentious issue or broader normative conflict that motivates their campaign through active efforts to generate public upheaval.[56] Civil unrest provides an important role for subversive organizations in setting the stage for normative contention in the public limelight and not entirely because civil incidents accurately reflect a tension between the mainstream and counterculture. Indeed, civil protests and unrest largely pivot on secondary issues bound up in the construction of the current status quo rather than on the main platform advocated by the subversive movement. Causing civil unrest can be beneficial for subversive organizations for a number of reasons. First of all, large-scale disruptions can consume valuable state and non-state opposition resources.[57] Second, the side effects of upheaval can exacerbate the exact society-government relations that subversive groups necessarily need to weaken in order to bring about a seachange in perspective on a given

[53] See, for instance, "Protesters storm Baghdad's Green Zone again, dozens hurt," Thompson Reuters, May 20, 2016.

[54] See *inter alia* Inspectors General, *Interagency Assessment of Iraq Police Training,* Washington, D.C.: U.S. Department of State and U.S. Department of Defense, July 2005; and "Insurgents 'Inside Iraqi Police,'" *BBC News,* September 21 2005.

[55] See Pike, *Viet Cong: The Organization* [...], 1966. Also see Prados, John, "Impatience, Illusion, and Asymmetry: Intelligence in Vietnam," in Marc Jason Gilbert, ed., *Why the North Won the Vietnam War,* New York: Palgrave, 2002; U.S. Information Service, Office of Policy and Research, "The Viet Cong: The United Front Technique," R- 13-67, Record 128321, Douglas Pike Collection: Unit 06—Democratic Republic of Vietnam, April 20, 1967; and U.S. Central Intelligence Agency (CIA), Directorate of Intelligence, "The Vulnerability of Non-Communist Groups in South Vietnam to Political Subversion," record 31052, CIA Collection, May 27, 1966.

[56] See Rosenau, "Subversion and Insurgency [...]," p. 7-8.

[57] See U.S. Marine Corps Intelligence Activity, *The Urban Threat: Guerrilla and Terrorist Organizations,* n.d. 1999.

issue. Third, civil unrest is a source of new allies valuable to the subversive enterprise. Though often uncompromising in the integrity of the subversive cause, countercultural organizations have regularly benefited from the patronage or partnership of sympathetic actors motivated by related concerns (such as the alliance between elements linked to Hamas and branch organizations of the Muslim Brotherhood in Europe). Public upheaval and disruption produces a crucible from which such relationships can emerge. Finally, encouragement of civil unrest is one way to shutdown a national system that does not revert to violence as a tool for structural transformation.[58] Much as might be the case with an old computer system, disruption to key functional processes can cause a national system to freeze up. This creates temporary political space in which subversive transformation of fundamental policy, process or system norms might be affected.

More generically, of course, if the main objectives of subversive groups have to do with socialization and codification of a particular set of transformative precepts, then subversive activities might logically be thought of as belonging to one of three different campaign phases – (1) mobilization, (2) mitigation, and (3) actualization (see Figure 2.1). To be clear up front, these phases can happen contemporaneously and can involve use of the same tactics and assets. Nevertheless, these phases reflect different operational approaches to the subversive enterprise.

[58] See Marighella, Carlos, *Minimanual of the Urban Guerrilla,* 1969; and Molnar, Andrew R., *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare,* Washington, D.C.: Special Operations Research Office, November 1963.

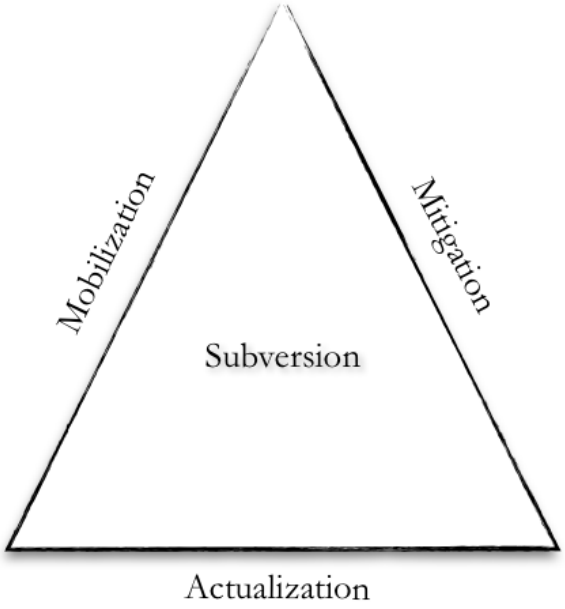

Figure 2.1. Three elements of subversive campaigns.

Mobilization refers to a series of actions taken to form and bolster the capacity of a subversive effort, namely self-replication, outreach and logistical preparation. Replication involves the expansion of a subversive movement or organization by means of recruitment and strategic proliferation. This can happen through a great number of mediums, including the use of media or personal connections to recruit new members and the establishment of branches in new areas. Though this can certainly involve a degree of public and private outreach, the fact is that outreach itself can additionally be seen as a separate mobilization effort. Though ultimate objectives might include socialization, it is often the case that the catalyst for such a normative shift requires a degree of awareness or positionality on the part of individuals or public groupings. Thus, outreach stands as a distinct mobilization activity. Finally, mobilization invariably

requires logistical preparation, including – but not limited to – the setup of front organizations, the development of infrastructural or social capital, and the securement of financial resources.

Mitigation refers to a unique set of activities that have to do with removing obstacles to the desired subversive transformation. Depending on the context of the subversive campaign, mitigation efforts might be minimal. After all, subversion targets a transformation that only might have to do with opposition to prevailing conditions. The range of activities that might fall into this category is broad and might include things as disparate as the use of criminal assets and involvement in public dialogue with opposition forces. Nevertheless, mitigation presents as a unique phase of subversive efforts that, as opposed to the focus on internal capacity that comes with mobilization, focuses on the manipulation of external conditions in a preparatory manner.

Finally, actualization refers to the steps taken to realize overall objectives. It is at this phase that persuasion, activation and mobilization of a broader population occurs in the process of affecting systemic transformation. With the case of the NSDAP in inter-war Germany, actualization included the bulk of public-facing political activities in the years prior to Hitler's election, while mobilization might be said to have been the more significantly limited set of efforts designed to recruit party soldiers and persuade key individuals. Of course, all activities – including those related to mobilization and mitigation – might be counted as part of a blanket effort to achieve subversive ends. But thinking about actualization as a distinct phase of operation for subversive entities

brings analytic advantages, as it allows for the categorical separation of the mechanisms that relate to preparation and execution. Moreover, it allows for specific analytic separation of grand objectives and those applied to periods or phases of a given campaign.

2.2. Why Studying Subversion in the Digital Age is Important

This dissertation is interested in subversion as it occurs in the modern era. Though for many projects this statement might present as somewhat imprecise, the focus of this study on the use of information technologies naturally limits the scope of the study to the timeframe of the information revolution. Thus, though some small variation is arguable, this project investigates the behavior of subversive actors in world politics over the past thirty years. Those actors studied in this project have operated across the period from 1985 to the present, a period that closely matches prominent accounts of the rise of cyberspace.

This project naturally studies a range of non-state actors that might otherwise rarely be discussed in the same study (see Figure 2.2). From racial supremacy groups in North America and sub-Saharan Africa (a handful of which are officially labeled hate groups by government or government-sponsored organizations) to ideological organizations of all stripes across Europe and Asia, subversive entities are not defined singularly by their mission, specific normative objectives or choice of tactics beyond a commitment to *ideational* transformation. Rather, as outlined above subversive actors are defined by their relationship with contemporary society and their stated objective of

altering the prevailing status quo by detaching the loyalties of a population from it and transferring them to an alternate version.

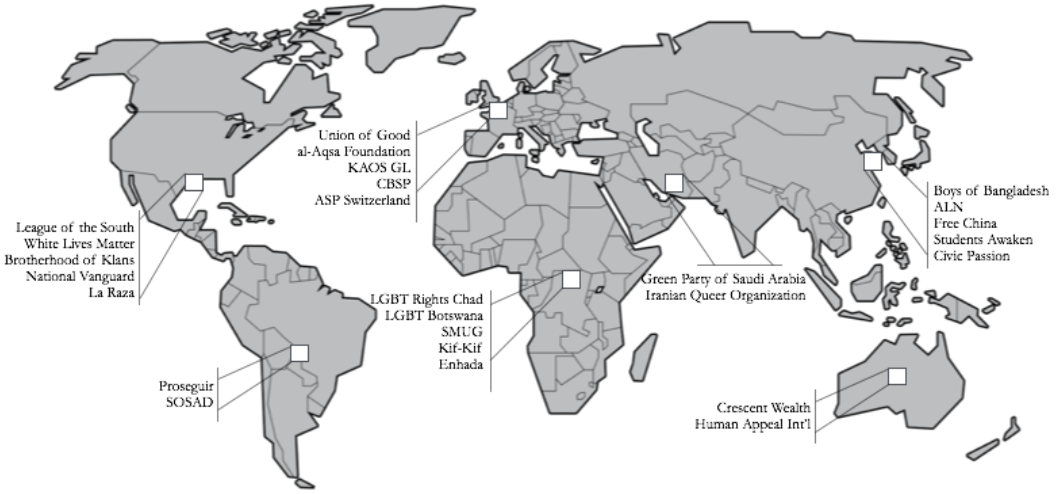

Figure 2.2. Graphic overview of subversive groups under study.

This dissertation project is built on the premise – commonly described in scholarship in the political communication, computational social science and geo-information science fields – that the information revolution has constituted a large-scale, systematic transformation of the fabric of international relations such that producing knowledge about different sociopolitical actors and phenomena is difficult without reference to the intercession of new technologies. Below, I specifically draw lines around three major kinds of transformation experienced by the global system over the past several decades – (1) the digitization of global infrastructure, (2) the adoption of new methods for access information and communicating, and (3) subsequent changes in the way that information is disseminated and presented in the global public sphere. In

describing the impact of the information revolution in this way, it becomes apparent that not only is there a need for better understanding of how subversive actors are using new technologies, but that addressing the link between ICTs and subversion is necessary for producing *any* useful comprehension of the phenomenon in the modern era. To not do so is to risk the production of theory based on outdated foundations with limited explanatory power.

I point out in sections above that scholarship on subversion tends to emerge in periods where there is unique empirical interest in the subject. The turn of this and related recent studies' to the subversion topic occurs in such a context. Broadly speaking, the 21st century has been characterized by a range of efforts that might be labeled as subversive. Though they are perhaps most visible to the layman, the transnational efforts of organizations like al Qaeda and Islamic State in attempting to affect ideational transformation among a range of populations joins less extreme campaigns – such as the efforts of anti-globalization organizations, gay rights groups in conservative countries and more – as example of the increasing commonality of subversion in world politics. This study is not the first to suggest that this trend has much to do with the transformation of the global public sphere in line with the outcomes of globalization, in particular the worldwide integration of ICTs across most social and economic functions. The clear need to study subversion in the context of such technologies is, thus, intrinsically tied to the multi-faceted social scientific effort to better problematize and produce policy-relevant knowledge about such developments.

Moreover, a study of subversion as a political phenomenon – i.e. not as a more constraining category of non-state actors or as a particular tactic – nicely matches the need to better generalize about the manner in which the information revolution and cyber technologies have impacted the behaviors and capabilities frontiers of radical non-state actors in world affairs.

2.3. The Global Public Sphere in the Information Age

Subversion is about information. Individuals form preferences and appraise ideas based on the information context of their social and political lives. Thus, understanding the information environment – and, in particular, accounting for the ways in which systematic changes to that environment manifest in decision-making – is perhaps the most critical element of any effort to comprehend and generalize on the subversive enterprise.

It is a common claim that information and communications technologies have transformed the global information environment over the past three decades. Here, I describe three distinct ways that ICT have transformed subversion and persuasion in both local and international settings. I then turn to the question of direct impact on the operation of non-state actors interested in political persuasion and review recent scholarship on how ICT have produced both new abilities and challenges for such actors.

The Digitization of Global Infrastructure. Perhaps more obviously than other changes, the ubiquity and sophistication of information technologies has augured profound changes the logistical infrastructure of the everyday functioning of global

system processes. This set of changes to the ways in which industry, government, militaries and most societal sectors function across a range of operations is the main focus of much scholarship in the security studies and international relations field on cyberspace, particularly in the literatures on terrorism, interstate conflict and crime.

For the security studies literature, in particular, the digitization of global infrastructure is the general form of highly specific challenges to both state security and a range of international normative, legal and economic regimes. In terms of both state and terrorist threats to the national security, the strategic rationale behind the design and deployment of advanced "cyber weapons," for instance, can broadly be found in the twofold digitization of information and control dynamics around the world – that is, the digitization of security systems and the digital inter-connection of previously discrete functions. Stuxnet, for example, was designed to circumnavigate "air-gap" defenses that would otherwise have rendered attempts at network intrusion impotent.[59] Likewise, Stuxnet – alongside other programs like Flame and, responsively, efforts such as Byzantine Foothold – was designed to take advantage of the widespread inter-connectedness of computer systems in recent years, transmitting component parts of

[59] For detailed accounts of the Stuxnet episode from technical, policy and political perspectives, see Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, "Stuxnet under the Microscope," eset, white paper (20 January 2011); Jon R. Lindsay, "Stuxnet and the limits of cyber warfare." *Security Studies*, Vol. 22, No. 3 (2013) pp. 365-404; David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges At the Natanz Enrichment Plant?" Institute for Science and International Security (22 December 2010) pp. 3–4; Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group (November 2013); and Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired Threat Level Blog, 11 July 2011, http://www.wired.com/ threatlevel/2011/07/how- digital- detectives- deciphered-stuxnet.

itself via otherwise innocuous network or media transfers over time.[60] As some work has argued, the massive integration of ICTs across societal and industrial sectors also constructs unprecedented security obstacles for national security in economic[61] and legal[62] terms, with broad-scoped inter-connection of systems allowing for varying degrees of access and control of information.[63]

Beyond the traditional purview of the security studies field, of course, the digitization of global infrastructure has had a much more direct impact on shape of the global economy, on processes of global governance and on the operation of various non-state actors. Across industry, government and public organization at almost every level, means of financial transaction, recordkeeping and utilities procurement look markedly

---

[60] This has elsewhere been described as a weapon of mass effect, differentiated from digital weapons that cause massive disruption of systems by the widespread deployment but low-intensity nature of the eventual effect. See Christopher Whyte, "Power and Predation in Cyberspace," *Strategic Studies Quarterly*, Vol. 9, No. 1 (Spring 2015) pp. 100-118.

[61] Among others, see Paul Cornish, David Livingstone, Dave Clemente and Claire York, "On Cyber Warfare," Chatham House (November 2010); Chintan Vaishnav and Nazli Choucri and David D. Clark, *Cyber International Relations as an Integrated System*, MIT Political Science Department Research Paper No. 2012-16 (June 14, 2012); Brandon Valeriano and Ryan Maness, "A Theory of Cyber Espionage for the Intelligence Community," EMC Conference Paper (2013); and James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, 22 July 2013).

[62] See, debating various aspects of international-oriented legal challenges, William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009); David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010); Peter Toren, "A Report on Prosecutions under the Economic Espionage Act," paper presented at the American Intellectual Property Law Association annual meeting, Trade Secret Law Summit, Washington, D.C. (October 23, 2012); Judith Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, The Center on Law and Security, New York University School of Law (October 2014); Judith Germano and Zachary Goldman, *After the Breach: Cybersecurity Liability Risk*, The Center on Law and Security, New York University School of Law (2014).

[63] For a fuller discussion of issues of access and control, see Jon R. Lindsay, Tai Ming Cheung and Derek Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford: Oxford University Press, 2015.

different than they might have thirty or more years ago, *even if the specific aims and parameters of a given set of processes remain the same.*[64] For non-state groups, and specifically in this case for subversive actors, this has augured in new opportunities for the evolution of operational abilities, in particular abilities to hide and more generally coordinate distributed activities.

The Nature of Inter-Constituent Communications. The change to the global system more focused on by the more loosely defined bodies of work on cyberspace and political organization has less to do with technical conditions than it does to do with agent behavior. Related to the broad digitization of global infrastructure, recent decades have seen unprecedented changes in the ways that global constituents (individuals, communities, organizations, etc.) communicate and consume information.[65] Though this certainly might be thought of as a consequent of global infrastructure digitization, however, changes to the nature of inter-constituent communication are both unique and fundamentally related to the dynamics of the global system in which specific actors are embedded. In short, new communication and information consumption modalities affect

---

[64] Choucri, *Cyberpolitics in International Relations*, 2012.

[65] For prominent work describing the various ways in which methods and habits of information consumption and communication have changed in the past several decades, particularly given the rise of the Internet, see Bruce Bimber, *Information and American Democracy* Cambridge: Cambridge University Press, 2003; Lance Bennett and Shanto Iyengar, "A New Era of Minimal Effects? The Changing Foundations of Political Communication," *Journal of Communication*, Vol. 58, No. 4, pp. 707-731, 2008; Earl and Kimport, *Digitally Enabled...*; Philip Howard, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*, Oxford: Oxford University Press, 2010; and Shirky, "The Political Power of Social..."

preference sets in a very basic manner.[66] Individual and organizational approaches to problem solving, self-representation and other fundamental political activities continues to adapt to match the network realities of an increasingly transnationally-oriented – rather than nationally-oriented – international system. For subversive and related actors, this portends new challenges and opportunities in recruiting and directing assets.

The Nature of Ideational Dissemination and Presentation. Finally, the global adoption and integration of ICTs across the full range of societal functions has augured significant changes in the way that ideas are not only communicated from individual constituents, but also disseminated and presented beyond the scope of inter-personal communications. [67] Whereas fundamental changes in the nature of communications possibilities for constituents of the global system have affected the

---

[66] Though earlier, Chafee and Metzger present one of the most prominent descriptions of one major change in global constituent preference sets in arguing that media consumption will (and has since) change(d) to reflect expectations regarding information desired over information received. In other words, people have increasingly come to expect to receive the types of information they want to receive, rather than the information that the media might offer without popular input. See S. Chaffee & M. Metzger, M., "The end of mass communication," *Mass Communications and Society*, No. *4*, pp. 365-79, 2001.

[67] A broad literature on the nature of information diffusion in the international system exists and has been significantly updated in recent years that focuses on the determinants of idea spread in world affairs. In addition to the intervening impacts of inter-state alliances, trade and more, the condition of technology in the form of media systems has regularly been controlled for. Recent research has consistently demonstrated that information flow is closely linked to the methods global constituents use to receive information, which are in turn influenced in terms of information disseminated by the structure of global commerce and the penetration of new media services (particularly social media). For seminal works in this tradition, see J. Galtung & M. Ruge, "The structure of foreign news the presentation of the Congo, Cuba and Cyprus Crises in four Norwegian newspapers," *Journal of Peace Research*, 1965; J.D. Dupree, "International Communication, View from a Window on the World," *Gazette* Vol. 17, pp. 224-235, 1971; T.J. Ahern Jr ., "Determinants of Foreign Coverage in Newspapers," in R.L. Stevenson and D.L. Shaw (eds) *Foreign News and the New World Information Order*, Ames: Iowa State University Press, 1984; and Dennis Wu, "Investigating the Determinants of International News Flow," *International Communication Gazette*, Vol. 60, No. 6, pp. 493-512, 1998.

formation of preference sets and methods of specific access in the aggregate,[68] dynamics of ICT utilization and development across both public and private sectors have had unique impact on patterns of ideational inter-connections across numerous types of boundaries in the digital age.[69] Though drastically understudied in comparison as a type of systematic change fueled by global ICT integration, a diverse body of scholarly work in the social sciences has for some years consistently demonstrated that the market-specific nature of ICT development has had noticeable effects on patterns of political organization and expression in world affairs. In one vein, for instance, patterns of public opinion and information consumption on different topics has been linked to the specific dynamics of Twitter usage.[70] In short, virtual polycentric communities centered around the use of specific social media platforms and activated by community attention to a topic – rather than more traditional governmental or old media focus on an issue – has at least to some degree altered dynamics of gatekeeping and agenda setting in

---

[68] Additionally, the notion that media systems play a significant role in changing the way that information is presented to global constituents, which then affects policy responses, is a common one in the communications literature more broadly. The CNN effect is an oft-cited example of just this phenomenon, where the 24 hour news cycle of major international news networks during the 1980s and 1990s significantly constrained the timeline for policymaker response to incipient issues. For the most complete account of this theoretical tradition, see Eytan Gilboa, "The CNN Effect: The Search for a Communication Theory of International Relations," *Political Communication*, Vol. 22, No. 1, pp. 27-44, 2005.

[69] See J. Allen-Robertson and D. Beer, "Mobile Ideas: Tracking a Concept through Time and Space." *Mobilities* Vol. 5, No. 4, pp. 529–545, 2010; D. Quercia, L. Capra, and J. Crowcroft, "The Social World of Twitter: Topics, Geography, and Emotions." *Proceedings of the Sixth International Conference on Weblogs and Social Media*, Dublin: Palo Alto, CA: AAAI Press, 2012; and Y. Takhteyev, A. Gruzd, and B. Wellman, "Geography of Twitter Networks." *Social Networks* Vol. 34, No. 1, pp. 73–81, 2012.

[70] See C. Greenhow and B. Robelia, "Informal Learning and Identity Formation in Online Social Networks." *Learning, Media and Technology* Vol. 34, No. 2, pp. 119–140, 2009; Lance W. Bennett, "The Personalization of Politics Political Identity, Social Media, and Changing Patterns of Participation." *The Annals of the American Academy of Political and Social Science,* Vol. 644, No. 1, pp. 20–39, 2012; and Anthony Stefanidis , Amy Cotnoir , Arie Croitoru , Andrew Crooks , Matthew Rice & Jacek Radzikowski, "Demarcating new boundaries: mapping virtual polycentric communities through social media content," *Cartography and Geographic Information Science*, Vol. 40, No. 2, pp. 116-129, 2013.

international relations. For subversive and related actors, where socialization and the normalization of a perspective against the prevailing informational dynamic is intrinsically required, such a development has broad and significant implications for strategy and practice.

2.3.1. Non-State Actors and ICT: What do we know?

What do these effects of the information revolution imply in terms of new challenges and opportunities for non-state actors? What about for subversive actors specifically? In this section, I identify specific capabilities available to non-state actors of various types and discuss both challenges and opportunities borne of commitment to the use of ICT for different tasks. I then argue, below, that the range of new abilities and corresponding technical instruments provided actors by new ICTs can be matched to the functions of subversive organizations as being useful for either clandestine mobilization or active ideational persuasion and advocacy. To be clear, I do not argue that the utility of ICTs for subversive activities is an exclusive dichotomy wherein tools are useful only for specific tasks at specific junctures. Rather, understanding the utility of new technologies in line with the spectrum of activities subversive organizations take at different phases of campaigns allows for clarity in understanding the pressures felt by subversive decision-makers faced with the need to address challenges bound up in their use. Moreover, it provides theoretical expectations in line with past scholarship about when and why subversive groups adopt certain kinds of strategies. These inform the central puzzle of this dissertation – that there exists unexpected variation in the

distribution of groups that abandon emphasis on clandestine techniques during activist phases of their campaign – and serves as the basis for hypotheses that are outlined in detail in Chapter 4.

2.3.1.1. A Spectrum of New Tools

In literature on the use of ICT by non-state actors of various kinds to augment core functions, there is general consensus that new digital technologies allow for unique opportunities in three categories. These three categories broadly align with the typologies of transformation experiences by the global public sphere described in the sections above in that they split on the utility of ICT for both actual disruption and normative disruption. First, non-state actors, from lobbying organizations and protest groups to terrorist cells, can use new information and communication techniques to persuade, organize and perform outreach of different kinds.[71] New information environment dynamics mean that digital platforms for information framing and dissemination are the new gates to the kingdom of public opinion and sentiment.[72]

---

[71] See, *inter alia*, Arquilla, John and David Ronfeldt. "The Advent of Netwar." *Networks and* Netwars. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica 2001; Arquilla, John and David Ronfeldt. "What Next For Networks and Netwars?" *Networks and Netwars*. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica 2001; Gehrett, Anne, Vice-President of Law Enforcement Program, CACI. Personal Interview, July 2004 Gehrett 2004; and Enders, Walter, and Todd Sandler (2002). Patterns of Transnational Terrorism, 1970–1999: Alternative Time- Series Estimates. *International Studies Quarterly 46*(2), 145.

[72] For some of the most influential work forwarding this assertion, see Bruce Bimber, *Information and American Democracy,* Cambridge University Press, 2003; Bruce Bimber, "The Internet and Political Transformation: Populism, Community and Accelerated Pluralism*," Polity*, 31 (1), 1998, pp. 133-160; Lance Bennett and Shanto Iyengar, "A New Era of Minimal Effects? The Changing Foundations of Political Communication," *Journal of Communication*, Vol. 58, No. 4 (2008) pp. 707-731; and Jennifer Earl and Katrina Kimport, *Digitally Enabled Social Change* (Cambridge: MIT Press, 2011).and Van Dijk, Jan. *The network society*. Sage Publications, 2012. For an overview of these perspectives, see Webster, Frank. *Theories of the information society*. Routledge, 2014. Some specific work on the relationship between the

Likewise, social, political and economic dynamics bound up in the development and use of such systems determines new gatekeeping and affords non-state actors of all stripes opportunities to lobby. Second, ICT allow for direct interaction with information in terms of the design and contents of digital systems. Non-state actors and state entities alike can steal or manipulate information stored on servers and, through a variety of network or media actions, can disrupt systems that undergird a multitude of social, economic and governmental functions.[73] Finally, ICT allow non-state actors the opportunity to accomplish non-informational disruption through the manipulation of computer systems.[74] Though incidence of such disruption is not common in the relatively short history of conflict and contentious politics online, it is certainly possible that a

---

global information environment and non-state actor operations has inevitably focused on Islamic State, and generally affirms this position of enhanced capability due to information framing and dissemination abilities. See, *inter alia*, Berger, J., The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion. *Perspectives On Terrorism, 9*(4), 2015; Zelin, A., Picture Or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output. *Perspectives On Terrorism, 9*(4), 2015; Gates, S., & Podder, S., Social Media, Recruitment, Allegiance and the Islamic State. *Perspectives On Terrorism, 9*(4), 2015; Berger, M., "The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion" (2015) in this issue; Jytte Klausen, "Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38 no.1 (2015): 1-22; Daan Weggemans, Edwin Bakker and Peter Grol, "Who are they and Why do they go? The Radicalisation and Preparatory Processes of Dutch Jihadist Fighters," *Perspectives on Terrorism* 8 no. 4 (2014): 104; and Rachel Briggs and Ross Frenett, 'Foreign fighters, the challenge of counter-narratives', Policy Brief, London: Institute for Strategic Dialogue, 2014.

[73] See, for instance, Morozov, Evgeny. *The net delusion: The dark side of Internet freedom*. PublicAffairs, 2012; and Hindman, Matthew. *The myth of digital democracy*. Princeton University Press, 2008.

[74] See, *inter alia,* Zanini, Michele and Sean J.A. Edwards. "The Networking of Terror in the Information Age." *Networks and Netwars*. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica, 2001; and Cox, Christopher, "Digital Repertoires: Non-State Actors and ICTs," *The Osprey Journal of Idea and Inquiry*, Paper 57, 2006. For a more specific description of how unprecedented physical disruption might occur in the digital age, see Michael Sechrist, "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems," in *Science, Technology, & Public Policy Program Discussion Paper Series*, Cambridge, MA: Explorations in Cyber International Relations Project at Belfer Center for Science and International Affairs, 2012.

non-state actor might cause kinetic disruption through actions like cyber attacks on state-operated utilities.

Naturally, the spectrum of new tools available to non-state actors – both from the adoption of new technologies and in the context of massive changes to the information environment of the modern global system – describes abilities that are as potentially benign as they are dangerous to civil society and governments. Moreover, the ICT label describes a diverse set of technologies that ranges from the primitive to the futuristic in terms of sophistication.[75] On the "low" end of the complexity scale, useful ICT might simply include smaller and more concealable media devices for storing and transporting sensitive information than have previously been available. At the "high" end of the scale, non-state actor use of ICT might entail the employment of logic bombs, trojans or SQL injection techniques in efforts to infiltrate, intrude or to vandalize opponents' websites and computer systems.[76]

New abilities in the first category of opportunity for non-state actors particularly tend to be amongst the simplest and it is in this category that we find most legitimate actors – interest groups, lobbying organizations, etc. Indeed, for the purposes of

---

[75] See Carr, Jeffrey, Inside Cyber Warfare Sebastopol, CA: O'Reilly Media, 2010; Reveron, Derek, "An Introduction to National Security and Cyberspace." In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Derek Reveron, Ed., Washington, DC: Georgetown University Press, 3– 20., 2012; and Cox, Christopher, "Digital Repertoires: Non-State Actors and ICTs," *The Osprey Journal of Idea and Inquiry*, Paper 57, 2006.

[76] For good descriptions, see Rid, Thomas, and Peter McBurney, "Cyber Weapons." The RUSI Journal 157 (1): 6– 13, 2012; Valeriano, Brandon; Maness, Ryan C., *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford University Press, 2015; Healey, Jason (eds.), *A Fierce Domain: Conflict in Cyberspace 1986– 2012*, Washington, DC: Cyber Conflict Studies Association, 2013; and Reveron, Derek, "An Introduction to National Security and Cyberspace." In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Derek Reveron, Ed., Washington, DC: Georgetown University Press, 3– 20., 2012.

operating in the new and expanded information environment of the digital age, the utility of different methods derives almost entirely from the sociopolitical context of non-state actors' circumstances.[77] Depending on the precise context of technology adoption and common practices, organizations and individuals interested in influencing public sentiment and opinion might choose to employ email for spreading a message, social media for mobilizing an audience or web ads for criticizing specific opponents.[78] Methods of approach here are far less about the context of complex technical systems than it is about how civil society and other actors use ICT for sociopolitical purposes. The use of invasive techniques to embarrass or challenge political opponents – through, for example, vandalism of websites or the theft of sensitive data for the specific purpose of gaining advantage of operation in activist efforts – also reflects the "low" end of the sophistication spectrum when it comes to using ICT to better operate in modern information environs.[79]

By contrast, new non-state actor abilities to disrupt computer systems to achieve either information or kinetic effects tend can be both very simple and highly sophisticated. Such attacks temporarily disable or diminish the functions of information

---

[77] See Whyte, Christopher, "Dissecting the Digital World: Old Questions, New Answers," *International Studies Review*, Forthcoming; and Whyte, Christopher, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy*, 35:2, 2015, pp. 93-102.

[78] See, for instance, Molly Sauter, *The Coming Swarm: DDoS Actions, Hactivism and Civil Disobedience on the Internet*, Bloomsbury: New York, 2014.

[79] See, among others, Christopher Whyte, "Power and Predation in Cyberspace," *Strategic Studies Quarterly*, Vol. 9, No. 1 (Spring 2015) pp. 100-118; and Brandon Valeriano and Ryan Maness, "A Theory of Cyber Espionage for the Intelligence Community," EMC Conference Paper, 2013.

systems to allow the antagonist some specific advantage.[80] At the "low" end of the spectrum, this might include the use of botnets to overwhelm server traffic abilities and temporarily shut down specific websites.[81] At the "high" end, this might entail the manipulation of security design flaws to infiltrate a network or the use of sophisticated combinations of gambits and malicious code to force entry to a guarded system. "High" end operations, it should be noted, are not always more expensive or and the knowledge of code and systems' design needed for implementation is not always difficult to access.[82] Information disruption always has temporary effects, at least in terms of the functionality of the systems involved, and can be undertaken for a variety of reasons. Common outcomes include the theft of sensitive data about, for instance, commercial products or an organization's members/customers and the defacement of websites for political reasons.[83]

---

[80] See Jon Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in Greenhill, Kelly and Peter Krause (eds.), *The Power to Hurt: Coercion in the Modern World,* 2016; Jensen, Benjami, Ryan Maness and Brandon Valeriano, "Cyber Victor: The Efficacy of Cyber Coercion," Working Paper, 2016; Jon Lindsay and Stephen Haggard, "North Korea and the Sony Hack: Exporting Instability Through Cyberspace," East-West Center, 2015; and Whyte, Christopher, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy*, 35:2, 2015, pp. 93-102.

[81] See Sauter, *The Coming Swarm* [...], 2014.

[82] See Sanger, David E., *The Reckoning: How President Obama Has Changed the Force of American Power*, New York: Crown, 2012; and Symantec, "Advanced persistent threats: How they work," 2014.

[83] It is important to note that the outcomes described here are entirely temporary in nature. Indeed, this is one of the main points made about cyber conflict potential by scholars studying cyberspace. Despite what some may argue or think (Liff 2011 or Kello 2014), conflict potential with cyber is entirely limited by the limited nature of "victories" that can be won online. See, broadly, Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 5 (February 2012), pp. 5–32; David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *Journal of Strategic Studies*, Vol. 35, No. 5 (October 2012), pp. 689–711; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon?' The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401–428; Libicki, *Conquest in Cyber- space: National Security and Information Warfare*; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (August 2013), pp. 365–404; Erik

Finally, non-state actor abilities to cause actual destruction or kinetic disruption through the use of ICT are almost entirely sophisticated, expensive and time-consuming in that such capabilities reflect the extreme difficulty involved in translating digital action into physical results[84]. While disruption of information systems can lead to the destruction of data or the temporary loss of control over specific organizational functions, the use of ICT for destruction describes information actions taken to maliciously pervert digital systems that actively control physical systems. Though the global adoption and integration of ICT across most global societal functions has entailed a massive transformation of infrastructure worldwide over the past three decades, examples of systems controlled by computers vulnerable to intrusion that could be used for actual violence are hard to come by. The most commonly cited examples of possible targets that fit the bill include power grids and utilities systems,[85] the widespread disruption of which could cause loss of life through, for instance, the disruption of emergency services or the failure of certain control systems. Meaningful disruption of such systems, which are highly distributed, very well protected and have multiple redundancies, necessarily implies the design of advanced and adaptable abilities. The expense and broad function knowledge needed to produce such capabilities, as well as

---

Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73; and Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3 (Winter 2014/15) pp. 7-47.

[84] See Carr ,J., The Myth of the CIA and the Trans-Siberian Pipeline Explosion, 2012.

[85] For a broad policy discussion of the topic, see Danzig, Richard. *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. 2014. For a description of the first actual attack on such infrastructure, see Bernat, Jose, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016.

the risk involved in designing a weapon with so many potential opportunities for failure in its employment, make them uncommon.[86]

2.3.1.2. Subversives' Antagonistic Use of Information Technology

In world affairs, subversive actors use ICT for a broad range of purposes. As described above, subversives are interested in hearts and minds, in securing funding, in coordinating activities and in checking the activities of opposing forces (governments, opposition advocacy groups, etc.). Much of what subversives do online is not criminal. Groups use social media to cultivate followings and message their intended audience. They use email to coordinate operations and often organize online petitions much as a political party might. But subversive actors have also taken advantage of the information revolution to expand and add nuance to their repertoires of antagonism – i.e. to their arsenal of tools and tactics for supporting or directly causing disruption in support of a subversive cause. Figure 2.3 enumerates the use of ICT for shady and antagonistic purposes among the 279 subversive organizations assessed in Chapter 4.

---

[86] This argument is commonly cited by cyber war skeptics to justify the analytic perspective that cyber conflict is of limited import in international relations. See, for example, Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001); Scott Borg, "Economically Complex Cyberattacks," *IEEE Security and Privacy Magazine*, Vol. 3, No. 6 (November/December 2005), pp. 64–67; Mike McConnell, "Cyberwar is the New Atomic Age," *New Perspectives Quarterly,* Vol. 26, No. 3 (Summer 2009) pp. 72–77; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010); Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conoict Debate," *Journal of Strategic Studies*, Vol. 36, No. 1 (February 2013), pp. 125–133; Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, Vol. 36, No. 1 (February 2013), pp. 120–124; and Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and State- craft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40.

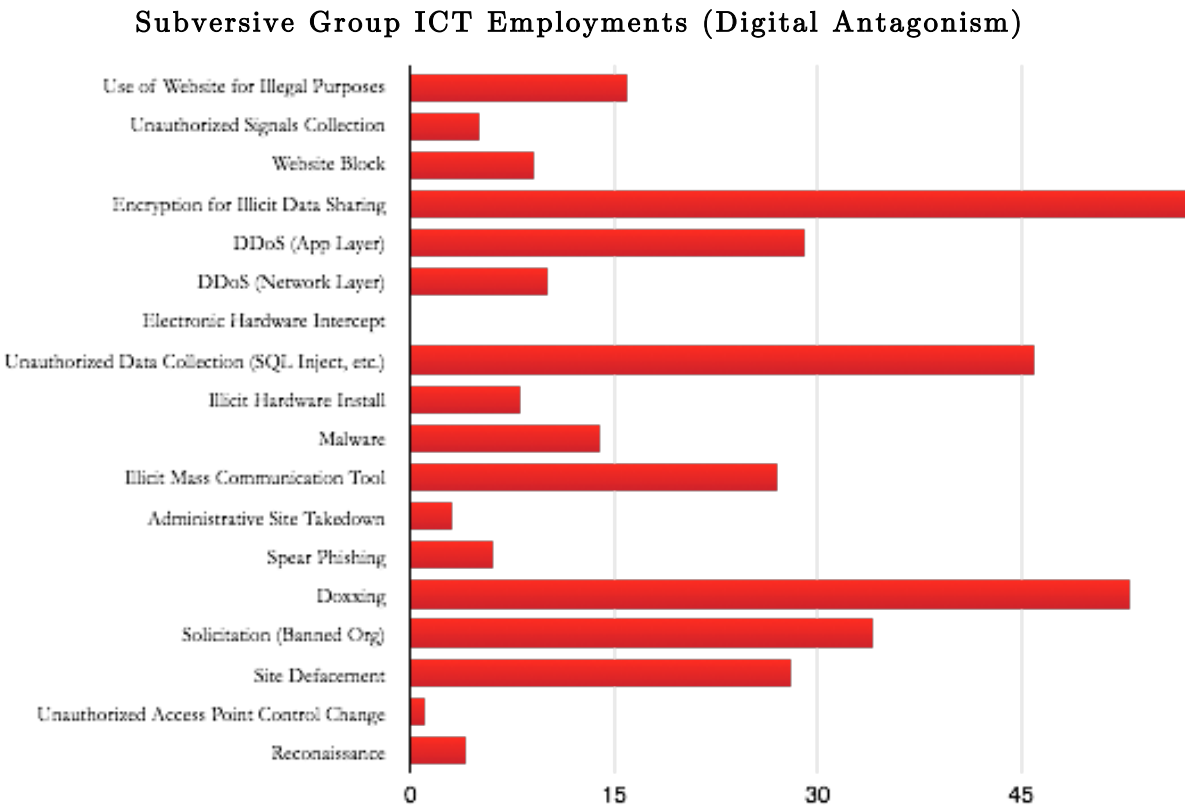

Figure 2.3. Subversive group use of ICT for antagonism.

As Figure 2.3 shows, this study's own data collection and analysis efforts clearly find broad support for the notion that many subversive actors use ICT for digital antagonism. In addition to the use of web technologies for everyday communication and advertising, subversives also engage in cyber attacks and use ICT to mask criminal efforts not infrequently. The distribution of these uses of web technologies is the subject of Chapter 3's outline of the central puzzle being investigated in this project. However, it is worth noting here that the various ICT employments outlined in Figure 2.3 are not uniform. Rather, they describe a broad range of techniques and tactics that aid various elements of subversive campaigns.

For instance, some of the techniques described in Figure 2.3 might be applied for the purposes of gathering information useful to the campaign. Whereas a group might choose to gather information through open-source data crawling, polling or the commercial acquisition of population information, subversives might want to collect information that is not meant to be publically accessible. And in some cases, such information is not simply unavailable, but rather is actively hidden and protected. In those instances, a group might use techniques – such as the use of illegally installed equipment for monitoring or basic network system intrusion for data exfiltration – that are explicitly illegal. ICT can also be used to enhance logistical functionality and to enable a range of funding and financial coordination efforts not permitted by law or etiquette. Different from coordination of funding efforts undertaken through commercial banks or the provision of population data in the context of an authorized political action organization, the use of encryption and other techniques can be used to enable the provision of illegally-obtained and –possessed information to members of a subversive organization. Likewise, ICT can be leveraged to hide relationships with organizations and individuals that are blacklisted, outlawed or simply seen as undesirable in a given national context.

Subversive organizations can use yet other web technologies described in Figure 2.3 to mobilize existing members and recruit new supporters. In this category, subversive and other extremist groups are not alone in their propensity to use ICT for low-key coordinative efforts, of course. Nevertheless, many subversive groups advocate the use of

encryption for communications as a matter of course for members, which is far less common amongst mainstream political parties (for instance). And subversive organizations might use the techniques described in Figure 2.3 for purposes of disruption and mitigation of opposition threats. Denial of service attacks, the employment of malware and even relatively simple – yet often illegal – operations like ping mapping can interfere with the operation of countersubversive non-state actors and can even – in the case of vandalism – offer subversive organizations a means of indirect demonstration useful for the task of simultaneously framing conflict and avoiding close public scrutiny.

2.3.1.3. New Abilities, New Challenges

What do new functional abilities from the use of ICTs actually mean for the operations of non-state actors and are there potential downsides to "going digital?" Naturally, the answer to this question is different depending on the purposes of the organization in question and the context of the operational environment in which it finds itself. The next section addresses the particular case of subversive actors in world politics in order more particularly address the use of ICT for subversion and to specifically demonstrate the puzzle that motivates this dissertation. However, it is first worthwhile to answer these questions in more general terms.

First and foremost, ICT-given abilities to disrupt and to access information through either legitimate or intrusive means allows non-state actors to potentially

"punch above their weight" in contending with states and other non-state actors.[87] At the same time, however, use of such abilities means greater risk of government and intergovernmental interdiction and observation.[88] Though a common meme about operation in cyberspace is that attribution is difficult,[89] the reality of using ICT is that problems of anonymity and complexity in planning operations portends opportunities and challenges that are relatively evenly distributed. Anonymity online does often protect actors looking to mobilize clandestinely or engage in cyber attacks. However, the sophistication of those technologies bound up in contentious digital interactions also awards governments and others great abilities to observe online activities, as well as broad-scoped opportunities to incorporate deception and redundancy into defense systems and doctrine.[90] In short, new forms of informational interaction centered on computer systems do constitute a new absolute advantage in deceptive operation for

---

[87] See James Adams, "Virtual Defense," *Foreign Affairs*, Vol. 80, No. 3 (May/June 2001); Joseph Nye, "Cyber Power," (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010); and Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, Vol. 192 (March/April 2012), pp. 80–84.

[88] See Weimann, Gabriel, *How Modern Terrorism Uses the Internet,* Washington, D.C.: United States Institute of Peace, Special Report No. 116, March 2004.

[89] For the most complete description of the attribution problem and extended work on the history and contemporary puzzles involved, see Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2, 2015: 4–37. For earlier work, see Richard Clayton, *Anonymity and Traceability in Cyberspace*, vol. 653, Technical Report, Cambridge: Univ. of Cambridge Computer Laboratory 2005; Susan Brenner, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law & Criminology*, 97/2, 2007, 379–475; and David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, Alexandria, VA: Institute for Defense Analysis, 2003.

[90] See Jon R. Lindsay and Erik Gartzke, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2 (2015) pp. 316-348; and Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol. 38, No. 1-2 (2015) pp. 4-37.

non-state actors, but rather carry with them a great many risks to balance the opportunities involved.

For non-state actors using ICT to augment social and political outreach efforts, new tools likewise present a balanced range of opportunities and problems. In particular, the use of ICT to persuade and to galvanize support for a wide range of sociopolitical activities has unique implications for the function of non-state actor processes. Information technologies, from those as common as email and social media to more sophisticated forms, certainly portend a great ability for more far-reaching communication than has historically been possible.[91] Advocacy organizations and terrorist cells alike can use a range of tools to get exposure for their activities and to interact with individuals from which they are geographically and culturally detached. And causes are not only more broadly communicable; non-state actors can also use ICT to place local or regional issues in a global context, an ability which has allowed groups as disparate in their character as China's New Citizens' Movement and al Qaeda to give their causes a global flavor.

But such opportunities also come with challenges borne of the global information environment. In attempting to gain broad-scoped exposure using ICT, groups must contend with global news cycles and are themselves labeled according to the context of policy and debate in non-local settings. Thus, media exposure campaigns can not only backfire on an organization, but can also force institutional changes – borne of the need

[91] See, *inter alia*, Jennifer Earl and Katrina Kimport, *Digitally Enabled Social Change* (Cambridge: MIT Press, 2011; and Weimann, Gabriel, *How Modern Terrorism* [...], 2004.

to adapt to new informational dynamics – that clash with original actor objectives and functions.

The use of ICT for digital activism also tends to have unique effects on non-state actors with regards to the "ownership" of the sociopolitical mission in question. Using ICT to expand a group and to increase exposure to a particular set of ideas or issues naturally means adopting a membership structure where members are highly mobile.[92] Much as is often the case with core supporters of political parties and those who vote for them in general elections, supporters of an organization often activate around particular elements of a platform or at specific critical junctures. And not only does such mobility complicate the task of operating on issues where members are not prone to activation, it also implies a trend towards decentralization of decision-making authority.[93] After all, expanded membership and the need to cultivate abilities to mobilize members in advantageous ways imply the need for a distributed command structure. Thus, organizations that use ICT to persuade and mobilize supporters naturally encounter tensions bound up in the need to accommodate new operational dynamics and the power of the organizational core.

2.4. Next Steps

The next chapter presents the puzzle motivating the specific research question in detail. In short, I ask why some groups that use ICT for activist purposes – i.e. to

[92] See Rid, Thomas, *Cyber War Will Not Take Place*, Oxford University Press, Chapter 5, 2013, pp. 137-143.
[93] Ibid.

engage with a constituency or broader population in a participationist, persuasive fashion – continue to employ digital techniques to perform circumventive, disruptive and illicit acts, despite clear incentives not to. Chapter 4, the design of which is discussed in depth in the next chapter, contains a large-N quantitative analysis designed to shed light on this question. Chapter 5, 6 and 7 then delve deeper with specific case study investigations of cases in which there is unusual variation on the dependent variable.

The findings, outlined in full in Chapter 4, lend support for a theory of subversion in the digital age that emphasizes the explanatory power of actor grievances. Though there is only limited evidence that more radically revisionist subversives actually direct their organizations to use ICT for shady purposes, there is a clear link between the rhetoric adopted by subversive group leaders and the actions of their followers. Simply put, explaining subversives' use of ICT for digital antagonism pivots on understanding the way in which group leaders encourage their supporters. Where a group's grievance is structural and the methods of activism are generally non-participatory, leaders appear to condone greater antagonism by members and incentivize civil disobedience. Where the grievance is structural but the methods change to focus on participation as the means of transformation, incentives for antagonism are muted.

Chapter 3
Subversion in the Digital Age

Christopher E. Whyte

In this chapter, I outline the main puzzle being investigated in this dissertation project and describe different possible explanations drawn from the literatures on terrorism, insurgency, organization theory and more. With hypotheses in hand, I then outline the project's overall research design and the approach taken in pulling together data to represent different explanations in Chapter 4's quantitative analysis.

3.1. The Puzzle: What We Might Expect of Subversives Using ICT

Given the new opportunities and challenges afforded to non-state actors by the materialization of ICTs, how might we expect subversive actors to employ them in their campaigns? As outlined in Chapter 2, subversive organizations aimed at triggering a normative transformation of the status quo by detaching the loyalties of a population from one set of institutions and transferring them to another are essentially engaged in three core tasks. First, subversive groups necessarily undertake activities to mobilize their resources such that their campaign is possible. This can involve a variety of tasks, including targeted outreach for the purposes of attracting operatives, fundraising and information gathering. Second, such organizations take action to mitigate challenges and

create space for subversion to take place. Mitigation is a preparatory category of activity that occurs in parallel to mobilization and does not describe the core persuasive activities bound up in affecting subversion itself. Rather, mitigation involves a group creating conditions for operation through the removal of threats – structural (i.e. government oppression) or ideational (i.e. normative competitors) – and the manipulation of system rules such that a persuasive campaign becomes possible. Finally, subversive groups broadly attempt to subvert. This process of actualization is, as with the others, a broad-scoped category of potential activities that describes efforts specifically designed to detach popular loyalties from the symbols of the status quo and transfer them through the transformation of preferences to other symbols. Naturally, these activities need not occur at different times.

As Rid notes, subversion implies an intrinsically participationist set of activities. The point, after all, is to persuade or activate a population such that normative transformation occurs as either the intentional or default outcome of a broad-scoped rejection of the preceding status quo. It is all, in other words, about hearts and minds. Thus, though the format of subversive campaigns as a contentious political activity involves much organizational preparation and environmental politicking, the main event is about interface with the target population. By definition, subversive organizations start as a countercultural phenomenon characterized by their advocacy for alternative imaginings of society and/or political order. Likewise, in line with the trappings of the subversive objective, such actors naturally move towards participationism insofar as they

aim to make their countercultural perspective a mainstream voice – and, ultimately, the mainstream perspective – in civil society. To be fair, many subversive organizations fail to make such a transition and end up shifting to alternative forms of political advocacy, even to terrorism or violent insurgency.[94] Nevertheless, as Blackstock, Rid and others suggest, successful subversion by definition entails a transition from counterculture to the mainstream as ideas are transmitted in a variety of forms designed to affect the preference set of a target population.

As implied above, ICTs award subversive groups a great set of opportunities to mobilize, persuade and mitigate the efforts of counter-subversive forces. Targeted outreach for recruitment purposes is made easier by social media and the ability to disseminate information without traditional geographic constraints. Likewise, organizations are able to make use of a great number of digital techniques to mask the occurrence or extent of different mobilization activities. Such uses of ICT are often, though not always, illicit. Far right organizations in Germany, for instance, have regularly encouraged members to encrypt communications. Furthermore, they have extensively prescribed use of darknet sites and browsers for the purposes of illegal information collection (i.e. gathering or distributing data illegally obtained from secure industry or government servers). The information revolution has also provided new

[94] For discussion, see *inter alia* McCormick, Gordon H., "Terrorist Decision Making," *Annual Review of Political Science,* Vol. 6, 2003; Weimann, Gabriel, *How Modern Terrorism Uses the Internet,* Washington, D.C.: United States Institute of Peace, Special Report No. 116, March 2004; and ———, "Subversion and Terrorism: Understanding and Countering the Threat," in Memorial Institute for the Prevention of Terrorism, *MIPT Terrorism Annual,* Oklahoma City, Okla., 2006.

means for arranging and hiding financial connections, particularly with crypto-currencies where beneficiaries are increasingly able to receive funds in bitcoin or other forms to then exchange for other tender. At the other end of the spectrum, ICT provide clear and easy means for performing outreach and undertaking advocacy in the public sphere. Email campaigns, blogs and social media allow for low-cost access to large segments of a given population and the proliferation of digital media devices provide a number of ways in which subversive groups can – through, for example, the sharing and framing of different images and graphics – enrich and add nuance to efforts to persuade or activate.

Though we might assess a great many determinants of decisions made by subversive groups to use digital techniques at different times and under different conditions, core challenges bound up in the use of ICTs for various purposes map well to the transitional shape of subversive campaigns in that clear expectations emerge around changing objectives between campaign phases. In the early phases, subversive groups are concerned with mobilization of resources and tend to interact with the population in highly targeted ways. Later, as groups move to actualize subversion through persuasion and activation, they must operate much more in the public limelight. Certainly, specific ICT methods can be employed in both phases of operation. Techniques for encrypting or otherwise masking communications, for instance, are not only useful for intra-organizational coordination; they can be used to communicate with elites in later phases in order to coerce or coordinate endorsement of the subversive platform. But, broadly speaking, groups transition from one portfolio of applications of digital technologies –

that of clandestine (and sometime illicit) operation and mobilization – to another – that of the digital activist organization.

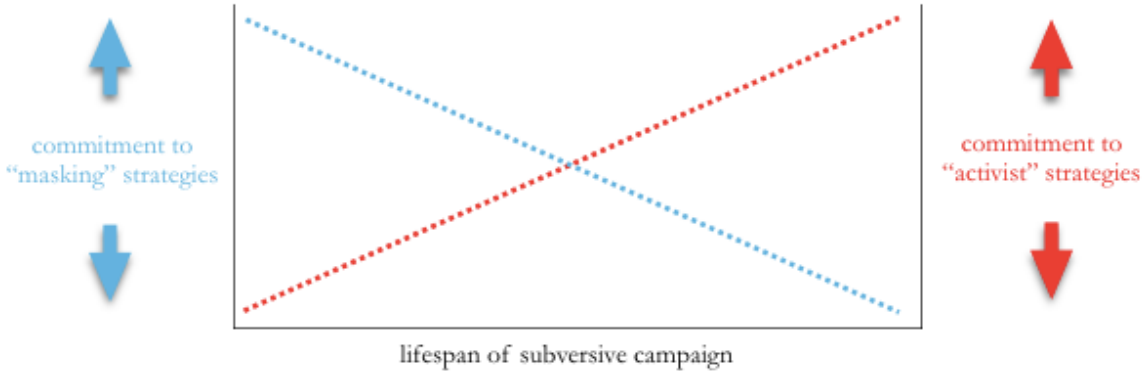

Figure 3.1. Spectrum of possible emphasis on competing strategies of ICT usage for subversive purposes.

More importantly, we might expect subversive actors' campaigns to be characterized by such a shift in portfolio of ICT application for a range of ideational and organizational reasons. Foremost among these is the degree to which an enhanced presence in the digital public sphere means (1) increased challenges for retaining secrecy in operations,[95] (2) elevated transparency of a group's campaign objectives[96] and (3) more opportunities for counter-subversive entities to themselves affect mitigation efforts.[97] Simply put, operation in the public limelight in such a way that allows for

[95] See Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2, 2015: 4–37.
[96] See Thomas Rid, *Cyber War Will Not Take Place*, Oxford University Press, 2013, Chapter 4, pp. 139.
[97] These assumptions are theoretically outlined throughout Chenoweth, Erica, and Maria J. Stephan. *Why civil resistance works: The strategic logic of nonviolent conflict*. Columbia University Press, 2011.

ideational interaction with elements of a population makes it harder to function with any degree of secrecy. This partly comes from the process of decentralization and increased mobility of relevant members that inevitably emerges from greater activist activities, and greater transparency – whether intentional or not – invariably makes illicit operations less concealable and, as a result, much more risky. Thus, actors are incentivized to scale back such activities in order to minimize counter-subversive abilities to mitigate the potential of the organization.[98] Additionally, subversive actors engaged in activist efforts must consider not only the operational integrity of their enterprise, but also the ideational integrity. Normative transformation towards a countercultural ideal has to be palatable to the target population and, though persuasion might occur more as a nuanced replacement of elements of a public agenda than as a broad-scoped replacement of sociopolitical foundations, selling the platform naturally implies a relationship between organizational image and ideational viability.[99] Tarnishing the former via visible connections to criminal activities or "sneaky" operations that are unsavory in the contemporary sociopolitical context risks the integrity of the ideational platform itself, further motivating the minimization or abandonment of such activities in later campaign phases.

[98] This assumption is outlined in, among other places, Roberts, H. (n.d.). The Evolving Landscape of Internet Control. Berkman Center for Internet & Society.

[99] See Robins, K., Cyberspace and the World We Live in. *Body & Society*, *1,* 3-4, 2015, 135-155.

3.2. The Puzzle: Keeping One Foot in the Shadows

The problematic at the heart of this dissertation project is a relatively simple one to understand. In spite of the dynamic described above in which subversive groups' portfolio of tricks shift in emphasis in line with new operating conditions in the public limelight, a significant number of groups involved in broad-scoped digital advocacy clearly maintain emphasis on "masking" and other clandestine activities, often prolifically. Members of Hizb ut-Tahrir in Turkey, for instance, have been regularly targeted and detained for both the use of encryption to coordinate activities and attempts to monitor encrypted communications by high-level government officials.[100] Likewise, member affiliates of the Muslim Brotherhood in Egypt continued to utilize banned techniques to encrypt communications and organize activities during the reign of pro-Islamist President Morsi. More broadly, a massive range of single case study analyses and corroborated media reports over the past two decades have outlined cases of activists turning to antagonism whilst still attempting to digitally engage the public. From Iran and China to the United States, the United Arab Emirates and the United Kingdom, a broad range of groups – including, among others, the National Vanguard, India's RPQT, Kaos GL and non-violent splinter descendants of ETA in Spain – have regularly engaged digital disobedience in antagonizing status quo forces.[101] Quite simply,

[100] See "The Law in Hizb ut Tahrir Lawsuits: Present But Not Present!" TheKhalifah, April 10, 2015.

[101] For a broad overview of the trend, see Krapp, Peter, *Noise Channels: Glitch and Error in Digital Culture*, University of Minnesota Press, 2011; Shantz, Jeff and Tomblin, Jordon, *Cyber Disobedience: Re://Presenting Online Anarchy*, John Hunt Publishing, 2014; "New Hacktivism: From Electronic Civil Disobedience to Mixed Reality Performance". *Hemispheric Institute of*

it is not clear why some subversive groups abandon while others reinforce commitment to digital antagonism – i.e. to clandestine, "shadowy" ICT usage (see Figure 3.2).

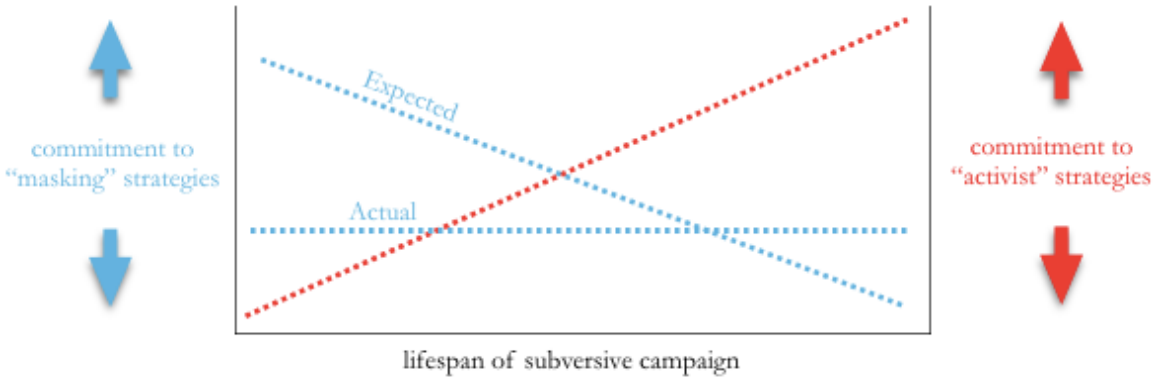

Figure 3.2. Expected vs. actual emphasis on competing strategies of ICT usage for subversive purposes across cases.

This problematic also emerges from work done on hactivism and seditious non-state actions over the past two decades. Specifically, a body of work on the digital activities of terrorist groups, insurgent organizations, militant activists and protest movements has noted a distinct move towards "grey" areas of contention by the full gamut of non-state actors in world politics.[102] These areas – categories of methods of approach to contesting issues, structures, territory and ideas – are labeled "grey" because

---

Performance and Politics at NYU, 2009; and Assange, Julian, "The Curious Origins of Political Hacktivism". *CounterPunch*, 2006.

[102] See *inter alia* Votel, Joseph, *Statement before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities,* March 18, 2015; Barno, David and Nora Bensahel, "Fighting and Winning in the 'Grey Zone,'" *War on the Rocks*, May 19, 2015; Barno, David, "The Shadow Wars of the 21st Century," *War on the Rocks*, July 23, 2014; Mazarr, Michael, "Struggle in the Grey Zone and World Order," *War on the Rocks*, December 22, 2015; and Smith, Jessica Malekos, "Twilight Zone Conflicts: Employing Gray Tactics in Cyber Operations," *Small Wars Journal*, 2016.

of the manner in which they seek to "secure their objectives while minimizing the scope and scale of actual combat" or other illegal activity.[103] The issue relevant to this study arises in the claim that such techniques and approaches are broadly being adopted across the full range of contentious non-state actors around the world, including some countercultural groups demonstrably engaged in digital activism in Ukraine, Lebanon and elsewhere. For some, such as terrorist or insurgent operators, the advantages are clear. But for others, particularly non-violent contentious actors, the move to using ICT for contention and antagonism has to be squared with the incentives and pressures on strategic decision-making outlined above. What prompts decision-making amongst subversive actors to retain emphasis on strategies of antagonism whilst attempting to digitally engage the public in some cases, but not in others? The two subsections that follow add evidentiary weight to this narrative in two formats – first with data drawn from a set describing a large number of subversive organizations and then in a brief case study example.

3.2.1. A High-Level Perspective on the Puzzle of Antagonistic Activists

This pattern of antagonism from subversive organizations actively trying to engage the public is borne out in the shape of group-level data collected for use in this project. The dataset, described in detail later in this chapter, includes 279 subversive organizations utilizing ICT for activist purposes worldwide and spread over three decades. Among the most common activities of groups included in the dataset are the

[103] Olson, Eric, "America's Not Ready for Today's Gray Wars," *DefenseOne*, December 10, 2015.

use of blogs for social/political messaging, the use of social media for a range of organizational and protest purposes, the publication of digital media (photos and short videos) for both messaging and citizen journalism purposes, and the employment of generic email campaigns.

As Table 3.1 below shows, it is certainly not the case that most subversive activist users of ICT are guilty of digital antagonism. Of those organizations studied, 189 have no discernable connection to those shady forms of ICT usage outlined in the sections above. Though not indicative of any particular explanation as to why, this broadly backs up the general supposition that there is a connection between staking out a presence in the digital public sphere and adherence to non-criminal advocacy practices.

But a non-trivial number of organizations studied *are* guilty of digital antagonism – i.e. of employing ICT for disruptive or circumventive purposes. In the set of groups studied, 90 were guilty of the kind deviation outlined in single case analyses and reports of groups like Muslim Brotherhood, Kaos GL, Falun Gong and others. Table 1 shows two cuts of the data on subversive organizations collected for this project as it relates to antagonistic ICT usage. First, it shows the overall distribution of groups wherein there is basic evidence (in the form of a raw positive value) of activity across both categories (i.e. evidence of additional antagonistic ICT employment or not). Second, the table shows the same result for both categories for those most digitally active groups. It does so by assessing the top 10% and 25% most active (calculated by raw score where each episodic employment of ICT is worth "1" and episodes are summed) groups for both categories.

Table 3.1. Breakdown of observed organizations by evidence of antagonistic ICT usage (or not)

	Number of Organizations	
Digital Activists	No Evidence of Antagonistic ICT Usage	Evidence of Antagonistic ICT Usage
All Observations	189	90
Top 10% Most Active	20	7
Top 25% Active	52	18

Not only are some subversive groups guilty of employing ICT for illicit or shady purposes; the information in Table 3.1 shows that deviation from what we might expect of digital activists is not minimal in the sense that digital activists only sparingly or occasionally employ ICT for antagonistic purposes. For both the top 10% and 25% categories, there is clear evidence of deviant behavior by a number of subversive organizations. In other words, some of the most prolific users of ICT for activist purposes also use ICT for digital antagonism – for circumventive, illicit purposes. Figure 3.3 below visually confirms this. Thus, it is clear in both the numerical and chart forms that ICT usage is spread non-randomly across a reasonably large set of subversive actors in world affairs. Digital antagonism is not rare among subversive groups, nor is it particularly less common amongst prolifically activist organizations.

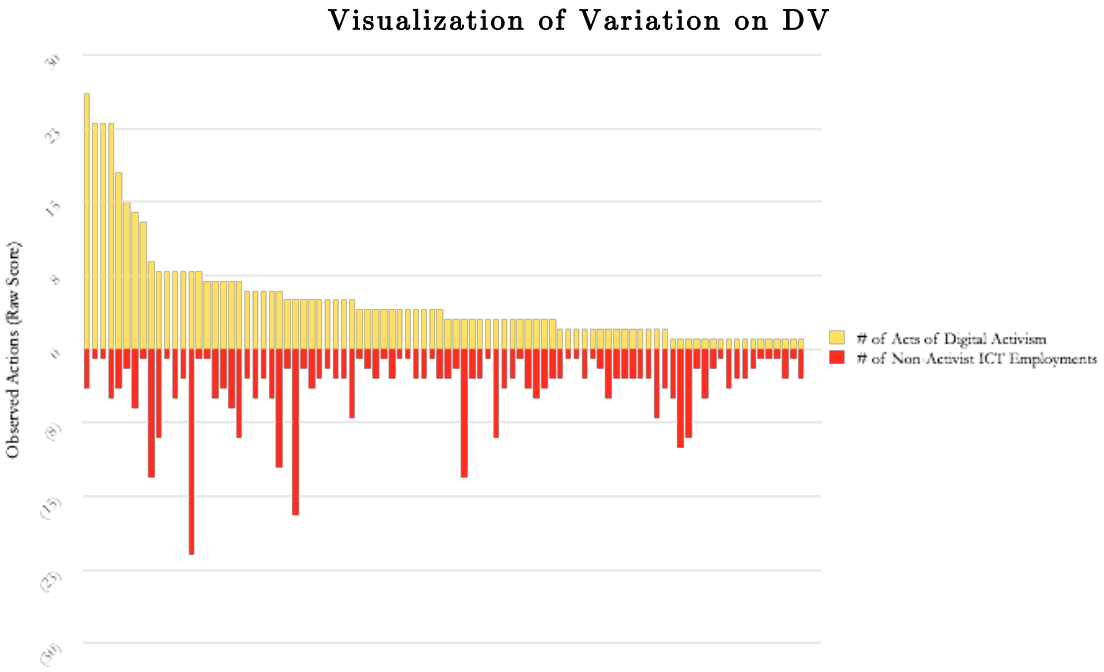

Figure 3.3. Visualization of variation on the dependent variable (i.e. the raw scores of total actions categorized as pertaining to digital activism or digital antagonism across the 90 deviator observations) ordered by number of activist employments.

Given this, when and why do some subversive activists use ICT antagonistically? The clear trend in the data outlined in Table 3.1 and Figure 3.3 suggests that an explanation beyond simple sporadic and random deviation amongst low-end ICT users is required. Basic correlation analysis of the groups under study further backs up this notion. Indeed, separate correlation analysis of both (1) the whole set of 279 groups and (2) the set of just 90 deviators itself preliminarily suggests an interesting story. Results show that greater involvement in digital activist efforts weakly predicts criminal ICT employments for the entire set of subversive actors described (r=0.089). By contrast, correlation analysis of *only* the set of 90 deviators indicates a strong correlation between greater involvement in both types of ICT employment (r=2.023). One clear

interpretation of this result would be that an expanded online presence during the activist phase of a subversive campaign does not itself incentivize deviant tactical choices, but that prior involvement in such ICT employments does predict a larger overall digital footprint. This suggests a potentially interesting link between organization capabilities and the incentives for decision-makers to green light ICT employments for antagonistic purposes.

For several reasons, there is a clear imperative to remedy our limited understanding of the way in which subversion actors in world politics operate in regards to their core persuasive activities. Foremost among these is the simple fact that there exists almost no theoretical basis from which robust empirical examination and explanation might occur. As was noted extensively in Chapter 2, subversion is extremely understudied by social scientists. Scholars attempting to shed new light on the activities of individual subversive actors must invariably cite analytic work dating back to the early days of the Cold War and reference examples from a time in which the global system arguably bore radically different ideational dynamics – i.e. the global struggle between communism and capitalism – than it does today. Particularly when coupled with the resurgent need to understand actors in world politics that bear the hallmarks of subversive operation without the complicating involvement in political violence, investigation of the problematic outlined above stands to produce valuable theoretical results for use by both scholars and analysts.

3.2.2. A Case Example: The Pussy Riot Collective

Any number of individual instances of non-state actors using ICT to achieve exceptional success in organization, mobilization or disruption efforts might serve to illustrate component parts of the new digital age toolset. From well publicized attacks by Anonymous to vandalism the websites of political and religious organizations to the for-hire efforts of black-hat hackers that install and execute malicious code for criminal purposes, the history of non-state adoption of ICT over the past two decades is replete with examples of how such actors are causing unprecedented social, political and economic disruption.

Here, the functional history of a reasonably prominent radical non-violent non-state actor – the Pussy Riot (PR) collective of protest groups operating in the Russian Federation – serves as both a robust example of this new toolkit as employed for activism and, simultaneously and puzzlingly, antagonism. The movement, which is commonly referred to in Western media via reference to the punk rock band *Pussy Riot*, is engaged in a broad-scoped campaign to affect normative and related structural changes focused on conservative policies promulgated by Vladimir Putin and his United Russia political party.[104] In fairness, the names "Pussy Riot collective" or "Pussy Riot movement" are misnomers in that they link a prominent symbol of anti-Putin rhetoric and activity in Russia to a broader movement that pre-existed now-famous incidents

[104] For description of the recent history of the movement, see Sharafutdinova, Gulnaz. "The Pussy Riot affair and Putin's démarche from sovereign democracy to sovereign morality." *Nationalities Papers* 42.4, 2014: 615-621; Prozorov, Sergei. "Pussy Riot and the politics of profanation: Parody, performativity, veridiction." *Political Studies* 62.4, 2014: 766-783; and Miller, Andrew. "Perfect Opposition: On Putin and Pussy Riot." *Juncture* 19.3, 2012: 205-207.

involving the band's protests, arrests and post-detainment statements.[105] The broader movement, which takes the form of a reasonably disconnected series of organizations and groups engaged in (mostly non-violent) resistance to what is perceived to be a status quo hostile to the tenets of Western liberal progressive social values and practices,[106] includes actors with radical designs on Russian society and relatively vanilla protest outfits that seek arguably attainable reforms politically centered on a rebalance of power between Kremlin and Duma. The movement, however, is regularly the target of Kremlin and state-media rhetoric that likens membership support to support of Nazism, Satanism and more.

The PR collective has a reasonably long and certainly turbulent history of using ICT for all manner of political advocacy activities.[107] Throughout the mid-2000s and into the 2010s, members of the anti-Putin regularly engaged in targeted cyber attacks against entrenched political elites. Through 2008, no fewer than 22 instances of doxxing – the strategic and illegal publication of private information to create scandal or encourage

---

[105] For a broader history of anti-Putin protest activities in Russia, see *inter alia* Robertson, Graeme B. "Managing society: protest, civil society, and regime in Putin's Russia." *Slavic Review*, 2009: 528-547; Koesel, Karrie J., and Valerie J. Bunce. "Putin, Popular Protests, and Political Trajectories in Russia: A Comparative Perspective." *Post-Soviet Affairs* 28.4, 2012: 403-423; and McFaul, Michael. *Russia's unfinished revolution: political change from Gorbachev to Putin*. Cornell University Press, 2015.

[106] See Storch, Leonid. "The Pussy Riot Case: Anti-Westernism in the Paradigm of the Beilis Trial." *Russian Politics & Law* 51.6, 2013: 8-44.

[107] For a description focused on the use of ICT by the movement, see Lysenko, Volodymyr, and Barbara Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013*. Academic Conferences Limited, 2013. Also see Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, Mass.: MIT Press.

popular dissent – were linked to the broader movement.[108] In 9 of those cases, members of the PR movement – albeit distantly related to the culturally-motivated direct supporters of the group – were arrested on charges of illegal data mining and information theft via manipulation of basic web-based vulnerabilities found in the sites of mainstream political parties.[109] In two other cases, affiliates of the movement were arrested and charged – ironically, as intelligence and academic analysis has regularly linked the bot economy and early private setup of troll farms to organized crime in Russia and the former Soviet Union (particularly Belarus) – with links to organized crime.[110] Likewise, through 2014, more than 40 instances of website defacements and vandalism against United Russia officials were reportedly linked to the movement,[111] a number which cannot be verified due to the sourcing of the claim from Russian state media but that seems indicative of actions undertaken by the movement according to foreign-based non-profit analysis.

Interestingly, and entirely in line with the puzzle being studied by this dissertation, the PR collective's experience with using the digital toolkit of protest and

---

[108] For a broad description of PR collective actions across the period discussed, see Yablokov, Ilya. "Pussy Riot as agent provocateur: conspiracy theories and the media construction of nation in Putin's Russia." *Nationalities Papers* 42.4, 2014: 622-636. Also see Gapova, Elena. "Becoming Visible in The Digital Age: The class and media dimensions of the Pussy Riot affair." *Feminist Media Studies* 15.1, 2015: 18-35.

[109] For related discussion of the fallout of such actions, see Tchermalykh, Nataliya. "Will Pussy Riot Dance on# Euromaidan? New Dissidence, Civic Disobedience and Cyber-Mythology in the Post-Soviet Context." Religion and Gender 4.2, 2014: 215-220.

[110] See Schuler, Catherine. "Reinventing the show trial: Putin and Pussy Riot." *Anthropology, Theatre, and Development*. Palgrave Macmillan UK, 2015.

[111] For discussion of related dissidence, see Lysenko and Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." 2013.

disruption has gone through three marked phases. During 2011 and 2012, in the lead-up to Russia's presidential elections and in the wake of the various clashes between protesters and government forces surrounding the Pussy Riot incidents, ICT usage manifested almost entirely in the use of social media for citizen journalism, in the use of e-petitions and in using off-the-shelf communications platforms – many of which were the target of surveillance operations – to coordinate anti-government dissent.[112] This was a marked difference from the preceding period, which is probably most notably characterized by the looseness of association between different wings of the movement. Much in the same way that La Résis in France suffered in early days from an inability to affect effective coordination strategies, the 2000s saw limited coordination in dissentious ICT activities, particularly between different urban associations. Low-level hackers claiming membership or flagship of the cause were among those most commonly prosecuting disruptive attacks of various kinds. This changed alongside the focus on digital activism in 2010 and 2011, and the following 12-18 month long period notably exhibited limited anti-government cyber activity beyond protest efforts.[113]

This changed again in 2012 with the arrest and prosecution of members of Pussy Riot. This third phase of ICT operation, which arguably has yet to end, has been characterized by a return to circumventive and disruptive uses of cyberspace to interfere with what members of the movement clearly perceive to be authoritarian government

[112] See Borkowicz, Jacek. "Pussy Riot and Cyber-Orthodoxy." New Eastern Europe 4.3, 2012: 37-44.
[113] Ibid, p. 39-40.

activities. The court trial of Pussy Riot in Moscow in 2012, in particular, was the target of various DDoS attacks and acts of vandalism.[114] In the years since, no fewer than 14 similar attacks have been alleged to be linked to the PR collective in protest against the shutdown of movement operations by the Putin government.[115] In 2014, three members of the movement were arrested for possessing information stolen from United Russia servers relating to Duma members' expenses.[116] Likewise, nearly two dozen prosecutions have gone forward since 2012 against anti-Putin movement members – not including several against anti-Putin politicians not directly linked to the movement – on charges of embezzlement and setting up financial relationships with blacklisted foreign entities.[117] In eight of these cases, the primary method of connection was the use of encryption – often simple P2P apps like WhatsApp – to accommodate such activities.[118] Again, the veracity of much of this cannot be confirmed because of the nature of the reporting on these cases and the questionable nature of the Russian government's prosecution. However, alongside other activities outlined above, it certainly illustrates – even if in only a counterfactual sense – the broad toolkit available to non-state actors interested in prosecuting dissentious advocacy campaigns.

---

[114] See *inter alia* "Pussy Riot Supporters Hack Court's Website," *The Telegraph*, August 21, 2012; "Pussy Riot court website up after hack attack," *BBC*, August 21, 2012; "Pussy Riot Convicted: Moscow Court Website Hacked 'By Anonymous' In Retaliation," Huffington Post, August 21, 2012.

[115] See Bessant, Judith. "The political in the age of the digital: Propositions for empirical investigation." *Politics* 34.1, 2014: 39.

[116] Ibid.

[117] Ibid.

[118] For discussion of relations activities, see Lysenko and Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." 2013.

One final point about the PR collective case bears additional emphasis. In the past several years, a number of cyber attacks and incidents of vandalism prosecuted against both government and mainstream party digital infrastructure were claimed by (1) members of the Anonymous hacker collective and (2) members of the anti-Putin movement claiming Anonymous patronage.[119] The link with Anonymous is interesting, not least because it demonstrates the availability of sponsorship in the form of skills transference and borrowed capacity to disrupt using ICT. Anonymous is a loose-knit collection of hackers drawn from around the world that regularly interfere with the systems and information of social and political actors the group finds to be overly-corporate or hostile to an ill-defined philosophy of progressive freedom and individualism. In truth, Anonymous is difficult to define and to quantify, but is certainly composed of dozens (if not many, many more) hackers that band together in various formats as dissent groups to hack for either entertainment (i.e. for the "lulz") or protest reasons. And Anonymous has directly aided a broad range of dissentious political groups around the world over the past decade or so, from anti-Putin protesters in Russia[120] to the anti-globalization movement and Arab Spring demonstrators.[121] The bottom line,

[119] Though partial in each instance, for descriptions of the full scope of involvement see Kosseff, Jeff. "The hazards of cyber-vigilantism." *Computer Law & Security Review* 32.4, 2016: 642-649; Klein, Adam G. "Vigilante media: Unveiling Anonymous and the hacktivist persona in the global press." Communication Monographs 82.3, 2015: 379-401; and Beyer, Jessica L. "The emergence of a freedom of information movement: Anonymous, WikiLeaks, the Pirate party, and Iceland." *Journal of Computer-Mediated Communication* 19.2, 2014: 141-154.

[120] For description, see Lysenko and Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." 2013.

[121] See Coleman, Gabriella. "Anonymous and the Politics of Leaking." *Beyond WikiLeaks*. Palgrave Macmillan UK, 2013. 209-228.

though far from the purpose of this project, is that non-state actors interested in using the Internet for dissent increasingly have potent resources for external bolstering of dissident efforts and that the Internet has increased the visibility and accessibility of otherwise national dissent issues in the eyes of transnational groups like Anonymous.

3.3. Explaining Subterfuge Amongst Digital Activists

What prompts decision-making amongst subversive actors to retain emphasis on strategies of antagonism whilst attempting to digitally engage the public in some cases, but not in others? The central argument and theory presented in subsequent chapters is the product of inductive testing designed to address the puzzle of deviant subversive activists. In the formative stages of this project, emphasis was placed on broad-scoped testing of a range of factors that would avoid the pitfalls of deductive modeling around such a complex political phenomenon. In short, the idea is to draw data and analyze subversion in the information age in such a way that any emergent theory is generalizable beyond the purview of a limited set of cases. Thus, data collection – and subsequent testing undertaken in Chapter 4 – is centered on the need to study several discrete categories of possible explanation of subversive group behaviors. This section describes these categories of possible explanation.

3.3.1. Possible Explanations

In Chapter 4, I outline a theory of subversion in the digital age before presenting the results of a large-N study that tests the explanatory power of the several categories

of arguments. These arguments reflect theoretical perspectives drawn from the diverse literatures on terrorism, insurgency, militant activism and social movements. They posit alternative approaches for understanding the decisions made by actors interested in making different types of political activities.

3.3.1.1. Strategic Prospects

The first set of explanations that I consider and test in Chapter 4 reflect the idea that actors are rational in a bounded sense. In the context of subversive groups, these explanations have to do with the political or ideological dynamics driving group behavior and the goals of the subversive campaign itself. In brief, the argument here is that the core ideological precepts that define group strategic objectives and ultimate outcomes are also the primary drivers of strategic decision-making across a number of formats (i.e. including the choice of specific tactics related to ICT usage).[122] The nature of the cause determines the strategies adopted, much as the "operational code" of leaders, it is often argued, drives strategic decision-making. With ICTs, we might expect to see strategies formulated from cost-benefit analyses of likelihood of moving towards eventual objectives in the context of unique historical, cultural or political conditions. In other words, the tactics we can expect to see used are those that best fit group or decision-maker expectations regarding the shape of successful subversion. This does not necessarily

[122] See, among others, Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, New York: Addision-Wesley Longman, 1999; Bruce Hoffman, *Inside Terrorism*, Columbia University Press, 2006; and Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*, Princeton University Press, 2011.

include the survival of the group or its favorable treatment, so long as normative transformation remains possible. Again, this set of arguments is, in many ways, the baseline (or bounded rationalist) expectation with regards non-state behavior. Group identity and stated objectives determine strategies in all instances.

This category of explanations is, in many ways, tricky to quantify for statistical testing. How does one quantify group psychology, ideology or the outputs of a range of cost-benefit analyses in a way that is useful to meaningful large-N analysis? One approach common in the literature on terrorism and insurgency is to focus on the nature of a group's objectives. This can be done in two ways. First, Abrams and others argue that the breadth of an organization's policy platform and intended reformations matters a great deal when it comes to decision-making.[123] In particular, groups with minimalist objectives – meaning that they espouse only one or a handful of highly specific grievances – are far less prone to non-strategic behavior than are those with maximalist objectives (where the portfolio of grievances is both numerous and diverse).[124] In the context of subversion, wherein the purpose of advocacy operations across the gamut of possible functions pivots on non-violent normative goals, the implication would be that minimalist organizations would have less incentive to employ ICT for shady purposes whilst trying to digitally engage the public than would maximalist ones. Thus, H1 is:

---

[123] See *inter alia* Abrahms, Max. "Why terrorism does not work." *International Security* 31.2, 2006: 42-78; Chenoweth, Erica, and Maria J. Stephan. *Why civil resistance works: The strategic logic of nonviolent conflict*. Columbia University Press, 2011; Jones, Seth G., and Martin C. Libicki. *How terrorist groups end: Lessons for countering al Qa'ida*. Rand Corporation, 2008; and Abrahms, Max. "What terrorists really want: Terrorist motives and counterterrorism strategy." *International Security* 32.4, 2008: 78-105.

[124] Abrahms, "Why terrorism [...]", pp. 43-45.

H1: *Subversive organizations with minimalist objectives will be less likely to move beyond digital activism in their ICT employments than will those with maximalist objectives.*

Second, a range of works in the literature on terrorism and insurgency hold that tactical decision-making pivots on the severity of the organization's grievance.[125] Generically, whether or not the organization intends different gradations of overthrow of the status quo determines the extent to which more or less radical tactics become more palatable to group leadership. In many ways, this dynamic is far easier to capture for subversive groups than it is for terrorist or insurgent operations. Since subversion is, again, about non-violent normative transformation, we can assess the question of structural overthrow as a discrete condition. Briefly, does a given subversive group also intend structural revision, structural modification or no significant structural change as a component part of the targeted normative transformation? Differing values on these three sub-questions, as is described further in Chapter 4, produces unique categories of subversive organizations as either revisionist or not. Then, following past work, H2 becomes:

H2: *Subversive organizations with explicit structural grievances will be more likely to move beyond digital activism in their ICT employments.*

---

[125] See, for instance, Ross, Jeffrey Ian. "Structural causes of oppositional political terrorism: Towards a causal model." Journal of Peace Research 30.3, 1993: 317-329; Newman, Edward. "Exploring the "root causes" of terrorism." *Studies in Conflict & Terrorism* 29.8, 2006: 749-772; Beck, Colin J. "The contribution of social movement theory to understanding terrorism." *Sociology Compass* 2.5, 2008: 1565-1581; and Ross, Jeffrey Ian. "Beyond the conceptualization of terrorism: A psychological-structural model of the causes of this activity." 1999.

Finally, one might think about prospects for systemic change across a number of categories as a function of how progressive and tolerant an extant political system already is to modification by the citizenry.[126] As will be described in Chapter 4, this can be measured in a number of ways. In general, however, the idea here is that more permissive and tolerant political systems will encourage subversive groups to be less confrontational and more sensitive to the expectations of a civil society that is already somewhat accepting of change (regardless of sentiment towards specific countercultural perspectives). Accordingly, more democratic and free countries should correlate to more pressure on subversive entities to opportunistically respond to the whims and opinions of the populace they need to win over. This assumption exists in various formats across a range of literatures on non-state actor decision-making, particularly the literatures on insurgency,[127] non-governmental organization (NGO) operations[128] and transnational advocacy networks (TANs).[129] Thus, H3 is:

---

[126] An essential point outlined in a number of works in the literature on terrorism and insurgency, including Schmid, Alex P. "Terrorism and democracy." *Terrorism and Political Violence* 4.4, 1992: 14-25; Chenoweth, Erica. "Terrorism and democracy." *Annual Review of Political Science* 16, 2013: 355-378; and Eubank, William Lee, and Leonard Weinberg. "Does democracy encourage terrorism?." *Terrorism and Political Violence* 6.4, 1994: 417-435.

[127] For instance, in Thapa, Ganga B., and Jan Sharma. "From insurgency to democracy: The challenges of peace and democracy-building in Nepal." *International Political Science Review* 30.2, 2009: 205-219; and Bohara, Alok K., Neil J. Mitchell, and Mani Nepal. "Opportunity, democracy, and the exchange of political violence: A subnational analysis of conflict in Nepal." *Journal of conflict resolution* 50.1, 2006: 108-128.

[128] For instance, in Unerman, Jeffrey, and Brendan O'Dwyer. "Theorising accountability for NGO advocacy." *Accounting, Auditing & Accountability Journal* 19.3, 2006: 349-376.; Davenport, Christian. "The promise of democratic pacification: An empirical assessment." *International Studies Quarterly* 48.3, 2004: 539-560; and Kamat, Sangeeta. "NGOs and the new democracy." *Harvard International Review* 25.1, 2003.

[129] Such as Jordan, Lisa, and Peter Van Tuijl. "Political responsibility in transnational NGO advocacy." *World development* 28.12, 2000: 2051-2065; Hudson, Alan. "NGOs' transnational

H3: *The more permissive the political system is to modification and redesign, the less likely a subversive group will be to move beyond digital activism in their ICT employments.*

In attempting to operationalize strategic objectives and prospects further, of course, one might think about the degree to which a cause is supported or opposed in contemporary society. This links directly to the calculus of members and group leaders in selecting tactics and techniques for use in strategic operations. As it does not directly speak to actor-stated perspectives, however, I discuss environmental support further below in section 3.5.1.3.

3.3.1.2. Organizational Processes

By contrast, the second set of explanations I consider argue that the intervening context of organizational processes do much – more than anything else – to determine the shape of approaches in different spheres. In line with a theoretical tradition stretching back beyond Allison's seminal work on the determinants of crisis policy, organizational process arguments hold that the institutional path to decision-making matters a great deal in the ultimate outcome.[130] Access to information, the involvement or non-involvement of different stakeholders, different operational procedures and more all determine, to some degree, the greater or lesser likelihood of a particular outcome. With regards subversive groups and ICT utilization, one argument would be that groups

---

advocacy networks: from 'legitimacy'to 'political responsibility'?." *Global networks* 1.4, 2001: 331-352; and Keck, Margaret E., and Kathryn Sikkink. *Activists beyond borders: Advocacy networks in international politics*. Cornell University Press, 2014.

[130] See Graham T. Allison, "Conceptual Models and the Cuban Missile Crisis," *American Political Science Review*, Vol. 63, No. 3 (September 1969), pp. 689-718.

retain emphasis on alternative strategies largely because the processes that support them are already in operation and dictate a sort of operational path dependency.[131] Groups continue to follow existing procedures even in the face of changing strategic circumstances, such as the appearance of uniquely *digital* methods. Thus, H4 is:

H4: *Subversive organizations that exhibit evidence of involvement in criminal enterprise prior to using ICT for digital activism will be more likely to use ICT for both purposes simultaneously.*

Perhaps more commonly, however, literature on political science on the relationship between non-state actor organizational structure and decision-making focuses on the difficulties highly diffuse groups have in preventing their membership from shirking leaders' dictates and engaging in unsanctioned operations.[132] The literature on predicting and explaining patterns in frequency and types of terrorist attacks, in particular, holds that highly decentralized groups are far more likely to have free agent

[131] The organizational perspective is discussed more fully in the context of non-state actors in, among many others, Lang, Jochen. "Policy Implementation in a Multi-Level System: The Dynamics of Domestic." *Linking EU and National Governance*, 2003: 154; van den Berge, Wietse, and Koningin Julianaplein. "Analyzing Middle Eastern Armed Non-State Actors' Foreign Policy." *Global Security Studies* 7.3 2016; and Grossman, Taylor, and Amy B. Zegart. "The Problem of Warning: Homeland Security and the Evolution of Terrorism Advisory Systems." 2015.

[132] See, for instance, Kilberg, Joshua. "A basic model explaining terrorist group organizational structure." *Studies in Conflict & Terrorism* 35.11, 2012: 810-830; Kilberg, Joshua. *Organizing for destruction: How organizational structure affects terrorist group behaviour*. Diss. Carleton University Ottawa, 2011; Pearson, Frederic S., Isil Akbulut, and Marie Olson Lounsbery. "Group Structure and Intergroup Relations in Global Terror Networks: Further Explorations." *Terrorism and Political Violence*, 2015: 1-23; Kiruthiga, A., S. Bose, and N. Buvaneswari. "An experimental simulation of hub-spoke terrorist organizational structure." *Advances in Natural and Applied Sciences* 9.9 SE, 2015: 41-45; and Jardine, Eric. *The Insurgent's Dilemma: A Theory of Mobilization and Conflict Outcome*. Diss. Carleton University Ottawa, 2014.

problems than are their more centrally controlled counterparts.[133] Free agent issues (principal-agent problems) arise when structural diffusion or poor design makes an organizational susceptible to moral hazards and adverse selection – where the leadership either cannot know/control the activities of all their agents and where leaders simply *don't* know the capabilities or responsibilities of those agents. With regards to subversive and related radical non-state actors, this takes the form of limited membership control and oversight to the point that dispersed members are not adequately dissuaded from taking self-determined measures in service to the cause. The exact nature and spectrum of formats of organizational structures amongst non-state actors is discussed further in Chapter 4. Nevertheless, H5 is:

H5: *The more highly decentralized a subversive organization is, the less likely that group will be to be able to prevent free agent defection in the form of ICT employments beyond digital activism.*

3.3.1.3. Environmental Pressures

The final set of explanations I consider in Chapter 4's examination focus on the nature of opposition to the functions of a given non-state actors in a given environment.[134] Though a group may have specific objectives and might be forced to operate under particular institutional conditions, the main factors that determine decision-making on competing strategic options are the conditions of opposition to the main activities or objectives of the group involved. With subversive groups, opposition

[133] See Kilberg, Joshua. *Organizing for destruction* [...], Chapter 2. This assumption is also outlined in Rid, *Cyber War Will Not* [...], 2013.
[134] See Hoffman, Bruce. "Inside Terrorism. Rev. ed." *NY: Columbia University Press,* 2006: 32-33.

might manifest in one of two forms. First, subversive groups might – and usually do – attract government opposition. Whether significant and centralized or the product of friction with particular political sub-units, this type of opposition can force decision-making that emphasizes different types of strategies than might otherwise have been considered, even to the point of changing objectives.[135] Second, subversive groups, almost by their nature, are likely to encounter a significant degree of sociopolitical opposition in civil society.[136] If the purpose of subversion is to affect radical ideational transformation that has a significant impact on some aspect of the prevailing sociopolitical order, it is almost inevitable that there will be some form of pushback to the activities of a given group. This might appear as natural competition in the public sphere with groups that emphasize different approaches to political issues, but it might also appear as pronounced organization-specific opposition to a given group. The latter form of opposition might manifest for a number of reasons, including linkages with more extreme forms of political advocacy (such as links with terrorist groups or rogue states), but the overall point remains the same – non-state actors are invariably forced to adopt strategic stances reflective of the state of environmental contention.

With regards to government opposition, the expectation outlined in a number of studies of participationist dissent groups is that explicit government opposition prompts risk-averse strategies on the part of such organizations. The logic is that, even if a group

---

[135] This assumption is outlined in McCormick, Gordon H. "Terrorist decision making." *Annual Review of Political Science* 6.1, 2003: 473-507.

[136] See in Crenshaw, Martha. "The psychology of terrorism: An agenda for the 21st century." *Political psychology* 21.2, 2000: 405-420.

ends up defending particular actions, further emphasis on criminal (or, at least, prosecutable) activities presents a potentially existential threat to organization cohesion. Thus, H6 is:

H6: *Subversive groups facing government opposition (in the form of active investigation of group activities and/or law enforcement interdiction) will be less likely to move beyond digital activism in their ICT employments.*

With regards to popular opposition to dissent groups, the logic – outlined in a similar set of works – is perhaps even easier to understand, in that widespread opposition amongst the target audience incentivizes risk-averse behavior amongst such groups for the purposes of resetting and re-engaging at a later time. Thus, H7 is:

H7: *Subversive groups facing widespread popular opposition will be less likely to move beyond digital activism in their ICT employments.*

Beyond domestic conditions, it seems logical that subversive group decision-making might further pivot on resources and support from beyond national borders. Indeed, several literatures – particularly that on transnational terrorism, insurgent links with criminal enterprise, and transnational advocacy – provide strong support for the notion that transnational support can drive tactical choices and incentivize deviant behavior amongst dissent groups, including the move to support more radical causes and political violence.[137] Thus, H8 is:

[137] See *inter alia* Byman, Daniel. *Deadly connections: States that sponsor terrorism*. Cambridge University Press, 2005; Cronin, Audrey Kurth. *How terrorism ends: Understanding the decline and demise of terrorist campaigns*. Princeton University Press, 2009; Staniland, Paul. "Organizing insurgency: Networks, resources, and rebellion in south asia." *International Security* 37.1, 2012: 142-177; Young Sr, Aaron M., and David H. Gray. "Insurgency, guerilla warfare and terrorism:

H8: *Subversive groups with foreign-based sponsorship will be more likely to move beyond digital activism in their ICT employments.*

Finally, there is a large literature on the degree to which the permissive nature of the international environment as functionally supportive of an organization's operational abilities matters a great deal for the decision-making calculus of dissent groups.[138] Paul McDonald, for instance, outlines evidence that the changing scope of state security considerations in the late 1800s and into the 20th century produced a dynamic wherein counter-insurgency effort simultaneously became more costly and less normatively acceptable. [139] Commitment to a transformation of military forces based on mechanization made counter-insurgency in Asia, Africa and Latin American terrain environments a more expensive prospect. Moreover, the support of certain non-state groups by great powers as a proxy element of interstate intrigue and conflict made brutal treatment of such organizations unpalatable to the broader global community.[140] The information revolution has also seen the promulgation of new technical and

---

Conflict and its application for the future." *Global Security Studies* 2.4, 2011: 65-76; Bapat, Navin A. "The Sponsorship Dilemma: State Support for Militant Insurgency." 2007; Salehyan, Idean. "Transnational rebels: Neighboring states as sanctuary for rebel groups." *World Politics* 59.02, 2007: 217-242; and Stephan, Maria J., and Erica Chenoweth. "Why civil resistance works: The strategic logic of nonviolent conflict." *International security* 33.1, 2008: 7-44.

[138] See, among others, Asal, Victor, and Joseph K. Young. "Battling abroad: Why some organizations are likely targets of foreign counterterrorism." *Civil Wars* 14.2, 2012: 272-287; Caverley, Jonathan D., et al. "Military Technology and the Duration of Civil Conflict"; Bapat, Navin A. "The Escalation of Terrorism: Microlevel Violence and Interstate Conflict." *International Interactions* 40.4, 2014: 568-578; Goddard, Stacie E., and Daniel H. Nexon. "The Dynamics of Global Power Politics: A Framework for Analysis." *Journal of Global Security Studies* 1.1, 2016: 4-18.

[139] See MacDonald, Paul K. "'Retribution Must Succeed Rebellion': The Colonial Origins of Counterinsurgency Failure." *International Organization* 67.02, 2013: 253-286.

[140] Ibid, pp. 254-256.

informational dynamics at the global level alongside shifting expectations regarding the norms of non-state and societal behavior in digital terms. As such, it seems logical that this study should include consideration of such change variables – the coding of which will be discussed on several fronts in Chapter 4 – in testing. Thus, H9 is:

H9: *Subversive groups operating in a mechanically permissive environment (in the form of limited legal and technical barriers to operation) will be more likely to move beyond digital activism in their ICT employments.*

3.3.1.4. Anonymous: A Special Consideration

Related to H8 and H9, one final element bears specific consideration in Chapter 4's testing – the actions of the Anonymous hactivist collective in either direct or indirect support of a subversive group. As suggested in the Pussy Riot collective example above, the intercession of Anonymous agents has been a notable feature of the experience of several subversive groups. Here, the assumption is that the inclusion of a control variable for either evidence of direct sponsorship of or assistance by Anonymous agents will proxy for the significance of developing transnational *ICT-capable* support networks for dissentious non-state actors attempting to enhance their operations via the use of ICT.[141] I argue that this differs somewhat from H8 above in that the intervening significance of Anonymous connections would indicate a more nuanced link between global access to

[141] This is not an uncommon assumption made by researchers. For instance, see Dahan, Michael. "Hacking for the Homeland: Patriotic Hackers Versus Hacktivists." *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013*. Academic Conferences Limited, 2013; Klein, Adam G. "Vigilante media: Unveiling Anonymous and the hacktivist persona in the global press." *Communication Monographs* 82.3, 2015: 379-401; and Coleman, Gabriella. "Anonymous and the Politics of Leaking." *Beyond WikiLeaks*. Palgrave Macmillan UK, 2013. 209-228.

useful ICT platforms and knowledge – essentially, access to cyber arms – than is implied in simply accounting for the specific sponsorship of a foreign actor. Thus, H10 is:

H10: *Subversive groups will be more likely to move beyond digital activism in their ICT employments wherein there is evidence of direct sponsorship or assistance (coordinated or otherwise) in mitigative efforts by Anonymous agents.*

3.4. Towards a Theory of Subversion in the Digital Age

The results of this study lend themselves to a theory of self-assessment and decision-making amongst subversive groups based on organizational assumptions about and machinations for political operation following the desired normative transformation. This theory, posed in Chapter 1 and presented in detail in subsequent chapters, emerges from a large-N research project that has seen data collection on 279 subversive groups engaged in digital activist efforts worldwide over a 33-year period of time. This section more completely outlines the research design of the next chapter.

3.4.1. Research Design

As the focus of the problematic here is the behavior of those groups who have stepped into the public limelight in order to affect meaningful normative transformation, data for testing and analysis was necessarily selected that describes organizations in the latter phases of the subversive campaign process. In the chapters that follow, I present a mixed methods investigation of the puzzle describes above that allows for consideration of a range of possible explanations and lends itself to the development of meaningful theory-building.

Specifically, Chapter 4 undertakes a large N quantitative analysis of the behavior of subversive groups involved in digital activism around the world. I employ the Global Digital Activism Dataset (GDAD) for testing. The GDAD, a multi-scholar project based out of the University of Washington, contains both qualitative and quantitative variables describing digital activism campaigns from around the world.[142] The GDAD has been published in two tranches and contains almost eighteen hundred entries (1,180 in the initial tranche, 426 in the second, and more than two hundred additional entries in a supplementary dataset) describing such campaigns. The dataset covers digital activism in more than 150 countries and spans three decades from 1982 to 2012. In addition to qualitative information on digital activist campaigns and basic descriptive measurements of different actions involved in the activist effort (website usage, blog usage, chat/IM coordination, email coordination, e-petition used, etc.), the GDAD also includes detailed data on the intended purposes of different campaign actions and 28 variables on environmental conditions (regime type, rule of law, etc.). All data is documented and freely available, all sources are catalogued and the project behind GDAD provides summary case information for every digital activist campaign covered.

The dependent variable – whether or not a subversive group retains emphasis on clandestine or illicit ICT practices whilst also engaging in digital activism – is the result of two types of coding passes through the GDAD. First, I code whether or not each group described in the GDAD can be said to be subversive (further details on this

[142] For more information, see http://digital-activism.org/projects/gdads/.

process are provided in Chapter 4). This narrows the dataset to including only those groups involved in digital activist campaigns that are also subversive. Then, I code for the use of alternative ICT usage (again, described further in Chapter 4). Coding for alternative uses of ICT for clandestine or illicit practices is based on a simple method of validation – such information must be corroborated by official reporting or analysis on the part of a legitimate government or intergovernmental agency, such as the Federal Bureau of Investigation (FBI), Interpol, etc. In coding whether or not a subversive group *has* retained emphasis on clandestine or illicit ICT practices whilst also engaged in digital activism, I produce a dichotomous measure of the independent variable that can be paired with different data representing different IVs to descriptively and statistically (primarily through logistic regression testing) analyze the determinants of DV variation.

This large N investigation is the basis for theorization on the determinants of DV variation. In essence, I use the quantitative component of this study to assess the competing possible explanations for why subversive groups often "keep one foot in the shadows" with regards to ICT usage described above, to control for the impact of different intervening variables, and to produce theory on the matter.

The case study analyses presented following Chapter 4 reflect a comparative case approach to understanding the determinants of digital antagonism. Each chapter examines a subversive organization operating in single-country context (i.e. not transnational organizations). Chapter 6 and Chapter 7 focus on the experiences of the National Democratic Party of Germany (NPD) and the German Left Party. Chapters 8,

9 and 10 examine three organizations in China – Falun Gong, Civic Passion and Eastern Lightning. Through comparison of the experiences of these subversive activists and their use of information technology, I add nuance to the correlative understanding of factors linked to incidence of digital antagonism that emerges from Chapter 4's large-N analysis. The shape of this added nuance is described in detail in Chapter 5.

The logic of this approach to qualitative analysis to complement large-N efforts reflects the need to vary values of the dependent variable and key independent variables in a controlled fashion. In essence, focus on two German groups reflects a "most similar" case study approach; Chapters 8, 9 and 10 reflect a "most different" investigation of three Chinese groups.[143] In other words, Chapter 6 and Chapter 7 study two groups that, because of the strict nature of German regulations on political party organization and more, are similar across all characterizing factors *except* the content of their sociopolitical messaging. Then, in looking at three groups based in China, my approach focuses on organizations that share a single defining feature – an official characterization of each group (in one case for a limited period of time) as a threat to state security – and differ broadly across others, including social/political objectives, group structure, public favorability rating, etc.

Perhaps most notable in the design of the qualitative analysis in chapters to come is the variation on group objectives and grievances – an explanatory factor found to be uniquely impactful in predicting a group's antagonistic ICT usage in Chapter 4 –

[143] See George A.L. and Bennett A, Case Studies and Theory Development in the Social Sciences, Cambridge, MA: Belfer Center for International Affairs, Harvard University, 2004.

across cases. Both groups in Germany maintain a structural grievance that is tempered in organizational commitments to participation in extant political processes. However, while one group (Die Linke) has taken steps to streamline party platform and better engage the electorate, the other (NPD) has refused to do so and has instead sponsored an unstructured fringe coalition intended to disrupt mainstream politics in Germany. In China, campaign objectives vary broadly across the cases being studied, from Eastern Lightning's lack of interest in contemporary politics to Falun Gong's moderate desire to restructure Chinese politics and Civic Passions claim that Beijing's authority is illegitimate.

Further, case chapters feature variation on the dependent variable in each national context. Whereas the NPD in Germany has either tacitly authorized or actively condoned such ICT employments, Die Linke (the Left Party) has not. Likewise, China's two "evil cults" (Falun Gong and Eastern Lightning) have and have not respectively broadly employed ICT against state law, while Civic Passion's deviancy is limited to a period between the end of the Umbrella Movement and recent attempts to moderate party efforts. And, finally, the selection of Germany and China for national-level analysis further allows for the influence of competing macro conditions, namely the degree to which access to digital capabilities is limited in each country and the nature of environmental obstacles to group operations.

3.4.2. Quantitative Testing: Data and Methodology

Subversion is not only understudied, it is also difficult to study. The focus of subversion is the hearts and minds of humans and not either violent outcomes or mechanical effects (i.e. on machine systems or infrastructure). Nevertheless, as the focus of this dissertation project is the practices and methods of approach employed by subversive organizations in the course of their campaigns, there is some degree to which I am able to avoid the empirical subjectivity and methodological creep that might characterize an effort to interpret the manifestation of subversive outputs.

This said, most datasets that describe extreme non-state actors either focus inappropriately – for the purposes of this study – on violence as a primary selection criterion or ignore the extreme actor itself in favor of emphasis placed on describing the effects side of the equation (focusing on, for instance, normative outcomes in public opinion trends or particularly types of disruptive incidents). Though these data sources might potentially be useful for a number of related efforts, they suffer in that they either do not entirely encompass the subversive enterprise in selection or themselves select on the dependent variable without proper consideration of efforts that fail or are in progress. Thus, they do little for the purposes of this project, where the point is to assess subversive group decision-making around new information technologies – which broadly proxy for subversive techniques and tactics in the modern era – and theorize on observed variation in usage in the public-facing phase of campaigns. Clearly, a new dataset is required.

Fortunately, the focus of this project on the public-facing element of subversive campaigns allows for selection of existing resources based on a clear criterion – the engagement of subversive groups in activities designed to publically advocate, persuade and mobilize public support for a cause (i.e. digital activism). Though additional work with any existing resource might be needed for any project that seeks to utilize research on political activism broadly writ for the study of subversion, it is the case that a range of options are available for modification and employment. This study looks to one dataset – the Global Digital Activism Dataset (GDADS) – as a basis for testing the premise and hypotheses outlined above. The dataset, used briefly above to demonstrate the puzzle, is described below alongside a discussion of dependent variable (DV) construction.

Testing of hypotheses outlined above is done both descriptively and statistically. In the sections below, I utilize the wealth of information that emerges from analysis of the dataset to demonstrate the project's premise and analyze the shape of subversive choices of different techniques and tactics. I then use the operationalization of the DV described below as the basis for statistical testing of a range of possible explanations of variation across cases. Because the primary variables are binary in nature, this testing will take the form of binomial logistic regression analysis. Likewise, though the dataset is sizable for our purposes (more than 350 episodic observations of ICT employments across 90 groups in the 279 group set), it is relatively small and so demands additional

attention for the purposes of robustness in producing results. Thus, testing in Chapter 4 also includes conditional log-link and rare events regression analysis.

3.4.3. The Dependent Variable

The dependent variable for Chapter 4's quantitative assessment is a dichotomous variable that operationalizes the DV by describing whether or not subversives involved in digital activism also employ the alternative techniques described. There are three tasks involved in measuring variation in the use of information and communication technologies for subversive purposes and constructing indicators useful to testing the hypotheses above. First, it is necessary to identify a population sample of subversive groups operating in world politics. Second, proper identification of different techniques and uses of ICT is required. And finally, there has to be a clear selection of cases for observation based on the conditional premise of the research question – that of involvement in those public-facing employments of information technologies that we might broadly label as digital activism. In order to accomplish all of these, I use as a basis for coding and testing the Global Digital Activism Dataset (GDADS).

The result of a broad-scoped collaborative project (the Digital Activism Research Project) founded in 2012, the GDADS is a large-N events database that describes incidents of and organizations involved in digital activist activities over a more than thirty year period. Based out of the University of Washington, the project is an ongoing effort to apply rigorous coding and testing methods to identifying instances of civic engagement, citizen activism, journalism and more in world politics. The project is an

increasingly useful resource for scholars seeking to reference or work with data that reflects the realities of political persuasion and activism in the digital age – i.e. largely linked to the shape of digital infrastructure and changing information environment dynamics. The project is financially supported by the United States Institution for Peace and has been the basis of a range of scholarly works designed to study, among other things, human rights organizations, citizen social movements, and American foreign policy and diplomacy centered on civic liberalism.

The database produced by the broader project itself consists of almost 2,000 observations – released in several tranches between 2012 and the present – of instances of digital activism. Each observation consists of a range of useful pieces of data, including information on the organization, individual or movement involved in an activity and contextual information on the nature of the operational political environment. The dataset also, naturally, contains source information and breaks down observations of digital activist activities via reference to a coding list of different types of actions. These actions are listed in Table 3.2. There are natural redundancies in the coding scheme employed, as actions like the use of digital video content can appear in email campaigns, on websites, blogs or in social media. This brings a benefit, however, in that summary variables are based on a nuanced understanding of the exact shape of activist activities. For the purposes of this project, I exclude a single activity variable from the list – the ANON variable, which generically describes the use of "circumvention" tools. I do so for two reasons. First, the coding for this particular digital

activity type is far more general in nature than is coding for other activities. Second, I undertake a parallel coding effort – described below – to aid this project's testing requirements on the topic of the use of ICT for a range of different obfuscating and illicit activities.

Table 3.2. Variables in GDADS for Digital Techniques/Applications

	Variable Name	Description
1	APP	Multiple applications employed
2	BLOG	Blog employed
3	CHAT	Chat or Instant Message applications employed (public-facing, not membership only)
4	EMAIL	Email campaign employed for either targeted or general information dissemination
5	EPET	e-Petition employed
6	FORUM	Internet forum employed
7	FOTO	Digital photo employed (any static image format)
8	GAME	Video or Internet-based games employed
9	ISN	Internet-based social network application employed
10	MAP	Embedded digital map included in content
11	MOBAPP	Mobile applications employed
12	MSN	Mobile-based social network application employed
13	OTHAPP1	"Other" application employed
14	OTHAPP2	"Other" application employed
15	SITE	Website employed (describes public-facing site development and usage; excludes database usage and private member-only platforms)
16	VID	Digital video employed (any non-static image format)
17	VOICE	Web-based voice applications employed
18	WIKI	Wiki platform employed

For inclusion in the GDADS, organizations and events needed to fit certain criteria. First, instances of digital activism needed to have a clear digital component constituted of one of the activities described in Table 3.2. Second, there needed to be a clear activist intention in the employment of information technologies. This means that

the use of information technologies needed to be specifically about political persuasion or participation in the service of a stated desire for social or political change. Coding criteria for this are listed and described in Table 3.3. Finally, the incident had to be verifiable beyond observation of the activity. This means that description of the activity by a third-party source deemed credible by the research team was necessary.

Table 3.3. Framing and strategic function variables in GDADS

Variable Name	Description
BRODPURP	Information sharing purpose
COPURP	Co-creation purpose (i.e. actions that emphasize collaboration around a cause or organization activity)
DOCPURP	Documentary purpose (i.e. actions intended to record or document cause/organization and related activities)
MOBPURP	Mobilization purpose (i.e. actions intended to mobilize either the organization's members or a broader population)
NETPURP	Network construction purpose
NVTYPE	Categorical description of the non-violent activist behavior being supported by the relevant digital activity. Variable is coded **"1" for protest/persuasion** peaceful opposition efforts to build a sympathetic audience; **"2" for non-cooperation**, including strikes and boycott activities; **"3" for intervention** efforts designed to non-violently mitigate opposition capacity to act; **"4" for semi-violent actions**, including cyber vandalism; **"55" for multiple behaviors**; **"99" for unclear episodes**; and **"0" for activities that cannot be categorized as non-violent or violent**, as they do not directly involve challenging status quo ideas/structures.
SYNTHPURP	Synthesizing purpose (i.e. actions intended to synthesize content)
TRANSPURP	Transfer of resources purpose (i.e. actions designed to reorganize financial or human resources)

Data collection for the GDADS took a range of different forms. According to database documentation, initial efforts revolved around expert suggestions for sources that were volunteered in response to an online form emailed out. This produced limited responses and so both volunteers and a large cohort of undergraduates were tasked with

searching a range of both public databases/media outlets and peer-reviewed journals to identify an appropriate set of selection sources for the database. Alongside well-known peer-reviewed resources in the archives of the publishing house SAGE's journal database, GDADS particularly draws information from a range of sites known to report on and index digital activist activities. These include, among others, Global Voices Online, MobileActive.org, Mashable, Tactical Technology Collective and Movements.org.

The GDADS product is defensibly comprehensive and both source lists and raw coding outputs are made available publically. This includes all narrative accounts that were used to verify digital activities and code for the variables provided in the dataset. As mentioned above, the dataset has been published in several tranches and is due to be updated further in either late 2016 or early 2017. Overall, the database includes almost 1,800 instances of digital activism – 1,180 in the initial tranche, 426 in the second and more than two hundred additional entries that include organization-level information based on a digital activity provided in supplementary materials. The dataset covers activities in more than 150 countries and spans 30 years from 1982 until 2012. Further additions to the dataset expected in the next year are anticipated to update this to the present. However, in the course of developing this project, I was able to provide a provisional extension to the database through early 2016 using the documented methods and sources outlined by the GDADS project. For the four years between 2012 and 2016, I find an additional 678 episodes and incidents of digital activism.

For the purposes of this dissertation project, the GDADS is particularly useful because it provides a pre-constructed data resource describing organizations and movements undertaking digital activist activities. Not all groups described in the GDADS are subversive, of course; the vast majority of groups, in fact, are not. Nevertheless, the dataset provides an exceptional foundational opportunity to identify subversive organizations amongst the broader universe of digital activist cases and to perform testing on possible explanations for variations in activity. As described above, operationalization of the dependent variable for this study includes several tasks.

First, it is necessary to identify those groups that we might consider subversive. In many ways, this is the single most methodologically sensitive element of data collection for this project. Naturally, identifying such groups is a difficult task insofar as the context of a group's sociopolitical environment determines whether or not the subversive label is warranted. Working with the GDADS, my first step in preparing the dataset such that it is useful for investigating the premise of the project was to code out organizations, movements and informal groups identified within the original dataset not subversive. The aim was quite simply to be left with a dataset that emerges from the same reliable original coding practices of the broader GDADS effort in which each observation describes the behavior of a subversive group. Initially, this task involves identifying subversive organizations broadly construed. More specifically, this task involves classifying activists by their relationship to the subversive organization. The links that exist between activist groups or movements and subversive organizations can

take a number of formats, from direct involvement in activist activities to activism enacted by front groups or surrogate organizations. Coding for this set of distinctions is discussed below as a component part of the effort to explain subversive techniques in organizational perspective.

To preliminarily identify subversive groups for the purposes of basic dataset construction, I apply the definition of subversion specified in Chapter 2:

> *Subversion is a transformation of the normative status quo among a significant community or population characterized by the detachment and transference of prevailing political and social group loyalties to the symbols and institutions of the subversive force. Though subversive actors need not consider prevailing conditions to be entirely illegitimate, successful subversion is itself characterized by the establishment of a status quo position that would previously have been considered illegitimate.*

Subversion is perhaps most identifiable by the condition of contested legitimacy. Indeed, this condition is a necessary one in any effort to identify subversive actors. A successful subversive outcome, either actual or stated by the subversive actor, involves not only a replacement of one status quo set of conditions with another; subversion is, in fact, principally characterized by institution of a new status quo that the former manifestation would consider illegitimate. Subversive groups themselves may not necessarily consider the prevailing normative status quo entirely illegitimate, but the subversive enterprise is by definition characterized by the countercultural mantle of an unsanctioned idea (or platform of ideas). To be subversive, a group or organization must aim for transformation and eschew the notion of normative adaptation or addition. Using the definition above, groups like Greenpeace, the Republican Party of the United

States and Amnesty International were eliminated from the set, leaving only radical activist organizations like League of the South, Millî Görüş and Eastern Lightning.

The dataset was analyzed on a case-by-case basis to identify subversive groups and movements. I find 232 subversive groups out of the nearly two thousand original observations presented in the GDADS. My own coding found 47 additional instances in the period of time between 2012 and 2016 in which the organization in question meets the definitional criteria of a subversive organization (for a total of 279 observations). They are enumerated on a regional basis in Figure 3.4.

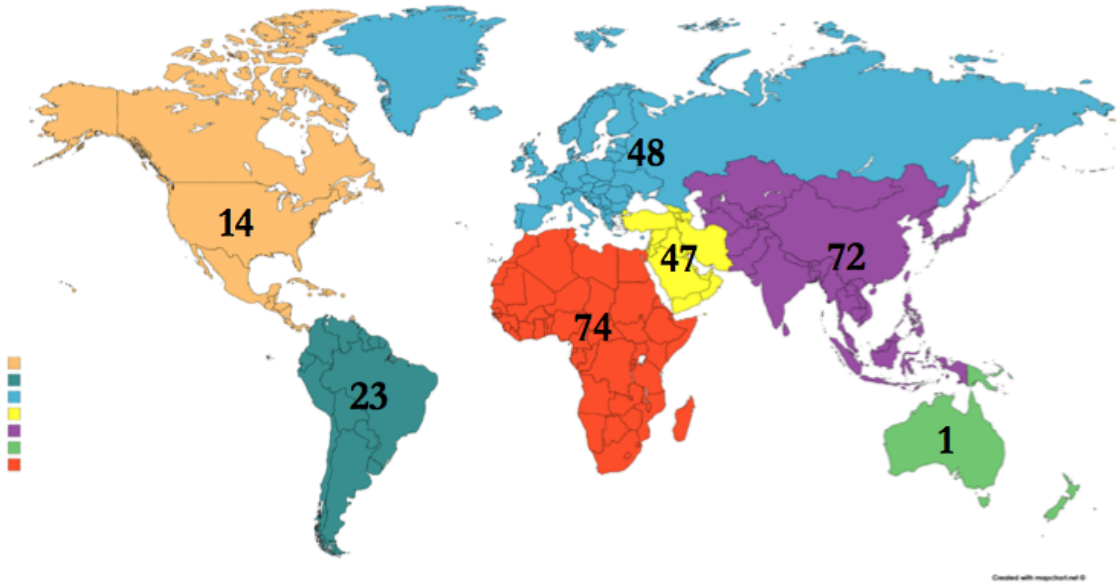

Figure 3.4. Number of subversive organizations catalogued by world regions (including the Middle East)

These subversive actors are not uniform. Some actors taking part in digital activist efforts are linked to core subversive causes and organizations distantly and appear to be front groups, "legitimate" sister organizations and more. Coding for the format those

actors described in the GDADS take and for their relationship to the core identifiable subversive effort are discussed below in the section on coding for independent variables, as it most directly relates to explanations of subversive behavior based on organizational structure and group strategy. Nevertheless, one point about inclusion in coding bears mentioning. Specifically, for a group to be included, the activist element must demonstrably be linked to leadership via clear executive command and/or coordinative actions (such as direct orders or post-activity expressed support). In essence, there is no inclusion of a group here wherein reporting includes only the suggestion of a link with a particular organization.

Operationalization of the dependent variable further requires identification of the broad range of techniques and tactics involved in ICT usage for shady or illicit – what the GDADS project calls "circumvention" – purposes. A broad range of sources were used to catalog common types of actions or categories of activity that might characterize the efforts of groups trying to (1) organize (i.e. overcome logistical challenges), (2) mobilize already-sympathetic supporters or (3) mitigate the counter-organizational efforts of opposition interest groups and law enforcement. Specifically, I utilized Factiva, Lexus Nexus and Google Scholar, among other database search engines, to survey groups included in the GDADS (primarily using keyword search). Source information is discussed further below.

These actions/action categories are summarized in Table 3.4. Importantly, coding for these categories of actions are episodic in two senses. Data are episodic in a temporal

senses, which is discussed below. However, data on ICT employments are also episodic in that one observation of, for instance, network layer distributed denial of service (DDoS) attack might include multiple disruptions against a target. This is not uncommon in cyber conflict research, as prosecution of a particular technique may include a series of repeated actions for tactical purposes. The demarcation point is that of distinct episodes in the form a significant period of time or a change in an organization-level target.

Table 3.4. Non-GDADS Variables coded for Digital Techniques/Applications

	Variable Name	Description
1	ADV	Use of website or social media for explicitly illicit or unconstitutional purposes
2	APT	Advanced Persistent Threat
3	AVG	Non-public, non-permission source data collection (i.e. hacking into CCTV systems, etc.)
4	BLOCK	Non-DDoS, non-administrative blocking of specific websites
5	DARK	Use of Darknet specifically for the purposes of illegal data sharing
6	DARKFUND	Use of Darknet or other encryption protocols specifically for the purposes of hiding funding activities that would violate law/regulations
7	DDOSAPP	App layer denial of service attacks wherein disruption is achieved via interference with specific softward/platforms
8	DDOSNET	Network layer denial of service attacks wherein disruption is achieved via network traffic overload
9	DOX	Online publication of private information obtained illegally (bank account information, IDs, addresses, etc.)
10	ELWAR	Electronic interception of unmanned platform
11	EXFIL	Private data theft from web-based or hard media vulnerabilities
12	INSTALL	Illegal installation of hardware used to interfere with digital systems
13	MALW	Employment of malware (through email, website, hard media, etc.)
14	MASS	Use of illicit mass-communication spamming programs
15	OFFBLOCK	Blocking of websites through administrative take-down requests
16	P2P	Use of P2P techniques specifically for the purposes of illegal data sharing
17	PHISH	Spear-phishing emails
18	RECON	Reconnaissance intrusions (ping mapping, access probe attempt, etc.)
19	SOLIC	Explicit solicitation of funding online from groups blacklisted/outlawed in host country (non-darkweb)
20	VANDAL	Website defacement and vandalism
21	WFC	Non-permitted change of access point control

Beyond the identification of the range of activities listed in Table 3.4, coding the use of circumvention techniques by subversive actors occurred in several steps. First, I established appropriate guidelines for verification of technique employment by the individuals and groups in question. A clear challenge in undertaking any research on

cyber conflict is the need to robustly attribute responsibility for particular actions to a specific actor. This challenge presents at two levels. First, actor attribution of cyber attacks or circumvention tools can be difficult because, though technical attribution is often easier than expected by the layman, the inherent anonymity and easy deniability of cyber actions presents challenges in connecting actions in the digital and physical realms. Responsibility, different from technical attribution, is the outcome of forensic investigation by law enforcement, intelligence actors and, increasingly, media examiners. Naturally, the challenge in undertaking this kind of research is in setting an appropriate standard of verification and reliability for data collection in this regard. Relatedly, and secondly, research on cyber conflict faces the challenge of bias in reporting on responsibility for different usages of cyber techniques. Reporting agencies may have political incentives to over- or under-report the full scope of activities discovered and journalists, though this is increasingly less true at high levels, may misreport cyber intrusions and actions insofar as they fail to differentiate between employments that appear similar in profile to the layman.

For the purposes of this project, I choose to attribute cyber technique usage to particular groups in the dataset via reference to governmental and inter-governmental entity reporting, to government-cited non-profit reporting, and peer-reviewed scholarly work. This follows a series of authors in using the investigations of national agencies (such as the Federal Bureau of Investigation), IGOs (such as Interpol) and non-profit (such as Freedom House or Quilliam Foundation) entities wherein information is cited

directly in government/IGO reporting as the basis for robust inclusion of incidents in data collection. For scholarly works, source material must be peer reviewed and the scholarly outlet cannot be state-owned or funded. The nature of the collection approach as focused on a range of specific digital techniques itself compensates for bias in reporting, as statements regarding illicit activities without details are discounted as a basis for linking a group to an IT application. Addressing the second challenge is actually something bound up in the data collection approach described above, wherein distinct categories are bounded so as to allow the researcher to more easily group broadly described actions (such as common data theft as distinct from APT espionage or disruption campaigns).

As mentioned above, the data collected are temporally episodic. For each subversive actor identified in the dataset, I code for incidence of each particular type or category of activity for 18-month periods spanning either side of the incidence of digital activism coded in the original GDADS set. The rationale for this is straightforward. First, the point here is to measure contemporaneous activities. Therefore, it makes sense that the data be bounded to capture actions within a short period of time. Moreover, much as occurs with terrorist and insurgent campaigns, subversive groups often either lose ground in their campaign efforts (and revert to actions typical to earlier non-activist phases) or transition to other kinds of organization (including criminal, terrorist or

political party).[144] The case of the Egyptian Muslim Brotherhood, which rose to prominence in the wake of Hosni Mubarak's fall from power and was forced out of the public limelight following the fall of President Morsi, is an excellent example of such a progression of circumstances. Episodic data collection controls for this possibility in that observations are limited to short time periods unless extended by the continued incidence of digital activist efforts. In the dataset, observations are set at a baseline of 18 months and considered still to be one observation if extended due to continued incidence of such activist efforts. If there is a gap between activist efforts such that the baseline time periods do not overlap, they are coded as separate organization observations.

Following recent research into the criminality of cyber conflict actions, I also code each incidence of a technique employed for (1) the prosecutability of the action and (2) target type. Prosecutability of actions is different from legality. In almost no instance was any of the 21 ICT employments described in the circumvention category legal in local jurisdictional context. This is as should be since the design of categories for data collection – as has been noted is common with cyber research – reflects the focus on criminal behavior. Prosecutability measures derived from past work wherein ICT type coding substantially matches that of this study and where a dichotomous prosecutability measure is provided for each (minus administrative blocking of websites and APTs) across more than 120 countries. Target type is coded for the 15 categories of action

[144] This assumption is perhaps most clearly laid out in Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*, Princeton University Press, 2011.

described above that involve intrusion. Target types include seven categories in line with work in the terrorism literature[145] including: business, government, police, military, journalist, private citizen and other.

In full, this produces a dataset of a broad range of digital techniques (21, to be exact,) employed by subversive groups. I then create two dichotomous index variables useful for descriptive and statistical testing – SHADOW, which operationalizes the DV by describing whether or not subversives involved in digital activism also employ the alternative techniques described above, and TARGETTYPE, which dichotomously describes targets as either government or non-government. I also employ a further dependent variable reflecting a different categorization of the techniques described that will be discussed below in the sections describing testing and incorporate a control variable for the target of a tactic as being either government, domestic non-government or foreign actor.

3.4.4. Operationalizing Strategic Perspective and Prospects

Operationalizing strategic goals and perspective is not an easy task. As a large group of political scientists engaged in research on actors from political parties to insurgent organizations have recognized, simply coding for the stated goal of particular subjects of study can provide data both imprecise and diverse to the point where it is

[145] Such as Kilberg, Joshua. "A basic model explaining terrorist group organizational structure." *Studies in Conflict & Terrorism* 35.11, 2012: 810-830; Kilberg, Joshua. *Organizing for destruction: How organizational structure affects terrorist group behaviour*. Diss. Carleton University Ottawa, 2011; Pearson, Frederic S., Isil Akbulut, and Marie Olson Lounsbery. "Group Structure and Intergroup Relations in Global Terror Networks: Further Explorations." *Terrorism and Political Violence*, 2015: 1-23.

inappropriate for use in a simple, robust testing regime. Coding needs to be adapted to fit the circumstances of a particular program of study. Here, that means coding for the most telling features of subversive organizations' strategic behaviors.

In line with past work, which has particularly emerged from studies of terrorist and insurgent transitions towards alternative forms of political participation (both criminal and legitimate), I argue that operationalization of strategic perspective means constructing a typology of strategic inclinations based on common characteristics. Those common characteristics relate to two categories – (1) the nature of a group's strategy as aimed at accomplishing discrete outcomes and (2) the commitment that group exhibits towards that strategy, both in terms of responding to strategic imperatives and in shaping tactics. I focus primarily on the first category in testing in this project.

Type of Agenda. I code in line with the work of Abrahms and others on the nature of a group's portfolio of objectives. Abrahms specifically is well known for work outlining how variation in the nature of this portfolio amongst subversive groups effectively predicts target choices and eventual campaign outcomes. He codes the portfolio of objectives of a given terrorist group as belonging to one of four categories: maximalist, limited, idiosyncratic or ambiguous. Maximalist objectives/policy portfolios cite a broad range of grievances held by a given organization. Following past work, I code a group as having a maximalist portfolio if there are five or more clearly identifiable and distinct (i.e. not incremental elements of a single desired process) goals. Groups that do not fall into this category can then fall into one of three categories.

Limited portfolios have clear goals but very few specific grievances or stated objectives. Groups with ambiguous portfolios state a broad grievance but do not outline clear operational or tactical objectives, while those with idiosyncratic portfolios have a variable range of campaign objectives that are unusually mixed with functions or goals not linked with the main stated objective. In many cases, "idiosyncratic" subversive entities take the form of niche advocacy groups with concentrated local support – and the accompanying need to provide community support services – but national opposition and macro objectives, such as elements of the Batasuna Basque separatist group. For the purposes of regression testing below, I construct these categories as dummy variables, omitting the "ambiguous" category in different models.

The Nature of Grievances. Second, I code for the nature of the grievance held by the subversive group. Here, I follow a well-known schema for differentiating levels of perceived legitimacy of a given sociopolitical regime.[146] I code for objection to prevailing normative conditions on two fronts. First, I consider whether or not the objection of the subversive organization – deemed illegitimate by the status quo – constitutes a policy grievance. Are there *specific* policies enshrined in either law or government practice that form the core of a subversive organizations efforts to achieve change (i.e. not just a general disavowment of current practices)? Are objections codified in the structures of the prevailing order? Second, I consider whether or not the grievance

[146] For a description of such work, see *inter alia* Lemieux, Anthony .F., and Victor Asal. 2010 "Grievance, social dominance orientation, and authoritarianism in the choice and justification of terror versus protest."Dynamics of Asymmetric Conflict 3 (3):194-207.

of the subversive actor is about systemic process, as opposed to a general concern about policy, an entrenched set of elites or prevailing sentiment. Does the subversive organization consider the fundamental construction of the national system to be illegitimate? In constructing my variables in this way, I aim to capture several different possible dynamics of subversive strategic goals. Specifically, variables that describe the nature of organization grievances speak to the desire of a subversive group to modify a policy regime, to modify a fundamental feature of the current order's process and to replace that underlying process. It is important to note here that I do not argue subversive groups are motivated by grievances against *only* policy or *only* process. Indeed, for many countercultural movements, objections to the essential tenets of the prevailing order are echoed in the policy outputs of the system they face. Subversive organizations may object to policies only or may do so in the context of broader objectives to modify or replace. Likewise, subversive organizations may disavow government practices without constructing a specific counter-policy mission.

3.4.5. Operationalizing Structure

In order to operationalize group structure for testing, I follow a range of scholars in the literatures on terrorism and, more broadly, political violence in insurgencies, organized crime and militant activism. In particular, I use the work of Arquilla and Ronfeldt – adapted by a number of others, including Rowlands and Kilberg) – to operationalize structure based on a series of organizational characteristics that are common across group types.

Characteristics of Structure. The first of these characteristics is leadership. To what degree does the existence of a clearly defined leadership structure explain variation in group practices? Leadership can take a number of formats. Non-state organizations, whether terrorist groups, subversive movements or protest formations, can be run by a single person in a discrete position of authority. Likewise, organization leadership can take the form of an oligarchic or plutarchic governing body where key members – often core funders and supporters – deliberate on direction and implement policy. Here, leadership is coded as a simple dichotomous variable (following Arquilla & Ronfeldt 1999; Arquilla & Ronfeldt 2001; and Kilberg 2011) on whether or not there is a clear leader or leadership structure in place for the organization in question.

The second characteristic is that of command and control. Coding for leadership is not the same as coding for centralized authority or the ability for a particular leader to effectively direct his organization. Many terrorist and subversive groups maintain figureheads that are more or less in control of the functional direction and activities of their organization. Whereas Osama Bin Laden was a relatively effective leader for al Qaeda and was involved in global operations of various arms of his organizations, groups like Shining Path have historically presented more of what might be called symbolic leadership institutions where a figurehead delegates functional operation of the organization to subordinates. To code command and control, evidence is required that demonstrates the involvement and direction of a central executive authority in the

actions of the group. I code dichotomously for such evidence (either command and control is evident, or it is not) and code an additional control variable for whether or not there is evidence of such direction for only digital activist activities (or for both activist and 'shady' activities).

The final characteristic is that of functional differentiation (or specialization). This characteristic describes the political and/or logistical specialization of distinct sub-organizations within an organization. Compartmentalization of functions within a group indicates several things about the ability of a group to both efficiently pursue objectives and effectively direct commands from an executive center. To code this effectively, evidence is required indicating the existence of specific arms of a group tasked with specialized functions. I code dichotomously for evidence of functional differentiation (whether it is apparent or not).

For each of these variables, I control for the reality that group information is often sparse or difficult to obtain with any measure of clarity in two ways. First, I limit data collection – as I do for the dependent variable – to the 36-month period surrounding the incident of digital activism recorded in the GDADS and on which the dataset selects. This helps control for structural changes that occur within an organization over time. Second, I record variables based on an ability to corroborate information about the group in question in one of two ways. First, I record information on leadership, functional differentiation and command and control when described in the reporting of government and intergovernmental organizations, as well as by available

public-facing scholarly databases. The Terrorism Organization Profile dataset based out of the University of Maryland and Jane's World Insurgency and Terrorism database were the primary sources used for corroboration purposes in the latter instance. Secondly, I record information for the above structural variables when reported consistently in a large volume of media reporting on the activities of the subversive group in question (20+ stories that corroborate the detail was the standard used) and corroborate wherever possible. Insufficient evidence was in all cases coded as inconclusive.

Variation on the three variables outlined above describe – depending on the combination of values involved – a set of four organization structures with unique patterns of authority and command over group functions. A range of scholarly works in the literature on terrorism and political violence describe these alternative structures in detail,[147] but I will briefly summarize them here.

[147] See, among others, Kilberg, Joshua. *Organizing for destruction: How organizational structure affects terrorist group behaviour*. Diss. Carleton University Ottawa, 2011; and Pearson, Frederic S., Isil Akbulut, and Marie Olson Lounsbery. "Group Structure and Intergroup Relations in Global Terror Networks: Further Explorations." *Terrorism and Political Violence*, 2015: 1-23; Kiruthiga, A., S. Bose, and N. Buvaneswari. "An experimental simulation of hub-spoke terrorist organizational structure." *Advances in Natural and Applied Sciences* 9.9 SE, 2015: 41-45

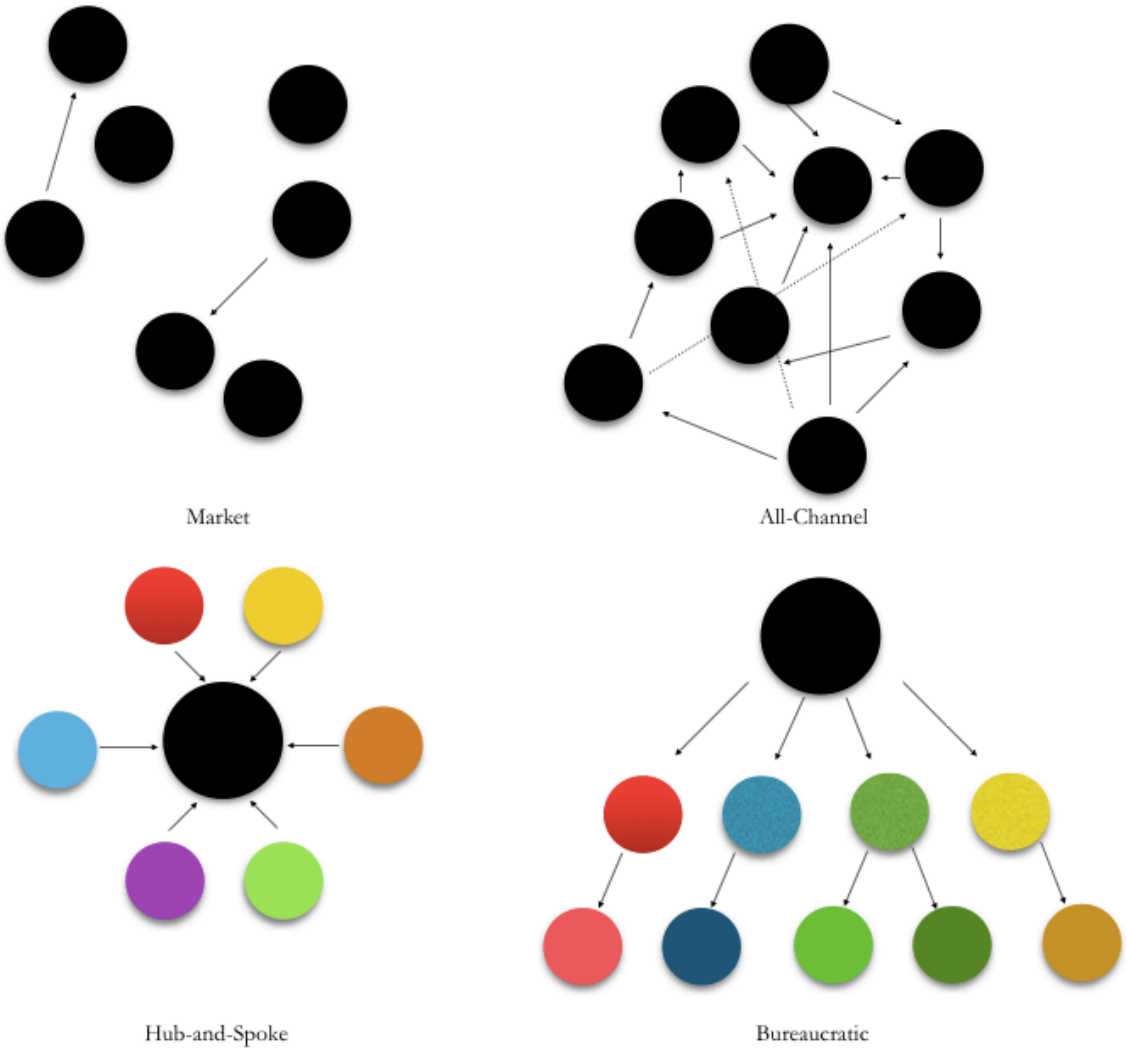

Figure 3.5. Structural patterns for organizational format.

Negative values on all three variables described above indicate the existence of an organizational structure known as a *market structure*. As described in Figure 3.5, market structured organizations lack a central executive to direct a group, determine strategy and implement policy. Naturally, with no executive, there is additionally no element of direction emanating from on specific section of an organization. Moreover, there is little in the way of functional differentiation. Members of an organization may have particular

skills and can tend towards specific types of tasks as the norm of their involvement in a group's mission, but there is no formal specialization. Much as governments have departments dedicated to specific functions, politically extreme groups often have elements dedicated to the procurement of materiel, accounting or strategic development. Subversive organizations might have sub-units dedicated to the function of front groups, the mitigation or political opponents or the crafting of political messages. Organizations with market structures have none of this.

Not significantly different from market-structured organizations, *all-channel* organizations are network entities with central leadership. Despite clear leadership, however, all-channel organizations lack directionality of direction and functional differentiation. There is no clear hierarchy of command and control. Likewise, there is no real degree of specialization between different elements of the group. A good example of this type of organization would be the Anonymous hactivist collective. Though there have at various points been clear leaders amongst the hackers of that organization, there is remarkably little power of authority that such a label – the leadership of Anonymous – holds. Likewise, operations are actually quite often not organized or planned in any centralized way, but rather a crowd-sourced set of actions improvised by those who are available and interested. In many ways, Anonymous – and all-channel organizations in general – are the archetypical form of political activist groups in the digital age, where (as Rid suggests) information technologies simultaneously enable individual members to

undertake diverse tasks, encourage high levels of membership mobility and discourage symbolic leaders from attempting to direct the efforts of the organization.

Hub-and-spoke organizations are structured such that leaders functionally, but not authoritatively, sit at the center of a web of competing specialized group elements. In essence, leaders – or a leadership association of some kind – are critical to the internal communication and coordination efforts of the group involved. In order to coordinate operations and clarify the role of different organizational elements in the context of overall strategy, it is necessary to go through the "office" of the central executive. However, the format of the organization is not hierarchical insofar as the role of the executive at the center of the setup ends with communication. There is little or nothing in the way of command and control. High levels of functional differentiation and limited authority on the part of leadership ensures that directionality of policy development and implementation remains with an organization's sub-units. This style of organization is common amongst transnational terrorist or activist entities where there is an increased need for leadership that can ameliorate the costs or tensions involved in broad-scoped communications challenges, but no need for improved authoritative coordination at the level of local operations. As Kilberg points out, al Qaeda prior to the events of September 11th fits the description of a hub-and-spoke entity remarkably well.

Finally, organizations can possess a *bureaucratic* structure, where there are positive values on all three structural variables described above. Bureaucratic organizations are highly hierarchical. Leaders or leadership bodies not only coordinate

the function of specialized sub-units; they also dictate strategy and policy, and give directions as to the implementation thereof. By contrast with al Qaeda, Islamic State – both within the territorial boundaries of the proto-state and in the context of links to Libyan and some other affiliates – appears to be highly hierarchical, with a clearly-defined set of leadership structures directing the operations of the organization across terrorist operations in Europe, black market trading and traditional battlefield functions.

Other Structural Descriptors. I also introduce dummy control variables for prior criminal activity of a group using the same selection criteria as was introduced for ICT employments in data collection (i.e. referenced in government, IGO, cited NGO reporting or peer-reviewed scholarship). I do this because criminal enterprise can determine the value of different elements of an organization beyond what hierarchy (or lack thereof) might tell us. In other words, criminality can indicate that a group won't fit our expectations regarding organization structure. Groups engaged in the narcotics trade, for instance, might organically adopt an oligarchic form of bureaucracy so as to better control a distributed supply chain and minimize risk of interdiction. Knowing whether or not criminality plays into the subversive enterprise will be critical for the effort to understand the experience of individual groups from Chapter 5 onwards. I code for prior criminal activity in three ways. First, I introduced a dichotomous dummy for involvement in economic crime prior to the episode observed in data collection on ICT employments. I then do the same for violent crime. Finally, to control for group longevity and format over many years, I introduce a dichotomous dummy for any prior

involvement in criminal activities that has taken place within three years prior to the observed episode.

3.4.6. Operationalizing Environmental Pressures

Subversive group operation, much as might be the case for terrorist organizations, insurgent movements and activist formations, have variously been shown to be sensitive to a range of environmental pressures. We might split such environmental pressures into two categories – (1) the degree to which there exists direct government or popular opposition to a group's operation and (2) the degree to which there exist either prohibitive or enabling operational conditions that affect an organization's tactical function. For the latter categories, the degree to which new operational possibilities (i.e. new digital abilities) are matched by government capacity to mitigate the effects of such activities is of particular interest. I discuss operationalization of these factors in this section in turn.

Official Opposition to Subversion. To operationalize opposition to a subversive campaign, I rely on three variables that describe both the potential for meaningful opposition and actual incidence of repression or opposition. First, I include a basic measure of GDP drawn from the most recent Polity IV dataset. Studies of terrorism, militant activism and insurgency almost universally hold that states with higher GDP are better able to devote resources to either oppressive or security activities. For terrorist groups, of course, this means better funding for counter-terrorism forces and more support for efforts to mitigate the underlying causes of terrorist success,

including poverty and border security. For subversive groups, though the emphasis is not on political violence and subversion can occur without the violation of state laws, the logic holds insofar as states with higher levels of economic growth and productivity have more resources to contribute to judicial and legal investigations of rule of law violations. Such states are better able to adjudicate on issues where the question is on a group's role as protected voice or seditious entity. Likewise, there is greater opportunity for broad-scoped funding of security and surveillance efforts aimed at not only core violent threats to state integrity, but also at dissidents across the spectrum of threat. Second, for each instance, I draw the most recent government approval rating and normalize to a 100-point scale (adaptation only required in one case) for each case. These are provided by Gallup over time and across all countries. Finally, I code dichotomously for specific evidence of government investigation, legal action, law enforcement employment or military action taken against the subversive group in question. Evidence is drawn in line with coding for activities used to operationalize the dependent variable in the section above. For inclusion, evidence has to present as more than simple reporting of an activity, though that action can qualify a group's case if the observation is made explicitly as the result of state investigation. In many cases, measurement of government opposition specifically pertains to the group, individuals linked to the organization or affiliated organizations being placed on blacklists.

Permissiveness of the Environment. I code for the permissiveness of national environments as more or less amenable to the types of activities subversive

groups undertake to affect normative transformation. Following a range of scholars working on democratization and dissent politics issues, I assume that more liberal national regimes will incentivize subversive groups away from risky tactics because of greater expectation of viable tactical options related to non-violent political advocacy. Thus, I include variables for regime type (in the form of the ordinal Polity score provided by the Polity IV dataset that describes a spectrum from full autocracy to full democracy), regime durability (drawn from Polity IV as the number of years since a political transition) and contestation (drawn from Polity IV as an ordinal score of competitiveness of political participation in a given country). Collectively, these provide controls for the degree to which protest and persuasion are *ceteris paribas* viable options for affecting transformation, for the degree to which a group may discount openness as being temporary, and for the nature of a group's national audience as monolithic and more or less susceptible to opposition perspectives.

Popular Opposition to Subversion. There is a degree to which the competitiveness of participation variable described above and drawn from the Polity IV dataset is also useful in measuring popular opposition to a given countercultural movement or organization. Measuring contestation, according to some scholars, indicates the degree to which groups considered to be countercultural and opposed to the prevailing normative status quo are opposed on grounds of contested legitimacy. Reasonably high contestation, in other words, dictates strong opposition to any group that opposes prevailing tolerant conditions, even if only on single issues. Thus, the

PARCOMP variable is relevant as a control for popular opposition as well as for structural constraints and pressures.

Constructing variables for the degree to which there exists prohibitive or enabling environmental conditions that affect group operation beyond specific opposition or support demands thinking about the environment in two distinct ways – (1) as including actors able to enhance an organization's capabilities and (2) more broadly permissive in terms of group access to relevant capabilities. Thus, I employ two sets of indicator variables. The first is a set of three dummy variables coded to reflect either financial or capabilities sponsorship of a group (attribution of the relationship assessed in the same manner described above for data collection on ICT employment). One variable assesses sponsorship from any domestic source, while the second assesses the same from a foreign source. The final variable assesses sponsorship directly from a foreign government or military, or not.

Access to Capabilities. The second set of variables are drawn from the World Bank's Digital Dividends project and database (the Digital Adoption Index), and include indicators describing degree of media freedoms in a country, extent to which the Internet is regulated and/or censored, national protection of civil liberties, Internet access statistics and more. Specifically, the Digital Dividends project constructs three indicator variables for the degree to which a given country has access to digital technologies (drawing on data regarding Broadband internet usage, mobile-cellular access, etc.), the degree to which a national population is able to use digital technologies

(drawn from data regarding national literacy and education) and the degree to which a national population is ready to adopt new technologies (drawn from data regarding use of e-governance services). These indicators are constructed of sixteen macro indicators and proxy for the degree to which a country is online and to which a non-state organization (1) is likely to have easy access to digital opportunities and (2) is able to affect desirable campaign outcomes through digital means.

Complex Opposition. Finally, in order to capture the degree to which an organization is affected by a permissive environment in the context of opposition, I introduce a dichotomous control variable drawn from data on adoption of digital technologies across society, business and government in the Digital Adoption Index. For society, adoption is measured as an index variable in reference to the purchase of computers, mobile-cellular devices, subscriptions to broadband or above Internet and more. For government, adoption is measured as an index variable in reference to spending on cybersecurity initiatives, e-government program usage and more. In line with work that suggests radical non-state actors are sensitive to government abilities to investigate and interdict their operations, I am most interested in operationalizing a mismatch in digital adoption in the national environment. Therefore, the introduced control variable holds that adoption trends are mismatched when the ratio of state to government adoption is greater than 2 (i.e. $\frac{societal\ adoption}{government\ adoption} > 2$, wherein original adoption index values are on a scale from 0-1).

3.4.7. Operationalizing Anonymous Involvement

Finally, I consider and operationalize the actions of the Anonymous hactivist collective in either direct or indirect support of a subversive group. The intercession of Anonymous agents has been a notable feature of the experience of several subversive groups. Again, the assumption here is that the inclusion of a control variable for either evidence of direct sponsorship of or assistance by Anonymous agents will proxy for the significance of developing transnational *ICT-capable* support networks for dissentious non-state actors attempting to enhance their operations via the use of ICT. I argue that this differs somewhat from controlling for foreign sponsorship writ large above in that the intervening significance of Anonymous connections would indicate a more nuanced link between global access to useful ICT platforms and knowledge – essentially, access to cyber arms – than is implied in simply accounting for the specific sponsorship of a foreign actor. Thus, I introduce a dichotomous control variable for evidence of Anonymous support, either direct or as an unsolicited aid to a particular subversive organization's cause.

3.5. Next Steps

Chapter 2 and Chapter 3 have presented theoretical foundations for the dissertation and showed that there exists compelling a puzzle in the behavior of a minority of groups that move into the public limelight but retain focus on clandestine, often illicit, operations. This chapter has also outlined different categories of possible explanation for the behavior of subversive activists that choose to employ ICT

antagonistically and described data collection amenable to broad-scoped quantitative analysis of the puzzle. Next, in Chapter 4, this dissertation examines the problematic in detail through a large-N analysis, before moving to assess different case experiences of subversive activist entities in Germany and China.

Chapter 4
Keeping One Foot in the Shadows:
A Quantitative Analysis

Christopher E. Whyte

In this chapter, I present a theory of subversion in the digital age that explains how subversive organizations utilize ICT and tend towards antagonism at different times. Then, I present the results of quantitative testing, the design of which was described in detail in Chapter 3. These results provide the high level basis for the theory presented in the next section and set the stage for case study analyses that add nuance on the actual mechanisms of antagonistic behavior among subversive digital activists. Analysis of quantitative findings also adds depth and context to the study in that results appear to secondarily tie incidence of digital antagonism to a set of permissive national conditions. The implication is that results in this chapter tell two stories – one about the specific shape of subversive group behavior and the employment of ICT, and another more broadly applicable to contentious non-state actors in their use of cyber tools.

4.1. A Theory of Subversive Digital Antagonism

My investigation of the practices of subversive activists in employing ICT around the world suggests that such groups' use of information technologies for antagonistic purposes is conditioned by group objectives in two distinct ways. First, adoption of ICT

for shady, circumventive and criminal purposes reflects subversive actor objectives insofar as cyber tools are seen to be useful for (1) favorably manipulating the information environment in which subversion occurs and (2) disrupting the activities of societal opponents. The particular repertoire of contention held by subversive groups dictates how they cultivate and support cyber conflict capabilities. They do so in indirect ways, favoring the development of abilities among peripheral members, affiliates and proxies over centralized units capable of prosecuting antagonism.

Incidence of digital antagonism is thereafter closely tied to how objectives are *expressed* by group leaders or governing units. Given such a decentralized common organizational dynamic among subversive actors that possess the potential for digital antagonism, failure or unwillingness to incorporate direct methods for coordinating cyber actions is normal. Therefore, proxies, derivative group members and organization sub-units not directly commanded by a superior primarily decide whether or not to antagonize based on their read of prevailing group objectives and chosen tactics. As the following analysis shows, where subversives favor structural revisionism (i.e. the replacement of current political systems) and where methods are non-participatory, leaders demonstrably act to incentivize civil disobedience and condone greater antagonism by members. Where grievances are either non-revisionist or where emphasis is placed on structural change through participatory methods, incentives for antagonism are muted and, often, actively restrained by executive efforts. Thus, it follows that the

use of ICT for circumvention and criminal action closely ebbs and emerges in response to the expression of subversive group objectives.

The next three sections focus on the ways in which subversive objectives manifest to shape the cultivation of antagonistic ICT abilities and drive the use of cyber tools for shady purposes. First, I describe in greater detail the logic of how the subversive enterprise dictates the development of one particular logistical format of cyber capabilities. Then, I discuss how revisionist intent and action functions as a signaling mechanism for peripheral and affiliated elements of a subversive movement. More than any other explanatory factor investigated in this study, expressions of group aims and methods for achieving sociopolitical change drive incidence of antagonism. Finally, I discuss the limits of understanding digital antagonism among subversive organizations. Naturally, this model of understanding subversive group operations is not applicable to efforts to understand other types of non-state actors without modification. Moreover, this study does not answer the question of what makes the development of antagonistic capabilities more or less likely. Data presented later in this chapter does, however, suggest what the scope of such an answer might be. Discussion of this is significant as it pertains to my effort herein to understand subversive cyber actors as unique among a broader global ecosystem of non-state actors engaged in cyber conflict.

4.1.1. Subversion and the Nature of Digital Antagonism

How might a terrorist group or an insurgent organization choose to cultivate the development of cyber warfare capabilities? What determines whether or not a non-state

actor funds the development of a hacking unit akin to those employed by countries versus relying on the abilities of amateur hackers? Past chapters have outlined the various uses non-state actors have founds for new information technologies. ICT allow terrorists to hide funding transactions from government eyes and to engage in specialized recruitment without geographic constraint. Cyber tools allow social activists new ways to shed light on injustice or to engage in protest via virtual sit-ins, website vandalism and more. In truth, however, answering the above questions does not require knowing about different kinds of ICT techniques so much as it does understanding the nature of different types of non-state actors and how actor objectives dictate adoption of technology for the purpose of conflict and contention.

As ICT usage reflects actor objectives and operating imperatives, subversive group adoption of ICT for antagonistic purposes has broadly reflected the intrinsic desire to minimize legal and normative risks while still taking advantage of new abilities to organize, mobilize and, where needed, remove obstacles. Importantly, for subversive groups new opportunities don't typically emerge from particularly sophisticated uses of ICT. As outlined in Chapter 3, data collected for this project shows us that subversive organizations almost never engage in sophisticated cyber attacks. This is discussed in the quantitative analysis section below, but it is generally the case that ICT antagonism among subversives constituted low-intensity efforts to disrupt and obfuscate. This makes significant sense, as such ICT employments are both intrinsically low risk and yet workable for those tasks that most interest subversives – targeted recruitment,

disruption of non-governmental opposition, hiding financing connections, email spamming, stealing data to be used to optimize messaging campaigns, etc. Below, I use the term *information enrichment operations* to label this toolkit of subversive antagonism online in recognition of the fact that it is clearly aimed at aiding the normative efforts of counterculture groups in a manner that is cohesively different that of other non-state actors.

That the natural repertoire of digital antagonism for subversives means low-intensity techniques and efforts has implications for how subversive groups logistically cultivate the development of such abilities. First and foremost, subversive organizations have few incentives to devote significant resources to the development of elaborate cyber warfare teams. By and large, such resources would be wasted, as sophisticated hacking is not needed for the vast majority of antagonistic operations undertaken by such groups. Instead, subversive groups are variously incentivized to encourage the development of such abilities in the periphery – i.e. among members not linked with group leadership, within extended elements of a group's popular support base or under the purview of affiliated organizations.

Beyond simply being a logical alternative to pouring resources into a cyber antagonism unit controlled directly by group leaders, encouraging the development of such abilities in areas one step detached from core organizational functions is naturally attractive to subversives for financial and operational reasons. Much as is the logic of state use of mercenaries and patriotic hackers as proxy agents, subversive encouragement

of fringe elements' development and use of cyber capabilities involves only minimal costs. Even in rare situations where group leaders decide to employ ICT for criminal purposes directly, organizations pay little to nothing for the hardware, training or upkeep of extended elements of a movement. More importantly – perhaps most importantly – is the fact that such a dynamic helps subversives maintain plausible deniability. This deniability manifests at several levels. Most notably, the use of peripheral members or affiliates as proxies (1) extends attribution challenges for countersubversive investigators and (2) ideally helps groups maintain reasonable distance from illicit activities in the eyes of their target audience. Further, depending on extended elements of a movement actually often ensures greater effectiveness in antagonistic operations online. After all, a constellation of enthusiastic hackers with diverse expertise is generally more likely to be up-to-speed on techniques and practices than is a small in-house unit tasked with a myriad of potential efforts by a subversive organization. And the existence of civil disobedience emerge from a fringe movement centered on an organizations' cause is further attractive to the standard countercultural group in that popular action in tandem with and organically extending from group efforts tends to be seen as part-and-parcel of success in the subversive enterprise.

The natural potential of ICT for a range of mobilization, coordination, mitigation and persuasion activities means that members of subversive movements have strong incentives to investigate and cultivate toolkits of both digital activism and antagonism. This simple notion is the core element of the premise outlined in Chapter 2 regarding the

subversive enterprise in the 21st century. Beyond adoption of ICT as instruments of subversion being common among countercultural groups in world affairs, however, the concentration of cyber capabilities in peripheral elements of a movement – i.e. those elements, like affiliate groups or membership cells, detached from the operational center of a subversive organization – emerges as a natural outcome of experiences that prompt in general the development of disobedience toolkits. To be clear, this dissertation does not attempt to describe what specifically prompts a subversive group towards the development of such toolkits. But among those that do, the natural tendency is to cultivate such abilities in satellite actors; rarely ever, as evidence described in the sections and chapters that follow suggests, are cyber warfare internalized and centralized.

4.1.2. Revisionism as a Signaling Mechanism

In the analysis that follows, I present strong evidence that incidence of digital antagonism is tied to the nature and expression of an organization's grievances. In the quantitative analysis specifically, structural grievances – i.e. explicitly focused on affecting structural revision (not simply policy modification) alongside ideational transformation as opposed to just focus on prevailing sentiment or opinion – make groups much more likely to employ ICT for antagonistic, disruptive purposes whilst also trying to digital engage the public. Indeed, when specific forms of ICT usage are viewed through this lens of "buy-in" or type of grievance, it strongly appears that structural revisionists are far less sensitive to the costs and risks of shady and criminal ICT usage

than are their counterparts. Moreover, structural revisionists – particularly those with maximalist agendas – appear clearly more likely to escalate their use of cyberspace to more disruptive formats of interaction, including malware employments, tailored distributed denial of services (DDoS) attacks and direct, unauthorized tampering with hardware. And such groups are more likely to target government or military assets directly and to employ ICT disruptively even where there is a clear precedent of prosecution of such actions. Finally, though no groups studied in the large-N analysis directly sponsor criminally violent acts, structural revisionists *are* also more likely to be linked to political violence in the form of sponsorship of/collaboration with more explicitly violent organizations, unsanctioned violent activity by members and links to past incidents of criminal violence.

What is happening with these groups? In studying the results of this project's large-N assessment below, one might be forgiven for assuming that the leaders of revisionist organizations simply care less about the consequences of their group's actions than do those not interested in structural reformation. Further, this dynamic seems to get stronger given a maximalist set of group objectives – i.e. given an agenda that seems less pursuable through narrow, participatory actions than might one with few policy aims. And yet, case study analysis of different subversive groups suggests that executive-level direction is rarely linked to specific incidents of digital antagonism. Rather, close inspection of various organizations suggests the dynamic described above – that of

capabilities and agency for digital antagonism concentrated in peripheral group elements – is the norm amongst subversives.

What subsequent chapters demonstrate is that and suggests that what structural grievances are closely tied to a willingness to condone criminality. In this way, revisionism *indirectly* produces antagonism. Far from seeing evidence of explicit executive-level direction of hacking or circumventive efforts, Chapters 6 through 10 suggest that there is a strong relationship between revisionism and the way in which groups interact with peripheral elements of their movement that employ ICT antagonistically. Across cases, the sources of web tools and the initiative to disrupt regularly stems from extended elements of subversive organizations. With Falun Gong in China, for instance, group circumventive capabilities stem specifically from the tight-knit and more highly revisionist exile community of members living abroad that act as path-breakers and doctrine-setters in the absence of willingness to act among domestic members. With Civic Passion, the group's limited use of ICT antagonistically falls clearly within a period of time where group leadership was in disarray amidst apparently failed efforts to achieve transformation in a legitimate, participationist manner. And in Germany, the National Democratic Party of Germany, though mostly guilty of condoning the antagonism of others, has nevertheless actively supported an unstructured fringe element beyond traditional party sub-units – intended to act as a "people's front" – that has been responsible for a range of disruptive digital acts.

Moreover, patterns of digital antagonism – of members and proxies using ICT to disrupt government services, vandalize websites, advocate illegal positions online, etc. – change directly in line with significant shifts in subversive groups' stated approach to transformation. Participatory rhetoric and emphasis on methods of achieving change that involve participation in extant political processes mute incentives for peripheral subversive elements to undertake acts of civil disobedience online. Specifically, in attempting to enhance the perception and prospects of a subversive cause through participationism, leaders are incentivized to explicitly denounce such acts and to veto, where possible, any antagonistic operation that does not meet strict threshold criteria for deniability (such as low-level encryption to hid intra-organization communication or actions taken against unpopular societal opponents, such as occasionally occurs in relations between Germany's far right and far left parties). Where a group turns from participatory approaches, however, both group leaders and peripheral elements are incentivized to antagonize. For leaders, fringe operations remain largely deniable, present as a unique set of options for mitigating the gains of sociopolitical opponents and offer opportunities for growth beyond those that accompany legitimate political participation. For peripheral elements in such a situation, digital antagonism is a cheap and arguably effective way for advancing a cause without (1) running the risk of harming efforts to garner broad public support or (2) running into the kind of significant law enforcement opposition to civil disobedience that often, offline, leads to arrests and negative publicity.

4.1.3. The Limits of an Objectives-Based Understanding of Digital Antagonism

This theory has significant implications for scholars and practitioners interested in cyber conflict, the use of ICT by contentious non-state actors and subversion. These are addressed in full in Chapter 12. However, it is worthwhile noting up front that there are limitations of this objectives-based understanding of how subversive groups utilize ICT. First and foremost, I do not claim that this theory is generalizable to non-state actors employing ICT antagonistically beyond subversive groups. Indeed, the logical basis of the theory and arguments made here – backed up in evidence presented through Chapter 10 – is that understanding ICT adoption and incidence of digital antagonism emerges from specific knowledge of the subversive enterprise and the way in which subversives methodologically approach it. This, however, is a valuable takeaway for future studies of cyber conflict processes and non-state actor behavior. In short, repertoires of antagonism form in line with group imperatives and objectives. This fundamental point is critical if effective risk assessment and analysis of other types of non-state actors is to be undertaken by scholars and policy researchers.

This theory also has limitations in what it can explain. Specifically, this theory explains when and why subversive organizations use ICT antagonistically when they are also undertaking efforts to engage the public online. As such behavior forms the premise and the puzzle this dissertation is concerned with, this is as it should be. However, this project does not make a conscious effort to answer the question of what makes development of antagonistic abilities particularly likely for a given subversive group – or,

for that matter, for any non-state actor. As Chapter 12 discusses, the results of this chapter's quantitative analysis *do* actually speak to this question in a limited fashion. Quite apart from the unique mechanics of subversive group operation as it pertains to digital antagonism, analysis of the large set below suggests that contentious subversive actors are reasonably risk sensitive to national-level dynamics. Specifically, criminal and circumventive ICT employments appear to be more likely when there is a mismatch between the availability of information technology nationally and government efforts to regulate the digital domain. Again, I discuss this further in Chapter 12. But the point is that the theory and evidence presented herein are valuable because they demonstrate the need for distinct investigations of both macro cyber conflict dynamics involving non-state actors and other specific types of non-state actors.

4.2. Quantitative Evidence

The testing in this chapter is geared towards empirically investigating the use of information technologies by subversive groups. The puzzle outlined in Chapter 3 describes a dynamic in which some subversive organizations shirk expectations regarding abandonment of certain techniques during the public-facing phase of their campaign to affect normative transformation of the status quo. Alongside activist efforts, some entities are guilty of what might be labeled *digital antagonism*. In short, they act non-strategically.

Naturally, this problematic contains vagaries on several fronts. Not all techniques are solely employable for illicit purposes and the national context matters a great deal.

And laws and norms regarding political group association with different societal elements vary widely by culture and under different types of governments. Nevertheless, by carefully identifying the specific actions undertaken by subversive groups during the phase of their campaign in which digital activism is also emphasized, it is possible to draw a nuanced picture of such episodes and develop theory as to what factors most impact choices groups make. Indeed, research operation under these conditions is increasingly the norm when it comes to cyber topics. The definitional issue – where use of some techniques can be illegal under certain circumstances and not others, or might be used for an incredibly broad variety of tasks – is both common and surmountable through in-context coding of actor activities.

Just as there is a challenge in controlling for both the subjectivity of and difficulties inherent in observing different subversive tactical behaviors, so too is there naturally a challenge in saying something of substance about the root causes of decision-making across such a diverse universe of cases. As the results below show, a range of factors seems to explain variation on the dependent variable. However, unique patterns emerge from the data that suggest that tactical choices that run counter to conventional wisdom are, from the outset, actually choices linked to a particular set of activities – those linked to data collection and analysis (and, secondarily, to disrupting the information operations of non-state opponents). In other words, most deviation from the expectations of past theories are acutely linked to one type of behavior – which I label *information enrichment* techniques or operations (IEOs) – with further use of

information technologies for criminal enterprise being limited to a relatively small number of actors. In those cases *and* more generally, the severity of deviation from expectations in the form of ICT usage for illicit and circumventive purposes seems to be predicted by one primary set of factors. These are explored in detail and discussed in the sections below.

This chapter seeks to employ testing in an effort to better understand what conditions prompt deviation from expectations. As will be made clear in the sections below, such testing is critically about scale and severity. The results presented in the descriptive testing sections below provide evidence that some types of ICT-related activities – not traditionally considered for inclusion under any categorization or conceptualization of digital activist efforts – are more common than others. In some cases, however, subversive organizations yet undertake a broad range of illicit activities whilst maintaining a robust activist presence. The question, beyond simply what explains variation in broad terms, thus becomes one of what prompts a commitment to more sever violations of our theoretical expectations? If, as will be argued below, certain information exfiltration and dissemination activities are common beyond the scope of activist efforts, what explains the propensity of a group to go further still and employ malware, solicit aid online from blacklisted entities or install illegal hardware? Testing on this front considers a range of possible explanations across several traditional categories drawn from past scholarly work on terrorism and activism. These are described previously in Chapter 3.

4.3. The Determinants of Subversive Group Decision-Making

In this section, initial testing for purposes of shedding light on the puzzle of subversive activist retention of emphasis on strategies of digital antagonism takes the form of regression analysis. Results are then explored in greater depth via descriptive breakdowns of the data and further statistical testing in the section below. Specifically, this section presents several binomial logistic regression models and an Ordinary Least Squares model that consider the various factors and explanations outlined in section 4.2 above.

Table 4.1 below presents the results of three logit models. Variation across the models comes in the form of alternative omission and inclusion of different theoretical and technical control variables. These are described below and the results are robust across modeling choices, principally the use of OLS regression to consider factors that can predict frequency of deviant ICT usage across cases (discussed at the end of this section). Again, the time frame for this study is 33 years from 1983 to 2016. For the models in Table 1, the break point of positive and negative impact on the appropriate dependent variable is 1.0, reported in the form of odds ratios.

Table 4.1. Binomial logit model results predicting deviant ICT Employment.

	Models		
	(1)	(2)	(3)
MAXIMALIST	1.535*	1.488*	1.512*
	(0.098)	(0.100)	(0.102)
LIMITED	0.843	0.794	0.821
	(0.031)	(0.028)	(0.030)
IDIOSYNCRATIC	1.020	1.009	1.018
	(0.443)	(0.429)	(0.442)
POLICY	0.649	0.701	0.653
	(0.360)	(0.371)	(0.362)
STRUCTURAL	2.013***	2.244***	2.261***
	(0.155)	(0.153)	(0.157)
POLITY	--	1.201	1.209
	--	(0.073)	(0.069)
DURABILITY	--	1.483	1.426
	--	(0.131)	(0.124)
PARCOMP	--	1.324**	1.342**
	--	(0.269)	(0.271)
ECONCRIM	0.720	0.759	0.801
	(0.494)	(0.483)	(0.405)
VIOLCRIM	1.132*	1.147*	1.139*
	(0.498)	(0.487)	(0.491)
CRIMPRIOR	0.944	0.957	0.883
	(0.823)	(0.817)	(0.824)
BUREACRATIC	1.249*	1.442***	1.459***
	(0.060)	(0.063)	(0.061)
MARKET	1.434**	1.479***	1.427***
	(0.080)	(0.084)	(0.083)
ALLCHANNEL	0.927	0.920	0.934
	(0.156)	(0.158)	(0.148)
GDP	--	0.847	0.869
	--	(0.151)	(0.147)
GOVPOP	--	0.908	0.923
	--	(1.289)	(1.292)
GOVINVEST	--	2.432*	2.516*
	--	(0.230)	(0.241)
SPONSDOM	0.986	0.942	0.973
	(2.130)	(2.228)	(2.208)
SPONSFOR	1.752**	1.723**	1.701**
	(0.146)	(0.142)	(0.138)
SPONSSTATE	1.110*	1.109*	1.111*
	(0.036)	(0.037)	(0.403)
GOVTSOCDIVIDE	--	--	3.141***
	--	--	(0.187)
ANONYMOUS	--	1.211	1.215
	--	(0.106)	(0.112)
PROSECUTE	0.890*	0.783*	0.769*
	(0.201)	(0.203)	(0.199)
TARGETTYPE	1.341*	1.209**	1.339**

	(0.336)	(0.217)	(0.329)
ACCESS	--	1.872***	--
	--	(0.624)	--
USE	--	2.421***	--
	--	(0.651)	--
READINESS	--	0.677*	--
	--	(0.082)	--
Observations	279	279	279
Ll	2834.122	2749.431	2543.493
Psuedo R^2	0.052	0.071	0.077

Robust standard errors in parentheses, ***p<0.01, **p<0.05, *p<0.1

The results show positive and significant values for a number of explanatory variables. The three models presented in Table 4.1 are constructed so as to test the different intervening effects of group-specific and environmental variables. Specifically, Model 1 contains all actor-specific variables, including those that control for group perspective, structure and sponsorship linkages. Model 2 then introduces relevant environmental controls. Model 3 will be discussed below.

With regards to the strategic perspective of subversive organizations, the most prominent result has to do with the nature of group grievances as being either structural or not. For that category, groups with a structural grievance are more than twice as likely to employ ICT for antagonistic purposes at the same time they attempt to digitally engage the public as are groups whose grievance relates to prevailing sentiment or specific practices/policies. Specifically, groups with what we might call modification grievances – i.e. resolution of the grievance need not manifest as a structural reformation of extant political systems – presents as negative, but not significant. By contrast, the structural grievance result is significant at 99% confidence. This result shows the clear

explanatory value of group grievance and specifically the explanatory value of system "buy in" (versus not) as a means for understanding how groups approach decision-making related to the tactical employment of ICT.

In line with the grievance result, results for the nature of group objectives reinforce the expectations outlined in Chapter 3 in that the only significant positive result (though, admittedly only at 90% confidence) predicting variation on the dependent variable is the measurement of maximalist group objectives. Here, groups where the portfolio of grievances is both numerous and diverse are more likely to employ ICT for shady and antagonistic purposes whilst at the same time attempting to digitally engage the public. However, the result is minimally significant and, as Model 2 demonstrates, not affected by the inclusion of additional controls. This implies that among those groups with maximalist objectives portfolios, the articulation of a revisionist agenda is of particular importance in predicting variation on the DV.

Finally, testing on those variables that describe the systemic prospects of subversive groups present significant values on one front. While there appears to be no meaningful relationship between the durability of a given political system or regime type and variation on the DV (positive but not significant), there is a significant and slightly positive relationship between the competitiveness of political systems and the likelihood of a group will deviate from expectations. Specifically, the more competitive a political system, the less likely a group will be to employ ICT for shady purposes whilst trying to digitally engage the public (significant at 95%). As will be discussed below, these results

lend some credence to the notion that uncompetitive political systems, regardless of type as nominally defined to be more or less autocratic, predict the willingness of a group to employ shady ICT for shady purposes.

Turning to structural explanations of variation on the DV, it appears that both highly centralized and decentralized groups are more likely (at different confidence levels) to employ ICT for antagonistic purposes than are other types of organization. This result is somewhat perplexing on the surface in that past theory suggests a clear link between the spectrum of group centralization and the ability of a group to centrally drive policy on tactics and prevent free agent issues (i.e. issues of loose cannon deviation from group doctrine by individual members). This link appears to exist, but so too does it appear to be the case that highly centralized groups are guilty of employing ICT for subterfuge and circumvention. I discuss this more below in the context of environmental controls present in testing.

Likewise, control variables for incidence of past involvement in criminal enterprise present a clear, if minimal, result for violent crime. Specifically, there is a slightly positive and significant relationship between past involvement in specifically violent crime and incidence of criminal ICT usage that does not exist for past incidence of non-violent crime. Interestingly, in addition, there does not appear to be a temporal element to this relationship, as evidenced by the almost neutral relationship (at 90% confidence) between recent involvement in criminal enterprise and DV variation.

In considering environment pressures that might impact upon group decision-making, four separate significant results bear mention. The first is the marginal evidence that direct government investigation predicts variation on the DV. While the GDP and government approval ratings produce insignificant results, there is clear evidence (at 90% confidence) that evidence of such a government-organization relationship appears to make it less likely a group will employ ICT for antagonistic purposes whilst attempting to digitally engage the public. Likewise, the sponsorship of foreign actors and particularly of foreign states appears to make it *more* likely that a group will employ ICT criminally and antagonistically. Finally, though there is marginal evidence that ICT 'readiness' in a given country predicts variation on the DV, both the 'use' and 'access' metrics drawn from the World Bank's Digital Adoption Index (DAI) present as positive at 99% confidence.

This last result is particularly interesting, as it suggests there is a relationship between the capabilities environment – i.e. those environmental considerations that ultimately affect group abilities to employ ICT criminally in an effective manner. As the obvious question leading on from such a result has to do with whether or not it is a sufficiently technically permissive environment or the condition of counter-subversive forces within such an environment that matter, of course, Model 3 takes the step described in sections above of omitting the three DAI indicators in favor of a dichotomous dummy variable that describes a digital technology adoption imbalance between government and society (or not). The result is positive and significant at 99%

confidence. This suggests not only that greater potential for digital antagonism in the form of technology availability and literacy improves the chances for variation on the DV, but specifically that shady ICT employments are likely when government adoption of digital technologies lag behind broader societal trends.

Perhaps even more interestingly, the inclusion of such an alternative measure of national adoption of digital technologies produced a non-trivial change in results for group structure. Though the trends remain the same, additional comparison of results between a model that does not include such environmental controls (Model 1) and those that do shows that highly centralized groups only marginally, *ceteris paribas*, appear more likely to predict variation on the DV than do less centralized ones. Indeed, if we consider the strength of the different results, Model 1 shows that decentralized groups, in line with expectations, are more likely to deviate and employ ICT for antagonistic purposes than are centralized organizations. The decentralized result then holds with the inclusion of digital adoption environmental variables. Where digital technologies are nationally widely available and in intense use, but where there is relatively limited government adoption of the same in the form of (1) spending on cybersecurity initiatives, (2) provision of digital services or (3) the adoption of digital technologies by law enforcement, more highly decentralized groups do appear to have significant difficulty in preventing members from employing ICT for circumventive purposes. Here, however, highly bureaucratic organizations show a similar, significant result. This strongly suggests that while decentralization of structure does lead to free agent issues,

subversive groups are highly opportunistic and opt to ICT for subterfuge and disruption when there is a relative mismatch between the opportunities for digital gain and the capacity of governments to prevent, investigate or legislate such actions. This matches the result value on the final control variable – presecutability of specific ICT employments across cases – where a positive value on the dummy produces a negative probability result for the DV (significant at 90%).

Table 4.2 below controls for modeling choice by presenting the same set of models in OLS testing with a scale dependent variable that measures the raw number of shady ICT employments by subversive activists (no deviation = '0'). To be clear, this measure of the dependent variable both proxies for the dichotomous measure of deviation from expectations outlined above *and* additionally provides insight on the severity of that same deviation. As a result, this approach to testing is, in many ways, superior. As is expected, it seems reasonably clear at first glance that the trends described by the results of the logit models presented in Table 4.1 above are borne out and reflected in these linear regression results. This is unsurprising and reflects a basic diagnostic check on the validity of the models presented above. Naturally, however, there is variation in the scale and intensity of the trends described that reflects predictions of severity of deviation different to simply the fact of it.

Table 4.2. Ordinary Least Regression model results predicting deviant ICT Employment.

	Models		
	(1)	(2)	(3)
MAXIMALIST	1.644*	1.791*	1.801*
	(0.036)	(0.041)	(0.040)
LIMITED	-0.414	-0.452	-0.435
	(0.004)	(0.011)	(0.013)
IDIOSYNCRATIC	0.203	0.243	0.249
	(0.102)	(0.105)	(0.107)
POLICY	-1.245	-1.222	-1.219
	(0.192)	(0.199)	(0.201)
STRUCTURAL	4.872***	5.012***	5.036***
	(0.087)	(0.091)	(0.092)
POLITY	--	1.782	1.811
	--	(0.033)	(0.028)
DURABILITY	--	2.234	2.313
	--	(0.047)	(0.048)
PARCOMP	--	2.224**	2.231**
	--	(0.192)	(0.187)
ECONCRIM	-1.116	-1.314	-1.311
	(0.251)	(0.274)	(0.277)
VIOLCRIM	1.420*	1.441*	1.446*
	(0.079)	(0.071)	(0.072)
CRIMPRIOR	-0.015	-0.028	-0.030
	(0.713)	(0.728)	(0.742)
BUREACRATIC	1.525*	2.020***	2.031***
	(0.017)	(0.022)	(0.024)
MARKET	3.081**	3.319***	3.352***
	(0.052)	(0.051)	(0.051)
ALLCHANNEL	-.327	-0.341	-0.352
	(0.024)	(0.031)	(0.033)
GDP	--	-0.012	-0.041
	--	(0.267)	(0.252)
GOVPOP	--	-0.234	-0.241
	--	(2.013)	(2.081)
GOVINVEST	--	4.111*	4.116*
	--	(0.324)	(0.353)
SPONSDOM	-0.032	-0.041	-0.045
	(3.213)	(3.532)	(3.424)
SPONSFOR	5.223*	4.943**	4.940**
	(0.087)	(0.093)	(0.099)
SPONSSTATE	1.532*	1.437*	1.428*
	(0.004)	(0.009)	(0.007)
GOVTSOCDIVIDE	--	--	7.225***
	--	--	(1.231)
ANONYMOUS	--	1.723	1.789
	--	(0.067)	(0.064)
PROSECUTE	-0.412*	-0.442*	-0.445*
	(0.523)	(0.565)	(0.532)
TARGETTYPE	0.895*	0.853**	0.834**

	(0.662)	(0.623)	(0.624)
ACCESS	--	4.232***	--
	--	(1.231)	--
USE	--	4.531***	--
	--	(1.432)	--
READINESS	--	-1.233*	--
	--	(0.032)	--
R^2	0.146	0.298	0.301

Robust standard errors in parentheses, ***p<0.01, **p<0.05, *p<0.1

Again, the use of a scale dependent variable allows for some additional insight into factors that predict varying levels of intensity in antagonistic ICT usage. In particular, regardless of similarly positive trends across the range of a dozen independent variables with significant results in the previous set of tests, there are exceedingly strong relationships between intensity of shady ICT employments and three variables – STRUCTURAL, SPONSFOR and GOVTSOCIDIVIDE. Subversive activist organizations are likely to employ ICT for circumvention and disruption about 5 more times when the group's grievance is structural in nature than when it isn't. Likewise, the existence of foreign-based sponsorship of a subversive organization predicts makes it so that such groups are on average likely to use ICT for antagonism almost 5 more times in a given 18 month episode than are those with either no sponsorship or solely domestic support (though the result is only significant at 95%). And where there exists a digital adoption gap between society and government, groups are likely to use ICT in a deviant fashion just more than 7 more times across the observed periods of engagement in digital activism than when there exists no gap. There are also strong results for group structure and target type. As with Table 4.1 above, however, the strength of these relationships

seems to be dependent on the inclusion of environmental control variables, with only the nature of group grievances and – to a lesser degree – the sponsorship of a foreign entity holding strongly across models. These results will be further fleshed out in the discussion section below.

4.3.1. Adding Nuance: Subversive Groups and IEOs

Regardless of the neatness of the dichotomous categorization of ICT employments as either activist or antagonistic described above or the fleshed out scale version, it would naturally not do to assume that all cyber techniques constitute the same kind of commitment to a particular strategic emphasis. Indeed, the results above, though indicative of a particular story about the way in which subversive activists employ ICT, do little to account for variation in the types of techniques being employed. Moreover, though the OLS results above do account for one manifestation of tactical intensity, they certainly do not predict variation in severity via the more reasonable understanding that comes from analysis of specific techniques. This section therefore breaks down data on ICT employments gathered across the set of 90 deviators present within the broader set of 279 subversive activist organizations, analyzes common techniques, breaks such usage out by different control categories and re-constructs the main dependent variable in line with new information about common ICT employments.

In short, despite raw confirmation of the claims of analysts regarding subversive group behavior, it would be disingenuous to simply say that a great number of subversive actors regularly prosecute cyber attacks, intrude into governments systems

and undertake all other manner of disruptive digital activity whilst engaged in activist efforts. When the data are broken out (see Figure 4.1), a reasonably clear trend appears. By far, the most common deviant or criminal ICT activity among subversive groups involves three related techniques – (1) basic information theft, (2) the use of encryption to share illicitly obtained information and (3) doxxing.

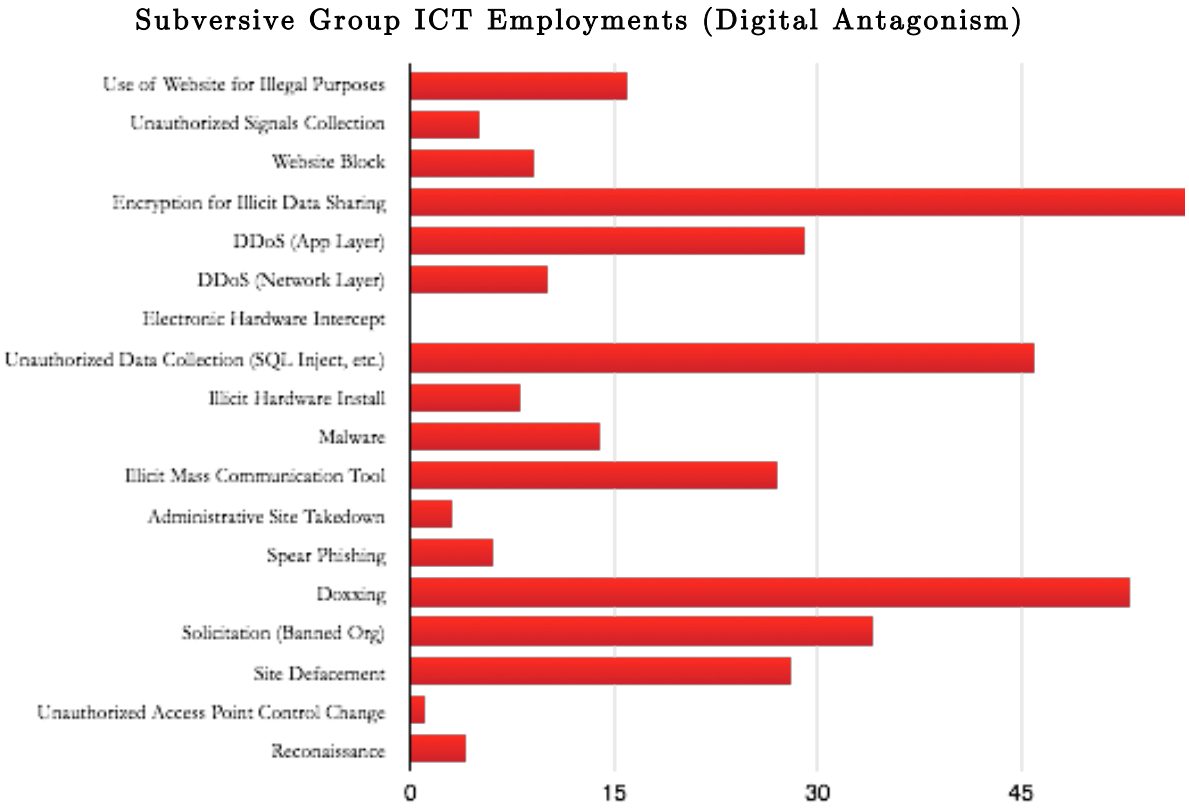

Figure 4.1. Subversive group use of ICT for antagonism.

The first – basic information theft/unauthorized data collection – involves the use of techniques like SQL Injections and Cross-Site Scripting that exploit web-based vulnerabilities in order to allow an intruder access to private information. These

exploits are, in many ways, the lowest form of data exfiltration techniques, as they often take advantage of known vulnerabilities and allow rapid downloads of private information databases. Cross-site scripting, for instance, takes advantage of known flaws in different website designs to allow either hackers or less sophisticated belligerents (i.e. "script kiddies") to script malicious code onto a page. The code then accomplishes one of a wide range of tasks, from directly downloading unprotected information to directing incoming traffic to a secondary site set up by the attacker. Again, this kind of action is non-sophisticated and can readily be practiced with a minimal amount of training or technical resources. Nor are such actions always found to be illegal in that the nature of such activities as prosecutable is entirely defined by local jurisdictional contexts and often pivots on difficult-to-obtain notions of intention surrounding an organization's involvement.

The second of these involves using the darknet and a range of peer-to-peer (P2P) encryption methods for disseminating such information. Naturally, since illicit data mining or theft is criminal in and of itself, the dissemination thereof is also illegal. The inclusion of the encryption category simply reflects the secondary use of ICT to enable illegal activity in aid of broader campaign objectives. The same can be said of doxxing, which describes the strategic publication of private data online for any number of reasons, including creating scandal involving entrenched political elites, embarrassing the government, embarrassing social opponents or even attempting to do the public a service. In both instances, of course, further illegal action is possible without the use of

ICT (i.e. a dossier may be printed and distributed physically), but the parallel trend in common among subversive groups to employ ICT for each part of the data theft enterprise tellingly suggests that information redistribution techniques are a key new part of subversive group tactical portfolios. And other less common ICT employments seem to parallel this emphasis on low-intensity information operations and include the use of encryption for communication with blacklisted organizations, the use of banned email spamming software and direct vandalism of websites. In stark contrast, malware employments, direct hardware tampering, denial of service attacks and other more disruptive ICT employments are, though not exactly rare, less common.

Figure 4. Example of Brown-Tullos Cyber Action Response Spectrum

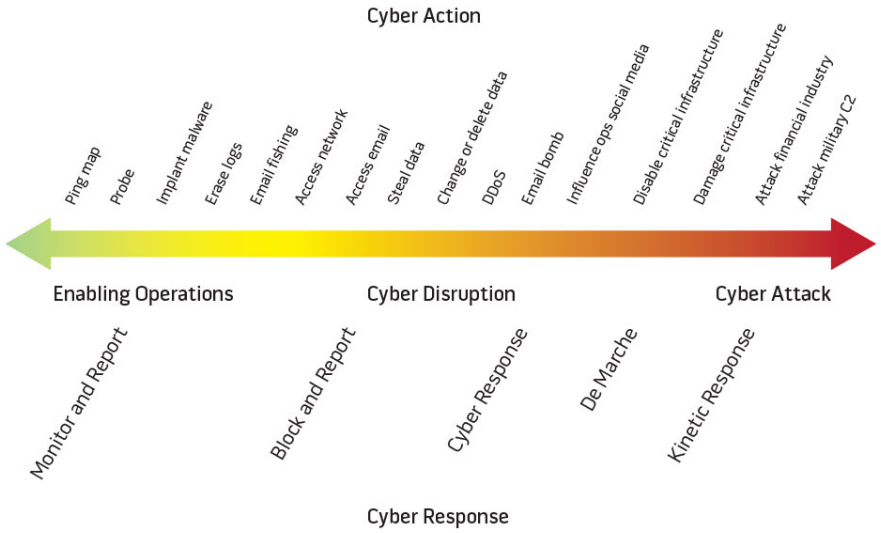

Figure 4.2. Schmitt analysis stack categorical breakdown of cyber techniques by impact and characterizing features

In many ways, this trend towards remarkably low-intensity circumventive and disruptive ICT activities among subversive activists is unsurprising. In much recent empirical work on cyber conflict issues, it has become standard practice to consider cyber attacks as fitting along a spectrum from low to high impact. Figure 4.2 shows a popular example of such a spectrum, the Brown-Tullos Cyber Action Response Spectrum that has been variously used to align policy and technical responses with different forms of cyber actions and threats. Given what we know about the goals of subversive organizations as interested in normative transformation and the conditions that allow for such an ideational inflection, one might be forgiven for simply assuming that there might be minimal evidence of high-level cyber assaults undertaken by subversive organizations. Aside from the fact that high-level attacks are inherently more expensive and time consuming to prosecute, subversion is less focused on systematic chaos and disruption than it is on targeted acts of manipulation and mitigation of opponents.

On a spectrum like the Brown-Tullos CAR Spectrum in Figure 4.2, the left-hand group of low-impact and low-intensity cyber interactions is labeled *enabling operations*. In other literature, analysts have labeled such techniques and methods of approach "grey tactics" and "twilight operations." The idea is that such methods are themselves adjunct enhancement tools that enable attacks that are more meaningful in the context of an attacker's portfolio of objectives. For studies of hactivists, spies or foreign militaries, such low-intensity techniques – if employed smartly and successfully – give way to greater abilities to prosecute highly disruptive cyber attacks, from sophisticated

persistent information exfiltration to assaults on critical infrastructure. For subversive organizations, the shape of cyber actions across *the entire campaign* is naturally likely to be quite different than may be the case for, for instance, terrorist groups. However, focus on low-intensity digital antagonism in the preparatory and mobilization stages of a subversive campaign corresponds with what we know about the payoffs involved with this group of cyber techniques across a range of characterizing categories.

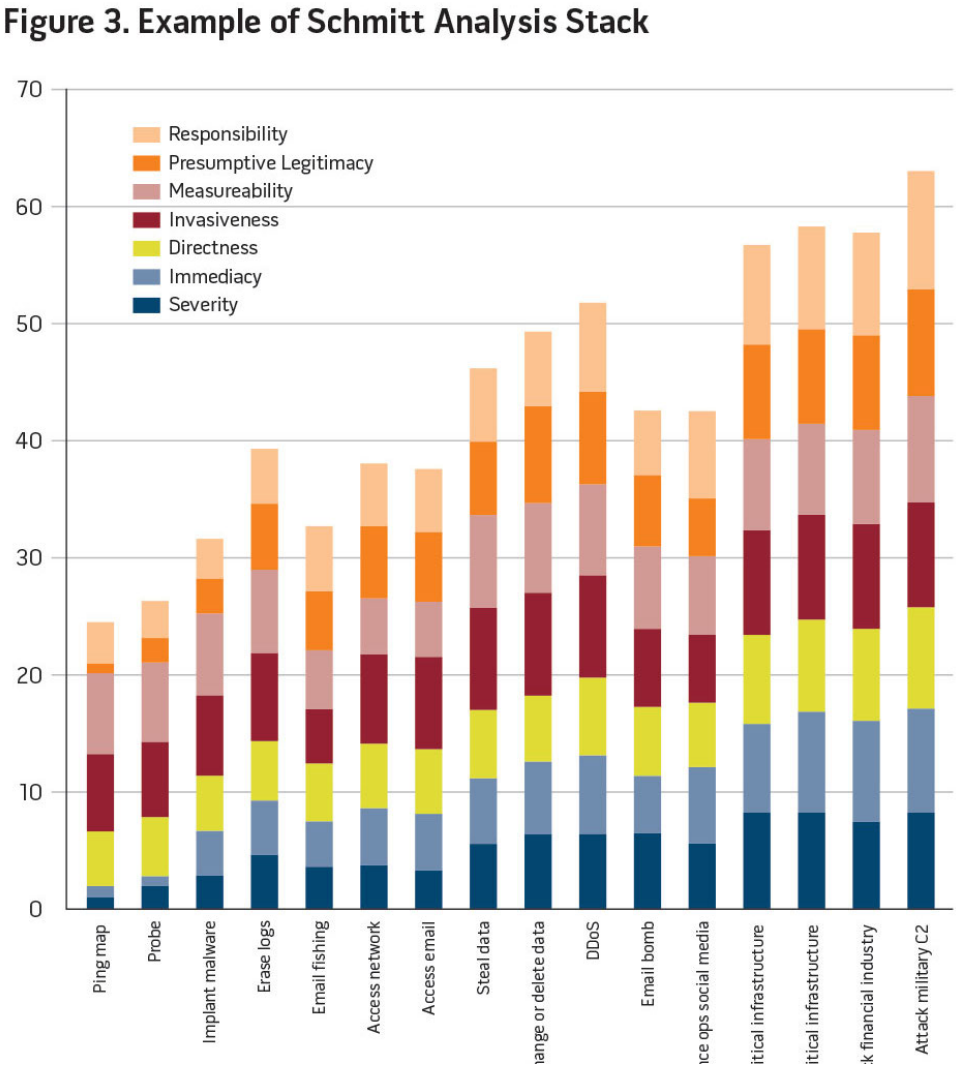

Figure 4.3. Schmitt analysis stack categorical breakdown of cyber techniques by impact and characterizing features.

Figure 4.3 breaks out the Brown-Tullos spectrum into a Schmitt Analysis Stack in which different characteristics of cyber attacks are estimated along the length of the impact scale. Actions taken that fall along the left-hand side of the spectrum, including simple reconnaissance, data espionage and information modification activities, are inherently low-risk/high-gain in that they tend to be minimally disruptive to system functionality and there are rarely delayed or unknown effects associated with them (thus reducing operation uncertainty in planning). Likewise, unlike more complex cyber attacks, there is little chance of "catching others in the blast" through unintended side effects, as is common with the employment of reasonably sophisticated cyber weaponry. Such activities, though somewhat easy to measure and attribute in technical terms, are relatively tricky to assess in terms of real-world criminal or political responsibility. And such activities are often difficult to legislate, particularly as jurisdictional standards for identifying intent and organizational involvement is highly variable. The attraction of such techniques to subversive organizations is clear. Indeed, this category of antagonistic techniques is unusual in the context of more traditional work studying the methods of subversive and related organizations in that the risk-to-potential-gain ratio is extreme. This, in itself, suggests an explanation for the basic deviation from expectations regarding subversive involvement in shady or criminal enterprise, though there certainly remains evidence that subversive groups take more disruptive actions.

Though common practice is to label low-intensity cyber activities as *enabling operations* in contextual reference to the more disruptive actions commonly undertaken

by states, black hat hackers and more, I hereafter label this category *information enrichment operations* (IEOs). Again, the implication here is slightly different than with the "information enabling" moniker often applied to low impact cyber attacks that then enable more severe attacks. Here, enrichment signifies the particular manner in which these types of techniques can help subversive groups enrich the information environment and produce favorable conditions for normative operation.

Naturally, this more nuanced understanding of subversive campaign employments of ICT for circumvention and disruption lends itself to greater nuance in testing. Specifically, by grouping observations of those low-intensity employments into an information enrichment category, it is possible to undertake testing to answer two questions. First, do different factors predict digital antagonism wherein only low-intensity information enrichment techniques are employed? Second, and in many ways more importantly, among the set of deviant subversive activists what factors predict the move from low-intensity ICT employments to more disruptive and risky choices of technique? Table 4.3 reruns binomial logit analysis with two new dependent variables in an effort to answer these questions. A positive value on the first DV denotes observation of *only* information enrichment techniques alongside activist efforts, while a negative value denotes either no deviant behavior or more severe actions alongside activism. For the second DV, testing covers only the group of 90 deviators in the broader set. A negative value denotes *only* observation of information enrichment techniques, while a positive value denotes more severe forms of cyber antagonism.

Table 4.3. Binomial logit model results predicting variation on the use of information enrichment techniques for (1) the entire set of observed organizations and (2) the set *minus* groups that do not move beyond activist ICT employments.

	DV#1			DV#2		
	(1)	(2)	(3)	(4)	(5)	(6)
MAXIMALIST	1.336*	1.212*	1.205*	1.183 **	1.188**	1.195**
	(0.142)	(0.078)	(0.079)	(0.065)	(0.053)	(0.056)
LIMITED	0.827	0.802	0.817	0.777	0.732	0.721
	(0.017)	(0.018)	(0.018)	(0.023)	(0.021)	(0.022)
IDIOSYNCRATIC	1.071	1.063	1.067	1.044	1.066	1.065
	(0.414)	(0.411)	(0.409)	(0.456)	(0.453)	(0.453)
POLICY	0.788	0.773	0.775	0.801	0.797	0.798
	(0.323)	(0.333)	(0.330)	(0.331)	(0.335)	(0.334)
STRUCTURAL	1.678***	1.703***	1.708***	4.007***	3.983 ***	3.979***
	(0.163)	(0.166)	(0.167)	(0.163)	(0.165)	(0.164)
POLITY	--	1.301	1.311	--	1.344	1.341
	--	(0.067)	(0.066)	--	(0.066)	(0.068)
DURABILITY	--	1.422	1.431	--	1.455	1.453
	--	(0.123)	(0.126)	--	(0.127)	(0.125)
PARCOMP	--	1.316**	1.322**	--	1.284**	1.288**
	--	(0.312)	(0.313)	--	(0.316)	(0.315)
ECONCRIM	0.697	0.694	0.699	0.645	0.642	0.640
	(0.512)	(0.516)	(0.511)	(0.510)	(0.532)	(0.536)
VIOLCRIM	1.210*	1.200*	1.197*	1.411*	1.409**	1.403**
	(0.421)	(0.468)	(0.469)	(0.451)	(0.456)	(0.454)
CRIMPRIOR	0.980	0.989	0.984	0.909	0.910	0.903
	(1.324)	(1.343)	(1.346)	(1.324)	(1.365)	(1.359)
BUREACRATIC	1.129	1.222*	1.223*	1.412*	1.631**	1.633**
	(0.050)	(0.053)	(0.055)	(0.039)	(0.041)	(0.043)
MARKET	1.644***	1.689***	1.688***	1.698**	1.703**	1.704**
	(0.079)	(0.077)	(0.073)	(0.088)	(0.083)	(0.084)
ALLCHANNEL	0.910	0.919	0.917	0.911	0.903	0.905
	(0.135)	(0.136)	(0.132)	(0.139)	(0.141)	(0.139)
GDP	--	0.913	0.923	--	0.899	0.895
	--	(0.178)	(0.177)	--	(0.180)	(0.183)
GOVPOP	--	0.968	0.965	--	0.966	0.969
	--	(1.355)	(1.352)	--	(1.351)	(1.352)
GOVINVEST	--	1.933*	1.934*	--	2.023**	2.022**
	--	(0.189)	(0.183)	--	(0.183)	(0.184)
SPONSDOM	0.942	0.953	0.953	0.935	0.944	0.941
	(2.684)	(2.648)	(2.643)	(2.476)	(2.477)	(2.474)
SPONSFOR	1.588*	1.581**	1.582**	1.892*	1.895***	1.888***
	(0.136)	(0.135)	(0.132)	(0.138)	(0.136)	(0.133)
SPONSSTATE	1.089*	1.079*	1.081*	1.198**	1.196**	1.195**
	(0.027)	(0.029)	(0.033)	(0.031)	(0.030)	(0.031)
GOVTSOCDIVIDE	--	--	2.313***	--	--	4.002***
	--	--	(0.200)	--	--	(0.203)
ANONYMOUS	--	1.363	1.359	--	1.339	1.341
	--	(0.130)	(0.128)	--	(0.120)	(0.127)

PROSECUTE	0.836	0.833*	0.830*	0.850	0.848*	0.847*
	(0.178)	(0.173)	(0.174)	(0.177)	(0.181)	(0.180)
TARGETTYPE	1.101	1.117*	1.121*	1.141	1.155*	1.153*
	(0.234)	(0.231)	(0.233)	(0.254)	(0.255)	(0.250)
ACCESS	--	1.645***	--	--	2.010***	--
	--	(0.741)	--	--	(0.732)	--
USE	--	1.928***	--	--	1.997***	--
	--	(0.578)	--	--	(0.583)	--
READINESS	--	0.578*	--	--	0.612*	--
	--	(0.065)	--	--	(0.060)	--
Observations	279	279	279	279	279	279
Ll	2398.342	2343.031	2384.039	1985.828	20348.242	2143.643
Psuedo R^2	0.033	0.059	0.057	0.061	0.083	0.084

Robust standard errors in parentheses, ***p<0.01, **p<0.05, *p<0.1

The results in for the first dependent variable are reasonably similar to previous sections' findings. Much as was true in previous models, there are variably significant results for competitiveness of a political system, decentralized organization structure and the condition of prior involvement in violent (though not necessarily organized) criminal enterprise. Of interest, there is an enduringly strong finding in terms of the nature of organization grievances and the government-society adoption divide (in the form of both the adoption control variable and the original adoption indicators). Where an organization holds a structural grievance, they are more likely – though the result *is* weaker than in the models presented above – to solely select to use information enrichment operations. Likewise, where there exists an adoption imbalance in the form of high societal digital adoption against low government buy-in, groups are more likely to only select the same. In this model, these two findings are the only ones significant at 99% confidence.

The natural question that emerges from such results has to do with the differentiation that can be made between digital antagonism that takes the form of low-intensity cyber operations and that which moves beyond to riskier employments, such as unauthorized hardware alterations or denial of service attacks. Models 4-6 addresses this issue with an alternative measurement of the DV as denoting observation of *only* enrichment behavior or not amongst the set of 90 deviators (thus ignoring organizations not engaged in digital antagonism), and descriptive treatment of the data further draws a picture of factors most relevant in explaining variation.

As the model shows, there is actually remarkably limited variation in results from models that use alternative dependent variables. Certainly, the strength of results changes across the board. Here, the inclusion of the foreign sponsorship control in particular predicts a much stronger and more significant relationship than in past models. At the same time, group structure and direct evidence of government investigation remain linked but are variably significant. But the general trends involved in this set of tests remain similar. Of note, the nature of grievance among organizations remains arguably the most interesting result predicting variation on the dependent variable, both in the scale of the result and the high p-value for significance.

The relationship between group grievances, though clearly modified by a broad range of intervening factors, appears to be a unique explanatory variable in efforts to predict variation on the dependent variable. This is further clear when volume data on specific techniques employed across the set of subversive organizations studied are

descriptively broken out using the different control variables described above. Figures 8 through 12 provide examples of this. Figure 4.4 below, for instance, does just this in splitting out raw episodic incidence of the techniques described in Figure 1 above by the grievance variables (i.e. does a group "buy-in" to the current political system or not?). Even in this format, there appears to be a clear discrepancy in the choice to move from information enrichment activities to more disruptive ICT employments across the categories of buy-in. Whereas unauthorized data collections and doxxing, for instance, remain common amongst groups that generally buy-in to the current structural setup, instances of malware employment, DDoS attacks and more are rare. Moreover, very few instances of explicitly illegal website usage – to advocate violent protest, for instance – exist amongst those groups. This suggests that subversive activists without structural grievances are willing to manipulate the information environment, but are reluctant to cross the line into activities that are more visibly disruptive.

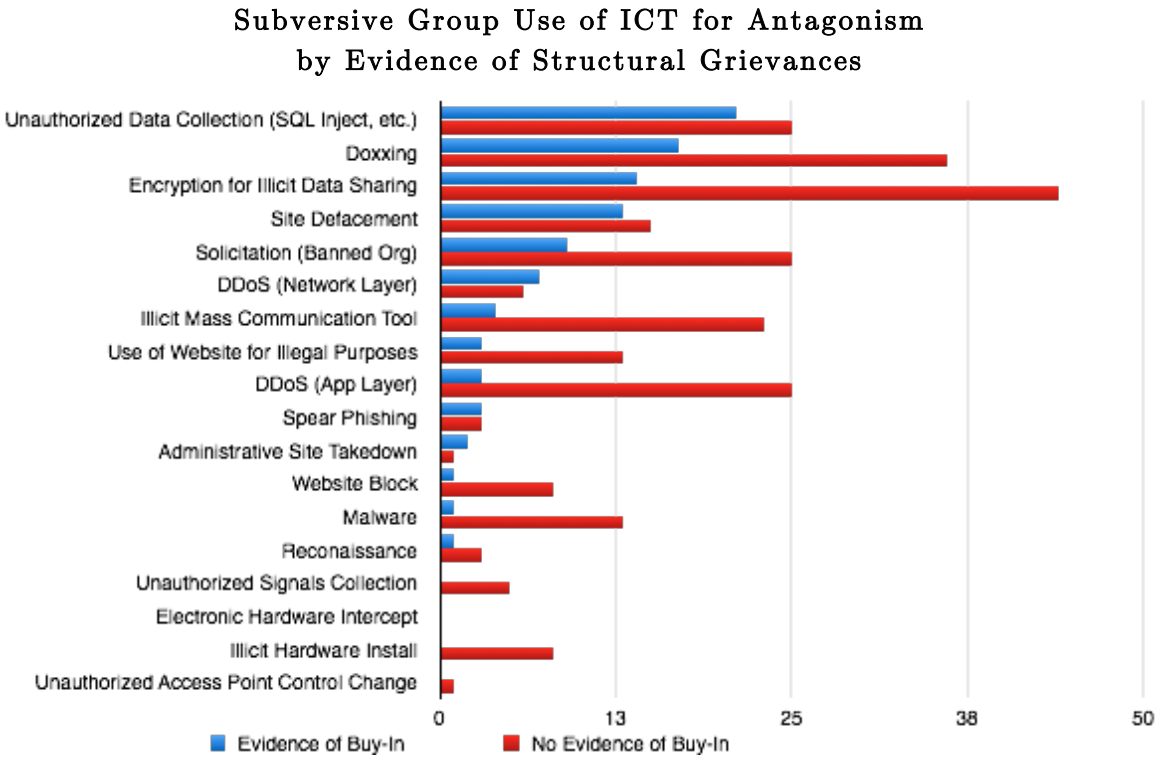

Figure 4.4. Subversive group use of ICT for antagonism by evidence of structural grievances (or not).

Breaking the data out further out further using a control variable for whether or not each specific ICT technique was prosecutable in the jurisdictional context (Figure 4.5), it appears that groups without structural grievances tend to use ICT for disruption and circumvention where it is legal far moreso than do those with structural grievances. Particularly with low-level disruptive activities that include basic network layer denial of service attacks, administrative website takedowns, simple acts of vandalism and simple data collection, actions taken by groups without structural grievances were far less likely to meet an admittedly low bar of prosecutability. This, again, suggests opportunism as

a key feature of subversive organizations that can be understood through the lens of group grievance.

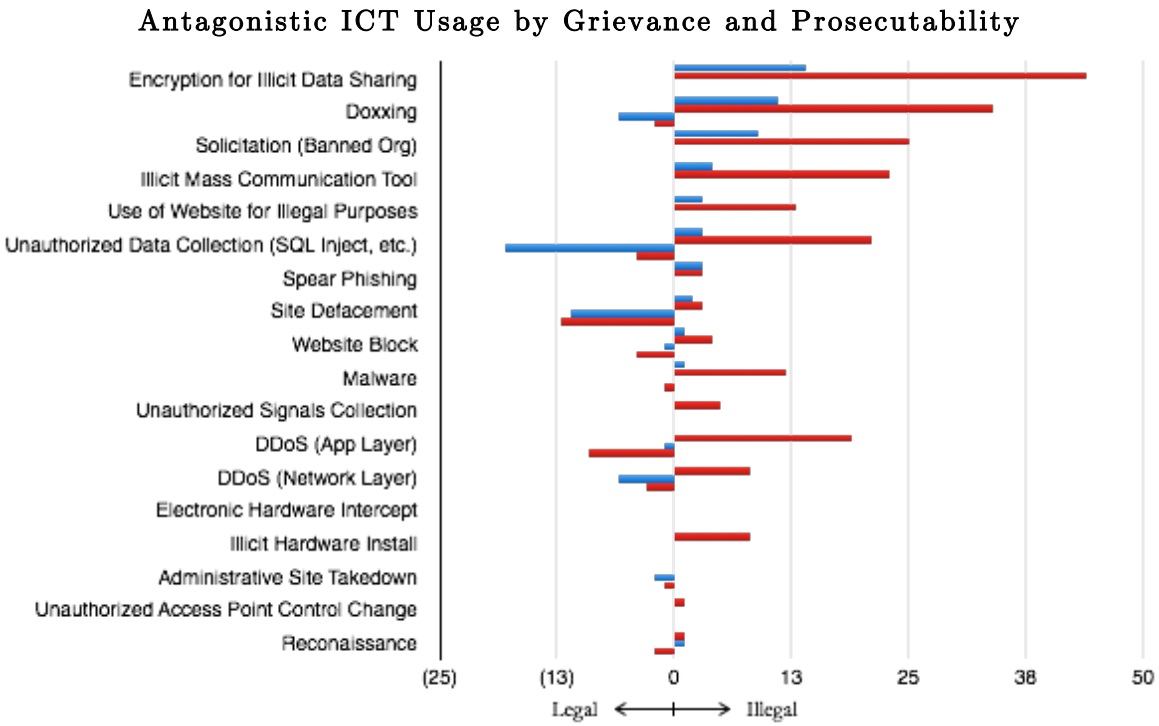

Figure 4.5. Antagonistic ICT usage by grievance and prosecutability.

Likewise, when split out using sponsorship variable data (in Figure 4.6, wherein a group can either have *only* foreign sponsorship or no sponsorship/both domestic and foreign sponsorship), we can visualize the greater likelihood some groups have to deviate from expectations in more severe ways than others. From Figure 4.6, it is clear not only that information enrichment operations are common across the gamut of subversive non-state actors, but that those with foreign sponsorship are additionally likely to employ ICT more disruptively. In particular, such groups are more likely employ malware,

engage in spearphishing campaigns, publically deface websites and solicit aid online from explicitly blacklisted organizations.

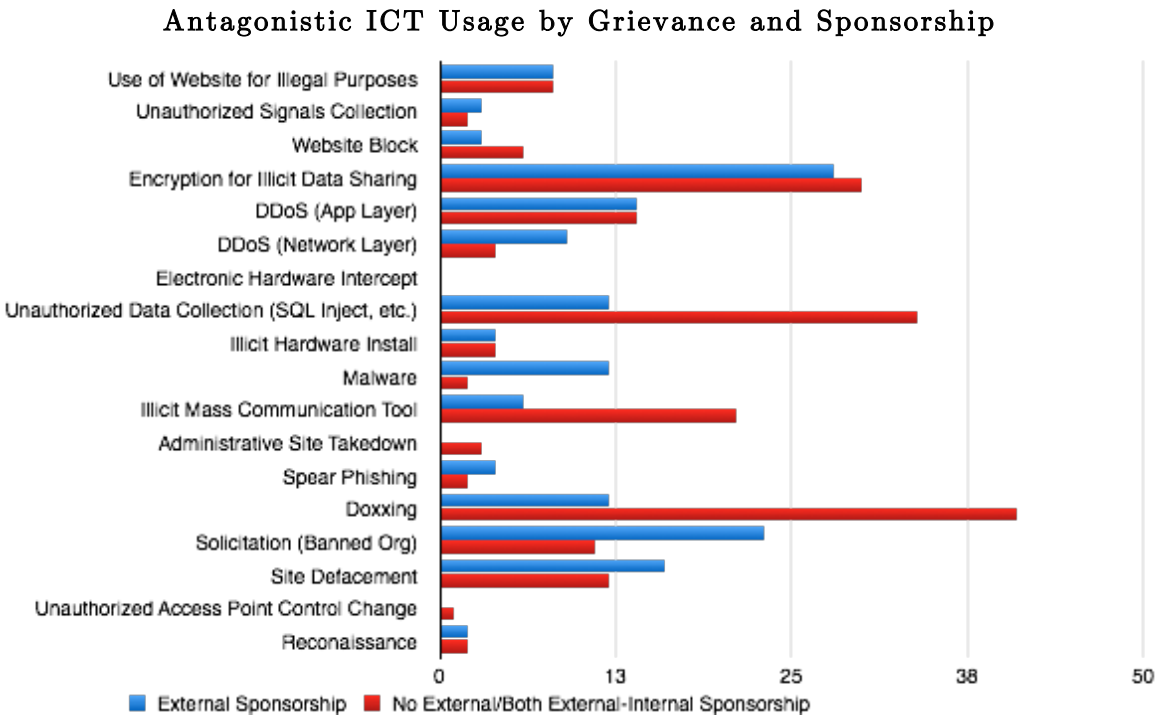

Figure 4.6. Antagonistic ICT usage by grievance and sponsorship.

And, when the data are broken out using target profile data, it likewise appears that such groups are highly unlikely to target government or military agencies or personnel in their digital activities. Groups without structural grievances, while still commonly employing techniques that pertain to illegal information theft, manipulation and publication, almost never engage directly with government personnel and institutions in stark contrast to their revisionist cousins. This suggests that such groups

are sensitive to the risks involved in attracting government attention depending on their objectives and strategically opt to exclusively target fellow societal actors.

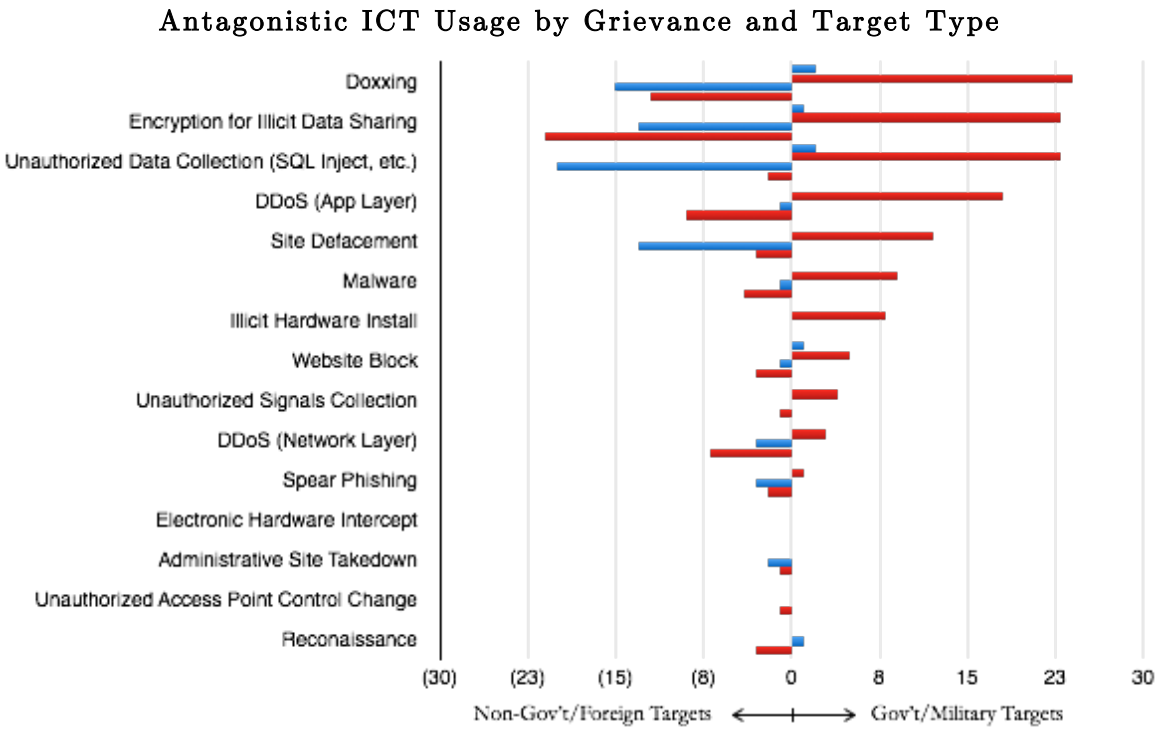

Figure 4.7. Antagonistic ICT usage by grievance and target type.

At a somewhat more technical level, there is even an interesting set of conclusions stemming from Figure 4.8's descriptive breakdown of denial of service attacks split out by the group grievance control variable and an ordinal variable that describes the standard severity spectrum (Schmitt and Tulos) for such attacks. Here, there is tangential evidence of greater linkages to criminal enterprise as a component part of the subversive enterprise amongst those groups with structural grievances. Again, in a generic sense, denial of service attacks essentially target machines that host a

particular service, such as email accounts or a database, and overwhelm it with traffic so as to prevent legitimate activities. The data here follows procedures common in cyber incident coding projects in splitting DDoS methods of approach into two main categories – (1) app layer DDoS attacks that target a function of a specific computer application and (2) network layer attacks target the network that a machine uses to access the Internet.

In Figure 4.8, the two types of attack are split amongst buy-in and non-buy-in groups and arrayed along a spectrum of severity of attack outcome. For groups without structural grievances, app layer attacks present as rare and accomplish only minimal disruption. For such groups, network layer attacks are more common, though again they seem to accomplish relatively little in the way of disruption. By contrast, network attacks are relatively uncommon for groups with structural grievances, but the few that are undertaken are quite relatively technically successful. Likewise, those groups employ a greater number of app-focused attacks and are able to achieve a range of technically meaningful outcomes. At first glance, given the apparent significance of grievance as an explanatory variable, these trends are somewhat unsurprising. App layer attacks are expensive and time consuming, and become moreso as the sophistication of the target increases. Limited success amongst groups without structural grievances might suggest limited resources devoted to such attacks. Likewise, network attacks are far easier to prosecute but there is a much wider scale of accessibility in that attacks that aim to achieve either broad-scoped or longer-term disruption imply extensive technical and

coordinative resources. The most effective attacks, for instance, often require the purchase of a botnet from a criminal entity. In short, the data here, wherein only groups with structural grievances affect reasonably successful network attacks, suggests that structural buy-in precludes the decision to either spend large amounts of money on such assaults or to link a group with criminal enterprise.

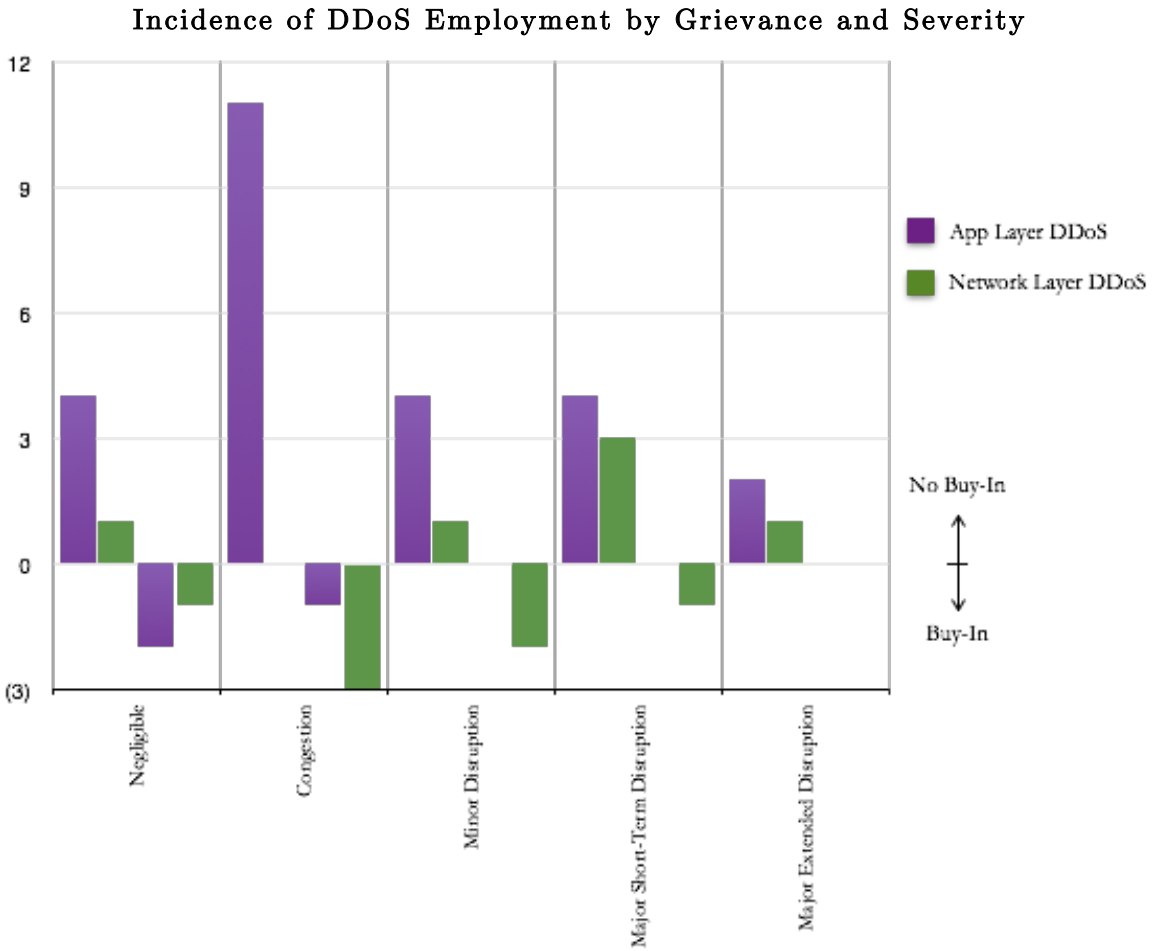

Figure 4.8. Incidence of DDoS employment by grievance and severity.

Naturally, there is a broad range of conclusions that might be drawn from such data and a number of stories to be told about the use of network technologies by non-

violent extremists in world affairs. However, there are some clear trends and strong relationships amongst the results presented in this section that lend themselves to greater understanding of both the subversive enterprise and the impact of information revolution on non-state actor behavior more broadly on a number of fronts. The next sections perform basic diagnostic robustness testing, discuss the results in the context of the hypotheses outlined in Chapter 3 and then reference the sizable amount of evidence presented here to articulate a theoretical perspective on subversion in the digital age.

4.3.2. Diagnostics

The use of a scale dependent variable useful for linear regression analysis in addition to the primary logit analysis presented in sections above reduces the need for extensive robustness testing. In secondary testing, trends appeared to match those predicted in Table 4.1's logit models. Thus, there is limited concern that primary testing suffers from multicollinearity (i.e. variation based on the nature of different independent variable measurements). This is further the case given the presentation of the several different basic binomial logit models above in which IVs are variably included to reflect different measures of significant potential intervening factors.

Nevertheless, it is certainly the case that primarily analysis above was performed using dichotomous measures of the dependent variable and that analysis was performed for a relatively small number of observations over a reasonably limited time frame of thirty-three years. Therefore, I repeat my analysis below in Table 4.4 using conditional log-link, rare events and fixed effects regression analysis. I do so twice – once for the

original SHADOW variable and then for the later operationalization of the DV as being incidence of *only* information enrichment operations or not among the set of 90 deviators. The purpose in doing so is to control for the small and potentially unrepresentative nature of the dataset versus the universe of possible cases, as well as to make sure that no single case factors skew the results for the set as a whole.

Table 4.4. Diagnostic models for results predicting deviant ICT Employment using the conditional log-link function, rare events logit and fixed effects.

	DV#1			DV#2		
	Log-link	Rare Events	Fixed Effects	Log-link	Rare Events	Fixed Effects
	(1)	(2)	(3)	(4)	(5)	(6)
MAXIMALIST	1.517*	1.522*	1.839*	1.301**	1.319**	1.504**
	(0.100)	(0.099)	(0.097)	(0.058)	(0.057)	(0.057)
LIMITED	0.824	0.808	0.738	0.698	0.696	0.676
	(0.033)	(0.032)	(0.036)	(0.030)	(0.029)	(0.025)
IDIOSYNCRATIC	1.111	1.098	1.210	1.047	1.040	1.093
	(0.420)	(0.421)	(0.439)	(0.489)	(0.482)	(0.488)
POLICY	0.651	0.654	0.654	0.803	0.804	0.777
	(0.365)	(0.363)	(0.360)	(0.330)	(0.335)	(0.340)
STRUCTURAL	2.328***	2.322***	2.467***	3.503***	3.518***	4.089***
	(0.150)	(0.149)	(0.161)	(0.168)	(0.165)	(0.160)
POLITY	1.442	1.438	1.530	1.398	1.409	1.564
	(0.072)	(0.069)	(0.077)	(0.065)	(0.064)	(0.071)
DURABILITY	1.278	1.282	1.383	1.301	1.307	1.423
	(0.128)	(0.126)	(0.130)	(0.125)	(0.126)	(0.125)
PARCOMP	1.678**	1.647**	1.808**	1.543**	1.542**	1.732**
	(0.272)	(0.278)	(0.275)	(0.321)	(0.324)	(0.320)
ECONCRIM	0.865	0.868	0.702	0.679	0.677	0.535
	(0.415)	(0.413)	(0.442)	(0.534)	(0.531)	(0.535)
VIOLCRIM	1.221*	1.224*	1.340*	1.356**	1.352**	1.565**
	(0.518)	(0.515)	(0.561)	(0.449)	(0.451)	(0.461)
CRIMPRIOR	0.793	0.797	0.734	0.934	0.935	0.878
	(0.828)	(0.827)	(0.832)	(1.367)	(1.369)	(1.367)
BUREACRATIC	1.324*	1.331***	1.642***	1.272*	1.275**	1.557**
	(0.064)	(0.061)	(0.069)	(0.039)	(0.041)	(0.049)
MARKET	1.801**	1.797***	1.948***	1.468**	1.463**	1.732**
	(0.082)	(0.086)	(0.090)	(0.077)	(0.081)	(0.080)
ALLCHANNEL	0.967	0.963	0.867	0.856	0.853	0.802
	(0.159)	(0.155)	(0.148)	(0.138)	(0.137)	(0.130)
GDP	0.920	0.915	0.832	0.954	0.951	0.879
	(0.149)	(0.151)	(0.151)	(0.182)	(0.179)	(0.189)
GOVPOP	0.953	0.952	0.899	0.900	0.905	0.867

	(1.332)	(1.334)	(1.341)	(1.360)	(1.358)	(1.351)
GOVINVEST	2.422*	2.423*	2.890*	1.623**	1.628**	2.134**
	(0.248)	(0.249)	(0.238)	(0.178)	(0.184)	(0.183)
SPONSDOM	0.888	0.883	0.834	0.902	0.904	0.823
	(2.239)	(2.236)	(2.237)	(2.470)	(2.473)	(2.479)
SPONSFOR	1.353**	1.356**	1.609**	1.542**	1.544**	2.043**
	(0.140)	(0.138)	(0.136)	(0.128)	(0.129)	(0.135)
SPONSSTATE	1.234*	1.239*	1.453*	1.167**	1.164**	1.363**
	(0.403)	(0.405)	(0.411)	(0.038)	(0.040)	(0.035)
GOVTSOCDIVIDE	3.580***	3.589***	5.245 ***	3.864***	3.859***	5.532***
	(0.180)	(0.178)	(0.173)	(0.211)	(0.213)	(0.209)
ANONYMOUS	1.093	1.099	1.235	1.153	1.155	1.303
	(0.111)	(0.115)	(0.111)	(0.130)	(0.129)	(0.127)
PROSECUTE	0.838*	0.835*	0.677*	0.882*	0.885*	0.730*
	(0.203)	(0.201)	(0.198)	(0.185)	(0.180)	(0.176)
TARGETTYPE	1.783*	1.780*	2.032*	2.356*	2.358*	4.984*
	(0.333)	(0.328)	(0.380)	(0.256)	(0.251)	(0.251)
ACCESS	--	--	--	--	--	--
	--	--	--	--	--	--
USE	--	--	--	--	--	--
	--	--	--	--	--	--
READINESS	--	--	--	--	--	--
	--	--	--	--	--	--
Observations	279	279	279	279	279	279
Ll	2768.345	2742.248	2693.352	2689.393	2664.849	2984.994
Psuedo R^2	0.069	0.068	0.081	0.071	0.070	0.084

Robust standard errors in parentheses, ***p<0.01, **p<0.05, *p<0.1

The results show no major variation in values across the odds ratios reported for any variable. Though there are various minor differences in the scale of results, new values do nothing to diminish the significance of earlier findings.

4.4. Analysis and Discussion of Results

The results of testing presented provide a large amount of evidence on the determinants of subversive group decision-making in the digital age. Naturally, interpretation of such evidence is no simple matter. After all, this project engages in testing in the context of two competing imperatives – the need to explain variation on

the dependent variable in terms of organization decision-making and the need to do so in such a way that I might gauge the specific impact of effects emerging from the information revolution itself. To some degree, the great amount of information emerging from results prompts the researcher to adjudicate on the strongest and clearest trends in evidence in order to construct an appropriate and useful narrative. Given this, I use this section to discuss the results first by revisiting and discuss the hypotheses outlined in Chapter 3, before turning to a discussion of those explanatory factors that seem most relevant to the effort to theorize on subversion in the digital age in the next.

Chapter 3 articulated four sets of hypotheses. The first of these had to do with the strategic perspective of subversive organizations. These three hypotheses were:

H1: *Subversive organizations with minimalist objectives will be less likely to move beyond digital activism in their ICT employments than will those with maximalist objectives.*

H2: *Subversive organizations with explicit structural grievances will be more likely to move beyond digital activism in their ICT employments.*

H3: *The more permissive the political system is to modification and redesign, the less likely a subversive group will be to move beyond digital activism in their ICT employments.*

In testing, this set of variables included to control for the impact of strategic perspective of an organization turned out to be among the most relevant. There is significant evidence in favor of H2, in particular, that subversive groups with explicitly structural grievances are more likely to move beyond digital activism to antagonism in there ICT employments than are groups without. This holds further in testing above that seeks to

shed light on the determinants of decision-making with regards to more highly disruptive ICT employments vis-à-vis simple information enrichment operations. Indeed, this result is arguably the most consistently strong and significant finding of the large-N study. In line with this result, there is also some evidence to affirm H1 wherein groups with maximalist objectives are positively linked with deviation beyond only digital activism *and* H3 where the permissibility of a political system itself predicts the likelihood of group decision-making to move beyond digital activism in ICT employments. All told, there is significant evidence to suggest that the strategic context of a group's campaign determines the tactics chosen. However, again, the strongest evidence pertains to H2, as results on the nature of the objectives portfolio and strategic context vary across the inclusion of different environmental controls.

By contrast, organizational factors seem to only minimally predict subversive group decision-making. Chapter 3 articulated two hypotheses/sets of expectations in this vein. They were:

H4: *Subversive organizations that exhibit evidence of involvement in criminal enterprise prior to using ICT for digital activism will be more likely to use ICT for both purposes simultaneously.*

H5: *The more highly decentralized a subversive organization is, the less likely that group will be to be able to prevent free agent defection in the form of ICT employments beyond digital activism.*

Though testing in Tables 1, 2 and 3 above *does* present some marginal evidence that affirms H4, this result does not hold across all models. In particular, this marginal result that past involvement in violent criminal enterprise only retains its minimal 90%

confidence result in Table 4.2's linear regression model and remains similarly minimally significant in further logit analysis, in spite of the addition of environmental controls that seem to explain the relationship between other structural factors and the dependent variable. There *is*, however, evidence to affirm the general expectation of a broad range of non-state actor behavior theories that centralization of organizational structure predicts a propensity towards more or less risky tactics. Specifically, there is an enduring suggestion that decentralized groups experience free agent issues in the minimal result for *market*-structured organizations controlled for in the analysis. However, though there *is* a more significant set of results for centralized structure across a range of models presented above, it is apparent that structure is predictively significant largely because of the intervening effect of variables included to control for a range of environmental pressures.

Chapter 3 presented four hypotheses and sets of expectations with regards to environmental pressures. They were:

H6: *Subversive groups facing government opposition (in the form of active investigation of group activities and/or law enforcement interdiction) will be less likely to move beyond digital activism in their ICT employments.*

H7: *Subversive groups facing widespread popular opposition will be less likely to move beyond digital activism in their ICT employments.*

H8: *Subversive groups with foreign-based sponsorship will be more likely to move beyond digital activism in their ICT employments.*

H9: *Subversive groups operating in a mechanically permissive environment (in the form of limited legal and technical barriers to operation) will be more likely to move beyond digital activism in their ICT employments.*

Results suggest both affirmation and null outcomes. There is marginal evidence that government opposition dissuades groups from choosing risky ICT employments, with the initial results are significant only at 90% confidence. However, the result does suggest a stronger link between government investigation and the propensity for deviant subversive activists to select between information enrichment and other more severe ICT employments. By contrast, there is no clear evidence to affirm H7 on the impact of popular opposition on group decision-making. Therefore, I reject H7 and affirm H6.

By contrast, though in line with the mixed evidence supporting H6, there is much more significant evidence to affirm both H8 and H9. Though variably significant, the results of testing in Tables 4.1, 4.2 and 4.3 suggest that foreign financial and/or capabilities sponsorship without requisite domestic sponsorship predicts decisions made by subversive groups to engage in digital antagonism, both in the form of information enrichment operations and more severe ICT employments. Likewise, results across all models strongly suggest that the there is a relationship between the mechanical permissiveness of an environment (i.e. the degree to which groups have access to capabilities and the degree to which such capacity translates to an ability to obtain outcomes) and group decision-making. Specifically, there are clear and significant results across all models that an imbalance in digital adoption trends at the national level predicts a higher likelihood of subversive group choices to employ ICT for digital antagonism. This relationship is further evidence in, as mentioned above, the unique manner in which the variable intervenes to alter results for organization structure.

The final hypotheses pertained to involvement of the transnational hactivist collective Anonymous in either direct or indirect support of the campaign efforts of a given subversive group. Again, the assumption was that the inclusion of a control variable for either evidence of direct sponsorship of or assistance by Anonymous agents would proxy for the significance of developing transnational *ICT-capable* support networks for dissentious non-state actors attempting to enhance their operations via the use of ICT. The stated hypothesis was:

H10: *Subversive groups will be more likely to move beyond digital activism in their ICT employments wherein there is evidence of direct sponsorship or assistance (coordinated or otherwise) in mitigative efforts by Anonymous agents.*

However, though there is a minimally positive result across all models, none are significant. I therefore reject H10.

Ultimately, a reasonably concise narrative emerges from this set of results. In short, subversive groups seem to be highly opportunistic and this opportunism seems to emerge from observation of environmental pressures in the context of group objectives. In many ways, this dynamic describes highly strategic decision-making that extends from rational, though bounded, cost-benefit calculations. I elaborate on this in the next section and articulate the clear theoretical perspective on subversion in the digital age that emerges from this analysis.

4.5. What Quantitative Testing Tells Us About ICT-Enabled Subversion

Clearly, there are a number of stories that might be told about subversive activism in the digital age. As such, there is naturally a challenge in the task of articulating theory appropriate for informing future efforts to problematize the subversive enterprise and to draw generalization for use in related research programs. Therefore, I suggest both theory – i.e. a falsifiable, testable analytic framework – and theoretical perspective in this section as I pose an answer to the two questions: (1) what explains subversive group decision-making in the context of the puzzle posed in previous chapters and (2) has the information revolution been uniquely impactful on the behavior of such non-state actors?

4.5.1. Key Determinants of Digital Antagonism

Given the evidence outlined above from quantitative testing and analysis, it seems clear that subversive group decision-making is primarily predicated on (1) whether or not a given group aims to replace an extant political system and (2) whether or not that aim is achievable. In the results presented above, no other variables so consistently predicted strong and significant variation on the dependent variable. Therefore, where the grievance is structural – i.e. explicitly focused on affecting structural revision (not simply policy modification) alongside ideational transformation – and not just focused on prevailing sentiment or opinion, groups are far more likely to employ ICT for shady and antagonistic purposes whilst also trying to digital engage the public than are their less revisionist cousins. Indeed, when specific forms of ICT usage are viewed through this lens

of "buy-in" or type of grievance, it seems clear that structural revisionists are far less sensitive to the costs and risks of shady and criminal ICT usage than are their counterparts. Structural revisionists are clearly more likely to escalate their use of cyberspace to more disruptive formats of interaction, including malware employments, tailored distributed denial of services (DDoS) attacks and direct, unauthorized tampering with hardware. Likewise, such groups are more likely to target government or military assets directly and to employ ICT disruptively even where there is a clear precedent of prosecution of such actions. And though no groups studied in the large-N analysis directly sponsor criminally violent acts (by definition), structural revisionists *are* also more likely to be linked to political violence in the form of sponsorship of/collaboration with more explicitly violent organizations, unsanctioned violent activity by members and links to past incidents of criminal violence.

Over and above this relationship between the nature of a group's grievance and online activities, there is a positive relationship between maximalist portfolios of grievances and the same. In essence, where a group's aims are stated broadly there is a greater likelihood that digital antagonism will occur. At first glance, one might be forgiven for developing a straightforward theory of self-assessment and decision-making amongst subversive groups from this quantitative analysis. Where there exists an assumption that subversion of national social and political conditions will entail a move to operate as a legitimate political force under current (or slightly modified) structural conditions, subversive groups are highly sensitive to the risks involved in what might be

seen as disreputable or illicit activities. Where this is not the case – i.e. where operation as a legitimate political force is not assumed to be premised on acceptance into extant processes – subversive groups adopt relatively risk dominant strategies.

Initial support for such a theory emerges not only from the direct result and descriptive evidence referenced above. Results for the nature of group grievances holds as strong and significant given the inclusion of a broad range of control variables. In particular, the inclusion of control variables in the large-N analysis above to account for the sponsorship of non-affiliates (i.e. not part of a group's functional sub-elements) indicate that the existence of foreign sponsorship without other forms of support positively predict variation on the dependent variable, even when other factors are controlled for. This indicates, again, that limited need for domestic support or legitimation is a key determining factor in the tactical outlook of subversive groups. In short, external sponsorship proxies for support beyond what might otherwise be needed in the domestic setting and compensates for the assumed need subversive groups have to garner internal support for transformative purposes. Likewise, there is suggestive evidence that lack of structural buy-in predicts greater propensity for commitment to or explicit linkages with criminal enterprise in several veins. Perhaps most notably, data on incidence and severity of denial of service attacks suggest that non-revisionist subversive activists utilize such techniques in a far more limited fashion than is the case for their revisionist cousins. Specifically, the data suggests that structural buy-in precludes the

decision to either spend large amounts of money on such assaults or to link a group with criminal enterprise.

Evidence in support of such a theory is both diverse and robust. However, the quantitative approach taken in this chapter can take us only so far. In reality, the mechanical nature of the relationship between subversive organizations, their objectives and instances of digital antagonism remains unclear at this stage. Thus, the next chapters outline additional findings from case study analyses that add to our understanding of the causal dynamics at play.

2.5.2. Digital Opportunism and Information Enrichment Operations

Before proceeding to case studies, however, there are clearly further implications of the results above as they relate to the question of the information revolution and non-state actor behavior in international affairs. Alongside the main result for the nature of group grievances, the data above shows that subversive activists most commonly employ what others have dubbed "twilight" techniques and "grey tactics" – low-intensity operations to, in this instance, digitally steal private data, to hide its redistribution, to disrupt opponents' activities and more wherein there is limited risk of attribution and blowback relative to the potential for favorable manipulation of the information environment. I label these *information enrichment operations*.

This distinction in the way that subversive groups employ ICT antagonistically is important because it allowed us, above, to think about severity of action. By extension, thinking about severity lets us then think about underlying drivers of the cultivation of

cyber conflict capabilities. And because we can tell the difference between more or less severe ICT employments, we can say something about the macro determinants of more or less sophisticated cyber conflict actors. Specifically, the data suggest that the digital environment is uniquely impactful when it comes to group decision-making, supporting a more general theoretical narrative that subversive groups are highly opportunistic because they opt to undertake information enrichment activities when there is a relative mismatch between the opportunities for digital gain and the capacity of governments to prevent, investigate or legislate such actions.

These findings are meaningful alongside evidence that addresses the puzzle being explored here because they constitute new knowledge on related points. The first finding regarding the general shape of subversive efforts to employ ICT antagonistically is interesting because it gels with recent literature that holds that state actors are, in the 21st century, increasingly possessed of the ability and incentive to operate in "grey" conflict spaces in international relations. The meaning of this is relatively simple. Increasingly, there are a range of abilities ceded to states by new digital technologies and new industrial processes that allow for operation for meaningful political gain below traditional thresholds of conflict initiation. Elkus, Malekos Smith, Mazarr and others have recently revitalized debate in about the manner in which such operations benefit state actors in the contemporary international environment. From prosecuting cyberattacks against localized elements of foreign critical infrastructure to building sand islands in contested maritime zones and using stolen information to create foreign

political scandal, new technologies are increasingly allowing nations to contest and irritate adversaries without risking major political or military backlash.

The findings above suggest that non-state actors are also significantly benefiting from and committing to the use of "grey tactics." Indeed, to the author's knowledge, this is the first study to empirically note and suggest that this is the case with non-state actors. Specifically, the results above empirically suggest that the information revolution has produced new space and new abilities for subversive dissidents to affect both disruptive and persuasive outcomes. More so than has been the case in decades past, radical non-violent dissidents *are* engaged in circumventive and disruptive efforts to degrade the strength of status quo forces, whilst at the same time attempting to digitally engage with the public. And yet, much of this activity takes the form of information enrichment operations designed to shape and improve the informational environment in which such actors operate. Contrary, perhaps, to the expectations of this study as set out in the dichotomous conceptualization of subversive behavior as criminal or otherwise, this category of low-risk/high-potential-gain is not as simple to characterize as traditional elements of the literatures on terrorism, insurgency and militant activism much lead us to think. Actions taken in this vein toe the line of permissibility and visibility. Too, tactics employed in this category are, in some cases, arguably more socially forgivable in the public eye than are traditional forms of criminal enterprise, either because actions can be masked or discounted by dint of the value of the informational outcome.

This category of techniques and organization capabilities simply has not meaningfully existed in decades past and there are significant implications for scholars, homeland security practitioners and threat analytic processes across military, intelligence and law enforcement. Of note, access to such new capabilities is perhaps more meaningful for non-state actors than they are for states, at least insofar as the portfolio of nation state security tools has always included some capacity to wage information warfare, to spread propaganda, to spy and more. As described in Chapter 2, subversion and propaganda are age-old instruments of statecraft and deception is so intrinsic to government doctrine on warfighting and intelligence gathering as to be a regular element of documents as prominent and diverse as Sun Tze's *Art of War* and Marx's *Communist Manifesto*. Though the 21st century has seen an expansion of this "grey" category of low-intensity possibilities for aggression and assertion between states, some actions have always descriptively fit this bill for states. For non-state actors, however, opportunities to be aggressive and to contest status quo conditions in a low-risk way without straying into the overtly criminal or violent are a rarity. Researchers would clearly do well to study this "new normal" of subversion further and to consider implications, a number of which are discussed in Chapter 12.

The second set of findings not directly linked to the main puzzle suggests that the operational contours of the digital environment present as reasonably impactful for decision-making amongst subversive activists. More specifically, these conditions seem to have unique modifying power insofar as the presence of an imbalance in national-level

adoption trends strengthens the predictive power of other explanatory variables. Though implications of this will be further discussed in Chapter 12 as well, a main takeaway for both researchers and practitioners is clearly that understanding the nature of information environment fragmentation presents as a pathway for better understanding non-state actor behaviors. Indeed, the results above not only back up an emerging consensus amongst scholars of cyber conflict issues that low-intensity operations are the norm of contentious interactions via cyberspace today; they also reinforce the notion that actor capacity in this vein inherently derives from environmental contexts. And, just as does the finding regarding IEOs, the digital adoption environmental results specifically provide support for the idea that the information revolution has produced new space and new abilities for non-state actors – particularly subversive dissidents – to affect both disruptive and persuasive outcomes. Naturally, further work is needed to explore the relationship between digital environs and the operational inclinations of such actors, not least so that governments and IGOs might marry cyber development and security initiatives to affect better deterrence and investigation outcomes.

4.6. Adding Nuance: Case Study Approach and Focus

This chapter engaged in testing designed to uncover the factors that explain decisions made by subversive activists to deviate from the expectations of past work in continuing to criminally employ ICT whilst functioning in the public eye. In investigating the explanatory power of different variables, results provide clear support for explanations that emphasize strategic perspective and prospects. Specifically, there is

strongest support across all models for H2: structural grievances are strongly linked to the decision made by subversive actors to maintain emphasis on digital antagonism whilst trying to digitally engage the public. The clear theoretical implication of this result is that buy-in to extant political systems tempers the inclination to engage in risky tactical behavior, while revisionism prompts risk-acceptance. Secondary support for this theory is strong across related results, particularly in the significant link between foreign sponsorship and digital antagonism.

As the previous section draws attention to, there are clearly a number of motivating and mitigating factors linked with the decisions such groups make to employ ICT in different ways. Indeed, the data outlined above suggest, almost more than anything else, that subversive groups are opportunistic and make bounded cost-benefit calculations in determining their courses of action. This is unsurprising. By their very nature, subversive groups are attempting to achieve a set of transformations wherein the contours of action and ideal outcome are dictated by prevailing status quo conditions. This inherently suggests that subversive actors *should* be highly adaptive. Further, the main result that structural grievance matters makes significant sense in the context of this broader narrative about opportunism. The emergence of new digital capabilities useful to subversive actors in efforts to enrich their operational environment in as low-risk a manner as possible suggests that explaining digital antagonism is a question of understanding (1) the propensity to accept great risk given (2) basic conditions necessary for digital operation.

And yet, as noted above, the mechanical nature of the relationship between subversive organizations, their objectives and instances of digital antagonism remains unclear at this stage. This chapter has found broad evidence linking strategic perspective and the operational nature of a given organization's environment to decision-making. But further work is needed and chapters 5-10 will now focus on the mechanical nature of these relationships. What is it about the way in which group's internalize and act on more or less revisionist objectives that prompts risky decision-making? And what is it about the digital environment that affects subversive group behavior? What cues do such groups receive that temper or modify campaign decisions?

Chapter 5
Case Study Overview

Christopher E. Whyte

In the chapters that follow, I extend the investigation of subversive groups' use of information and communications technologies (ICT) for antagonistic purposes to organizations operating in the Federal Republic of Germany and the People's Republic of China. The purpose in doing so is to assess the strength of those linkages outlined in results in Chapter 4 and to add nuance on the nature of causal mechanisms involved in subversives' ICT employments. In other words, I seek to both examine the nature of correlative relationships outlined previously and use evidence regarding the actions of different groups to adjudicate on the mechanics of the phenomenon. Specifically, given Chapter 4's notion that structural grievances dictate willingness to action antagonism via the web, what is it about that relationship that actually leads to cyber attacks, digital vandalism and broader illegal use of ICT?

This chapter has two objectives. First, I outline the argument being made in the context of the case study analyses contained in Chapters 6 through 10. Specifically, I describe the added nuance that emerges from these cases as it pertains to the broad trends described in Chapter 4. Then, I discuss the macro context of the cases involved –

national experiences with subversion and the freedom of action that groups are faced with in Germany and China. Here, I discuss the history of counterculture in both countries and how both have responded to counterculture and hacking in the recent past. Doing so sets the stage for better explication of the drivers of decision-making and incidence of digital antagonism across different organizations.

5.1. Case Study Results: The Argument

The evidence outlined in Chapter 4 suggests that subversive group decision-making is primarily predicated on whether or not a given group aims to replace an extant political system. In testing, almost no other variable so consistently predicted strong and significant variation on the dependent variable. Secondarily, analysis of the results of quantitative testing suggests that this is particularly pronounced where revisionism is broad-scoped (i.e. not attainable through a limited number of modifications). This point reinforces the notion that participation either has to be compatible with a subversive group's objectives or a feasible means to obtaining extreme transformation. Therefore, in sum, evidence shows that where the grievance is structural – i.e. explicitly focused on affecting structural revision (not simply policy modification) alongside ideational transformation – and not just focused on prevailing sentiment or opinion, groups are far more likely to employ ICT for shady and antagonistic purposes whilst also trying to digital engage the public than are their less revisionist cousins. But what is it about such revisionism that produces antagonistic outcomes more frequently than non-revisionist subversion? Does structural criticism directly manifest in executive-

level decision-making or is some other dynamic responsible for the greater frequency of disruptive and circumventive ICT employments among such actors?

Table 5.1 below outlines the case conditions, expectations and findings of each of the five cases included in subsequent chapters. Based on the findings of Chapter 4, expectations are clear-cut – variation on the dependent variable should occur primarily in line with the value for group grievances, modified by the type of agenda pursued and the degree to which domestic contestation exists.

Table 5.1. Summary expectations and findings across primary independent variables for case studies in Chapters 6, 7, 8, 9 and 10.

Group	Eastern Lightning	Civic Passion	Falun Gong	NPD	Die Linspartei
Type of Agenda	Idiosyncratic	Limited > Maximalist	Limited	Maximalist	Maximalist > Limited
Nature of Grievance	Non-Structural	Structural	Non-Structural	Structural	Structural
Permissive (Summary)	No	Mixed	No	Yes	Yes
Regime Type	Autocracy	Autocracy	Autocracy	Full Democracy	Full Democracy
Regime Durability	High	High	High	High	High
Contestation	Repressed Competition	Repressed Competition	Repressed Competition	High	High
Type of Structure	Bureaucratic (Pyramid)	Weak Bureaucratic	Mixed All-Channel	Hub-and-Spoke	Bureaucratic
Criminal History	Yes	No	Yes	Yes	No
Foreign Sponsors	No	No	Yes	No	No
Gov't Inquiry	Yes	No	Yes	Yes	No
Expectations	Minimal or no incidence of digital antagonism	Some incidence of digital antagonism	Minimal or no incidence of digital antagonism	Occasional incidence of digital antagonism	Pronounced incidence of digital antagonism
Findings	No incidence of digital antagonism	Punctuated incidence of digital antagonism	Consistent low-level incidence of digital antagonism	Punctuated incidence of digital antagonism	Punctuated incidence of digital antagonism

Analysis of organizations in Germany and China validates the broad relationship between revisionist organizations – and elements within an organization – and digital antagonism, and suggests that structural grievances do indeed (even beyond the use of ICT) produce a willingness to condone criminality. However, case study comparison suggests that revisionism *indirectly* produces antagonism. Far from seeing evidence of explicit executive-level direction of hacking or circumventive efforts, the content of the five cases presented in Chapters 6 through 10 suggest that there is a strong relationship between revisionism and the way in which groups interact with proxies that employ ICT antagonistically. Across cases, the sources of web tools and the initiative to disrupt regularly stems from peripheral elements of subversive organizations. With Falun Gong in China, for instance, group circumventive capabilities stem specifically from the tight-knit and more highly revisionist exile community of members living abroad that act as path-breakers and doctrine-setters in the absence of willingness to act among domestic members. With Civic Passion, the group's limited use of ICT antagonistically falls clearly within a period of time where group leadership was in disarray amidst apparently failed efforts to achieve transformation in a legitimate, participationist manner. And in Germany, the National Democratic Party of Germany, though mostly guilty of condoning the antagonism of others, has nevertheless actively supported an unstructured fringe element beyond traditional party sub-units – intended to act as a "people's front" – that has been responsible for a range of disruptive digital acts.

In short, a revisionist agenda clearly appears to (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone shady and criminal behavior among fringe members. As such, the narrative of subversive activists as digital antagonists is misleading in that there appears to be little executive direction, if any, involved in such deviation from the expectations outlined in Chapter 3. Instead, antagonistic activist organizations appear where circumstances make shady activity by free agents more likely. From the results of Chapter 4 and case analysis, it seems clear that an environment conducive to such a development most often emerges from limited interest in participationism alongside broad focus on targeted structural change. When such conditions prevail, the primary mechanism producing antagonism is the more permissive relationship that exists between party leadership and the functional fringe.

At the simplest level, this theory fits the dynamic seen in the results of basic correlation analysis in Chapter 3 that revisionism does not produce subversive hacker outfits so much it leads to the development and condoning of elements willing to hack. This theory also explains antagonism against expectations (i.e. those few instances where antagonism occurs with groups that don't generally espouse revision of political systems), such as in the case of Falun Gong. With Falun Gong, circumvention tools and expertise exist exclusively within the group's self-funded exile community; there is no evidence, aside from the publication of content deemed to be illegal in the short period following China's initial effort to ban Falun Gong, of homegrown antagonism. And the theory further explains variation in practices based on changing party objectives and

structures. With Die Linke, in Germany, antagonism – which admittedly manifested in a limited fashion in with group commitment to participationism – fell off following the 2005 party reorganization and manifesto streamlining. With Civic Passion, disruptive acts by affiliates and members have ceased in line with the reemergence of party leaders in 2015-2016 and decisions made to move away from social activism.

These narratives and the nuance they add to our understanding of subversive groups' uses of ICT circumventively and antagonistically are fleshed out through Chapter 10. Chapters 11 and 12 then recap the theory presented previously, consider specific markers that validate the theory and discuss implications for both policy and scholarship. The remainder of this chapter addresses relevant case content that nevertheless does not pertain to any one case study – the significance of national-level conditions. The following sections outline the different experiences China and Germany have had with counterculture, as well as the general approaches both countries take to censorship and repression of subversive groups. I then return to the question of national-level variation in country-level variables in Chapter 11.

5.2. Comparing Cases Across Countries

The remainder of this chapter explores counterculture in Germany and China. In Germany, largely *because* of Germany's strict laws and regulations on the shape of political advocacy groups, the two organizations described share a great number of characteristics and strategic approaches to persuasion. Both are revisionist entities; while they differ in the content of their messaging, both see the replacement of the current

political system in the far future. However, one organization – Die Linkspartei – has demonstrably committed to democratic participation as a legitimate approach to achieving political objectives. The other largely – the NPD – has not and, indeed, actively resists situational pressure to conform. In China, the opposite is true. The organizations are similar in that each faces repression and censorship from authorities on a number of fronts. However, each espouses remarkably different messages and aims for unique forms of social and political transformation. The question is, beyond the analytic narratives specific to each organization case, does national context matter? Do national conditions determine in any way the propensity a group has to employ ICT for shady behavior?

5.2.1. National Context: The History of Counterculture in Germany

The history of Germany is replete with examples of counterculture and organized subversion among groups aimed at fundamentally changing mainstream society. In the 100 years prior to World War II, in particular, Germany and its predecessor states were no less prone to the regular emergence of radical non-state social movements and political revisionists than were other countries in central and western Europe. The decades leading up to unification in the latter half of the 19th century saw the rise of a great number of cultural nativist organizations – what would afterwards become, for a limited time, separatist movements – resisting broad-scoped political changes in areas of Prussia, Bavaria and elsewhere. The early 20th century also saw the emergence of unique

countercultural associations like the famous intellectualist White Rose group[148] or the Swingjugend ("Swing Kids"), an Anglophilic movement of youth socialites that pushed back on the Nazi Party's rejection of British and American progressive social customs and gradually became a notable thorn in Hitler's attempts to reshape German culture.[149] Groups like the Swing Kids were common between 1919 and the early 1940s, though admittedly few acted in the political arena.[150]

Germany's experience with counterculture and active sociopolitical subversion has been more pronounced but less diverse since the end of the Second World War. The reasons for this, arguably, have entirely to do with the conditions of Germany's defeat in the war and the resulting experience of the country as a focal point of the Cold War. The division of the country into East and West augured an era of competing cultural perspectives formalized by the division between Soviet- and U.S.-influenced zones. West Germany rapidly rebuilt from the destruction visited on the country by Allied forces during the war to become a vibrant and notably progressive democratic state. East Germany's reconstruction was less remarkable in economic terms, but the country's significant role on the "front line" in the Eastern Bloc allowed the Soviet-installed communist government a degree of access to resources not afforded other Eastern European states. Throughout the 1950s, '60s and '70s, the experience of both Germanys

[148] For description, see Scholl, Inge. *The White Rose: Munich, 1942–1943*. Wesleyan University Press, 2011.

[149] See McDonough, Frank. *Opposition and resistance in Nazi Germany*. Cambridge, UK: Cambridge University Press, 2001.

[150] For a good overview of such groups operating up to and through the reign of the Third Reich, see Schattkowsky, R., Separatism in the Eastern Provinces of the German Reich at the End of the First World War. *Journal of Contemporary History*, *29*(2), 1994, pp.305-324.

with counterculture and subversion mirrored the broader global struggle of ideologies that defined the Cold War, with pro-democracy groups and communist organizations operating in each country with varyingly radical degrees of advocacy.[151] Likewise, both countries – uniquely aligned in their contempt for such forces – suffered the holdover influence of dispersed fascist organizations still loyal to the ideas, policies or persons that led Germany through defeat in 1945.[152]

Towards the end of the Cold War and in the almost three decades since the fall of the Berlin Wall, Germany's experience with subversion and counterculture has almost entirely revolved around a resurgence of right-wing nationalism in various forms. In reality, there *are* a small number of alternative countercultural organizations might be said to additionally qualify as subversive irritants to mainstream society. In particular, as will be seen in this chapter, there remain a shrinking number of highly radical left-wing entities. But here, as will be the case in reverse in later chapters' discussion of Chinese experiences with subversion, national context matters a great deal. By and large, the national culture and political perspectives the developed in Germany following World War II are probably best characterized by shared wariness of restrictive social

---

[151] Kahin and Kahin's excellent work on Eisenhower's clandestine counter-subversion policies contains perhaps the best overview of the nature of such groups in global context during the early part of the Cold War. See Audrey Kahin and George Kahin, *Subversion as Foreign Policy: The Secret Eisenhower and Dulles Debacle in Indonesia*, New Press, 1995.

[152] Overviews of the national experience during this period can be found in a range of works. For instance, see McGowan, Lee. *The radical right in Germany: 1870 to the present*. Routledge, 2014; Katsiaficas, George. "The subversion of politics: European autonomous movements and the decolonization of everyday life." *Atlantic Highlands, NJ: Humanities Press*, 1997; and Lee, Martin A. *The Beast Reawakens: Fascism's Resurgence from Hitler's Spymasters to Today's Neo-Nazi Groups and Right-Wing Extremists*. Routledge, 2013.

policy and common belief in the inherent value of a tolerant, participatory society. As with many Western states, the bar for qualification as a truly subversive entity – as opposed to a quirky interest group protected by tolerant norms and state laws – is extremely high. Sparingly few groups in Germany, one of which is discussed below, thus might be included in any analysis of Germany's contemporary experiences with subversion. In other words, Germany's ideological threat landscape notably lacks diversity.

Again, limited diversity of threats gives way to pronounced counterculture in the form of Germany's diverse ecosystem of far right social and political groups. From the mid-1980s to today, the number of neo-Nazi, racial supremacy and more generic far right organizations with conceptual ties to the National Socialism of the 1930s and '40s has gone up by more than 800%.[153] Naturally, this is somewhat due to the splintering of existing organizations, the evolution of one group into another and the branch development of different entities across German states. However, the past two decades in particular have seen a proliferation of new far right organizations and, more worryingly, the blossoming of a support base for various elements of the far right ecosystem. Support for more mainstream figureheads of Germany's right-of-center political parties has grown around issues related to the European Union's economic issues and the relationship

[153] Lee (2013), p. 27.

between German society and new immigrants to the country.[154] In particular, the past few years have seen the rising popularity of groups that take a hard line on accepting refugees and paying for efforts to integrate such immigrants quickly into German society. Of course, not all – or even most – of Germany's right-of-center advocacy can be considered to be subversive. In many cases, organized right-wing extremism (particularly in terms of member support) is best understood as a reluctant conservative reactionary shift away from progressive social developments. Nevertheless, the membership of extremist organizations has certainly expanded in line with the development of fault lines on issues related to apparent national cultural fragmentation and the past decade has seen a marked uptick of extremist activism (from traditional advocacy and protest to terror attacks).[155]

A key feature of Germany's increasingly pronounced, if not conceptually diverse, subversive landscape has been the move of radical perspectives online. Though not the case universally, many of Germany's new extreme activists are defined and are enabled entirely through their use of ICT. Much as is the case with subversive organizations – and more extreme groups – elsewhere in the world, German subversives – from the far right to the country's environmentalist factions – utilize ICT for targeted recruitment, for mass messaging, for coordination and the securing of logistical support, and occasionally for disruption.

---

[154] See *inter alia* Karapin, Roger. "Far-Right Parties and the Construction of Immigration Issues in Germany." *Shadows over Europe*. Palgrave Macmillan US, 2002, pp. 187-219; and Wodak, Ruth. *Right-wing populism in Europe: Politics and discourse*. A&C Black, 2013.

[155] A fact consistently noted in German government documents and non-profit reporting. See, for instance, 2005 Annual Report of the Office for the Protection of the Constitution, p. 17.

5.2.2. National Context: Approaches to Counterculture in Germany

The NPD and Die Linke operate in Germany under similar national-level conditions. Later chapters describe the extent of China's sophisticated censorship regime and the various tactics employed to allow Beijing a degree of social control. In contrast with that, Germany broadly practices almost no censorship and the rights of free speech and protest are enshrined in national law.[156] Beyond that, the German courts have regularly ruled in favor of anti-constitutional parties and a landmark 2016 case stymied efforts to ban such groups from receiving state funding, thus protecting small countercultural organizations from undue restrictions on operation.[157] There are, however, some specific exceptions to these protections.

One specific exception to the rule of thumb about censorship in Germany comes in the form of a 2010 federal law designed to censor child pornography.[158] This was a broadly supported proposal and remains a popular concession even among the government's staunchest critics.[159] Enforcement of the law, however, is a point of some controversy in Germany. In particular, law enforcement agencies have been accused of more broadly censoring regular pornography and explicit material on dozens of websites

---

[156] German constitutional document containing provisions for protection against censorship available at http://www.iuscomp.org/gla/.

[157] See "German politicians seek way to bankrupt 'neo-Nazi' NPD", Ben Knight. Deutsche Welle. January 20, 2017.

[158] "Kabinett beschließt Netzsperren gegen Kinderpornos" (German) (Cabinet approves blocking against child pornography), Pressestelle Bundesministerium für Wirtschaft und Technologie (Press Office Federal Ministry for Economics and Technology), 22 April 2009.

[159] "New German government reaches key internet security agreements", Neil King, Deutsche Welle, 15 October 2009.

over the past several years under the auspices of the 2010 law. This led to the law's repeal and, though there is no general criticism of the aims of such a law, the development of an enduring set of demands for keen oversight of Internet enforcement activities and better articulation of what might be banned.[160]

Though not a federal practice, a number of Germany's regional governments also take active measures to censor extremist political content. Specifically, neo-Nazi, fascist and racial supremacy content is censored primarily through removal from search results and the blocking of IP addresses of known extremist outlets.[161] Regional governments accomplish this through direct arrangement with ISPs and other companies like Google, and in doing so blur the line between censorship for incitement and general censorship of material deemed undesirable. The federal government has also solicited content removal from ISPs in recent years, though there was no blanket practice at the national-level until 2015 when the German government concluded an agreement with Google and social networking companies Twitter and Facebook to remove material deemed to qualify as hate speech.[162]

---

[160] German Internet blocking law to be withdrawn, EDRi-gram newsletter, European Digital Rights, 6 April 2011.

[161] Such censorship is enacted through observation of a dual set of provisions banning (1) indecent material and (2) anti-constitutional material. The latter category has a broad definition. Though it is generally agreed-upon that racist, homophobic, sexist and other discriminatory language qualifies under one or sometimes both provisions, explicit political disagreement *sans* incitement of overthrow or indecent messaging is generally protected. To what degree is the subject of a range of suits brought by government lawyers surrounding the question of banning the NPD since 2001.

[162] Conrad Chan, Anthony Dao, Justin Hou, Tony Jin, Calvin Tuong, "German Censorship Policy," 2011.

Broadly speaking, these specific actions taken to censor hate speech and incitement to violence constitute the main consideration for activists operating in Germany both physically and via the web. Any speech or action (such as the release of private identifying information obtained via illegal methods) opens such groups up to federal prosecution. Likewise, political speech that crosses the threshold – vaguely defined – of persecution of specific ethnicities, religions, etc. is subject to censorship.[163] In reality, however, the federal government has been remarkable slow to construct a universally employable method for finding and dealing with such content.[164] Moreover there are distinct obstacles to federal abilities to cast a wide net on this front. Sophisticated surveillance and interdiction capabilities are seen by many as authoritarian in nature and resisted based on civil liberties protection grounds.[165] Likewise, such capabilities would require buy-in from ISPs and technology companies – based both domestically and abroad – that simply does not exist at present. Rather, most takedowns of content or specific IP addresses occur through a report-and-react system wherein civil society organizations or individual citizens report offensive content to the authorities, which then act. There are many such groups operating in Germany, particularly focused on monitoring neo-Nazi and white supremacy movements. Again, however, there are a number of obstacles to censorship of hate speech in this way, from

[163] Ibid.
[164] Ibid.
[165] Efroni, Zohar, "German Court Orders to Block Wikipedia.de Due to Offending Article," *Center for Internet and Society Blog*, Stanford University Law School, 16 November 2008

unclear lines for reporting violations in some instances to the use of off-the-shelf means for ensuring more private content distribution by extremists.

Another macro condition that impacts upon how Germans go about using information technology is the broad popularity of hacker culture and ethics.[166] Germany is home to, among other groups, the Chaos Computer Club (CCC). CCC is a well-known hacker collective formed in the 1980s and active to this day. The collective's goals are variously to popularize the hacker ethos – which emphasizes freedoms of access, information and digital movement – through vigilante watchdog operations.[167] Group hackers famously used the web to steal large amounts of money (before returning it one day later) from a nation-wide credit exchange system to demonstrate the insecurities involved in emerging banking systems. They also published the fingerprint information of public officials to demonstrate the ease by which new scanners could be fooled and to protest the use of identification devices in 2008. Likewise, CCC was one of several pivotal publishers in 2011that put out details of Staatstrojaner, a surveillance program being used by state law enforcement to remotely search hard drives and otherwise access active use information (i.e. through taking screenshots, activating the camera, etc.).[168] These and other actions have popularized the collective and its mission. CCC holds a major annual event that is well attended by experts and international officials,[169] is

[166] For perhaps the best overview, see Steinmetz, Kevin F. *Hacked: A Radical Approach to Hacker Culture and Crime*. NYU Press, 2016.
[167] See ENCURVE, LLC. "Hacktivism and Politically Motivated Computer Crime," 2008.
[168] For full details offered by CCC on all counts, see https://www.ccc.de/en/.
[169] See "Hacks and Highlights of the Chaos Communication Congress," *Tech the Future*, 20 August 2014.

regularly invited on media programs and maintains an education outreach program. In short, CCC and Germany's white/gray hat hacker culture is broadly accepted as in line with national value sets.

5.2.3. National Context: The History of Counterculture in China

The People's Republic of China (PRC) has, in the past five decades, had a remarkably full history of combating homegrown dissident activity aimed at affecting broad-scoped transformation of norms and policy. Indeed, according to some sources, China has encountered at least 1,712 unique countercultural and revolutionary (in this case, counterrevolutionary) organizations operating within the state since the 1970s (See Table 1).[170] Not all of these groups are subversive in the sense outlined in previous chapters. Much of China's experience in countering homegrown dissent, perhaps particularly apparent due to the authoritarian nature of the national government, has dealt with localized protest to specific economic conditions, politics, business developments and more. In this way, any researcher studying China's engagement with dissident forces must recognize a basic categorical disparity between conceptual bases and official characterization of different actors – the Chinese Communist Party (CCP) regularly labels as subversive those who are merely engaged in basic protest or violent separatism.[171] Clearly, this is conceptually problematic, as the aims of many domestic "subversives" are policy modification, the removal of specific elites or terror more than

[170] See Wedeman, Andrew. "Enemies of the state: mass incidents and subversion in China." (2009), p. 10.
[171] Ibid, pp. 8-9.

they are a sea change in the normative status quo.[172] Nevertheless, past scholarship on unrest in China *has* produced significant evidence over time of counterrevolutionary activities by groups that can, in line with the definitions employed in Chapters 2 and 4, defensibly be labeled subversive.[173]

Perhaps more than any other fact, what is interesting about opposition to national status quos in the PRC is the extent to which unrest is organized across a range of different – often non-violent[174] – perspectives.[175] China boasts a large number of sectarian, ideological, cultural and civic groups that pursue political change through a variety of means.[176] In many cases, of course, PRC government objection to and interdiction of individuals linked to such groups is a matter of CCP security, not state security.[177] In other words, it is the action and function of the government as run by the Communist Party that official forces protect. At least some of the time, however, anti-

---

[172] For examples, see Kevin J. O'Brien and Lianjian Li, *Rightful Resistance in Rural China,* New York: Cambridge University Press, 2006; and Ralph A. Thaxton, *Catastrophe and Contention in Rural China: Mao's Great Leap Forward Famine and the Origins of Righteous Resistance in Da Fo Village,* New York, Cambridge University Press, 2008.

[173] See, for instance, in Manoucher Parvin, "Economic Determinants of Political Unrest: An Econometric Approach," *Journal of Conflict Resolution* 17:2 (June 1973): 271-96; Carl Minzner, "Social Instability in China: and Causes, Consequences, and Implications," Center for Strategic and International Studies, December 2006, available at http://csis.org/files/attachments/061205_Minzner.pdf, accessed March 29, 2017.

[174] The Dui Hua Foundation, "Statistics on Political Crimes in the People's Republic of China," Volume 3, Occasional Publications, no. 23, December 2006, p. 11.

[175] Wedeman, 2009, p. 2.

[176] Murray Scot Tanner, "China Rethinks Unrest," *The Washington Quarterly* 27:3, Summer 2004, pp. 138.

[177] State statistics label dissidents broadly as subversive or seditious. Between 2008-2009, almost 3,000 such dissidents were arrested in Xinjiang around various protests, riots and individual criminal incidents. Similar numbers were reported in Tibet in 2009. In both cases, most of those arrested were little more than street brawlers or individuals joining protesters in indiscriminate petty crime. See the Dui Hua Foundation, "Dialogue," 34, Winter 2009, p. 7 and the Dui Hua Foundation, "Dialogue," 35, Spring 2009, p. 2.

state protest is constituted of direct objection to government functions as illegitimate (i.e. the goal is not modification, but transformation or transformation by separation).[178] And even more commonly, particularly outside of China's coastal provinces, counterrevolutionary actions are regularly prosecuted by groups – from Protestant and Muslim organizations to ethnic separatists and liberal reformists – with fundamental grievances about the basis of the state of national culture and, secondarily, the supporting trappings of official policy. Given this, and despite the fact that such a statement might in some senses offend critics of oppression on the part of China's government, it does seem fair to say that the PRC is faced with a larger and more diverse body of dissident subversive threats than most other countries in the world.[179]

To say that subversion and counterculture in China is organized and diverse, however, is not to say that opposition to the PRC government in this radical format is particularly cohesive. While several prominent protest episodes and movements have garnered international attention and strong state responses in recent years, [180] organization of the threat to the Chinese state is fragmented, with political will, resources and support variable across the country's massive territory, population and intra-regional cultural diversity. Wedeman, in gathering data on mass protest and unrest in China, codes "inciting subversion" to simply mean the elements of the subversive

[178] For a discussion of the population of such groups in China and state responses broadly writ, see Stacy Mosher and Chine Chan, "Reviewing a Quarter Century of Political Crime," *China Rights Forum* no. 2, 2003.

[179] Wedeman, 2009, pp. 2-4.

[180] For a good overview of these particular protests in the context of international recognition and state response, see Weiss, Jessica Chen. *Powerful patriots: nationalist protest in China's foreign relations*. Oxford University Press, 2014.

enterprise devoted to persuasion and the encouragement of seditious behavior.[181] He then (appropriately, as his unit of analysis is acts, and not groups or group-based actions) captures various other elements and forms of the subversive enterprise in other categories of unrest, including illegal publication, propaganda, various kinds of espionage and heretical declamation. These cases appear below in Table 5.2:

Table 5.2. Documented cases involving counterrevolutionary organizations either accused of or investigated for state security endangerment offenses in China (1970-2009).[182]

Type	1970s	1980-4	1985-9	1990-4	1995-9	2000-4	2005-9	Total	Percent total
Counterrevolution	11	133	279	146	50	1		620	36.21
Heretical or reactionary sect		56	48	48	113	220		485	28.33
Disturbing social order and illegal demonstration		4	27	17	66	71	2	187	10.92
Inciting subversion			2		34	92	4	132	7.71
Espionage and state secrets		7	14	14	38	18	9	100	5.84
Violence			42	1	4	6	1	54	3.15
Separatism				1	17	18	16	52	3.04
Illegal business or publishing					28	8	8	44	2.57
Endangering state security					2	17	0	19	1.11
Other		1	2	3	3	1	3	13	0.76
Not specified				5		1		6	0.35
Total	11	201	414	235	355	453	43	1712	
Percent total	0.64	11.74	24.18	13.73	20.74	26.46	2.51		

Whereas other countries might be said to suffer from a relatively uniform set of counter-status quo forces or perspectives, however, he then notes that these cases involve more than 132 named groups within China that themselves tend to be relatively decentralized or linked to a network of affiliated organizations of varying levels of radicalism.[183] These include religious groups, liberal reformists, hardline communist organizations and more.

[181] Ibid, pp. 28-36.
[182] Data drawn from *Zhejiang Gong'an Nianjian* (浙江公安年), various years, cited in The Dui Hua Foundation, *Reference Materials on China's Criminal Justice System*, Volume 2, June 2009, pp. 23-26.
[183] Wedeman, 2009, p. 34.

And beyond this, as Table 5.3 outlines, individuals that do not hold membership in an organization have further been responsible for hundreds of dissident acts over time. China's dissident scene, quite clearly, is exceptionally fragmented.

Table 5.3. Documented cases involving counterrevolutionary organizations in China (1970-2009) by named groups.

Type	Frequency	Number of Individuals
No group		704
Sectarian	43	274
Protestant Sect	23	257
Falun gong	1	161
Political	24	119
Subversive	24	104
Communist	5	67
Uighur Separatist	4	29
Tiananmen	8	15
Catholic	2	11
Spy	3	8
Other	1	1
Protester	1	1
Subtotal	132	1032
Total		1736

Just as a clear trend in China's dissident scene (visible in Table 5.2's outline of cases by activity type) has been the diversification of perspectives and grievances driving active opposition to the status quo, so to have protest movements and subversive organizations increasingly moved online in attempting to actualize change in China. Given the sophisticated command of digital services and processes attained by the PRC government via social engineering, economic control of certain industrial developments and the construction of the "Great Firewall" for the purposes of censoring sociopolitical uses of the Internet, adoption of ICT for a range of dissentious activities has certainly

not proven to be a silver bullet of liberation.[184] Nevertheless, much has been the case elsewhere in the world, ICT afford Chinese opposition organizations great opportunities to obfuscate and mask activities, perform outreach and engage in disruptive protest.

5.4.2. National Context: Approaches to Counterculture in China

Each of the three groups described in Chapter X's discussion of subversion in the Chinese context operate under similar macro conditions. China is one of the world's foremost censors and the government in Beijing has had in place a sophisticated apparatus for quelling dissent and gathering information about the social and political activities of Chinese citizens for many years now. Chinese censorship essentially takes two formats. First, the state itself maintains a broad information collection apparatus that has broad-scoped purview and abilities to further PRC interests. Second, there exists a culture of and nepotistic economy for ensuring private sector buy-in to government control initiatives.[185] From building in design back-doors and sharing

---

[184] Brief discussion of different modes of digital censorship in China appears below. However, for further analysis of the state of information technology restrictions and the relative success of the PRC in determining the effectiveness of ICT employments by dissidents, see *inter alia* Diamond, Larry. "Liberation technology." *Journal of Democracy* 21.3, 2010, pp. 69-83; Diamond, Larry, and Marc F. Plattner. *Liberation technology: Social media and the struggle for democracy*. JHU Press, 2012; Christensen, Christian. "Discourses of technology and liberation: State aid to net activists in an era of "Twitter Revolutions"." *The Communication Review* 14.3, 2011, pp. 233-253; Hughes, Christopher R. "Google and the great firewall." *Survival* 52.2, 2010, pp. 19-26; and Ziccardi, Giovanni. *Resistance, liberation technology and human rights in the digital age*. Vol. 7. Springer Science & Business Media, 2012.

[185] For good in-context descriptions of this dynamic see *inter alia* Chase, Michael S., and James C. Mulvenon. *You've got dissent! Chinese dissident use of the Internet and Beijing's counter-strategies*. Rand Corporation, 2002; Walton, Greg. *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*. Rights & Democracy, 2001; and MacKinnon, Rebecca. "China's" networked authoritarianism"." *Journal of Democracy* 22.2, 2011, pp. 32-46.

customer information with Beijing, both state-run and fully autonomous enterprises across the board provide China the ability to enact a form of tailored censorship. The resulting doctrine and set of censorship practices emphasize social unrest risk mitigation balanced against effective suppression of dissent. Most commonly, this means suppression of efforts to mobilize opposition to the Chinese government rather than active suppression of individuals' speech, expect for (an admittedly large number of) highly specific cases of outspoken activism and celebrity.[186]

With regards to the efforts of subversive actors operating in China, the PRC government employs a range of tactics that blunt group activist efforts and, in some instances, prompt a digital response. Briefly, we might organize these tactics into six categories.[187] The first is direct cyber attack. Quite simply, the Chinese government is demonstrably engaged in military-grade cyber attacks against non-state opponents and related sponsors.[188] Increasingly through the 2000s, the websites and online member services of dissident groups opposed to Beijing's edicts, the CCP or specific elites are bombarded with malicious cyber activity. In many cases, dissident groups have endured weeks-long outages to web services such that there is a constant move to move content around. In other cases, journalists and activists have had data deleted and personal

[186] See King, Gary, Jennifer Pan, and Margaret E. Roberts. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107.02, 2013, pp. 326-343.
[187] See MacKinnon, 2011, pp. 39-42.
[188] See Morais, Richard C. "China's Fight With Falun Gong", *Forbes*, 9 February 2006; and Associated Press, *China Dissidents Thwarted on Net*. Retrieved 10 April 2017.

email accounts hijacked. In many instances, the targets of cyber attacks are foreign services or individuals engaged in enabling the activity of anti-Beijing dissidents.

The second category is device and network control activities. Despite problems with designing software that effectively monitors consumer behavior without leaking information to the public or to private firms, China has a long history of attempting to mandate that software be included in devices sold domestically wherein user content and credentials can be scanned for information.[189] At present, there are few nationally mandated examples of this kind of surveillance by infiltration but it exists on a massive scale across China's various administrative sub-units, with local councils and regional administrations sponsoring a broad variety of Internet Service Provider tracking initiatives.

Third, China has taken steps to affect control over dissident activity where there is no legitimate organization linked to such efforts. The main way that this has been done is through control over domain name registration domestically. For groups that are interested in using the .cn domain ending, there has since 2009 been a requirement that registration requires corporate bona fides *or* that individuals need a government ID in order to register. Sites owned by individuals have variously been shut down due to the

[189] See, for instance, Owen Fletcher, "China Clamps Down on Internet Ahead of 60th Anniversary," IDG News Service, 25 September 2009; available at *www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html*; and Oiwan Lam, "China: Blue Dam Activated," *Global Voices Advocacy*, 13 September 2009; available at *http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated.*

administrative control this gives Beijing and human rights groups regularly accuse the PRC of attempting to regulate the digital activities of freelance journalists.[190]

Fourth, the government has regularly resorted to disconnection tactics to control civil unrest. This tactic is not unique to China. Even the United States (or rather, U.S. states) has asked ISPs to cut network access to specific locales in unique situations. Nevertheless, China has shown great willingness to disconnect entire city sections and townships in times of crises. Doing so allows for crisis response in an environment of limited information leakage. Naturally, human rights activists and anti-Beijing protest groups claim that this gives Beijing a greater ability to undertake violent acts in suppressing revolt for a period of time, a fact that has been corroborated through examination of data on violence during periods of unrest in China. Possibly the best-known example of this, as well as one of the most extreme examples of forced disconnection, occurred in Xinjiang following ethnic riots in 2009 when Internet access was cut for more than six months.[191]

The fifth category of digital tactic employed by the Chinese government is traditional surveillance. China's surveillance capabilities are primarily rooted in state laws about the nature of criminal enterprise, specifically that it can include political dissent or the intent to cause societal unrest. Given these legal standards, the PRC has been able to institute a broad range of controls that provides information about the

[190] See, for example, Oiwan Lam, "China: More than 100 Thousand Websites Shut Down," *Global Voices Advocacy,* 3 February 2010; available at *http://advocacy.globalvoicesonline.org/2010/02/03/china-more-than-100-thousand-websites-shut-down.*

[191] See Josh Karamay, "Blogger Describes Xinjiang as an 'Internet Prison,'" BBC News, 3 February 2010; available at *http://news.bbc.co.uk/2/hi/asia-pacific/8492224.stm.*

population. These controls are different from the design-centric ones describes above because they are, in a legal sense, entirely legitimate. They include set statues regarding business functions and the monitoring of Internet connections in different kinds of public venues (to include private venues where the purpose is to provide Internet access, such as Internet cafes). They also include requirements placed on businesses to release information to the government with only minimal authorization from law enforcement upon the incidence of suspected acts of political dissent.[192] Naturally, this "legitimate" surveillance is objectionable and a great number of companies have taken steps to protect consumers. Unfortunately, in many cases this simply means that compliance efforts are localized in Chinese branch entities, allowing international companies to escape the spotlight on issues of surveillance and allowing Beijing to proceed with domestic monitoring unimpeded.[193]

Finally, the Chinese government undertakes what the Russians and Western counterparts might think of as "active measures" – essentially efforts to shape and manipulate sociopolitical discourse to achieve a desirable outcome (in this case, the mitigation of potential for unrest). To do this, Beijing sponsors an extensive cadre of personnel responsible for shaping content and for "astroturfing" to take part in citizens' conversations (essentially hiding the actual identity of an online conversant).[194] In the

---

[192] See Nart Villeneuve, "Breaching Trust: An Analysis of Surveillance and Security Prac- tices on China's TOM-Skype Platform," Open Net Initiative and Information Warfare Monitor, October 2008; available at: *www.nartv.org/mirror/breachingtrust.pdf*

[193] See MacKinnon, 2011, p. 41.

[194] See David Bandurski, "China's Guerilla War for the Web," *Far Eastern Economic Review*, July 2008.

broadest sense, the purpose here is to simulate grassroots efforts and to portray an image of diverse civil conversation around controversial issues that minimizes the potential of dissentious discourse. In reality, this tactic allows China to present itself as more progressive, more politically diverse and vibrant, and less traditionally authoritarian than might be the case.[195]

5.3. Next Steps

The next five chapters present case study analyses of the groups mentioned above – two in Germany and three in China. Each chapter includes a summary of each organization's portfolio of activism and antagonism, their experiences in employing ICT and those mechanisms that seem to most directly drive incidence of shady cyber activities. Presentation of evidence and narrative discussion of each case is then organized by variable categories first presented in Chapter 3 – those that relate to group structures, strategic objectives, environmental conditions and societal opposition. Chapter 11 then picks up the analytic thread by summarizing trends across cases, assesses specific sign markers that support this dissertation project's theory of digital antagonism by subversive activists, and discusses both shortcomings of this project and directions for future work.

[195] SCIO, "The Internet in China."

Chapter 6
Germany's Far Right:
The National Democratic Party of Germany

Christopher E. Whyte

In this chapter, I extend the investigation of subversive groups' use of information and communications technologies (ICT) for antagonistic purposes to organizations operating in the Federal Republic of Germany. The purpose in doing so is to assess the strength of those linkages outlined in results in Chapter 4 and to add nuance on the nature of causal mechanisms involved in subversives' ICT employments. In other words, I seek to both examine the nature of causal relationships outlined previously and use evidence regarding the actions of different groups to adjudicate on the mechanics of the phenomenon. With Chapter 4's notion that structural grievances dictate willingness to action antagonism via the web, for instance, what is it about that relationship that actually leads to incidents?

The chapter proceeds in four parts. First, I briefly summarize the case findings. Second, I outline the body of evidence regarding digital antagonism and the NPD. Then, I discuss the history and objectives of the National Democratic Party of Germany (NPD). Finally, I analyze the case with an eye to gauging the explanatory power of competing explanations for incidence of digital antagonism. I do so in parallel fashion

across each case study presented through Chapter 10, considering group perspective, structure and operating environments as possible explanations. Then, in Chapter 11, I present an overarching narrative based on evidence found in the following case studies, consider additional elements of each case that strengthen the emergent argument and discuss opportunities for future work.

6.1. Summary

The NPD is guilty of digital antagonism on a number of fronts. However, this antagonism is punctuated. Organization rhetoric and sponsorship is evident on several thousand far right websites in Germany, several dozen of which have been shut down and had site administrators pursued by law enforcement for espousing illegal positions (namely speech considered to be hateful or aimed at inciting violence). This basic use of the web, some of which is antagonistic by the standards of the German state and Germany society, has been almost constant since the mid-2000s. At various points since 2009, however, peripheral members and affiliates of the NPD have taken more severe steps in using ICT for shady purposes, including various instances of denial of service attacks, website vandalism and theft of state-produced private data on citizens. Of interest, while NPD leadership has at times appeared to directly condone and even direct such actions, there are also various instances in which officials have either denounced them or distanced their own political platforms from all but core NPD activities.

The NPD sees itself as bound to inspire a people's movement. As such, it has variously funded and encouraged the development of a loosely affiliated fringe of member

groups and individual advocates over the past several decades. While the core organization certainly sponsors far right websites and has been associated with hate speech on those sties in a number of instances, most digital antagonism emerges from this peripheral fringe. Furthermore, incidence of cyber vandalism, email spamming and more oscillates in direct relation to the line NPD leaders have taken around several inflection points since the 1990s where party political prospects have risen and dipped. In short, statements from NPD leaders and online mouthpieces changes in line with greater or reduced focus on legitimate participation to encourage (tacitly or explicitly) antagonistic behavior by supporters. At these times, cyber antagonism is particularly evident, suggesting that the decisions made by peripheral elements responsible for shady ICT usage are directly affected by how leaders express the methods and aims of the movement.

6.2. The NPD and Digital Antagonism

Beyond the sponsorship of right-wing websites that have occasionally been cited for hate speech, a sizable number of members of the NPD have been accused of or arrested for low-level denial of service (DDoS) attacks,[196] vandalism attempts[197] and information theft operations targeting left-wing groups[198] over the past three decades. Specifically, group affiliates launched three series of DDoS between 2008 and 2014 and

[196] Perhaps the best overview of such types of attempts is in Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes, 2013.
[197] 2005 Annual Report of the Office for the Protection of the Constitution.
[198] Ibid.

have been blamed for website vandalism in more than 23 instances since 2004. In each instance, NPD leadership has effectively distanced the organization from the actions of individuals, though in several cases provided the means for legal defense.[199] The NPD has also been linked to a broad range of spamming schemes wherein the use of illegal spamming software was used to send far right propaganda to a large number of constituents in Southwestern Germany ahead of regional elections.[200] And the group has been named in government documents, though never explicitly charged, as supporting the hack of left-wing websites and the subsequent release of user data.[201] At the same time, there is evidence to suggest that the group employs ICT for circumventive purposes. Group emails released through Wikileaks by Anonymous-backed hackers reveal a range of uses of ICT to hide NPD connections – both personnel and financial – with both extremist organizations either banned or under active state investigation.[202] In such cases, ICT usage ranged from simple use of email to a series of alternative messaging options. Likewise, the dissemination of demographic information revealed in leaked information suggests illicit access to state-held data and itself constitutes a form of doxxing.

---

[199] Such cases are outlined in Brandstetter, Marc: *Die NPD unter Udo Voigt. Organisation. Ideologie. Strategie*, Nomos Verlag, Baden-Baden, 2013.

[200][200] O'Brien, Kevin J., "Spam attack linked to German election," *New York Times*, May 19, 2005.

[201] 2005 Annual Report of the Office for the Protection of the Constitution, p. 36.

[202] These documents are partially available across several repositories, particularly in https://wikileaks.org/gifiles/docs/53/532157_central-europa-nazi-terrorism-npd-prohibition-strategic.html.

Though there has not been a full value change in the dependent variable over the modern lifespan of the NPD – i.e. the group has not clearly undertaken and then ceased (or vice versa) shady digital activities – such activities have become more pronounced since 2009. As the sections below show, this uptick in the frequency of cyber attacks and other illegal uses of ICT mirror the changing prospects of the NPD at the ballot box and in the public eye.

6.3. The National Democratic Party of Germany (NPD)

The National Democratic Party of Germany is one of Germany's two main ultranationalist political parties.[203] It is also one of the oldest far right organizations currently in operation in the country. The party was founded in 1964 from the union of a range of extremist organizations operating in West Germany to oppose the democratic reforms of the post-war government. Much like its various predecessor organizations, the NPD has never achieved its goal of broad electoral success at the highest levels in Germany. That is not to say, however, that the group is inconsequential. In truth, the NPD has regularly won seats in regional legislatures and councils for more the past half century,[204] though it has never breached the 5% vote yield threshold required for inclusion in the process of allotting seats in the German Parliament.

---

[203] For perhaps the best overviews of the NPD, see *inter alia* Von Mering, Sabine, and Timothy Wyman McCarty. *Right-wing radicalism today: perspectives from Europe and the US*. Routledge, 2013; Ackermann, Robert: *Warum die NPD keinen Erfolg haben kann – Organisation, Programm und Kommunikation einer rechtsextremen Partei.* Budrich, Opladen 2012; Philippsberg, Robert: *Die Strategie der NPD: Regionale Umsetzung in Ost- und Westdeutschland.* Baden-Baden 2009; and Mudde, Cas. "The far right and the European elections." *Current History* 113.761, 2014.

[204] Including a range of surging electoral successes through the late 1960s and into the '70s. See

The NPD is broadly considered to reflect a marginal and objectionable element of German society that advocates for racial nationalism and extreme modification of the policies of the German state.[205] In no fewer than four episodes over the past two decades, serious efforts have been made to officially ban the NPD and it's operations.[206] In each instance, requests in this vein have enjoyed massive popular support and the official sponsorship of elements of the national government. In each case, however, Germany's courts have erred on the side of protecting basic civil freedoms to speech and assembly.

Massive opposition to the NPD in Germany pivots on the group's radical philosophy and is magnified by the clear historical tie to National Socialism in the 1930s and '40s. Politically, the group favors a reimaging of the federal boundaries and jurisdiction of the German government. Briefly, the NPD seeks a return of all territories lost at the end of World War II to expand the federal limits of Germany into areas with German-speaking peoples.[207] The group also rejects the current version of European supranationalism as a circumcising reorganization of the continent that harms German

---

Chapin, Wesley D., *Germany for the Germans?*. Greenwood Publishing Group, 1997.

[205] McGowan (2014), p. 38. Also see the NPD party programme (in German) http://npd.de/inhalte/daten/dateiablage/br_parteiprogramm_a4.pdf.

[206] These attempts are variously described in Brandstetter, Marc: *Die NPD unter Udo Voigt. Organisation. Ideologie. Strategie*, Nomos Verlag, Baden-Baden, 2013; Ackermann, Robert: *Warum die NPD keinen Erfolg haben kann – Organisation, Programm und Kommunikation einer rechtsextremen Partei.* Budrich, Opladen, 2012; Brandstetter, Marc: *Die „neue" NPD: Zwischen Systemfeindschaft und bürgerlicher Fassade. Parteienmonitor Aktuell der Konrad-Adenauer-Stiftung.* Bonn, 2012; and Mudde, Cas, "Germany wants to ban the neo-Nazis of the NPD again, but why now?" *The Guardian*, March 4, 2016.

[207] Party program, p. 13. ("Deutschland ist größer als die Bundesrepublik! ... Wir fordern die Revision der nach dem Krieg abgeschlossenen Grenzanerkennungsverträge.")

influence and interests.[208] Much as is the case with designs on German society and domestic politics, these positions are rooted in a range of criticisms of foreign cultures and individuals. The NPD has opposed Turkish accession to the European Union on cultural-linguistic grounds and has articulated a broad platform of border control and anti-immigration policies for both Germany and Western Europe. At home, the NPD's rhetoric and teachings pivot on an interpretation of natural law that holds individuals emerge from their unique cultural roots as unequal. In a manner harking back to the Nazi Party's own teachings, members of the organization claim the inherent inferiority of individuals from foreign cultures and racial stock, particularly from Africa and the Middle East.[209] In short, widespread opposition to the NPD and support for efforts to suppress the organization pivot on the shared (and arguably quite reasonable) assessment that the group's homophobic, anti-Semitic, racist, nativist and misogynistic philosophy is entirely incompatible with contemporary Germany society.[210]

Though the organization is more than half a century old, the rise of the NPD to national prominence over the past three decades seems uniquely linked to its wholesale adoption of information technologies for spreading influence. By 2009, more than 1,700 neo-Nazi German websites could be found online, almost a third of which were directly linked to the NPD.[211] By 2016, this number had pushed beyond 3,000.[212] Both website

---

[208] Ibid, p. 12.
[209] Ackermann (2012).
[210] And indeed, words to this effect have been included in virtually every Annual Report on the Protection of the Constitution of Germany since 2004.
[211] Caiani, Manuela and Parenti, Linda, *European and American Extreme Right Groups and the Internet*, Routledge, 2016, p. 43.

development and the adoption of abroad range of alternative communication platforms are focused on outreach to Germany's youth. Indeed, Germany's far right stands as a phenomenal example of how Web 2.0 technologies can expand the demographic footprint of an organization. The NPD's websites, much like those of other far right groups, makes extensive use of music, video and interactive portals designed to help build communities centered on the organization (or, more specifically, on sub-entities like the Junge Nationalisten, NPD's youth wing).[213]

Given the size of the organization, it is perhaps unsurprising that the casual observer might see the NPD as having rarely been involved in highly visible employments of ICT for disruption and antagonism. However, as noted above, the group *has* been tied in official government reporting and, on occasion, in legal actions to such acts. Indeed, despite reasonable ability to mask such actions, it is clear that the NPD has regularly engaged in digital antagonism designed to mitigate the efficacy of societal opponents, recruit youth and reach targeted audiences at critical junctures.

6.4. Case Analysis: Competing Explanations for Digital Antagonism

What factors influence the decision these German subversive organizations have made to either employ ICT antagonistically alongside broader activist efforts or not? Where no clear decision was made, what factors nevertheless most causally seemed to determine incidence of digital antagonism? In this section, and in similar sections in each

---

[212] Ibid, p.43.
[213] Ibid, pp. 43-44.

case chapter to follow, I break down the history and context of each group's use of ICT over the past two and a half decades using the various hypotheses outlined in Chapter 3 as a guide for structuring the narrative. In particular, I focus on those factors highlighted in Chapter 4 as those most closely tied to incidence of antagonism by subversive activists.

In each case, I take steps to consider not only the direct variation in outcomes predicted by each hypothesis, but also variation in related factors. Doing so is necessary for any effort to determine the significance of any one set of driving forces. Specifically, with each unique type of possible explanation, I consider the overall shape of the relationship between driving factors and the dependent variable before focusing on features of group experiences that might disproportionately suggest significance (critical junctures and secondary driving forces). I then return to the hypotheses in the next section to discuss. To briefly recap, with the NPD there is clear evidence of antagonistic ICT usage across the period studied. Incidents of such in the NPD's experience are punctuated, however, with no clear campaign being waged. The next section discusses the experiences of the NPD in employing ICT in-depth, asking how the group has institutionalized information technology adoption and what institutional mechanisms appear to either impede or encourage use of ICT for circumvention or disruption?

6.4.1. The NPD: Aims, Structure and Environment

Subversive Objectives. The National Democratic Party of Germany is an ultranationalist political organization. The party sees itself, in essence, as the sole

legitimate successor to the traditions, values and beliefs of the National Socialism of the 1930s and '40s.[214] Though it is not the direct successor of the Nazi Party – no organization is – it emerged from German Reich Party in the mid-1960s, a group constituted of large numbers of previous members of the Nazi Party and their children.

As noted above, the primary philosophical belief of the NPD is the natural law notion that human beings can be inherently superior than others based upon a range of factors, including ethnicity, nationality, culture of origin (and perpetuations thereof through family ties, etc. amongst immigrant populations), language and religion.[215] From this simple proposition springs a great number of assertions that situate the NPD on social, economic and political issues in Germany. Broadly writ (and echoing the national socialist messaging of Mussolini and Hitler), the NPD sees liberal democratic and communist formats of political rule as inherently set up for plutocratic developments – for control of governance by the wealthy. Oligarchic political machinations feed off of a capitalist infrastructure and weak social understanding of the sources of national vigor to produce a liberal version of Germany – the current one, that is – that does little to further German national interests.[216]

In many ways, the far right and far left in Germany share a unique combination of characteristics. When it comes to defining the nature of organizational grievances,

---

[214] This is evident in both statements and official publications of the NPD. See, for instance, Party program 2012, p. 16. ("Deutschland ist größer als die Bundesrepublik! ... Wir fordern die Revision der nach dem Krieg abgeschlossenen Grenzanerkennungsverträge.").

[215] Ackermann, Robert: *Warum die NPD keinen Erfolg haben kann – Organisation, Programm und Kommunikation einer rechtsextremen Partei.* Budrich, Opladen 2012.

[216] Von Mering, Sabine, and Timothy Wyman McCarty. *Right-wing radicalism today: perspectives from Europe and the US*. Routledge, 2013.

both Die Linke and the NPD are clearly structural revisionist entities that seek the eventual abolition of contemporary German political processes. True, Die Linke might seek to replace elements of Germany's political infrastructure with bodies resembling those of today's liberal democracy (i.e. there is a role in communist/socialist systems for legislative representation *alongside*, among other things, the secretariat). But both clearly seek to bring into being an alternative vision of Germany that differs from that of today in *both* normative and structural terms. The NPD seeks the abolishment of today's democratic constitutionalism and a nationalist, expansionist form of government.[217]

Likewise, both the NPD and Die Linke have for the entirety of their contemporary existences eschewed violent overthrow and embraced parliamentary participationism as necessary.[218] Much like the slightly more successful Left Party, the NPD regularly receives between 1% and 4% of the national vote, earning seats across a smattering of regional legislatures (though not in the Bundestag), and has found new support in the wake of the European refugee crisis that began in 2014-'15.[219] In short, both the far left and the far right in Germany are revisionist entities that nevertheless buy-in to the current political setup.

---

[217] A position held across annual government reporting on both organizations over the past two decades. See, for instance, statements in the Annual Report[s] (on the Protection of the Constitution) in 2001, 2004, 2006 and 2011.

[218] For the NPD, see apabiz e. V.: *Die NPD – Eine Handreichung zu Programm, Struktur, Personal und Hintergründen.* Zweite, aktualisierte Auflage. 2008. Die Linke is discussed below.

[219] See *inter alia* Zicht, Wilko. "Wahlergebnisse" (in German). Wahlrecht.de. 2014.

The expectation set by Chapter 4's positive results for H1 and H2 suggests that we should see deviant behavior by revisionist groups and by those with maximalist policy portfolios. With the NPD, despite participationist efforts, that certainly seems to be the case. Beyond the use of ICT, the NPD and affiliated members of the party have been linked with hate speech, with support for violence during protest events and with involvement in criminal enterprise (most often arson and property destruction in, for instance, immigrant neighborhoods).[220] With information technologies, the NPD has been linked with a broad number of efforts to circumvent increasing government efforts to censor hate speech, with the online publication of hate speech and with basic disruptive attacks against societal opponents.[221] Most commonly, NPD content has been spread illicitly via the use of spamming software purchasable on the web.[222] Six separate instances of this kind of spamming exist between 2000 and 2014.[223] Likewise, group emails released through Wikileaks by Anonymous-backed hackers reveal a range of uses of ICT to hide NPD connections – both personnel and financial – with both extremist organizations either banned or under active state investigation, as well as group use of demographic data not available to the public.[224]

Conjecturally, the crime fits the profile we might expect for the NPD. Moreover, through Wikileaks there exists direct confirmation of foreknowledge of illicit uses of ICT

[220] Ackermann (2012), p. 45.
[221] Ibid, p. 52. Also see Chan et al. (2011); Caiani and Parenti (2016), p. 142; and 2004 Annual Report of the Office for the Protection of the Constitution, p. 67.
[222] O'Brien (2005).
[223] Ibid.
[224] Available at https://wikileaks.org/gifiles/docs/53/532157_central-europa-nazi-terrorism-npd-prohibition-strategic.html.

by group leadership. On October 3, 2009, for instance, Herman Leip wrote in an email exchange that he expected "new turnout data" to be of specific use in targeting messaging for the upcoming local elections in Saxony.[225] Moreover, group leaders have expressed clearly their approval of the illegal spread of NPD content even where it appears that a non-NPD mouthpiece is to blame for the actions. In May of 2011, Udo Voigt wrote to colleagues that "the front [was] spread[ing] the word to new minds"[226] and went so far as suggesting the possibility of future sponsorship (or of encouraging off-the-books sponsorship) of fringe far right elements undertaking criminal acts to aid the NPD in saying "we must and will take every step needed to forward the People's Front."[227]

And yet, it cannot be definitively said that NPD leadership does more than support the use of ICT antagonistically. Though there is conjectural evidence of complicity in the use of stolen data, this information could have been obtained in a number of ways that do not mean NPD responsibility for the initial theft. Moreover, most ICT employments are by actors either claiming NPD patronage or disseminating NPD messaging. Supporters of the NPD linked to website defacement in 2007 and 2009, for instance, were not card-carrying members, but rather occasional attendees of meetings and online fans of the movement.

Organizational Processes. Has the NPD's use of the web and web tools been shaped by the structure of the organization itself? Though there is a clear link here

[225] See https://wikileaks.org/gifiles/docs/53/532159.
[226] See https://wikileaks.org/gifiles/docs/53/532163.
[227] See https://wikileaks.org/gifiles/docs/53/532192.

between the NPD's broad-scoped structural revisionism and incidence of antagonistic ICT usage, the simple answer has to be yes. The clearest mechanical explanation of group involvement in such employments has to do with the unstructured fringe that the NPD not only tolerates, but actively supports. Digital antagonism is, thus, not a choice made by group leaders so much as it is intended by them and actioned by a broad range of variously capable civil society actors that claim NPD patronage.

Structurally, the NPD looks like many political parties around the world.[228] The party has a federal executive board that directs a series of state associations in accordance with German national law. The chair of that federal executive board, currently Frank Franz[229] and, before him, a hardline national socialist called Udo Pastörs,[230] leads the party. Broadly, the NPD has three sub-groups or organizing divisions – the Junge Nationaldemokraten ("Young National Democrats"), the Ring Nationaler Frauen ("Ring of National Women") and the Kommunalpolitische Vereinigung der NPD ("Local Politics Union of the NPD").[231]

However, though the NPD enjoys almost no external sponsorship itself,[232] the party maintains a "people's front of the nationals" beyond the traditional party structure

---

[228] Indeed, because of the stipulations of the Act on Political Parties of 1994 in Germany, the NPD looks extremely similar to other political parties operating in Germany. This common structure and set of requirements surrounding organizational responsibilities is common to the NPD and Die Linke, ensuring a core set of similar variables for the purposes of analysis in this chapter.

[229] See http://frank-franz.de/.

[230] See https://www.landtag-mv.de/index.php?strg=3_45&modStrg=5&baseID=45&memID=101.

[231] See 2005 Annual Report of the Office for the Protection of the Constitution, pp. 79-83.

[232] O'Brien (2005).

that includes a great number of non-members and a sizable network of militant far right groups, some of whom have links with criminal and terrorist elements.[233] This fringe part of the organization is, in many ways, difficult to draw a line around for the purposes of this analysis. Though the many individuals and groups involved are not among the NPD's sub-organizations or the roughly 7,000 active members,[234] there is strong evidence that they receive financial support, benefit from NPD coordination and claim without contest the patronage of the NPD's cause.[235] According to government reports from 2005, 2007[236] and 2011,[237] this fringe includes perhaps as many as three-dozen neo-Nazi and other far right local groups. Nearly half of these have been involved in criminal acts, from vandalism to arson and physical assault.[238] Four groups that receive NPD funding play a coordinative role with two other main far right political organizations – one in Germany and one in Austria.[239]

The existence of such an unstructured element underneath the clearly structured official party setups *does* make sense insomuch as the purpose of maintaining such a fringe is the cultivation of a "German people's movement" that will aid the NPD and

---

[233] "Report of the Verfassungsschutz". Verfassungsschutz.de. April 19, 2014.

[234] The group grew from about 5,300 active members in 2004 to just more than 7,000 by 2006. See
Jennifer L. Hochschild; John H. Mollenkopf (2009). *Bringing Outsiders in: Transatlantic Perspectives on Immigrant Political Incorporation*. Cornell University Press. p. 147; and "Verfassungsschutzbericht 2008". Verfassungsschutz.de. May 2009. p. 79. Retrieved 23 August 2009. "Mit rund 7.000 Mitgliedern verzeichnete die NPD im Vergleich zum Vorjahr (7.200) einen leichten Rückgang, bleibt jedoch mitgliederstärkste Partei im rechtsextremistischen Spektrum."

[235] See Caiani and Parenti (2016).

[236] See 2007 Annual Report of the Office for the Protection of the Constitution.

[237] See 2011 Annual Report of the Office for the Protection of the Constitution.

[238] Ibid.

[239] Ibid.

others in restructuring German society. As is the case with many subversive groups, the NPD understands that transformation requires organic popular support. The unstructured fringe around official NPD organizations and activities provides a direct connection to that kind of potential movement and the means by which the NPD might direct support that exists outside the party.

In this context, the NPD's digital antagonism is not so much a directive from on high but broad condoning of irregular use of digital technologies by the far right movement punctuated by timely support – either coordinative or rhetorical – given to those on the fringe. By far, most incidence of digital antagonism linked with the NPD involves members of the fringe element of the party.[240] In 2002, website vandalism in Saxony of local far left activists was linked to teenagers whose parents were NPD members.[241] Between 1999 and 2014, spamming attributed to a niche ultranationalist social group in Bavaria has included direct links to NPD content,[242] a fact that group leaders have lauded as patriotic expression of preference.[243] And apparent possession of state roll data revealed through Wikileaks reporting has been linked with federal cases on intrusion into and theft of data from regional census bureaus in Bremen and Western Pomerania against three hackers sympathetic to the far right between 2012 and '13.[244] In short, there is clear evidence to suggest that the benefit accrued to the NPD by

[240] Caiani and Parenti (2016).
[241] Ibid.
[242] Ibid.
[243] See https://wikileaks.org/gifiles/docs/53/532192.
[244] Ibid. Also see https://wikileaks.org/gifiles/docs/53/532163 and https://wikileaks.org/gifiles/docs/53/532159.

antagonistic ICT employments comes directly from the contribution of fringe elements of the broader subversive movement. Though the group certainly condones both traditional and digital antagonism, willingness to hack appears not to be an executive-level imperative. Rather, it appears to be the choice of free agents who receive no discouragement from a revisionist patron.

Support and Opposition. Finally, has the nature of support for or opposition to the NPD and its platform shaped group ICT usage? The simple answer is yes – perception of support seems to drive tactical choices, expressions of which then play a role in encouraging antagonism.

To the casual observer, it might certainly seem that the NPD has enjoyed increasing support over the past few decades and, in particular, since the 2009 elections. However, that increasing support is relative to the sharp decline in national support experienced within a decade of the party's founding. The NPD's highest electoral tally of seats came only five years after the party's founding in 1964 as an amalgamation of other far right groups in Germany. In the elections of 1965 and '69, the NPD pulled 1.8% and 3.6% of the total vote respectively.[245] Though the party has never breached the 5% threshold for election of members to the Bundestag,[246] 1969 came close and demonstrates how enduringly appealing an alternative National Socialism was to the dominance of liberal capitalist parties in the post-war transformation years. Following the country's reconstruction and the incorporation of war-guilt in new generations of

[245] Caiani and Parenti (2016), p. 35.
[246] Zicht, Wilko, "Wahlergebnisse," Wahlrecht.de. Retrieved 9 April 2017.

young Germans, however, the story of the NPD has until recently been one of membership contraction and minimal electoral success at the regional level. Between 1976 and 2002, support for the NPD plummeted and electoral draws consistently netted between 0.1% and 0.5% of the total vote count.[247] Simply put, for most of the Cold War period and much of the post-Cold War period, there has been only marginal support for a party that is seen by many as an enabling platform for neo-Nazi violence (both structural and direct) and overwhelming support for government attempts to legally ban the organization. Since 2002, electoral draws have risen to between 1.5% and 1.8%.[248] However, this boost at the national level is really a function of greater support for the NPD in a few specific areas like Mecklenburg-Western Pomerania and much of the NPD's gains since 2002 seem to relate to the broader support for conservatism in policy-making championed by sister groups like *Alternative für Deutschland*. Elsewhere, the NPD has sunk below even the 5% threshold of electoral support at the state level, leaving a single elected official (the party chair, Udo Voigt, an MEP) in the party's ranks.[249] The reality is that the NPD, though as present in German politics as they have ever been, is losing the small pieces of ground it holds in all but a few areas.

This diminishment of the NPD in the public eye is, naturally, a relative decline insomuch as Germans' overwhelmingly object to the group and support the banning of

[247] Caiani and Parenti (2016), pp. 36-39.
[248] Ibid, p. 40.
[249] Ibid, p. 40.

the party.[250] A primary reason for the decline of the NPD relative to the rise of new far right groups like *Alternative* is the refusal to separate party dogma and platform from the history of National Socialism – and, thus, of Adolf Hitler and the Nazi Party – in Germany.[251] Whereas the NPD maintains a broad portfolio of grievances in line with the rich history and philosophy of fascist thinkers in Europe, other radical far right groups in Germany, Austria, Spain, Italy and elsewhere have taken active steps to distance themselves from the fascism of the 1930s and '40s.[252] Instead, such organizations focus on specific policy issues related to immigration, conflict in the Middle East and more.[253] Though similarly anti-Islamic, anti-Semitic and nativist positions are still the bread and butter of such campaigns,[254] the perspective presented to voters is a shorter hop from mainstream discourse on such topics.

Though the NPD has experienced lulls in support before, this inability to distance the party from its Nazi origins increasingly hurts among conservative Germans that, at one point, were at least open to the group as a protest choice. This is particularly true when considered alongside the rise of extensive government opposition to the NPD in the form of active efforts to ban the groups between 2001 and 2017.[255] On no few than five occasions, the federal government has brought cases to the Constitutional Court to ban the NPD and to force the disbanding of the organization on

[250] Ibid, p. 61.
[251] Peter Davies, Derek Lynch, The Routledge companion to fascism and the far right, Psychology Press, 2002.
[252] Ibid.
[253] Ibid.
[254] Ibid.
[255] Caiani and Parenti (2016).

hate speech and incitement grounds.[256] On top of these proceedings, which have failed to produce a verdict against the organization itself, police actions against the NPD have multiplied in recent years based on rampant accusations of, among other things, incitement of racial hatred through publications and private communiqués.[257]

The lens of decreasing public support in all but a few regions of Germany and the increased frequency of state-led efforts to ban the party do provide a correlative explanation for choices made by group leadership to either action or condone the use of ICT antagonistically. In 2015, for instance, seat losses in elections in Saxony and elsewhere were followed by defacements of the websites of left-wing party opponents of the NPD.[258] Group leaders actively condoned the intrusions as understandable and a natural reaction to what Voigt decried as liberal misinformation employed during the campaign season.[259] Likewise, NPD-linked incidents in 2009[260] and 2015[261] involved the use of email spamming software to incite racial hatred and to disseminate stolen government roll information specifically in areas and against candidates deemed to be direct obstacles to NPD electoral success.

However, just as noted above, there is little in the way of clear evidence – in public statements, Wikileaks divulging of emails, etc. – that NPD leadership authorizes the use of ICT for disruptive purposes. Again, the most compelling link between national

[256] Ibid.
[257] Ibid.
[258] Ibid. Also see Mudde, Cas, "Germany wants to ban the neo-Nazis of the NPD again, but why now?" *The Guardian*, March 4, 2016.
[259] Ibid.
[260] "NPD – einzige ernstzunehmende nationale Kraft!". npd.de. 28 September 2009.
[261] Caiani and Parenti (2016).

conditions of support/opposition and incidence of digital antagonism is the nebulous, unstructured fringe supported by the NPD as a "people's front." According to Caiani and Pareni, this fringe is constituted largely of activist elements – many extreme – linked to the NPD's traditional voter base in Western Pomerania and elsewhere.[262] The pattern that emerges from the case of NPD ICT antagonism is one of frustration among proxies wherein uncoordinated elements of the broader activist base that the party supports broadly interpret their mission to include the mitigation of opponents and protest of "unfair" treatment.

6.5. Conclusion

In conclusion, case study comparison suggests that revisionism *indirectly* produces antagonism. Far from seeing evidence of explicit executive-level direction of hacking or circumventive efforts, the analysis above suggests that there is a strong relationship between revisionism and the way in which groups interact with proxies that employ ICT antagonistically. Across cases, the sources of web tools and the initiative to disrupt regularly stems from derivative elements of subversive organizations. The NPD, though mostly guilty of condoning the antagonism of others, has nevertheless actively supported an unstructured fringe element beyond traditional party sub-units – intended to act as a "people's front" – that has been responsible for a range of disruptive digital acts. This notion – that a revisionist agenda clearly appears to (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone

[262] Ibid.

shady and criminal behavior among fringe members – will be explored further in the next chapter's study of Germany's Left Party.

Chapter 7
Germany's Far Left:
Die Linke

Christopher E. Whyte

This case chapter investigates the experiences and history of Germany's primary far left chapter party organization – the Left Party – with ICT. The chapter proceeds in four parts. As with Chapter 6, I briefly summarize the case findings. Then, I outline the body of evidence regarding digital antagonism and the Left Party. Third, I discuss the history and objectives of the Left Party. Then, finally, I analyze the case with an eye to gauging the explanatory power of competing explanations for incidence of digital antagonism. Again, I do so in parallel fashion across each case study presented through Chapter 10, considering group perspective, structure and operating environments as possible explanations. Then, in Chapter 11, I present an overarching narrative based on evidence found in the following case studies, consider additional elements of each case that strengthen the emergent argument and discuss opportunities for future work.

7.1. Summary

In many ways, Die Linkspartei's experience is a flipped version of the NPD's. Just like the NPD, Die Linke has rarely – if ever – directly sponsored digital antagonism.

What incidence of digital antagonism exists emerges from the actions of fringe organizations and peripheral members of the core party. Whereas the NPD's fringe has expanded and has arguably been empowered to act with greater discretion in line with the party's downward trajectory in legitimate political processes, the Left Party acted in the mid-2000s to formalize its fringe into a political coalition that was then subsumed into the main party entity. Indeed, following this process in 2004, almost no incidents exist to speak of compared with several clear uses of ICT for shady purposes through the late 1990s. In short, much as was the case with the NPD, evidence suggests that digital antagonism among subversive groups emerges from the nature of the relationship between the core and periphery, and that this relationship is dictated by the nature and expression of overarching group objectives.

7.2. Die Linke and Digital Antagonism

In reality, there is quite limited evidence that Die Linke as it has existed from the late 1980s onwards is guilty of what we might call digital antagonism. A single notable 2008 incident in which leftist hackers ostensibly linked to Die Linkspartei hacked a series of far right forums is particularly worthy of mention. This is because, though the anti-fascist group hit in responsible hacks was not linked to Die Linke, party leaders did not disavow the original intrusions and condemned retaliatory hacks against Antifa (anti-fascists) as the opposite of political actions taken in service to the public. Additionally, during the 1990s, a range of party sub-groups were brought to court by the government on grounds of publication of illegal content on websites (inciting property

damage)[263] and previous work indicates that party members also linked to the country's autonomist community prosecuted denial of service attacks against far right websites.[264] However, beyond this Die Linke appears to have almost entirely refrained from disruptive digital activities, particularly since 2005.[265] At most, since then, Die Linke might be said to condone disruptive efforts, as a range of parties officials have excused vandalism of far right websites and more by individuals not linked to the party as understandable.[266]

7.3. Die Linke

Subversive organizations naturally exist on a spectrum of status. Depending on how organized a group is, the degree to which ideas are being accepted by part or much of mainstream society, the ability of the group to operate in legitimate political processes and more tells us much about the shape of a subversive effort and whether or not a particular group might be best classified as radical extremist, terrorist, broadly accepted fringe interest group or political party. Much like the NPD, Germany's Left Party (Die Linkspartei or Die Linke, meaning simply "the Left") has traversed this spectrum and currently plays a small-but-notable role in the country's various legislatures.[267] At the

---

[263] 2001 Annual Report of the Office for the Protection of the Constitution.

[264] See Caiani and Parenti (2016), p. 45.

[265] See the assessment of the 2009 Annual Report of the Office for the Protection of the Constitution.

[266] See, for instance, Streit über Präsidentenwahl: Linke verteidigt Anti-Gauck-Kurs, Spiegel Online, 1 July 2010; or "Linkspartei diskutiert über Lötzsch-Nachfolge". tagesschau.de, 2012.

[267] For the best overviews of the life and evolution of Die Linkspartei in Germany, see *inter alia* Dominic Heilig, Mapping the European Left: Socialist Parties in the EU, Rosa Luxemburg Stiftung, April 2016; Elo, Kimmo, "The Left Party and the Long-Term Developments of the

time of writing, Die Linke held about 10% of all seats in the Bundestag, signaling a degree of success – arguably through advocacy on specific policy issues – in selling an alternative vision of Germany.

Though objectionable to many, Die Linke is seen as a far more acceptable alternative to the NPD or other far right political entities, such as the group *Alternative für Deutschland.*[268] Past work has regularly attributed this to Germany's history with National Socialism.[269] Despite the installation of a communist government in East Germany between 1945 and 1990, there is much greater space for discounting the corrupting influence of the Soviet Union than there is for excusing Nazism. German's view Die Linke with skepticism, but the open hostility to the organization has fallen in line with the party's moderating move towards operation as a legitimate voice in national politics. Nevertheless, the Left Party and other more extreme leftist organizations like the Marxistisch-Leninistische Partei Deutschlands or Deutsche Kommunistische Partei unquestionably qualify as subversive actors. In charter documents, manifestos and public statements, Die Linkspartei explicitly self-describes its organization as aimed at establishing a counter-hegemony that calls out the fundamental

---

German Party System". *German Politics and Society*. **26** (88), 2008, pp. 50–68; and David F. Patton. *Out of the East: From PDS to Left Party in Unified Germany*, State University of New York Press; 2011.

[268] Alternatives for Germany is a reasonably new entrant to the political scene in German. The party bills itself as an alternative conservative option to traditional right-wing elements of the German political arena. In reality, Alternatives looks remarkably like a range of entities across Europe that embrace the philosophies of the far right but seek to distance the agenda from the legacy of National Socialism in Germany and Italy.

[269] For instance, McGowan (2014).

errors of economic neoliberalism and eschews Germany's "current fascist influences."[270] Though its politicians gain support by articulating policy modifications, there is a clear revisionist endgame stated in party material that drives Die Linke's effort.

Again, regardless of stated aims, the fact that Die Linke presently operates with some sizable amount of legitimacy earned from participation in the Bundestag should be overlooked in deciding whether or not to think of the party as genuinely subversive. Die Linke's extreme left-wing positions – extreme enough to regularly earn the label "far left"[271] – have been tempered over time. But through at least 2005, the Left Party housed a broad range of radical sub-groups focused on socialist and communist advocacy.[272] According to government reporting through 2005, when the party voted to moderate its platform presentation in preparation for an expanded federal election bid, there is concrete and recurring evidence that, through various sub-entities, Die Linke was guilty of a range of leftist extremist acts.[273] These ranged from militancy in organization attacks on property and assaults[274] (mostly minor and intended to embarrass) to political violence aimed at the far right[275] and what might best be called influence operations against what is seen as fascist influences in contemporary Germany society. And openly extremist elements, many of which demonstrably support anti-fascist criminal activity, have been actively empowered to drive party policy in

[270] *Neues Deutschland*, 20/21 August 2005, p. 22.
[271] Kate Connolly in Erfurt and Berlin, "Die Linke party wins German votes by standing out from crowd," *The Guardian*, 2012.
[272] 2005 Annual Report of the Office for the Protection of the Constitution, p. 162.
[273] Ibid, pp. 150-164.
[274] Ibid, pp. 150-153.
[275] Ibid, pp. 154-155.

appointments across various Die Linkspartei positions.[276] Members of sub-elements of Die Linke like the Kommunistische Plattform der Linkspartei ("Communist Platform of the Left Party"), the Geraer Dialog/Sozialistischer Dialog ("Gera Dialogue/Socialist Dialogue"), the Marxistische Forum der PDS ("Marxist Forum of the PDS"), and the Arbeitsgemeinschaft Junger GenossInnen in und bei der PDS ("Working Group of Young Comrades in and with the PDS") are represented in important positions.[277] Thus, in many ways, it is almost best to think of Die Linke as a legitimate face for a veritable network of counter-hegemonic operatives and interest groups interested in subverting the present shape of German society.

Germany's far-left has an involved history with hacker culture and digital activism. Today, Die Linke maintains an extensive digital support apparatus that covers the gamut from legitimate (and common) political party media feeds and online advertisements to custom communications software for members and an extensive blogosphere of citizen advocacy sites. Historically, elements of the broader Marxist movement in Germany have close ties to groups like the famed Chaos Computer Club, a hacker collective interested in exposing corruption and failures in governance.[278] To a degree, it might be fair to say that the left in Germany was borne online in a way that the far right or non-political groups were not. In particular, former members of East

[276] Ibid, p. 157. Also see Elo, Kimmo, "The Left Party and the Long-Term Developments of the German Party System". *German Politics and Society*. **26** (88), 2008, pp. 53–58.
[277] 2005 Annual Report of the Office for the Protection of the Constitution.
[278] See *inter alia*, Steinmetz, Kevin F. *Hacked: A Radical Approach to Hacker Culture and Crime*. NYU Press, 2016; and Jordan, Tim, and Paul A. Taylor. *Hacktivism and cyberwars: Rebels with a cause?*. Psychology Press, 2004.

Germany's communist political ecosystem that now flesh out the ranks of Germany's more extreme leftist groups claim a range of ties to both hacker collectives and communist security services.[279]

7.4. Die Linke and Competing Explanations for Digital Antagonism

Subversive Objectives. As noted before, Germany's principal leftist political party is perhaps the most explicitly subversive entity described in this chapter (or, for that matter, in Chapter 6) by dint of the organization's self described goal of "establishing a counter-hegemon[ic]" system[280] – an alternative Germany with political and social processes that differ massively from current iterations. That said, the organization has a unique approach to what can only *technically* be labeled structural revisionism. Die Linkspartei, unlike many of Germany's historically more radical left-wing activists groups, operates with a mechanism of change in mind more than simply an end goal. Die Linke advocates that socialist changes to Germany via parliamentary process are necessary for the construction of a political system that is both effective and durable.[281] In this way, Die Linke differs from organizations elsewhere in the world that might aim for structural revision without the desire to function within existing process (such as, at various points in their existence, FARC or Saudi Arabia's Green Party).

---

[279] Jordan and Taylor (2004).

[280] *Neues Deutschland*, 20/21 August 2005, p. 22.

[281] See Elo, Kimmo, "The Left Party and the Long-Term Developments of the German Party System". *German Politics and Society*. **26** (88), 2008, pp. 50–68.

Of interest, the expectation set in Chapter 4 by positive results pertaining to H1 and H2 above – that groups with structural grievances and broad policy portfolios are more likely to exhibit signs of deviant behavior – hold true when it comes to Die Linke at least to the extent that the party has moved towards participationism over time. Given the group's revisionist aims, we might expect to see support for antagonistic actions taken by group members and this is certainly the case for Die Linkspartei before the past decade. In 2005, for instance, regional Left Party leadership in Hamburg called for solidarity with members of the leftist Autonomer Zusammenschluss Magdeburg (Autonomous Alliance of Magdeburg),[282] a group that is considered to be a terrorist organization by German authorities[283] and which has regularly been found guilty of arson and personal assault made on political opponents.[284] Further, the Left Party has variously condoned or only nominally reprimanded violence by members against the NPD during political marches in 1992, 1995, 1997 and 2003,[285] going so far as to consistently organize protests in line with the NPD calendar of events and then praising violent outbreaks as "tremendous success[es]" for the "broad-based anti-fascist alliance."[286] These kinds of actions further make sense given the broad-scoped nature of Die Linke's

[282] See Patton, (2011).
[283] For an overview of these and other groups, see "Significant Terrorist Incidents, 1961-2003: A Brief Chronology". *Office of the Historian: Bureau of Public Affairs*. United States Department of State. Retrieved 9 April 2017.
[284] Patton, (2011).
[285] See Heilig (2016).
[286] Ibid.

decades-old critique of German society as "fascism wrapped in capitalism" that requires "fundamental restructuring of politics" and "Germanic social culture."[287]

The relationship between support for antagonism and party perspectives is further in evidence when one considers that the recession of Die Linke's ties to militant elements of the left clearly began in 2005 and has continued since that time.[288] In that year, party membership voted to reorganize the group to focus on victory in key elections based on a small set of social issues (much as groups like the Scottish National Party or former members of ETA in Spain have), a strategy that has led to increasing electoral gains.[289] During the last decade, Die Linke leadership has increasingly called out violent acts by members and as banned certain violators from membership permanently.[290] Beyond that, the only outbreaks of member violence in clashes with the far right where Die Linkspartie officials have remained silent have been concentrated in areas and periods where Die Linke has lost to conservative opponents (in 2005, 2006, 2009, 2013 and 2016).[291] This suggests that the far left consider antagonism of the far right to be broadly acceptable to the broader electoral audience, even where rioting and other criminal forms of protest might not be.

Given these trends, it seems fair to say that there is broad explanatory support for H1 and H2 in Die Linke's case beyond the question of ICT usage. However, the Left Party's ICT employments for antagonistic purposes have been more historically limited

[287] Ibid.
[288] Ibid.
[289] See Patton, (2011).
[290] Ibid.
[291] Ibid.

than has its condoning of non-digital criminal behavior. Actions taken by members, affiliated groups and individuals citing the Left Party's platform include the publication of illegal content on websites in the late 1990s,[292] denial of service attacks against far right websites in 2001 to 2002[293] and light use of encryption in apps like WhatsApp in recent years.[294] Beyond 2005, Die Linke's only major involvement with criminal ICT usage lies with a 2008 incident of illegal cyber attack, data theft and doxxing that, though not prosecuted by the party, was widely praised by officials. That incident targeted far right forums linked to *Blood and Honour*, a neo-Nazi organization with extensive membership, and involved the publication of member information obtained through a simple SQL injection intrusion.[295] The attack was quite unusual in its flagrancy, as was the response of Left Party commentators who were subsequently lambasted by right-of-center politicians for their disrespect towards private property.[296] Why is the Left Party's experience with digital antagonism the story of criminal actions by affiliated individuals? Why has Die Linke itself not seen fit to employ ICT for more than recruitment and the promotion of the party message? What prompted the clear supportive response to the 2008 incident? And why is even free agent deviancy now a rarity with the far left?

Here, there are a number of similarities to the case of the NPD and some important differences to note. Certainly, like the NPD, Die Linkspartei is a revisionist

[292] Caiani and Parenti (2016).
[293] Ibid.
[294] Patton, (2011).
[295] Caiani and Parenti (2016).
[296] Ibid.

organization with broad-scoped policy positions and an initial goal of change through participation in existing political processes. However, as Caiani and Parenti note,[297] the lack of violent overtones provides a clear contrast between Germany's far left and far right movements. The far right – and the NPD, in particular – present a vision of Germany intrinsically violent in a structural sense.[298] A Germany reshaped under NPD supervision would aim to reincorporate large tracts of territory and populations that exist beyond German borders in order to restore the country to what the far right considers its true extent.[299] Immigration laws would not only be toughened; policy would likely explicitly incorporate separate conditions for movement, employment and more based on nationality, religion and possibly ethnicity. In short, the NPD's Germany would be one of negative violence – i.e. absent direct violence against the population, but characterized by extreme structural violence.[300] Though Die Linke suggests broad-scoped revision of German society, the far left platform contains no manifest construction of a system without justice.

There is also a contrast to the NPD's political activities in Die Linkspartei's gradual elevation to national prominence as one of the four parties – albeit the smallest by far – represented in the Bundestag. Party restructuring that began in earnest in 2005 saw Die Linke streamline the organization platform and clarify the strategic vision of the

---

[297] Ibid.
[298] Ibid.
[299] Party program, p. 13. ("Deutschland ist größer als die Bundesrepublik! ... Wir fordern die Revision der nach dem Krieg abgeschlossenen Grenzanerkennungsverträge.")
[300] For literature on negative violence/peace, see Johan Galtung, "Positive and negative peace," *School of Social Science, Auckland University of Technology*, *30*, pp.23-26.

left in manifesto documents.[301] The result, quite simply, was a simplification of the policy portfolio via a strategic move to de-emphasize the party's own mission statement in actual political campaigns.[302] Much as separatist political parties have done elsewhere in Europe, Die Linke was able to win support across a much broader range of constituencies by presenting a liberal alternative to right-of-center traditionalists and extremists without the baggage of the group's linked to organized communism.[303] Thus, post-2005, Die Linke transitioned from a revisionist entity with a broad policy platform to a revisionist entity with a selective and more broadly accessible one.

Finally, though Die Linke might certainly be best described as the collaborative product of many elements of Germany's far left, it certainly cannot be said that the group is decentralized or lacking in cohesion. Wherein the NPD maintains an intentionally unstructured fringe of affiliated groups and individuals, Die Linke has built support from coalition-building actions at the regional and national levels. The left's modus operandi, particularly following success in the 2009 elections that saw Die Linke awarded seats in the Bundestag for the first time, has been to act as a liberalizing necessity in alliances with Germany's moderate political parties. In doing so, the left affects political transformation and reorganization from direct participation in the political system and determines the placement of fault lines on core issues of interest.

[301] See Patton, (2011).
[302] Ibid.
[303] Ibid.

Organizational Processes. Though there is no clear mechanisms dictating when Die Linke members and proxies will engage in digital antagonism, incidents clearly drop off following the move by Left Party leadership to consolidate control over its peripheral affiliates. In this way, this restructuring of both the organization and the tactical objectives of the movement in 2005 is at the heart of a narrative about Die Linke similar to that described above with the NPD and it's unstructured fringe. As an organization, Die Linke is an umbrella network of far left groupings that themselves lack the organizational cohesion to coordinate a subversive campaign.[304] Prior to 2005, however, Germany's far left was composed of a less structured network of left-wing parties and activists with the Party of Democratic Socialism (PDS, Die Linkspartei's direct predecessor) at its heart. In 2005, PDS merged with what had until that point constituted the party's fringe.[305] That same year, fringe dissidents and far left groups that had up until then operated as simply as elements of the far left ecosystem in Germany coalesced – for the purposes of sustained support of socialist candidates and eventual merger with the PDS – into the Electoral Alternative for Labour and Social Justice (WASG) party.[306] In essence, PDS formalized its fringe ecosystem and organized a new entity with which it could merge in an effort to expand the appeal of the political ticket.[307] Counter to the rising support for the NPD for an unstructured fringe of core supporters that will produce grassroots political change regardless of party success, Die

[304] Ibid.
[305] Ibid.
[306] Ibid.
[307] Ibid.

Linke doubled down on the power of the party to participate and brought previously unorganized elements into the fold.

Much as the narrative of free agents acting antagonistically is key to understanding NPD support for using ICT disruptively, so too is this narrative of left-wing coalition critical to comprehending the contraction of *criminal* elements of the far left in Germany. The sharp drop in incidents of arson, property theft and damage, personal assault and vandalism by left wing extremists reported in government statistics between 2007 and 2014 is remarkable, with many times fewer incidents (37 reported) between those years than in the decade prior to the PDS/WASG merger (213 reported).[308] Moreover, three neo-Marxist outfits linked to WASG and to website defacements following electoral upsets in 2002 were labeled defunct in annual federal reporting in 2009,[309] with analysis suggesting that members had been absorbed into "seven regional recruitment committees"[310] focused on expanding the Left Party's roll count in historically underperforming areas. The Left Party has even, since 2015, discouraged the use of WhatsApp and several other off-the-shelp P2P encryption programs amongst its members,[311] noting that German law enforcement has been concerned about use by "extremists acting to disrupt public safety"[312] and suggesting that avoiding scrutiny altogether is desirable. In short, the infrastructure and rhetoric of antagonism has largely disappeared within Die Linkspartei since 2005 where before there

[308] See 2014 Annual Report of the Office for the Protection of the Constitution, p. 39.
[309] See 2009 Annual Report of the Office for the Protection of the Constitution, p. 47.
[310] Ibid.
[311] "Emanzipatorische Linke". Emanzipatorische-linke.de. Retrieved 6 April 2017.
[312] Ibid.

was a great diversity of radical factions aimed at disrupting right-wing or competing far left influences.

Support and Opposition. If the PDS/WASG merger and the streamlining of the Left Party platform was directly responsible for the recession of antagonistic elements of the movement, then why did party leaders like Gregor Gysi and Oskar Lafontaine speak favorably of left-wing hackers that stole and published private information from the servers of the neo-Nazi group Blood and Honour?[313] Given that the far right is broadly unpopular (particularly skinhead groups like Blood and Honour) and that hacking for civic benefit *a la* the Chaos Computer Club has long been considered favorably in Germany, one explanation would be that Die Linke leaders found themselves in a unique and uncommon position for potential gain. Over the years, Die Linke has resorted to a number of what have been labeled "bizarre and embarrassing" statements [314] designed to build short-term support among liberal supporters of Germany's other main parties. At the heart of this tendency is the fact that greater gains in Germany's legislatures since 2005 have actually not emerged from success in selling a philosophical message. Though support for Die Linke surged following the 2005 party expansion and reorganization (8.7% of the national vote in 2005 up from 4.0% in 2002), newfound electoral success has not reflected a sea change in support for other major parties in favor of left-wing perspectives so much as it has represented a diminishment of prospects for other minor left-of-center parties. The restructuring of Die

[313] Caiani and Parenti (2016).
[314] Ibid.

Linke to incorporate the relatively diffuse coalition of fringe supporters in WASG brought in a large number of dissident interest groups and voters who had previously focused on local and regional alternatives to center and center-right parties. Such actors have, without alternative, voted for the Left Party.

And yet, wooing German's from the Christian Democrats or Social Democrats has been difficult. Die Linke has regularly chosen to distance itself from the platform positions of Germany's next most liberal organizations, the Social Democrats and the Greens, going so far as to reject a compromise sociality candidate in 2010 fielded by other left-of-center parties in favor of its own. With the 2008 hacking incident, as Patton suggests,[315] the pattern of responses suggests that Left Party leaders saw an opening for political gain. Neither the far right NPD, who defended Blood and Honour on privacy grounds, nor the hacked group are popular. Where centrist and left-of-center politicians were muted or cautiously negative about such an action, Gysi and others took care to highlight the potential for citizen activism to prevent the further encroachment of far right influence in Germany at a time when other countries in Europe were experiencing nativist backlashes to economic problems.[316] Time-and-place support for hacking, in other words, constituted a circumstantial opportunity to turn criminal antagonism to political gain.

[315] Patton, (2011).
[316] Ibid.

7.5. Case Analysis: Determinants of Digital Antagonism

Both Chapter 6 and the sections above present a specific narrative about the experiences of the NPD and Die Linke with disruptive information technology employments, namely that they have almost exclusively been the resort of fringe proxies and that variation can be explained by understanding the organization's demonstrable commitment to revisionism. Reduced commitment to affecting revisionism through non-participatory methods (in the form of platform streamlining and the centralization of directive power in legitimate party units) is directly linked to non-incidence of free agent hacking. Where subversive activists refuse to transition away from more extreme forms of agenda and looser forms of organization (even in the context of Germany's strict political party format rules), free agents are incentivized – both by demonstrable willingness to condone criminality by party leaders and the maintenance of distance in formal relations between elements of the movement – to antagonize societal and government opponents. But does this link between group grievances, structures and antagonistic outcomes hold up in the face of other potential intervening factors?

7.6. Conclusion

In conclusion, case study comparison suggests that revisionism *indirectly* produces antagonism. Far from seeing evidence of explicit executive-level direction of hacking or circumventive efforts, the analysis above suggests that there is a strong relationship between revisionism and the way in which groups interact with proxies that employ ICT antagonistically. Across cases, the sources of web tools and the initiative to

disrupt regularly stems from derivative elements of subversive organizations. The NPD, though mostly guilty of condoning the antagonism of others, has nevertheless actively supported an unstructured fringe element beyond traditional party sub-units – intended to act as a "people's front" – that has been responsible for a range of disruptive digital acts. Die Linke, by contrast, has acted to formalize its fringe and to incorporate dissident elements that previously served alternative purposes as an unstructured way to exert influence via illegitimate means.

In short, a revisionist agenda clearly appears to (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone shady and criminal behavior among fringe members. This theory broadly explains variation in antagonism by organizational elements with party support/opposition to such actions – in the form of direct statements and capabilities support – acting as critical mechanisms. The chapter also notes the close relationship between changes in strategic perspective and other variables, particularly the support of the broader population and direct government investigation. However, though variation on those factors varies with and may certainly directly impact upon the incentive group leaders have to change practices, it is the articulation of new direction in different formats that produces more or less antagonism by group elements.

The case study analysis of three organizations operating in China over the next three chapters will extend this examination of subversive activists' use of ICT and will seek to adjudicate on the question of macro context. Does the relative permissiveness of

Germany's political and legal systems encourage different basic behavior amongst such groups? And does access to tools of digital antagonism dictate the propensity a group might have to use ICT disruptively?

Chapter 8
Spiritualism in China:
The Case of Falun Gong

Christopher E. Whyte

This case chapter investigates the experiences and history of Falun Gong. The chapter proceeds in four parts. After summarizing summarize the case findings, I outline the body of evidence regarding digital antagonism and Falun Gong. Then, I discuss the history and objectives of Falun Gong and analyze the case with an eye to gauging the explanatory power of competing explanations for incidence of digital antagonism. Again, I do so in parallel fashion across each case study presented through Chapter 10, considering group perspective, structure and operating environments as possible explanations. Then, in Chapter 11, I present an overarching narrative based on evidence found in the following case studies, consider additional elements of each case that strengthen the emergent argument and discuss opportunities for future work.

8.1. Summary

Falun Gong's experience is unique in China in that a sizable portion of the organization's active membership – active, at least, from a political perspective – is based outside China. In fact, in many ways this dynamic is key to understanding the

experience of Falun Gong in using ICT for coordination and activism. The group's early experiences in using information technology mirror the experiences of protest and interest groups across the West – i.e. experiences included the adoption of email for logistical purposes, the construction of websites to create communities and the encouragement of photo-video journalism as an effective means via which to broadcast messages. Post-1998, when the government in Beijing outlawed the practice of Falun Gong and labeled the organization itself an "evil cult," those efforts – which would previously have fit the categorical definition of digital activism offered in previous chapters – in many instances clashed with state and local law. In this way, Falun Gong's early digital activism might be called an artifact of China's approach to civil society management.

Since that time, however, Falun Gong's use of ICT for antagonism, though arguably limited, has entirely fit the profile of antagonism described in Chapters 2 and 3. Of interest, however, is the fact that antagonistic and circumventive efforts have emerged almost exclusively from both peripheral and core members of the movement based outside of China, particularly in the United States. Foreign-based developers have been responsible for designing programs and maintaining servers employed to allow people in China to circumvent state censorship systems. Content targeting Chinese citizens that advocate protest of state brutality and further Falun Gong's community development has moved to websites based overseas. In short, what's clear in the case of

Falun Gong is that antagonism is encouraged and bolstered by the efforts of actors that exist on the fringe of the domestic movement and protest effort in China.

8.2. Falun Gong and Digital Antagonism

Falun Gong is a subversive activist organization. As noted above, however, the distinction between digital activism and antagonism is variable depending on specific national context. Here, the illegal funding and operation of Falun Gong, as well as the use of off-the-shelf encryption apps and e-petitions not permitted by Chinese authorities, are antagonistic; in a Western country, they would not be considered so. That said, there exist many claims and some clear evidence that Falun Gong has regularly engaged in antagonistic efforts to mobilize, organize and persuade elements of the Chinese population beyond the scope of such nebulously definable actions. Falun Gong members have reportedly used encryption (particularly using TOR to mask darknet activities) beyond basic app encryption to organize and hide funding details, disseminate content and share meeting plans.[317] A well-known Falun Gong member exiled in the United States has developed several versions of a custom email and social media spamming software designed to allow for illicit, targeted messaging inside China.[318] Indeed, this software is famous and is regularly used beyond Falun Gong by dissidents in Iran, Saudi Arabia, Russia and Botswana. Relatedly, members have demonstrably vandalized

[317] See Gordon, Bennett, "Iranian Protesters, Web Censors, and the Falun Gong," UTNE Reader, September 4, 2009.

[318] See *inter alia* Ibid, pp. 214-238; Xia, Bill. "The Coming Crash Of The Matrix." *China Rights Forum*. Vol. 3. 2004; Gutmann, Ethan. "Hacker nation: China's cyber assault." *World Affairs*, 2010, pp. 70-79; and Stone, Brad, and David Barboza. "Scaling the digital wall in China." *New York Times* 16, 2010.

websites and utilized malware purchasable online to infect CCP computers and more.[319] And finally, if one considers the reporting of the Chinese government (the validity of which will be discussed further below), Falun Gong adherents have been linked to cyber attacks on government information infrastructure that have caused limited Internet outages and service disruptions in 2002 and 2003.[320]

8.3. Falun Gong

Falun Gong is a spiritualistic organization that was founded in 1992 by Li Hongzhi.[321] Variously called a loose-knit movement and a discrete group, Falun Gong is remarkably similar to a range of spiritual organizations across China that practice variations of *qigong*. *Qigong* is a form of exercise that encourages deep spiritual connection with one's body and a range of activities taken that divert human energies towards healing purposes. In reality, *qigong* is remarkably like exercise forms found elsewhere in the world that, regardless of how spiritual practitioners are, emphasize meditative physical exercise as a means of achieving highly specific health benefits (yoga is one such practice). What sets Falun Gong apart and what has qualified the organization for special investigation and prosecution by the Chinese state has to do with supernatural elements added by Li Hongzhi in the initial years of his operation.[322]

---

[319] Discussed in Ronfeldt, David, and John Arquilla. "Networks, netwars and the fight for the future." *First Monday* 6.10, 2001.

[320] For a description of these claims, see Yu, Haiqing, "The new living-room war: Media campaigns and Falun Gong," 2004.

[321] *Renmin ribao*, 23 July 1999; "A brief discussion on *falun gong*."

[322] For a broad overview of Falun Gong, the organization's variation on *qigong* practices and philosophical tenets, see *inter alia* Tong, James (2009). *Revenge of the Forbidden City: The*

In the early 1990s, Li – then a government clerk – began teaching *qigong* in the context of supernatural wisdom and lessons he had apparently received from a series of masters that trained him throughout his childhood. His story, elements of which would not be entirely unfamiliar to students of the life of Buddha or (to a lesser degree) Jesus Christ, involved an education at the hands of various masters of the spiritual practice who came to him at key junctures in his early life.[323] The result was a mystical philosophy that is today adhered to by tens of millions of Chinese citizens (most recent estimates range from 10 million up to 40 million, with as many as 100 million adherents worldwide[324]) and organized into thousands of local and regional organizing cells. In essence, spiritual exercise can alter human energies to achieve what the PRC labels "supernatural" abilities. In many cases, this allegedly goes far beyond bodily healing and can include the capacity to fly, teleport, cure terminal disease or achieve higher states of awareness.[325] Li's ideas gained popularity throughout the 1990s as he spread his message through pamphlets, magazines and word of mouth, to the point that ten thousand or more of Falun Gong members and devotees marched on government centers in Beijing

---

Suppression of Falungong in China, 1999-2005. New York, NY: Oxford University Press; Palmer, David A. (2007). *9. Falun Gong challenges the CCP. Qigong fever: body, science, and utopia in China*. Columbia University Press; and Spiegel, Mickey (2002). *Dangerous Meditation: China's Campaign Against Falungong*. Human Rights Watch.

[323] *Renmin ribao*, 23 July 1999.

[324] Estimates vary. The most common estimates hold that between 70-80 million adherents exist worldwide. See "Falun gong zhenshi di gushi" ("The real story of *falun gong*") 14 August 1999, in www.Mingui.ca. Other estimates have been as low as 2 million in the mid-1990s to between 40 and 80 million at a peak in the early 2000s. See *Renmin ribao* (*People's Daily*), 15 August 1999, p. 1; *Nanfang ribao*, 18 March 1999, p. 11; Xinhua, 27 October 2001; and Zong Hairen, "Zhu Rongji zai yijiujiujiu nian" ("Zhu Rongji in 1999"), p. 15.

[325] See Han, Sam, and Kamaludeen Mohamed Nasir. *Digital culture and religion in Asia*. Vol. 4. Routledge, 2015, p. 53.

and around the country after Li was quietly made to leave the country in 1999. Though protest was muted, these marches led to police clashes and began a spiral of dissident interactions with authorities that saw Falun Gong outlawed in China as a cult.

Of the various groups studied in Chapter 4's large-N analysis and this project's case studies, it might be argued that Falun Gong is the organization most tenuously identifiable as subversive. This is largely because the organization has no stated aims, but rather a communal set of beliefs and approaches to society not commonly enumerated in anything so material as a manifesto document. The organization itself is also incredibly decentralized, a point that will be discussed in detail below. It might additionally be difficult to think of the movement as subversive because Falun Gong practitioners and members, beyond being relatively common in some communities in China, are not generally disrespectful of other citizens and do not engage in political activities that might usually inspire the ire of mainstream interest groupings.[326] However, Falun Gong certainly qualifies as subversive in that members see themselves as set apart from a normative status quo in the PRC that requires large-scale modification. This is evident in a range of operations and statements made by advocates of the

[326] The group actually actively discourages or forbids various forms of political organization. As Tong notes, " "Demands on *falun dafa* guidance stations" (4/20/1994), Art. 1 stipulates that the guidance stations should not engage in management practices of economic enterprises (*jingji shiti di guanli fangfa*). "Regulations on propagating the doctrine and method for *falun dafa* disciples" (4/25/1994), Art. 4, prohibits the acceptance of fees and gifts during the propagation of *falun gong* doctrine and method. "Norms for *falun dafa* guidance counsellors" (n.d.) Art. 5 stipulates the same. "What *falun dafa* practitioners ought to know" (n.d.), Art. 4, forbids practitioners to heal the sick, and especially to accept fees and gifts for such healing." See Tong, James. "An organizational analysis of the Falun Gong: Structure, communications, financing." *The China Quarterly* 171, 2002, pp. 636-660.

movement and the practice based in China, the United States, Australia and elsewhere over the past two decades.[327] Moreover, membership – beyond being criminal – is generally viewed with apprehension by the population writ large. Recent polling on the subject suggests that Falun Gong is generally considered to be a relatively harmless-but-illegitimate deviation from otherwise harmless and common spiritualistic practices.[328]

Having said that, Falun Gong is, from the perspective of this study's focus on non-state uses of ICT, perhaps one of the most interesting cases of subversive employments of digital techniques for activism and antagonism anywhere in the world. Despite a remarkably diffuse organizational structure and a number of obstacles of operation in the sophistication of China's state repression apparatus, which will be discussed in detail below, Falun Gong has made extensive use of the Internet for all manner of activist efforts for almost two decades.[329] Indeed, perhaps the most remarkable feature of the early history of the movement is the central role that electronic devices and information technology played in enabling protest and dissent beyond the ability of the Chinese government to interdict.

---

[327] In just the two month period from being banned in 1999 by the Chinese government, Falun Gong launched more than 300 protests repudiating all reporting on the group as illegitimate and calling for rapid reversals. See *Renmin ribao*, 5 August 1999, p. 1. Since 1999, membership has launched rhetorical attacks on the judgment of the CCP in dictating the requirements of state security. See Research Department, Ministry of Public Security, "Li Hongzhi."

[328] See "The critical masses: Officials increasingly ask people a once taboo question: what they think," *The Economist*, April 11, 2015; and Porter, Noah. *Falun Gong in the United States: an ethnographic study*. Universal-Publishers, 2003.

[329] For perhaps the most extensive overviews of Falun Gong's use of the Internet, see Bell, Mark R., and Taylor C. Boas. "Falun Gong and the Internet: Evangelism, community, and struggle for survival." *Nova Religio: The Journal of Alternative and Emergent Religions* 6.2, 2003, pp. 277-293; and Huang, Bi Yun. *Analyzing a social movement's use of Internet: Resource mobilization, new social movement theories and the case of Falun Gong*. Indiana University, 2009.

In 1999, as mentioned above, large numbers of Falun Gong protesters appeared in Beijing and other cities across China to protest the effective deportation of Li Hongzhi. Their presence was not expected by government agencies at either the local or national levels, largely because there had been no public call to action and because Falun Gong protests – which were overwhelmingly peaceful – were not precipitated by riots or some kind of violent clash with authorities.[330] Remarkably, the organization of tens of thousands of Chinese citizens from across the country in support of what was then being called a cult movement was almost entirely achieved by telephone, email and Internet chat.[331] More than ten thousand members and related adherents responded to the call for mobilization that came through electronic and digital means – Li famously responded to questions about the protest's organization by saying that members "learned it from the Internet"[332] – a fact perhaps most incredible given the limited level of access most Chinese citizens still had to the Internet and even landline telephones in the 1990s. And perhaps even more notably, Falun Gong's activities in the following months and years relied almost exclusively on digital technologies – an unusually intense adoption of ICT even in the late 1990s – to avoid government interdiction and achieve a number of PR coups in spite of CCP efforts. In October of 1999, for instance, Falun Gong succeeded in arranging and holding a clandestine press conference with a range of foreign journalists

[330] *Renmin ribao*, 13 August 1999, p. 5.
[331] See Richard Madsen, "Understanding Falun Gong," *Current History* 99, no. 638, September 2000, pp. 243-247.
[332] See <http://falundafa.org/fldfbb/news990502.htm>, accessed 14 August 2001.

in Beijing.[333] The tools of their coordination were basic Instant Messaging, Internet chat rooms and email. Over the past two decades, Falun Gong members have maintained a broad range of websites that must regularly be reconstructed and moved in the face of pro-government or direct government interference. Some such websites are explicitly illegal in their anti-government messaging; others, the constant target of disruption, are veiled support forums for Falun Gong that focus on *qigong* practices. And, increasingly, Falun Gong membership coordinates public protests – which have dropped in frequency since the mid-2000s – and a range of advocacy operations through the use of publically available communications applications (WhatsApp, Snapchat, RenRen, Weibo, WeChat, etc.).[334]

8.4. Falun Gong and Competing Explanations for Digital Antagonism

What factors influence the decision Falun Gong has made to, at times, employ ICT antagonistically alongside broader activist efforts? In this section, I break down the history and context of Falun Gong's use of ICT over the past two and a half decades using the various hypotheses outlined in Chapter 3 as a guide for structuring the narrative. As with previous chapters, I structure my analyses in by focusing on those factors highlighted in Chapter 4 as those most closely tied to incidence of antagonism by subversive activists.

---

[333] See "The crackdown on Falun Gong and other so-called *heretical organizations*," Amnesty International, 23 March 2000.

[334] See Huang, Bi Yun. *Analyzing a social movement's use of Internet: Resource mobilization, new social movement theories and the case of Falun Gong*. Indiana University, 2009, pp. 195-213.

In each case, I take steps to consider not only the direct variation in outcomes predicted by each hypothesis, but also variation in related factors. Doing so is necessary for any effort to determine the significance of any one set of driving forces. Specifically, with each unique type of possible explanation, I consider the overall shape of the relationship between driving factors and the dependent variable before focusing on features of group experiences that might disproportionately suggest significance (critical junctures and secondary driving forces). I then return to the hypotheses in the next section to discuss.

The next three sections discuss the experiences of Falun Gong, particularly focusing on employment of ICT. Again, the questions being asked are, simply: How have Chinese subversive organizations institutionalized information technology adoption and what institutional mechanisms appear to either impede or encourage use of ICT for circumvention or disruption?

8.4.1. Falun Gong: Aims, Structure and Environment

Subversive Objectives. What links these subversive groups to the use of ICT for circumvention and antagonism? In broad terms, the findings of Chapter 4 lead us to expect the manifestation of digital antagonism particularly among groups that articulate broad policy and objective portfolios. Likewise, the expectation is that organizations with a structural grievance – i.e. a stated or demonstrated desire to revise and replace the political system of the People's Republic of China – are far more likely to be antagonistic in their employment of ICT than are those without such revisionist

tendencies. At least at first glance, there is much evidence in the experience of Falun Gong to support these hypotheses. Moreover, there is clear evidence to link group doctrine to antagonistic behavior in the form of punctuated revisionism amongst exiled members that then provide the tools of digital circumvention.

Falun Gong maintains a generally minimalist policy portfolio, the shape of which stems from a general criticism of and objection to the Chinese government without explicitly stated goals of revision.[335] Indeed, Falun Gong, a group that is remarkably peaceful and lacks many key features of cultism, is often characterized first and foremost by its explicit rules regarding doctrinal development.[336] In short, members are discouraged (forbidden in many instances) from articulating social or political objectives beyond the practice of Falun Dafa. The prohibition is so ubiquitously observed that, in a Western country, one would be hard pressed to call Falun Gong revisionist. Rather, the group's main objection has to do with freedom of action in the authoritarian PRC.[337]

---

[335] In reality, there is no policy portfolio held by the organization or movement as a whole. Falun Gong does not focus on politics beyond the survival of the organization itself. However, since 1999, this has meant the adoption of a range of survival strategies that necessarily include decentralized resistance to and protest against the PRC. The main policy critique has to do with the outlawing of Falun Gong itself and related *qigong* organizations. Adherents criticize Beijing and have increasingly coalesced around the criticism that the PRC is not in a legitimate position to dictate the health of Chinese civil society.

[336] See Tong, James. "An organizational analysis of the Falun Gong: Structure, communications, financing." *The China Quarterly* 171, 2002, pp. 636-660 in citing "Demands on *falun dafa* guidance stations" (4/20/1994), Art. 1, "Regulations on propagating the doctrine and method for *falun dafa* disciples" (4/25/1994), Art. 4, "Norms for *falun dafa* guidance counsellors" (n.d.) Art. 5, and "What *falun dafa* practitioners ought to know" (n.d.), Art. 4.

[337] For perhaps the best outline of Falun Gong objectives and the evolution of group strategy, see Tong, James (2009). *Revenge of the Forbidden City: The Suppression of Falungong in China, 1999-2005*. New York, NY: Oxford University Press.

A number of features of Falun Gong stand in stark contrast to the actions and experiences Eastern Lightning (the other spiritualistic group covered in this study) has had over the past three decades. First, Falun Gong has an almost unusually limited history of member involvement in criminal enterprise.[338] Several instances of Falun Gong members assaulting police officers and civilians during protests in the late 1990s exist, all of which took the form of unorganized brawling in busy streets. Likewise, more than 500 members (though some estimates put arrests from direct protest in the thousands[339]) have been arrested for unauthorized protest over the years.[340] However, Falun Gong adherents were, prior to state campaigns to identify and detain members, reasonably well known for their cooperation with police and for acting responsibly (by removing trash, escorting elderly members, etc.) in attempting to maintain peace around protest events.[341] In the wake of various police brutality episodes from 1999 to the present day, member responses have rarely been violent and tend towards pacifist (if illegal) protest.

Second, Falun Gong's spiritualism does not manifest in prophetic vision and so the group has no stated objectives that impact upon the political system in China (beyond a desire to practice and interact with all Chinese communities). In this way, again, Falun Gong might be said to have a structural objective that does not manifest in a targeted fashion. The group's structural objection is, in fact, contextually focused on

---

[338] See *inter alia* Thomas, Kelly A. "Falun Gong: an analysis of China's national security concerns." *Pac. Rim L. & Pol'y J.* 10, 2000, p. 471.

[339] Tong (2009) notes that some Hong Kong-based protest publications estimate that arrests in 1999-2000 were as high as 50,000 people detained.

[340] See Spiegel 2002, p. 21.

[341] Benjamin Penny, "The Past, Present and Future of Falun Gong," A lecture by Harold White Fellow, Benjamin Penny, at the National Library of Australia, Canberra, 2001.

the existence of a PRC campaign to remove the group as a source of social discontent. The reality of Falun Gong's experience is actually one of broad acceptance of contemporary society. The group was, for several years, officially recognized, prior to the onset of a suppression campaign that members now desire to end.[342] Finally, critical elements of the Falun Gong organization exist abroad. Though group membership within China is estimated at between 10 million and 40 million, important membership clusters that perform specialized functions largely operate abroad and mostly from either the United States of Canada.[343] Thus, while group activity under the radar continues to plague the counter-subversion activities of the PRC, it is functional arms beyond China's borders that play a significant role in determining group policy and the extent of group capacity.

Several of these factors impact upon hypotheses relating to environmental pressures and organizational structure. However, they come to bear on the question of a relationship between group grievance and ICT activities in unique ways. Falun Gong is certainly guilty of ICT antagonism to a limited degree. Members of group have employed a range of off-the-shelf email spamming applications[344] and encryption software,[345] the use of which is outlawed in China. Falun Gong arrestees have used TOR ('The Onion

---

[342] David Ownby, *Falun Gong and the Future of China*. New York, NY: Oxford University Press, 2008.

[343] See Porter, Noah. *Falun Gong in the United States: an ethnographic study*. Universal-Publishers, 2003.

[344] See brief discussion in Karatzogianni, Athina. *The politics of cyberconflict*. Routledge, 2006, Chapter 3.

[345] Porter reports Li's own description of group use of email encryption and burner mobile phones to maintain secrecy in intra-group communications. See Porter (2003), p. 184.

Router,' which is used to anonymously access different kinds of websites on the Internet, Deep Web and Dark Web),[346] have allegedly purchased malware[347] and is, broadly speaking, the developer of a range of software tools designed to circumvent state censorship (in the form of the Golden Shield system).[348] Moreover, the group, much as is the case with EL, is guilty of violating state law insofar as members proselytize online. Indeed, Falun Gong is perhaps more guilty of this than EL is, as web interfaces on Falun Gong websites emphasize the creation of communities around *qigong* and group beliefs.[349]

Of interest, however, ICT employments for antagonistic purposes by Falun Gong members within China almost exclusively originate with operatives and spokespersons in the West. Custom software employed by the group is sourced from several group activists in the United States that, counter to the broadly disorganized and non-engagement minded ethos of the broader movement, have opted to be a focal point for group-specific anti-Beijing advocacy. Indeed, according to various scholarly works and

---

[346] See Leigh, David, Luke Harding, and Charles Arthur. *Wikileaks: inside Julian Assange's war on secrecy*. PublicAffairs, 2011, p. 183.

[347] See Vuori, Juha A. *Critical Security and Chinese Politics: The Anti-Falungong Campaign*. Routledge, 2014, pp. 38-45.

[348] For a good overview of Dynaweb and Falun Gong's response, see *inter alia* Gutmann, Ethan. "Hacker nation: China's cyber assault." *World Affairs*, 2010, pp. 70-79; Stone, Brad, and David Barboza. "Scaling the digital wall in China." *New York Times* 16, 2010; Thornton, Patricia M. "Manufacturing dissent in transnational China: boomerang, backfire or spectacle?." *Popular Contention in China*, 2008; and Johnsson, Stefan. "China: The Silence Behind the Wall." *Information Warfare*, 2013.

[349] See Thornton, Patricia M. (2003) The new cybersects: Resistance and repression in the reform era, in E. J. Perry and M. Selden (eds), Chinese society: Change, conflict and resistance. 2nd edition, pp. 247–70 (London/New York: RoutledgeCurzon), p. 265; and Bell, Mark R. and Taylor C. Boas (2003) Falun Gong and the internet: Evangelism, community, and struggle for survival. Nova Religio: The Journal of Alternative and Emergent Religions 6(2), pp. 277–93.

journalistic reports, foreign sponsors and members are the sole sources of ICT capabilities that link to digital circumventive by Falun Gong groups.[350] In particular, a series of foreign-based volunteers were the enabling mechanism for the development of Falun Gong's most well-known contribution to the circumventive abilities of protest groups around the world – a piece of software that allows users to access the Internet free from censorship.[351] Important to the functioning of this program is a series of proxy servers maintained around the world by individuals and groups supportive of Falun Gong. Of further interest, the software has become popular in Iran and elsewhere amongst dissident groups and supporters of web freedom broadly writ, and these secondary users have been the source of various modifications made to Falun Gong-sourced program design over the past decade.[352]

Digital antagonism practiced by Falun Gong, a group with no clear structural grievance, is non-disruptive. Preliminarily, though it might seem mechanically tenuous to link the group's antagonistic ICT employments to the nature of the movement's grievances, Falun Gong *does* fit the expectations outlined in H1 and H2. In general, Falun Gong adherents do not, beyond the practice of their beliefs, appear to actively attempt to use ICT to avoid government attention or disrupt state processes. Rather, elements of Falun Gong operating within China act as punctuated nodes of advocacy and organization, using tools provided by foreign and foreign-based sponsors to express

[350] Tong, 2009, pp. 82-92.
[351] See Gutmann, Ethan. "Hacker nation: China's cyber assault." *World Affairs*, 2010, pp. 70-79. Dynaweb can be downloaded at www.dongtaiwang.com.
[352] See Gordon, Bennett, "Iranian Protesters, Web Censors, and the Falun Gong," UTNE Reader, September 4, 2009.

anti-Beijing sentiment in an active fashion not common domestically and to perform outreach beyond the bounds of PRC censorship.

Of particular interest here, however, is the unique dynamic of foreign sponsorship that is intrinsic to members' circumventive abilities. Such a dynamic suggests a two-part explanation for the variation in Falun Gong's use of ICT for circumvention beyond the basic expectations set by grievance-based hypotheses. With Chinese subversive organizations, foreign sponsors present as a unique means for accessing the ability to employ ICT antagonistically. Where the PRC's censorship regime is so sophisticated, domestically purchased systems are to be treated with suspicion. Moreover, external connections – for the purposes of maintaining servers abroad, for instance – are required for the successful implementation of some techniques for circumvention. Therefore, foreign sponsorship and involvement in procurement and design is necessary to mitigate access challenges born of increasingly effect state control of access to digital technologies.

The prominence of foreign sponsors in the provision of circumvention tools and institutions also suggests a diffusion of grievances between China-based and exiled members of Falun Gong. Wherein most group adherents and operatives evolutionarily understand objectives in the context of the group's spiritual practices and the specifics of Beijing's suppression campaign, foreign-based members are influenced by specific cases of exile. As several such advocates have noted in interviews, Beijing's approach to political representation and social policy is wholly objectionable insofar as persecution of Falun Gong has become part-and-parcel of state efforts to deny basic rights. This doctrinal

outlook is a stark departure from the plight of domestic adherents, who demonstrably see suppressive policy as a function of elite corruption more than inherent political function.

Organizational Processes. Close analysis of Falun Gong in scholarly work and the reporting of different governments suggests that the group is possessed of a hub-and-spoke structure, a fact that comports with the group's relatively minimal observance of antagonistic ICT practices. However, to the casual observer, determining Falun Gong's organizational structure is a difficult task and it is worthwhile discussing the competing perspectives involved.

The difficulty in determining group structure in the case of Falun Gong is largely, as James Tong notes, due to the fact that the organization is represented differently by the Chinese government and by members of the group itself.[353] Two competing narratives exist about the nature of group leadership, the shape of intra-organizational communications, the degree of functional specialization across elements of the movement and the basis of Falun Gong's finances. As one might expect, these narratives reflect extreme ends of the spectrum of group centralization outlined in Chapter 3. The PRC claims Falun Gong is a highly hierarchical organization with clear lines of communication, direction and funding. Falun Gong, by contrast, claims few organizational trappings. Though study of groups like Falun Gong is naturally difficult, historical analysis of documents of various kinds suggests that the organization might

[353] See Tong, James. "An organizational analysis of the Falun Gong: Structure, communications, financing." *The China Quarterly* 171, 2002, p. 637.

best be described as hub-and-spoke owing to a decoupling of directorial links between upper echelons and local stations since 1996.

Falun Gong leaders have variously described the organization as a distributed spiritualistic movement focused on *qigong* instruction and practice at the individual level. To this end, there exist a broad number of "stations" across China.[354] From the perspective of the organization, these stations function as guidance bureaus for facilitating learning of *qigong* techniques.[355] Through the 1990s, teaching stations operated under the jurisdiction of society organizations officially registered with authorities in different regions of the country. Local stations have no set infrastructure – phones, business equipment, staff or office space requisitioned at the national level – and are often found in residential buildings. As Tong describes, Falun Gong organizationally looks much more like a hobby movement or an interest group than it does a religious or political entity. This is by designed following 1996's decision to reorganize the group in preparation for a future without official patronage.[356] Following that decision, Falun Gong leaders hold that the organization, beyond being a social grouping, doesn't officially exist.[357] In line with this, group doctrine – officially, in any case – prohibits cash contributions and there are no fees for *qigong* instruction.[358]

---

[354] *Guangming ribao*, 3 August 1999, p. 1; Xinhua, Beijing, 27 October 2001.
[355] "Norms for *falun dafa* guidance counsellors" (n.d.) Art. 5
[356] *Renmin ribao*, 4 August 1999, p. 1.
[357] See "The real story of *falun gong*," *Minghui*; and China Law Workers, "Incompatible with law."
[358] "Regulations on propagating the doctrine and method for *falun dafa* disciples" (4/25/1994), Art. 4.

The PRC view of Falun Gong's organizational structure is strikingly different. In essence, authorities claim that the group has replicated the administrative shape of the Chinese state itself in providing for effective coordination of the national mission.[359] Directive and communicative power is centralized in group leaders (originally Li Hongzhi) who practice direct control over the Falun Dafa[360] Research Society based in Beijing. The Research Society is an administrative mechanism for supporting a broad bureaucratic base for Falun Gong. Within and beneath the Research Society is a central station whose oversight includes main stations in different regions, a range of committees with oversight of specialized functions (propaganda, financing, etc.) and a hierarchy of practice-oriented states (branch, guidance and practice).[361] This structure is similar to the committee-based structure of China's administrative state, with the leadership positions and the Research Society paralleling the functional power of the Standing Committee and Secretariat. The question with Falun Gong is: to what degree is one narrative about Falun Gong's organizational structure more accurate than the other?

Naturally, any attempt to unpack Falun Gong in this vein must recognize the competing, antagonistic polemics that clearly drive public assessments of group operations. Falun Gong maintains its assertion that the group has no objectives other than function as a social organization popular with large tracts of the domestic population. The PRC, by contrast, maintains a campaign that labels the group an "evil

[359] See Tong (2002), p. 642.
[360] Synonymous, as Tong notes, with Falun Gong in publications by the organization.
[361] *Beijing wanbao*, 7 August 1999.

cult." The possible explanations for PRC policy towards Falun Gong are many. However, persecution of the group is far too ingrained in state policy to retreat at this time and official rhetoric is likely guilty of exaggeration on several fronts.

In 1999, when the Chinese government first suppressed the group, official reports claimed that Falun Gong maintained 39 main stations, 1,900 guidance stations and 28,263 practice sites around the country.[362] According to Tong, the hierarchical narrative of Falun Gong's neat organization and extensive distribution at various functional levels suffers from a number of irregularities. First among these is the fact that various subdivisions of the organization do not map perfectly to different regional and local boundaries.[363] There is duplication in the main stations, branch stations and practice sites servicing different locales, and this duplication is extreme in some areas. This implies that a great amount of inefficiency in coordination. Likewise, Falun Gong designated the Wuhan main station as controller of other main stations in the late 1990s,[364] introducing new layers of administrative control, prompting some enduring confusion about the jurisdiction of different main stations and causing a gradual devolution in planning authority to lower levels.[365] And finally, changing standards set by Chinese authorities across different regions on the standards for organization format –

[362] *Guangming ribao*, 3 August 1999, p. 1; Xinhua, Beijing, 27 October 2001.
[363] See Tong (2002), p. 643.
[364] Ibid, p. 646.
[365] *Renmin ribao*, 7, 8 August 1999.

mostly becoming stricter over time – has created massive variation in station local structure, further loosening the coordinative and directive abilities of group leaders.[366]

Overall, the image that emerges from an examination of the different elements of Falun Gong's organizational structure is one of diminished hierarchy. The group certainly began as a highly bureaucratic organization in 1992. However, by 1996 Falun Gong started to suffer from a lack of mechanical resiliency. Some of this was intended[367] and some appears to be subsequent bureaucratic blunder. Though there is clear and strong leadership in Li Chang, Wang Zhiwen, Yu Changxin and Li Hongzh – and while Falun Gong was for a brief time quite well organized – the enduring regime narrative about an authoritarian organization fails on several fronts. First, as noted above, the various subdivisions of Falun Gong suffer from duplication and unclear links to higher levels of the group. Though Falun Gong maintains a number of committees with specialized focuses, these have increasingly been disbanded, reformed or brought under the direct control of group leadership.[368] As a result, arms of the wing cannot be said to have specific functional value so much as the Research Society itself has increasingly centralized the organization of publications, irregular forums and more. Likewise, group funding, though certainly benefiting from sale of merchandise and teachings counter to the claims of Li Hongzhi, suffers from the need to keep prices for such services low and

---

[366] See *Fujian ribao*, 5 August 1999; and *Haerbin ribao*, 1 August 1999.

[367] *Renmin ribao*, 4 August 1999, p. 1.

[368] For an overview of Falun Gong's committee structure, see Ye Hao, "An explanation." For an overview of the functions of distributed committees among doctrinal, practice and publication tasks, see Gongli-gongfa zu, Houqin banshi zu, Xuanchuan zu, see *Beijing wanbao*, 7 August 1999; *Beijing ribao*, 25 July 1999; and *Renmin ribao*, 7 August 1999, p. 2.

appears to minimal.[369] Finally, Falun Gong's doctrinal evolution, despite the centralization of most functions beyond basic instruction to group leadership, has been fragmented since 1999. Though messaging has become clearer with the gradual removal of administrative strata to enable clear communication with group members, there has increasingly been limited control exercised over a large number of branch stations that advocate locally specific solutions to state repression, including violent protest.

Given this hub-and-spoke structure, Falun Gong's relatively minimal observance of antagonistic ICT practices is unsurprising. Though group leadership exercises poor control over the most devolved segments of the organization, previous hierarchical administration ensures that deviant adherents have extremely small jurisdictional interests and limited resources. Likewise, though there exists a clear directional core, there has realistically been little in the way of functional strengthening of group leadership over time. Falun Gong's leaders have always played a strong coordinative role in organization planning and expansion, and the removal of much administrative strata has improved this ability. And yet, doing so has done almost nothing to improve the directional capacity of the Research Society or its ability to distribute resources, resulting in a large hub without specialized abilities amongst spokes.

Support and Opposition. In terms of ICT usage by Falun Gong members and leadership, the development of Falun Gong's circumventive toolkit and the organization of such efforts in the early 2000s suggest a correlation between Beijing's

[369] See Tong (2002), p. 650-658.

suppressive actions and ICT antagonism. Much as was the case with the NPD in Germany, greater scrutiny by society and the government corresponds with a period of increased focus on antagonism. As with the NPD, however, mechanisms of antagonism are not entirely clear.

It is best to consider Falun Gong's relationship with both the Chinese government and with mainstream society as having existed across two distinct phases. Prior to Li Hongzhi's exile and subsequent protests in 1999, Falun Gong was generally accepted as a spiritual, but not religious social organization whose core precepts – regardless of how supernatural they appeared – had understandable roots in the traditional exercise routines practiced by millions of Chinese citizens every day.[370] During the seven-year stretch from Li's founding of the group until 1999's crackdown, Falun Gong enjoyed broad acceptance and rapid expansion in the form of millions of adherents across the country.[371]

During that period, opposition to the group was minimal. In terms of social opposition, government polling itself demonstrates minimal concern amongst the Chinese population that Falun Gong was a unique source of societal disturbance.[372] Indeed, the operation of the organization in line with other social interest groups – with regular branch practice stations, open to the public, distributed about China's cities and towns –

[370] Tong (2002), pp. 643-645.

[371] Ibid, p. 645. Also see Porter, Noah. *Falun Gong in the United States: an ethnographic study*. Universal-Publishers, 2003; and Richard Madsen, "Understanding Falun Gong," *Current History* 99, no. 638, September 2000, pp. 243-247.

[372] Around the events leading to banning, see Xinhua, 21 October 1999; and Xinhua, Beijing, 21 October 1999. Otherwise, see "The critical masses: Officials increasingly ask people a once taboo question: what they think," *The Economist*, April 11, 2015.

departs from the image of spiritual cultism that the government has since attempted to cultivate in that there is little in the way of money collection or secrecy. Even Falun Gong's doctrine presented (and continues to present) as unorganized and unfocused beyond specific individualistic goals.

Following the government's crackdown on Falun Gong and various actions taken to censor members in the years after 1999, social opposition to the group increased. However, there is limited evidence that Falun Gong adherents are ostracized from society in meaningful ways beyond forums that link communities with the national government. For instance, there is significant evidence of bias against suspected Falun Gong members on entry examinations for high schools, universities and the civil service.[373] Likewise, concerned members of the public have betrayed Falun Gong stations to local authorities on a number of occasions.[374] Nevertheless, where subversive organizations operating in the public in Germany and elsewhere regularly prompt countersubversive protests and organization development, no such outcomes are evident with Falun Gong. Nor is there evidence to suggest that the Chinese government itself has suppressed opposition to Falun Gong,[375] as it often has in situations where pro-government efforts would themselves bring about social unrest.

As with social opposition, government opposition can be thought of as taking on different forms across the periods before and after 1999. Prior to Li Honghzi's quiet exile

[373] Tong (2009), pp. 81-82.
[374] Discussed in "Huangyan mengbi buliao xueliang di yanjing"("Lies cannot deceive bright eyes"); "Suowei shijie mori" ("So-called end of the world"); and "A brief discussion of *falun gong*," in *Minghui*.
[375] Tong (2009), p. 56.

and subsequent actions taken against the broader organization that year, Falun Gong's relationship with the Chinese government transitioned from broad-scoped acceptance and official sponsorship to suspicion focused on the group's supernatural teachings.[376] Li's initial move to publically teach his version of *qigong* in 1992 was met with widespread popular adoption of the practice and Falun Gong was officially sponsored by a range of government agencies, including the state-run Qigong Association.[377] A turning point in China's interaction with the organization was in 1996-97. Three years in, Falun Gong had successfully attracted members in the tens of millions and Beijing feared the social power of such an organization as a potential destabilizer of the status quo.[378] Beijing was faced with something of a dilemma, however, in that the organization and practice of Falun Gong was widely popular, with as many as 70 million "students" in China;[379] the practice of *qigong* more broadly was even more popular, with as many as 300 million practitioners across the country. Thus, the main step taken by Beijing to reel in Falun Gong and affect some control was in many ways minor – the government decreed that all *qigong* groups establish official branch ties to the CCP.[380] Falun Gong leadership, however, refused this attempt to formalize the relationship between state and

[376] For a description of state sponsorship and oversight during this period, as well as changing opinion on the relationship between government and Falun Gong on both sides, see David Ownby, *Falun Gong and the Future of China*. New York, NY: Oxford University Press, 2008.
[377] See Palmer, David, *Qigong Fever: Body, Science and Utopia in China*. New York, NY: Columbia University Press, 2007.
[378] Ibid, p. 31.
[379] Seth Faison, "In Beijing: A Roar of Silent Protestors". *The New York Times*, 27 April 1999.
[380] Ownby (2008). pp. 43-45.

non-state actors, and attempted to withdraw from connections to all state-run associations and affiliations.[381]

In the period between 1996 and 1999, the Chinese government undertook a propaganda campaign against Falun Gong. The supernatural elements of the group's practices, which previously had been dismissed as clearly irreligious in nature, were the subject of many publications claiming the organization was theistic, superstitious and anathema to communist precepts.[382] In 1999, tensions between the group and the government culminated in violence against peaceful Falun Gong protesters.[383] The Ministry of Public Security directly authorized these violent arrests.[384] Three days later, many thousands of adherents marched on Beijing in a civilized and non-violent protest of treatment at the hands of the state. At first, it seemed as though a civilized reconciliation might be possible and meetings with the CCP Premier were conciliatory.[385] However, Jiang Zemin, the Party Chairman, explicitly expressed a desire that the group be disbanded and defeated as a threat to societal peace.[386]

Government opposition since 1999 has been ebbed and risen with administrations. However, arguably in response to massive preemptive demonstrations

---

[381] Ibid, p. 46.

[382] For core claims, see Research Department, Ministry of Public Security, "Li Hongzhi." Also see the overview of such publications in Mingxia and Shiping Hua (eds.), "The battle between the Chinese government and the falun gong," *Chinese Law and Government*, September-October 1999.

[383] See Schechter, Danny, *Falun Gong's challenge to China: spiritual practice or 'evil cult'?*. Akashic Books, November 2001, p. 56. Also see Ownby (2008), p. 171.

[384] Schechter (2001), p. 56; Ownby (2008), p. 171; and Ethan Gutmann, An Occurrence on Fuyou Street, *National Review* 13 July 2009.

[385] Gutmann (2009).

[386] *Renmin ribao*, 23 July, 11 August 1999, p. 1; *Guangming ribao*, 13 August 1999, p. 5.

held across more than thirty cities in protest of a perceived crackdown on Falun Gong practice and assembly, Beijing quickly transformed a propaganda campaign against the group to active suppression. In July of 1999, hundreds of senior members and public faces of the organization were seized from branch stations and private residences across the country.[387] Beijing ordered active suppression of Falun Gong, though it took steps to single the group out from non-theistic versions of *qigong*, and mandated that any support of the group was a violation of the atheism demanded by communist doctrine.[388] In short, Beijing quickly and unequivocally banned Falun Gong and actively sought "group disintegration."

Again, in terms of ICT usage by Falun Gong members and leadership, the development of Falun Gong's circumventive toolkit and the organization of such efforts in the early 2000s suggest a correlation between Beijing's suppressive actions and ICT antagonism. In the roughly yearlong period between October 1999 and October 2000, the Chinese government engaged a number of companies in helping them make their Internet censorship campaign against Falun Gong more effective.[389] The PRC's Public Security Bureau stipulated a desire to effectively track Falun Gong adherents, monitor activities and, where possible, retrieve information on the organization.[390] A number of companies, some like Nortel and Cisco based in the West, responded and provided the PRC with a range of tools for tracking down Falun Gong members using the web. By

[387] Spiegel (2002), p. 21.
[388] Julia Ching, "The Falun Gong: Religious and Political Implications," *American Asian Review*, Vol. XIX, no. 4, Winter 2001, p. 12.
[389] See Bell and Boas (2003), pp. 279-282.
[390] Ibid, p. 284.

early 2000, more than four-dozen Falun Gong members had been arrested based on web-based activities.[391] Perhaps more significantly, hundreds of thousands of adherents were increasingly denied access to Falun Gong websites and information repositories through the enhanced countersubversive efforts of the state in denying access.[392] Search terms linked with Falun Gong became the most stringently censored on Chinese social media sites, a trend that continues today.[393] Within nine months of this year of increased digital censorship in the form of a system called Golden Shield, Falun Gong volunteers masterminded the development of DynaWeb, a system designed to allow members to circumvent state-imposed restrictions via rotating access to proxy servers located around the world. This was quickly joined by practitioner-developed tools like Ultrareach and FreeGate to form a web of mechanisms via which a staff of sympathizers – calling themselves the Global Internet Freedom Consortium – could reroute traffic to allow for unfettered access to the web.[394] The proximity of these developments suggests that group

---

[391] See Huang, Bi Yun. *Analyzing a social movement's use of Internet: Resource mobilization, new social movement theories and the case of Falun Gong*. Indiana University, 2009, p. 146.

[392] See, among others, Hong Kong Voice of Democracy, "Chinese Government Blocked E-Mails During Falun Gong Crackdown," <http://www.democracy.org.hk/EN/jul1999/mainland 18.htm>; Melinda Liu, "The Great Firewall of China," *Newsweek*, int. ed., 11 October 1999, <http://discuss.washingtonpost.com/nw-srv/issue/15_99b/printed/int/wb/ov1315 1.htm>; Shanthi Kalathil, "A Thousand Websites Almost Bloom," *Asian Wall Street Journal*, 29 August 2000; "China Bolsters Censorship Tactics on the Internet," *San Jose Mercury News*, 19 September 2000; and "China Tightens Internet Restrictions," Associated Press, 7 November 2000. For a fuller outline, see Ian Johnson, "The Survival of Falun Dafa Rests on Beepers and Faith," *Wall Street Journal*, 25 August 2000.

[393] Bambauer, Derek E., et al., "Internet filtering in China in 2004-2005: A country study," 2005. Also see Hartley, Matt. "How a Canadian cracked the great firewall of China". The Globe and Mail, 3 Oct 2008; and David Bamman, Brendan O'Connor, Noah A. Smith Censorship and deletion practices in Chinese social media firstmonday.org Volume 17, Number 3–5 March 2012.

[394] Gutmann, Ethan. "Hacker nation: China's cyber assault." *World Affairs*, 2010, p. 74.

operatives directly responded to increasing digital censorship by developing circumvention tools.

Falun Gong was also the first target of state-affected denial of service attacks.[395] Falun Gong's main web portal, Clearwisdom.net, was repeatedly attacked for a period of months by hackers based in Beijing and Shenzhen in 2001.[396] Here, the proximity of these actions to Falun Gong's efforts to diversify its online presence based in Western countries suggests a response to rising censorship abilities on the part of the Chinese government. In particular, group members noted the need to diversify the sources of Falun Gong teachings and the need to build a multi-faceted community in 2002, 2004 and 2005.[397] The result has been a proliferation of Falun Gong teachings across the Internet aided by the decentralization of the organization and the move by adherents to establish instruction/outreach portals on personal blogs and social media. Though less mechanically clear, this fragmentation and diversification of Falun Gong's web presence[398] likewise suggests a clear response to the efforts of the Chinese government to interfere with web activism in the years since 1999.

Development of Group Capabilities. As noted above, the development of Falun Gong's ICT operations capabilities is clearly linked to the sponsorship of

---

[395] Ibid, p. 75.
[396] Ibid, p. 76.
[397] See, repectively, See "On Important Matters, Practitioners Must Watch the Position of Minghui Net," <http://www.clearwisdom.ca/eng/2000/July/16/AW071600 1.html>; and Kutolowski, "The Role of Clear Wisdom Net in My Cultivation" referencing <http://www.clearwisdom.net/emh/articles/2000/6/17/9122.html> and <http://www.clearwisdom.net/emh/articles/2000/8/14/9117.html>.
[398] Described in detail in Bell and Boas (2003), pp. 279-282.

foreign-based adherents, sympathizers and (as has been the case with DynaWeb) adopters of the groups dissent toolkit.[399] That said, though the development of sophisticated circumvention tools again demands note of the foreign-based sponsorship of ICT capacity development, the diversification of web presence following disruptive attacked against Clearwisdom.net described above has been the result of actions from thousands of adherents *both* in China and abroad. In particular, the rise of social media has seen a proliferation of efforts to produce interactive communities touting (though not explicitly) Falun Gong precepts and perspectives in a targeted fashion to a domestic audience.[400] Given this and considering the timeline of Falun Gong's online experiences, it seems reasonable to argue that (1) sophistication of the digital environment *did* incentivize Falun Gong to use the Internet for activism but that (2) it was the Chinese government's sophistication of the censorship apparatus that encouraged the employment of ICT for circumvention. At the same time, (3) actual development of sophisticated circumventive abilities has emerged principally from relationships with foreign sponsors. However, given the degree to which *technically* illegal uses of the web have proliferated at in the least sophisticated sense, it appears that (4) access connections beyond borders matter *far* more for more sophisticated efforts to use ICT antagonistically.

[399] A point firmly noted in, among others, Bell and Boas (2003); Bambauer et al. (2005); Ownby (2008); and Tong (2009).
[400] Yu, Haiqing, "The new living-room war: Media campaigns and Falun Gong," 2004.

8.5. Conclusion

The analysis presented in this chapter reinforces the notion that revisionism *indirectly* produces antagonism. A revisionist agenda clearly appears to (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone shady and criminal behavior among fringe members. Chapter 10 further examines subversive activists' use of the web via analysis of Civic, a pro-democracy group active in Hong Kong.

Chapter 9
Nativism and Separatism in Hong Kong: Civic Passion

Christopher E. Whyte

This case chapter investigates the experiences and history of Civic Passion. The chapter proceeds in four parts. First, I summarize the case findings. Then, I outline the body of evidence regarding digital antagonism and Civic Passion. Third, I discuss the history and objectives of Civic Passion and analyze the case with an eye to gauging the explanatory power of competing explanations for incidence of digital antagonism. Again, I do so in parallel fashion across each case study presented through Chapter 10, considering group perspective, structure and operating environments as possible explanations. Then, in Chapter 11, I present an overarching narrative based on evidence found in the following case studies, consider additional elements of each case that strengthen the emergent argument and discuss opportunities for future work.

9.1. Summary

In this chapter, I find that Civic Passion's experience with digital antagonism directly parallels the soul-searching experience the party has gone through over the course of its short life. By soul-searching, I mean to indicate that the party has distinctly

moved from an emphasis on social activism over the course of its life to, quite recently, one of moderate political participation in Hong Kong's electoral and governance processes. The group emerged originally as a social activist outfit focused on reformation of Hong Kong's political system and relationship with mainland China. Perhaps different from other organizations, the group has had and maintains nativist inclinations. This has at times meant unpopularity, particularly when compared with the island's many other pro-democracy outfits.

In the early 2010s, Civic Passion focused on protest of a range of what it saw as excesses by national Chinese authorities and their puppets in local government. In 2014, these efforts coalesced around the Umbrella Movement, a protest of Beijing's installation of a non-elected executive that gained international coverage and for which Passion was a co-founder. Following the end of Umbrella, however, Passion experienced internal turmoil and was especially hampered by the arrest or self-imposed exile of key members. It is during this period of time that the group's main experiences with digital antagonism occurred. Since 2016, however, there have been no apparent employments of ICT for antagonistic or circumventive purposes. This mirrors a move by party leaders to refocus organization efforts on legitimate participation in political processes. In short, the details of this case suggest that cyber attacks by Passion members occurred only when disincentives to antagonize offered by group leaders disappeared following the end of Umbrella.

9.2. Civic Passion and Digital Antagonism

There is limited evidence of digital antagonism on the part of Civic Passion over the past five years that it has been in existence. Towards the end of the Umbrella episode in 2014, a range of cyber attacks took place that vandalized or otherwise disrupted government websites.[401] Several members and leaders of Civic Passion denounced such attacks,[402] which, even in government statements,[403] appeared to be the result of black hat hackers (grey hat, depending on one's perspective) and not the direct intervention of one of the major pro-democracy organizations involved. However, the end of Umbrella in 2014 has seen a range of defacement attacks and disruption of pro-government web services linked to Passion,[404] as well as increased volume of content publication by Passion members that expresses anti-state sentiment[405] and, in many cases, has advocated actions of assembly deemed illegal under state security laws. The last of these attacks, however, was in late 2015 and no other incidents are evident since that time. Thus, it seems fair to say that variation on the dependent variable in this case revolves around the aftermath of Umbrella where Passion reeled from the dissolution of the movement and the absence of key leaders. Prior to that time, the group and its

[401] See Tsui, Lokman. "The coming colonization of Hong Kong cyberspace: government responses to the use of new technologies by the umbrella movement." *Chinese Journal of Communication* 8.4, 2015, pp. 1-9.
[402] See Kwong, Ying-Ho. "The Dynamics of Mainstream and Internet Alternative Media in Hong Kong: A Case Study of the Umbrella Movement." *International Journal of China Studies* 6.3, 2015.
[403] Tsui (2015).
[404] Hjorth and Khoo (2015).
[405] Ibid.

members refrained from using ICT in ways that might have been considered criminal and recent refocusing efforts have produced a similar dynamic.

9.3. Civic Passion

Civic Passion emerged from the unique context of China's integration and regulation of the Hong Kong territory following the 1997 transfer of power from the United Kingdom. The group, founded in 2012 by Wong Yueng-tat, is perhaps most notable for its radical views regarding the separation of China's political system from Hong Kong's.[406] In many ways, Civic Passion is the quintessential liberal subversive organization wherein group direction and messaging has been shaped by a commitment to digital operations.[407] Though it played a unique supporting role in Wong's 2012 election bid (after which he left the group), Passion is like few other advocacy organizations in that its mission statement includes a commitment to Internet-based coordination of a unique political message.[408] It has almost exclusively used ICT for logistical and messaging purposes.

Likewise, whereas China's many pro-democracy groups might be counted as extreme interest groups (i.e. interested in massive modification of political processes without a fundamental grievance about social or cultural norms), Civic Passion diverges from the pan-democracy movement in the PRC in its advocacy for radical separation of

[406] Sataline, Suzanne, "Meet the Man Who Wants to Make Hong Kong a City-State". *Foreign Policy*, 18 May 2015.
[407] Ibid.
[408] Retrieved from https://www.facebook.com/civicpassionpage on April 2, 2017.

Hong Kong form China on all fronts. Though it is sympathetic to China's more radical pro-democracy organizations and has variously organized memorials for the Tiananmen Square massacre,[409] among other incidents, the group maintains a unique nationalistic flavor. It has been labeled as xenophobic, separatist and nativist in its criticism of China's political system as not only fundamentally flawed, but also fundamentally incompatible with Hong Kong's existing sociopolitical and economic structures, colonial history and attitude towards the rest of Asia.[410] In this vein, it also criticizes the broader pan-democracy camp as in the pocket of the government.[411] That said, in 2014, Civic Passion acted as a founding and driving force in the Umbrella Movement that saw large-scale protests against Beijing's installation of a chief executive against Hong Kong electoral tradition.[412] It also fielded election candidates in elections in 2016 in alliance with related pro-democracy movements.[413] However, relatively unique among such groups, Civic Passion remains singularly qualified as a subversive entity. Though statements made by standing government officials and agencies must always be treated

[409] See Ip, Kelly, Phneah, Jeraldine and NectarGan, "Undampened". *The Standard*, 5 June 2013; and Tiananmen massacre remembered at massive Hong Kong vigil, chinaworker.info, 6 June 2014.
[410] "Commission on Strategic Development: Hong Kong's Relationship with the Central Authorities/the Mainland," *Central Policy Unit. Hong Kong Government*. 26 May 2014.
[411] Ibid.
[412] For an overview of the events leading to the Umbrella Movement, see *inter alia* Ortmann, Stephan. "The umbrella movement and Hong Kong's protracted democratization process." *Asian Affairs* 46.1, 2015, pp. 32-50; Lee, Francis LF, and Joseph Man Chan. "Digital media activities and mode of participation in a protest campaign: A study of the Umbrella Movement." *Information, Communication & Society* 19.1, 2016, pp. 4-22; and Lee, Francis LF. "Social movement as civic education: Communication activities and understanding of civil disobedience in the Umbrella Movement." *Chinese Journal of Communication* 8.4, 2015, pp. 393-411.
[413] "Out with the old: Two big-name pan-democrats ousted in tight district council election races". *South China Morning Post*. 23 November 2015.

with skepticism in the case of subversive organizations, particularly in case such as this where the government is authoritarian in format, regular labeling of Civic Passion as possessed of a "localist ideology" demonstrably carry weight insofar as the group aims at fundamental normative transformation of the status quo accompanied by structural change.[414]

Much as is been the case with Falun Gong, Civic Passion is perhaps uniquely understood in the context of how it employs ICT. Financially, it draws operational capabilities from the income of Passion Times (熱血時報), an online-only sister organization that publishes criticism of the government in Beijing and commentary on Hong Kong policy affairs.[415] It makes extensive use of social media to publicize its messages and coordinate assembly in protest of various government actions. In this way, it has increasingly operated much like a traditional interest group or political party, and there is clear evidence that this is the desired outcome Civic Passion is driving towards. In early 2017, Passion spokesmen and leaders announced their intention to act as a more moderate voice in Hong Kong and southern Chinese politics.[416]

9.4. Civic Passion and Competing Explanations for Digital Antagonism

What factors influence the decision Civic Passion has made to, at times, employ ICT antagonistically alongside broader activist efforts? In this section, I break down the

[414] "Commission on Strategic Development: Hong Kong's Relationship with the Central Authorities/the Mainland," *Central Policy Unit. Hong Kong Government*. 26 May 2014.
[415] Lee, Terrence, "Anti-communist news site Passion Times banned from China's Apple App Store". *Tech in Asia*, 11 November 2014.
[416] "Radical Hong Kong group Civic Passion to become 'moderate' political party," *South China Morning Post*, January 6, 2017.

history and context of Passion's use of ICT over the past five years. As with previous chapters, I structure my analyses in by focusing on those factors highlighted in Chapter 4 as those most closely tied to incidence of antagonism by subversive activists.

The next three sections discuss the experiences of Civic Passion, particularly focusing on employment of ICT. Again, the questions being asked are, simply: How have Chinese subversive organizations institutionalized information technology adoption and what institutional mechanisms appear to either impede or encourage use of ICT for circumvention or disruption?

9.4.1. Civic Passion: Aims, Structure and Environment

Subversive Objectives. With Civic Passion, there is clear evidence to support the assertions of H1 and H2 that agenda and expression of grievances strongly play into the move a group makes to use ICT antagonistically. Much as is the case with the other pro-democracy groups operating in China and abroad, Civic Passion maintains a broad portfolio of grievances.[417] Even though Passion's advocacy is couched in the context of the management of Hong Kong and the relationship between China's political system and the adapted version the island enjoys, the organization has regularly joined others in protesting Beijing's treatment of citizens engaged in peaceful protest,

[417] Though mission statement, organizing messages and more can be found at https://www.facebook.com/civicpassionpage, most of Civic Passion's agenda must be cobbled together via analysis of public statements and actions. An overview of this agenda can be found in Ortmann, Stephan. "The umbrella movement and Hong Kong's protracted democratization process." *Asian Affairs* 46.1, 2015, pp. 32-50.

journalists attempting to report on state officials and other elites, and outspoken liberal voices held on either bogus or minimal charges.[418]

Whereas the portfolio of grievances held by organizations like the China Democracy Party has been focused on structural reform consistently across the lifetime of the organization, the same cannot be said of Civic Passion. Passion's origins are in the lead up to the 2012 elections in Hong Kong wherein the group's leader was among several protest candidates seeking office.[419] Following electoral losses that year, Civic Passion stepped up its criticism of Beijing[420] and, in 2014, became one of several founding groups of the Umbrella Movement that sponsored and coordinated large-scale protests of the mainland installation of a chief executive for Hong Kong.[421] From 2012 through 2016, the turn from broadly participationist reform group to revisionist organization took on several unique flavors. Key members of the group were joined by a host of online commentators and casual bloggers in emphasizing the dynamic cultural-historical divide between mainland China and the island that Great Britain had ruled for 100 years.[422] Beyond simply requiring autonomy for economic reasons,[423] Hong Kong

---

[418] See Sataline, Suzanne, "Meet the Man Who Wants to Make Hong Kong a City-State". *Foreign Policy*, 18 May 2015; and Buckley, Chris and Alan Wong, "*Factions Seeking Escalation Put Pressure on Hong Kong Protest*," New York Times, November 24, 2014.

[419] Organisers say 510,000 people take to the streets for July 1 march, *South China Morning Post*, 1 July 2014.

[420] Buckley, Chris and Wong, Alan, "Pro-Democracy Movement's Vote in Hong Kong Abruptly Called Off". *New York Times,* 26 October 2014.

[421] Tsang, Emily; Sung, Timmy; Chan, Samuel, "Split within Occupy deepens as splinter group challenges leadership". *South China Morning Post*, 21 November 2014.

[422] Sataline (2015). Also see "Hong Kong's angry young millennials: an interview with Joshua Wong," *Open Democracy*, 1 November 2015; and "黃洋達辭任熱血領導 黃毓民：樹敵多累選情". *AM730*, 6 September 2016.

exhibited superior cultural and racial dynamics that should be maintained.[424] For some, this was framed as beneficial to the PRC; to others, it was a rationale for separation and the limitation of immigration with the PRC.[425] And yet, Passion's leadership is pulling the group back from the revisionist brink, in 2016 and 2017 announcing a moderation of the group's positions in preparation for electoral efforts in the next several years.[426] In short, Civic Passion has evolved in just the past five to seven years from a radical participationist entity to a staunchly revisionist group to, increasingly, a reasonably moderate reformist political interest organization.

This evolution is critical for understanding the relationship between group grievances and tactical decision-making. There is strong evidence to support H1 and H2 in the experience of Civic Passion, much of which emerges from the changing shape of the group's approach to reformation. As noted above, Civic Passion is also only minimally guilty of acts of digital antagonism, most of which are focused on the time period between 2013 and 2015 in which the group transitioned from a critical reformist entity to a more radical revisionist one. During that time, hackers linked to Passion have engaged in seven distinct denial of service attack series (mostly basic TCP SYN Flood

---

[423] See Steger, Isabella, "Two years after the Occupy protests, Hong Kong's pro-democracy parties are their own worst enemy," QZ, September 1, 2016.

[424] For an overview of Hong Kong's localist political scene and Civic Passion's role from 2014 onwards, see Lo, Sonny Shiu-Hing, *Hong Kong's indigenous democracy: Origins, evolution and contentions*, Springer, 2016. Also see Rath, Robert, "The politics behind Hong Kong's Pikachu protests," ZAM; and Beam, Christopher, "The Uglier Side of the Hong Kong Protests," *New Republic*, October 2014.

[425] Ibid, p. 137.

[426] Kang-chung, Ng, "Radical Hong Kong group Civic Passion to become "moderate" political party," ViewHK, 6 January 2017.

attacks) against Hong Kong government services,[427] have likely been behind several defacements of websites linked with serving PRC officials and have been cited for the use of illegal spamming software.[428] In this situation, Passion's interpretation and subsequent reinterpretations of group prospects and objectives seem to have weighed in quick significantly on decisions to hack or not. In 2012, the group suffered through a massive number of cyber attacks of various kinds likely prosecuted by the Chinese government.[429] In reality, defacements of the group's websites, denial of service attacks against the same and disruption of leadership digital activities beyond that appeared to be the work of non-affiliated online trolls.[430] However, anecdotal evidence and limited technical evidence in the form of IP addresses linking hackers to the People's Liberation Army indicate state involvement.[431] Passion was quick to denounce such tactics.[432] In stark contrast, group leaders made permissive comments linked to the actions of hackers and script kiddies affiliated with the Umbrella protests throughout 2014 [433] before, in 2016,

[427] According to official reporting in "Commission on Strategic Development: Hong Kong's Relationship with the Central Authorities/the Mainland," *Central Policy Unit. Hong Kong Government*. 26 May 2014.
[428] Lo, Sonny Shiu-Hing, *Hong Kong's indigenous democracy: Origins, evolution and contentions*, Springer, 2016, pp. 123-143.
[429] passiontimes.hk brutally attacked by 200,000,000 requests per second, *Passion Times*, 16 November 2014.
[430] Hjorth, Larissa, and Olivia Khoo, eds. *Routledge Handbook of New Media in Asia*. Routledge, 2015, p. 152.
[431] Ibid, p. 152.
[432] See https://www.facebook.com/passiontimes/posts/772681142795055.
[433] See https://www.facebook.com/passiontimes/posts/785429823473298.

addressing civil disobedience online as an undesirable toolkit for the kind of organization Passion hoped to become in moderating its stance out into the future.[434]

Organizational Processes. Civic Passion's structural set up provides an interesting explanation for the group's limited ICT antagonism that fits expectations. Passion is a small and highly decentralized organization with about 300 members.[435] In reality, however, the group's membership might be considered somewhat bigger as advocates of both the group and the cause have surged and ebbed in line with the tumult of Hong Kong's political crises over the past five years. Wong Yeung-tat founded the group in 2012 with the notion that Hong Kong's pro-independence political environment needed the unique form of pressure that only a "militant" social activist outfit could provide.[436] Civic Passion is not only pro-democracy in Hong Kong and arguably not even foremost about democratic revision. In fact, Civic Passion is a localist organization that touts the need for Hong Kong's independence and for the downfall of the Communist Party. As noted above, perhaps the most interesting thing about Passion's evolution in recent years has been the move the group has made from radical participationism to radical revisionism and back towards moderate advocacy for political reformation.

There is an argument to be made that Passion is centralized *only* because of the small membership it enjoys. However, from the perspective of group organization

---

[434] See https://www.facebook.com/passiontimes/posts/744539823098399; and Ng (2017).
[435] Miegel, Fredrik, and Tobias Olsson. "Civic Passion: A Cultural Approach to the "Political"." *Television & New Media* 14.1, 2013, pp. 5-19.
[436] Ending the party ... with thought power?, SCMP, 12 June 2014.

outlined in Chapter 3 that is simply not the case. Cheng Chung-tai heads the party alongside his deputy, Alvin Cheng.[437] Both have attempted electoral runs under the party banner over the past several years.[438] Cheng chairs a small running committee and Wong, who left the organization for some time and still faces accusations of splitting with Passion on several issues, remains involved in high-level decisions.[439] Party decisions are subject to consensus among those few high-level members with only major decisions being put before all members at an annual meeting for an advisory vote.[440] Beyond this, group organization is loose and anything but uniform. Passion maintains no functionally specialized arms beneath party leadership and the boundary between group membership and the broader involvement of individuals in Hong Kong's various pro-independence camps is porous.

Again, this structural set up provides an interesting explanation for the group's limited ICT antagonism that fits expectations. As noted above, Passion eschewed circumventive and disruptive use of the web from the group's formation through the 2012 elections, instead undertaking large-scale mobilization of protests through traditional and social media and disavowing censorship.[441] At this time, Passion threw its weight behind a coalition of pro-independence groups and functioned as part of a protest movement structured far more like a hub-and-spoke organization than anything

[437] "黃洋達辭任熱血領導 黃毓民：樹敵多累選情". *AM730*. 6 September 2016.
[438] "Out with the old: Two big-name pan-democrats ousted in tight district council election races". *South China Morning Post*. 23 November 2015.
[439] "【專訪】鄭松泰：黃洋達退出熱血公民　熱血公民撤出社運　加強社區服務　下月政黨化". *Stand News*. 5 January 2017.
[440] https://ar-ar.facebook.com/passiontimes/posts/1238693692860462.
[441] Ortmann (2015) pp. 39-42.

else.[442] In reality, the movement had several hubs – leaders from various pro-independence and pro-democracy groups that collaborated closely to spread the message and generally coordinate protests.[443] And yet, the group was not hierarchical in that there was minimal functional specialization split out amongst the various sub-units involved.[444] Indeed, for the most part members of the coalition were not organized beneath the leadership level. And, as a number of scholars have noted, Umbrella suffered from acute directional problems.[445] While communicative power rested with a sizeable core group of individuals, directional control was unclear. Moreover, the message espoused by the group was focused on electoral success and the removal of a Beijing-installed chief executive to make way for participatory political outcomes. In short, the movement held no power to make tactical decisions and individuals were being successfully (if ineffectually) directed towards the protest *against* state-caused local disruptions.[446]

Following Umbrella in 2014, Passion continued to sponsor protests on a range of policy issues and prepare candidates for local election runs. However, a range of actions punctuated the 2015-16 period that critics argue demonstrated party radicalization. Establishment of a youth camp to instill radical "militant style training" and lectures on

[442] Ibid, p. 44. Also see Lee (2015), pp. 387-401.
[443] Lee (2015), p. 401.
[444] Ibid, p. 402.
[445] Ibid, p. 404.
[446] In addition to those cited above, see Tang, Gary. "Mobilization by images: TV screen and mediated instant grievances in the Umbrella Movement." *Chinese Journal of Communication* 8.4, 2015, pp. 338-355; and Lee, Alice YL, and Ka Wan Ting. "Media and information praxis of young activists in the Umbrella Movement." *Chinese Journal of Communication* 8.4, 2015, pp. 376-392.

the nature of localism, for instance, were established against a backdrop of rhetoric about the need to solidify Hong Kong's city-state status in preparation for full autonomy.[447] As of early 2017, Passion has begun to back off from some of these radical actions in stating an intention to become a more moderate voice in Hong Kong politics by withdrawing from all social activism efforts.

Again, Passion's use of ICT for activism is extensive and has been a defining characteristic of the party's "militancy" from day one. The party's employment of ICT antagonistically, however, has been remarkably limited and has been concentrated almost entirely within the period between late 2014 and early 2016. Though Passion disavowed cyber attacks against Hong Kong's pro-democracy movement in the lead up to and during Umbrella's main phase, several amateur hackers linked to the group undertook to deface the websites of state officials and agencies in the last days of the movement.[448] Notably, sympathetic web denizens disrupted service to two government agency websites following the 2014 arrest of Wong Yeung-tat.[449] Following Umbrella, Passion supporters have variously been cited for posting illegal content to social media and websites, mostly advocating anti-state sentiment or assembly.[450]

This transition from disavowing online protest and antagonism to acceptance of it lines up remarkably well with changes in the group's mission and structure at the end

[447] Ng, Kang-chung (May 4, 2016). "Pro-independence Hong Kong radicals start recruiting youth corps for 'military' summer camp". *South China Morning Post*. Retrieved December 6, 2016.
[448] Hjorth and Khoo (2015) p. 152.
[449] On arrests, see Barber, Elizabeth, "Hong Kong Police Arrest Prominent Radicals in Home Raids," TIME, December 10, 2014. On defacements, see Hjorth and Khoo (2015) pp. 152-154.
[450] Phillips, Tom and Eric Cheung, "Hong Kong elections: anti-Beijing activists gain foothold in power," *The Guardian*, September 5, 2016.

of 2014. Whereas the group functioned as a part of the broader Umbrella movement in 2014, disintegration of the protests led to the re-fragmentation of Hong Kong's pro-independence landscape and loss of focus on the objectives of the protest movement. The arrest of Passion's leader and several members further decentralized the group and contributed to not only the absence of messaging, but also of direct party direction.

Support and Opposition. In the case of Civic Passion, strict government opposition does not play a clear role in determining the move in 2014 to at least occasionally employ ICT antagonistically. Though Passion has a demonstrably poor relationship with the Chinese government, it is not an outlawed organization in the same vein as either Falun Gong or Eastern Lightning. Nor does Passion endure broad-scoped social opposition to its operation; rather, Hong Kong citizens regard Passion as radical but understandable. Certainly, polling shows general discomfort with the localism espoused by Civic Passion's leaders.[451] Outspoken critics label Wong and others xenophobic, nativist and worse. But Passion maintains broad support particularly among Hong Kong's youth and Passion Times, the party's sister publication, maintains a circulation in the hundreds of thousands.[452]

To the casual observer, there might appear to be a clear temporal link between the group's antagonistic uses of ICT and the actions of the Chinese government, just as in the case of Falun Gong. Following the arrest of Wong and other party leaders towards

[451] Tweed, David, "Hong Kong Independence Goes From Fringe Cause to Contender," *Bloomberg*, February 25, 2016.
[452] Data from www.onlinenewspapers.com/hk.htm.

the end of the Umbrella protest movement,[453] Passion reeled and reformed as something less than a party with clear direction. During the period immediately following the arrest of group leadership, Passion membership took greater steps towards expanding the digital presence of the organization in antagonistic ways. As described above, this included vandalism and disruption of pro-government web services,[454] as well as increased volume of content publication that expressed anti-state sentiment[455] and, in many cases, advocated actions of assembly deemed illegal under state security laws.

However, in terms of causal mechanisms there is little strength in the notion that sudden state opposition to Civic Passion caused the shift in tactics insomuch as the loss of both directional leadership and the cohesion of the Umbrella movement incentivized new, disruptive behavior. In particular, Beijing's arrest of Wong and others was not the first serious opposition to Civic Passion and other pro-democracy groups mounted by state subsidiaries. Throughout 2014, Passion's website and social media channels were among the most frequently hit by denial of service attacks from sources with Beijing, Wuhan and Shanghai IP addresses.[456] Likewise, Passion members were arrested alongside other pro-independence and pro-democracy advocates throughout 2014.[457] Even earlier, government limitations on movement and assembly were leveled at Passion members via regulation off the back of protests over school curriculum and new building

[453] Barber (2014).
[454] Hjorth and Khoo (2015) pp. 151-152.
[455] Ibid, p. 155.
[456] See Sauter, Molly, and Ethan Zuckerman. *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet*. Bloomsbury Publishing USA, 2014, p. 212.
[457] See Hui, Victoria Tin-bor. "The protests and beyond." *Journal of Democracy* 26.2, 2015, pp. 111-121.

development.[458] Nor have such provocations from the government entirely ceased in the meantime. A number of protesters and several leaders were arrested off the back of Passion-led protests on illegal economic enterprises and more.[459] In short, though Beijing's opposition might be tangentially linked with Passion's use of the Internet, the reality – as is the case with both Falun Gong and Eastern Lightning – seems to be that internal group dynamics much more closely drive group decision-making and behavior on this front.

9.5. Conclusion

The analysis presented in this chapter reinforces the notion that revisionism *indirectly* produces antagonism. A revisionist agenda clearly appears to (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone shady and criminal behavior among fringe members. Chapter 10 further examines subversive activists' use of the web via analysis of Eastern Lightning, a messianic Protestant cult active in China.

[458] Tsui (2015), p. 7.
[459] Chan, Kevin, "Chinese shoppers latest target of Hong Kong protest anger". *USA Today*, 2 March 2015.

Chapter 10
Cybersects: Protestant Cultism in China

Christopher E. Whyte

This case chapter investigates the experiences and history of Eastern Lightning (EL). The chapter proceeds in four parts. After summarizing summarize the case findings, I outline the body of evidence regarding digital antagonism and EL. Then, I discuss EL's history and objectives and analyze the case with an eye to gauging the explanatory power of competing explanations for incidence of digital antagonism. Again, I do so in parallel fashion across each case study presented through Chapter 10, considering group perspective, structure and operating environments as possible explanations. Then, in Chapter 11, I present an overarching narrative based on evidence found in the following case studies, consider additional elements of each case that strengthen the emergent argument and discuss opportunities for future work.

10.1. Summary

Eastern Lightning is perhaps unique among the cases included in this dissertation project in that there is no evidence of ICT usage that meets the criteria Chapters 2 and 3 use to describe digital antagonism. In the analysis below, this appears to be a function of the manner in which organizational objectives have dictated the practices of members

and local arms of the cult. Quite apart from an interest in political revisionism, EL's goals are idiosyncratically focused on short-term proselytization and conversion, and long-term preparation for the End of Days. Members are incentivized – through both teachings and financial rewards – to only undertake action against other Christian sects. The result is a distributed organization with little functional specialization among members and a general unwillingness to focus on broader sociopolitical issues. In other words, the aims of the "movement" and the stated method of approach have produced a decentralized organization wherein members don't have the skills or incentives – because the aim is conversion and recruitment – to antagonize even other Christian sects online.

10.2. Eastern Lightning and Digital Antagonism

Much as is the case with other organizations in China, Eastern Lightning's online efforts have regularly brought the group into contentious contact with Chinese authorities. Per the Decision of the Standing Committee of the National People's Congress on Maintaining Internet Security, the organization of "an evil cult, or contacting members of evil cults, or using the Internet to undermine the law enforcement and administrative regulations of this country via the Internet" will lead to prosecution and interdiction by law enforcement.[460] Eastern Lightning has regularly been labeled an "evil cult" [*xiejiao*] in both official statements and the rhetoric of CCP leadership.[461] In

[460] (2003 [2000]) Announcement from the first division of the Shijiazhuang Public Security Bureau. Chinese Law and Government 36(2), pp. 65–73.

[461] Wu (2005). Also see Resolution on Opposing Evil Cults and Resisting Heretical Beliefs, Amity News Service 11:5/6, 2002. Available at http://www.amitynewsservice.org/page.php?page1/4674.

particular, Eastern Lightning is especially guilty of the kind of digital antagonism described in the introduction to this section – that counted as antagonism and sedition by the Chinese government in stark contrast with what might be the case in a Western country. Within China, the group pours large amounts of resources into recruitment and conversion in the central and western regions of the country.[462] Members and cult leaders have regularly been sought for violating state law in service of such goals, specifically through the use of IM and email to proselytize.

That said, Eastern Lightning has not appeared to move beyond basic digital antagonism that exists in a unique fashion in China – what we might call structural or passive antagonism due to the way in which vanilla activism flaunts national regulation. Whereas Falun Gong and Civic Passion have employed information enrichment techniques (such as illicit spamming software or basic defacement techniques) in service of their campaign objectives, Eastern Lightning has not. Furthermore, there is no evidence of interest in the use of ICT for more severe forms of circumvention or disruption. Indeed, as Dunn and others have noted,[463] Eastern Lightning's behavior in this regard suggests a unique sensitivity to the lessons and experiences of other countercultural groups in China. Specifically, the behavior of the group in responding to crackdowns aimed at members of Falun Gong and Zhong Gong in the 2000s, wherein Eastern Lightning took steps to clarify their policy on distributing bibles and

[462] See Guo, Luke, Dangxin! "Dongfang shandian" yudang zhengzai liyong QQ laqun, 3 March 2006. Available at http://bbs.loves7.com/viewthread.php?tid1/423353, accessed 6 April 2017; and Forney, Matthew, Jesus is back, and she's Chinese. Time 158:8, 2001. Available at http://www.time.com/time/world/article/0,8599,181681,00.html.
[463] Dunn (2007), p. 452; Thornton (2003) pp. 254–256.

proselytizing through its principal websites,[464] suggests a keen awareness of the operational position being taken in relation to the Chinese government.

10.3. Eastern Lightning

Over the past four decades, a broad range of Protestant religious movements have emerged in China. Of these, by far the most prolific and controversial is the Church of Almighty God (better known, in reference to a verse in the gospel of Matthew, as 'Eastern Lightning')[465]. Eastern Lightning is remarkably different from the broader universe of Protestant groups operating across East Asia in that the group moves beyond common sectarian contestation of points of doctrine to assert that we currently live in what they call the "Age of the Kingdom."[466] In short, the group believes that Jesus Christ has been reincarnated as a Chinese woman who is tasked with cleansing and preparing contemporary society in preparation for the end of days.[467] The verse in Matthew that cedes the name 'Eastern Lightning' holds that lightning seen in the east will become visible in the west and will signal "the coming of the Son of Man."[468] In short, they believe that a second incarnation of God has appeared among them in the form of a Chinese woman and that their teachings are destined to spread to Western Christianity prior to the coming judgment. From the perspective of the Chinese

[464] See http://english.hidden-advent.org/book_request.php, accessed 15 April 2007.
[465] For perhaps the best overview of the origins of the organization and its inspirations in scripture, see Dunn, Emily C. ""Cult," Church, and the CCP: Introducing Eastern Lightning." *Modern China* 35.1, 2009, pp. 96-119.
[466] Ibid, pp. 99-102.
[467] Ibid, pp. 100-101.
[468] Ibid, p. 97.

government, Eastern Lightning is, in many ways, the purest manifestation of a subversive threat to contemporary society. After all, the group is not merely a religious organization that proselytizes and practices without the legal or nominal blessing of the government; EL preaches a cult-like doomsday ethos that *emphasizes* the hidden nature of a transforming force in current Chinese society (i.e. the Second Coming of Jesus Christ in the form of a human whose face is as yet hidden from the public).

The Eastern Lightning organization appeared in China about 1990, ostensibly founded by a man called Zhao Weishan.[469] The objective of the movement is to spread their philosophical musings and doctrine across China and the West to lay the foundations for the coming of the "Son of Man." To this end, Eastern Lightning has extensively undertaken activism via the use of ICT. In fact, Eastern Lightning's logistical apparatus is best known for its extensive online presence and its unusually adaptive approach to spreading the group's version of the gospel.[470] The group, which is broadly considered to be a cult and is officially labeled as a subversive, "evil cult" by Chinese authorities,[471] maintains an extensive set of web-based resources across several websites and numerous affiliated forums, blogs and more.[472] As Dunn notes, however, Eastern Lightning's effort contrasts with that of Falun Gong in that the cult is primarily focused on pushing content and teachings to a broad audience across China and the

[469] Ibid, p. 98.
[470] See Emily C. Dunn, Netizens of Heaven: Contesting Orthodoxies on the Chinese Protestant Web, *Asian Studies Review*, 31:4, 2007, pp. 447-458.
[471] Wu Dongsheng, Xiejiaode mimi: dangdai Zhongguo xiejiao juhe jizhi yanjiu (English title: The secrecy of evil cult – A study on the regime of evil cult assembly in today's China), Beijing: Shehui kexue wenxian chubanshe, 2005.
[472] Dunn (2007), pp. 448-450.

West.[473] Falun Gong, by contrast, has demonstrated considerable interest in building interactive and responsive communities of contention in direct contravention of prevailing societal conditions.[474] In short, Eastern Lightning's flavor of subversion is passive, for the most part, and aimed at selling a broader image of eventual transformation over attempting to actualize it. Though this strategic approach to the subversive enterprise is less common among subversive organizations than a layman might guess, research undertaken in the course of this project suggests that it is not particularly uncommon amongst religiously or spiritually motivated groups wherein there is a sense of inevitable transformation nested in forces beyond the social (i.e. when God wills it).

10.4. EL and Competing Explanations for Digital Antagonism

What factors influence the decision EL has made to, at times, employ ICT antagonistically alongside broader activist efforts? In this section, I break down the history and context of Passion's use of ICT over the past five years. As with previous chapters, I structure my analyses in by focusing on those factors highlighted in Chapter 4 as those most closely tied to incidence of antagonism by subversive activists.

---

[473] Ibid, p. 449. Also see Bell, Mark R., and Taylor C. Boas. "Falun Gong and the Internet: Evangelism, community, and struggle for survival." *Nova Religio: The Journal of Alternative and Emergent Religions* 6.2, 2003, pp. 279-282.

[474] See Bell and Boas (2003), pp. 279-282; and Thornton, Patricia M., The new cybersects: Resistance and repression in the reform era, in E. J. Perry and M. Selden (eds), Chinese society: Change, conflict and resistance. 2nd edition, 2003, pp. 247–270 (London/New York: Routledge Curzon).

The next three sections discuss the experiences of Eastern Lightning, particularly focusing on employment of ICT. Again, the questions being asked are, simply: How have Chinese subversive organizations institutionalized information technology adoption and what institutional mechanisms appear to either impede or encourage use of ICT for circumvention or disruption?

10.4.1. Eastern Lightning: Aims, Structure and Environment

Subversive Objectives. For the most part, Eastern Lightning has not demonstrated an interest in fundamentally restructuring the Chinese political system. Rather, the group's aims are simultaneously idiosyncratically focused on messianic salvation and short-term conversion of non-believers. Though structural from some points of view, this grievance format is in no way revisionist as the coding in Chapter 3 describes. Given this, a complete absence of antagonistic ICT usage makes some significant sense. As sections below show, however, there is greater nuance in EL's disinterest in and inability to use ICT effectively than the nature of their grievance suggests. In short, it is how expressions of aims have led to unique membership practices that has determined the group's lack of focus in this area.

Eastern Lightning has maintained a clear and extensive web presence since 2000.[475] At that time, the group's digital outreach consisted largely of a single informational website with an access portal and a range of resources proclaiming the

[475] Dunn (2007), p. 447.

various elements of the group's philosophy and objectives.[476] Since then, the group's presence online has grown more sophisticated and specialized in terms of its methods for targeting an ever-expanding audience in China and around the world. Specifically, Eastern Lightning's diverse administration has constructed a range of web pages and separate sites designed to invite attention from new markets in the West and in rural China,[477] and has shown strategic forethought in naming and cultural conventions, adapting URLs, site content and methods of content delivery (such as email listservs, newsletters, etc.) to better communicate their message.[478] The group's primary U.S. based website, for instance, has regularly been updated to include graphical representations of the groups theological positions (cartoons, real-life portrayals of worship, etc.). Moreover, the group has adopted a range of popular messaging methods for pushing audience access to content,[479] though EL is notable for its strategic exclusivity in its outreach efforts wherein it provides a clear path for converts and others to group content but *never* links EL to other organizations.[480] Despite this extensive and regular digital activist footprint, there is no evidence that the group has been responsible for either circumventive or disruptive ICT employments since 2000. Insofar as the group has clashed with the Chinese government and is subject to scrutiny, it could at most be

[476] That website, godword.com, was copyrighted in 2000. Archived pages for 2001-2004 can be found here: http://web.archive.org/web/http://www.godword.org, accessed 9 April 2017.
[477] Beyond godword.com, principle sites include truthwaylife.org, thealmightyhasreturned.com, voicefromthethrone.org, holyspiritspeaks.org, hidden-advent.org and endtimeworkofgod.org.
[478] Dunn (2007), pp. 448-450.
[479] Mclelland, Mark. "Internet Domains between China and India: Beyond Anglophone Paradigms." *Asian Studies Review* 31.4, 2007, pp. 387-395.
[480] Dunn (2007), p. 451.

said that the group performs outreach and messaging on pertinent sociopolitical issues via an expanding web of seemingly partly affiliated blogging sites designed to mask user input as much as to present the image of a popular movement.[481]

Again, Eastern Lightning has not demonstrated an interest in fundamentally restructuring the Chinese political system. That is not to say that EL has never been the source of civil unrest in China. Nor is that to say that the group has not made rhetorical attacks on Beijing. From 2012 to 2014, the Chinese government arrested more than 1,000 EL protesters and adherents for spreading rumors, in line with group doctrine, that the world was coming to an end.[482] Authorities seized a broad range of EL materials used for proselytizing, including digital media on hard storage devices, VHS, etc.[483] and group members were cited as encouraging followers to rise up to "exterminate the red dragon and found a country under the rule of Almighty God."[484] Indeed, this is indicative of EL's somewhat violent and anti-establishment past. According to various reports, the group has been responsible for dozens of kidnappings of both Chinese and foreign nationals over the past three decades.[485] For the most part, these kidnappings – some of which have brutally involved personally injury through torture, blackmail and forced conversion – have been focused on expanding the EL following and indoctrinating

---

[481] Ibid, p. 453.
[482] Hunt, Katie, "China arrests 1,000 members of banned religious cult 'Eastern Lightning'" *CNN*, August 20, 2014; and Kaimin, Jonathan, "China arrests 500 followers of religious cult over Mayan apocalypse rumours," *The Guardian*, December 19, 2012.
[483] Kaimin (2012).
[484] Ibid.
[485] For perhaps the best overview of this vein of EL's history, see Shea, Matt, "The Cult Who Kidnaps Christians and Is at War with the Chinese Government," VICE, July 21, 2013.

outsiders in the cult's doctrine. In some instances, where Hong Kong-based members of the group spoke out against mainland counterparts,[486] these events seem to be a function of the group's decentralized nature where local cult members break with group direction and execute their own operations. This history of violence is a radical departure from the profile enjoyed by Falun Gong, an organization considered in roughly the same category as EL – i.e. an "evil cult" – by the Chinese government.[487]

In sum, EL is certainly rhetorically opposed to the "red dragon"[488] (the CCP) and has been behind low-level protests of state policy on religious organization. However, it cannot be said that Eastern Lightning is in any way a cohesive revisionist organization. Indeed, the church has variously made statements that there is "no anti-government sentiment" held by the group.[489] Rather, its logistical operations are entirely focused on proselytizing and conversion. In many ways, EL shares features of Scientology in the United States and elsewhere; it is occasionally violent, cultist in its coercion of members and subversive in a fantastical sense that few subversive groups tend to be. But it is not explicitly revisionist so much as it is generically anti-establishment. Likewise, this lack of specificity regarding the Chinese government and political system means the lack of a complex policy portfolio. Insofar as there is no direct objective bound up in criticism of the PRC (or, rather, a fantastical doomsday objective), EL maintains a highly minimalists policy portfolio. Given this, a lack of emphasis on digital antagonism falls in

[486] Ibid.
[487] For a description of EL's status over time, see Andrew Jacobs, "Chatter of Doomsday Makes Beijing Nervous". *The New York Times*, December 19, 2012.
[488] Ibid. Also "the great dragon" or "the great red dragon."
[489] For instance, see godword.com/e/qve/78326423984.

line with expectations regarding the relationship between the nature of group grievances and decisions not to employ ICT antagonistically.

Organizational Processes. While EL's lack of use of ICT for disruption or circumvention fits expectations stemming from the grievance hypotheses, the same cannot be said if one considers group structure at first glance. Eastern Lightning is a highly centralized organization with extremely clear theological leadership. To clarify, communicative and doctrinal power is highly centralized in the hands of leaders like Zhao Weishan (the group's founder), Zhang Dakai and Yang Xiangbin (the female Chinese reincarnation of Jesus Christ).[490] Yang Xiangbin is the head of the church in theological terms, though real power sits with Zhao, the Chief Priest.[491] Mirroring elements of CCP structures, the Chief Priest sits on a supervisory committee of seven members that rotate in and out of power as they gain or lose Zhao's favor.[492] Importantly, Zhao is not the head of this committee and others have held that role. Nevertheless, the committee functions in line with his favor and wishes.

The structure of the Eastern Lightning organization beneath this supervisory committee and Zhao is technically hierarchical. Group elements are organized at the provincial, local and cell levels, with leaders at each unit size answering directly to those

[490] See Bennett, William, "Where Did Eastern Lightnings Leaders Come From?" ChinaSource, April 2, 2014.

[491] This narrative has appeared across government reporting and academic works on the subject. See, for instance, Dunn (2007) and Wang Zaihua 王在, "Quannengshenjiao mudi shi tuifan zhengfu jian 'shen de guodu'" 全能神教目的是推翻政府建"神的國度" [The goal of the Church of the Almighty God is to overthrow the government and establish "The Kingdom of God"], China Central Television 中国中央台, December 22, 2012.

[492] China Anti-Cult Association, *Shipo xiejiao "quannengshen"* 破邪教"全能神" [Seeing through the "Almighty God" cult], http://zt.kaiwind.com/a/qns/shipin/2013/0124/284.html.

above all the way to Zhao.[493] However, though there is great functional specialization among these units (specifically stemming from highly specific publication and proselytization tasks set by the supervisory committee), there is also an emphasis on duplication of functions and redundancy.[494] In short, though the organization appears bureaucratic in its organizational structure, it might best be described as a form of a pyramid scheme. Branch elements are expendable and replicable, as are individuals placed as leaders all the way up through the supervisory committee.[495] Moreover, functional specialization is limited to specific activities like the publication of pamphlets. As such, in some senses, the organization is thus remarkably decentralized in directional terms. The head of the group communicates but only controls a core set of activities. Beyond this, cells tend to be remarkably independent in their ability to strategize and adopt different local approaches to conversion and proselytizing. This unique format is evident in the broad range of conversion efforts undertaken by cell units of EL, including bribery, sexual persuasion, financial and sexual blackmail, torture and use of narcotics.[496]

Again, at first glance, EL does not appear to fit with what we might expect from an analysis of the organization's structure. EL does not employ ICT antagonistically. Whether you consider EL to be highly centralized or meaningfully decentralized, this does not fit the logic laid out in Chapter 3. Relative autonomy beyond basic tasks among diverse cell branches of the group implies a propensity for free agent action on

[493] Dunn (2009), p. 107.
[494] Ibid, p. 109.
[495] Wang Zaihua (2012).
[496] Again, see Shea, Matt, "The Cult Who Kidnaps Christians and Is at War with the Chinese Government," VICE, July 21, 2013.

this front. Likewise, the results of Chapter 4 suggest that clear centralization also increases the likelihood that the organization would respond to the oppression of the Chinese government, discussed further below, via organized ICT antagonism. Not only is this not the case, but EL rarely engages in non-digital antagonism or protest of the state, clearly preferring to focus on conversion and theological efforts.

And yet, EL's lack of commitment to organized antagonism makes some sense in the context of the organization's unique pyramid scheme form of hierarchy. Though leadership is highly organized and hierarchy is clear, the operation of the supervision committee and its subsidiaries is likely a function of Zhao's effort to maintain power. Much as a dictator might toy with his winning coalition[497] by introducing new group leaders from a broad selection of alternatives, Zhao dismisses leaders that differ on key points or inspire some sort of personal ire. Thus, the leadership of Eastern Lightning lacks the logistical unity of bureaucracies. At the same time, three obstacles to free agent behavior exist with the group's otherwise reasonably independent cells. First, cells are directed to engage in few, highly specific tasks and are provided no additional training in the context of EL's overall objectives. Second, the inability of individual members to "defect" and use ICT disruptively likely stems additionally from group demographics, wherein converts often come from poor communities or rural areas. Finally, the cultist mindset of Eastern Lightning, which touts an internal system of promotion based on particular behaviors and success in converting others, has created a culture that

[497] De Mesquita, Bruce Bueno, *The logic of political survival*, MIT Press, 2005.

discourages such deviation from established practices. In other words, there is little in-group incentive to innovate in group practices offered to adherents.

Support and Opposition. Eastern Lightning has experienced broad-scoped social and government opposition in recent years. However, the group has consistently demonstrated a lack of concern with public perception and the limited footprint of the organization has meant that government repression is less sophisticated than it has been with Falun Gong. Given any lack of impetus to respond to outside conditions, it is unsurprising that the group has not felt the need to expand its toolkit with digital instruments.

Eastern Lightning's experience with social opposition stands in stark contrast with that of Falun Gong, where there is general ambivalence to *qigong* and related activities. With EL, there is broad social opposition to what is seen as a cult group.[498] In particular, opposition to EL and paranoia about the actions of its adherents are strongest among China's large-but-underground Christian population. As a communist state, the PRC is atheist and allows only certain organized religions that must maintain formal relations with the state. Nevertheless, there is a broad Protestant and small Catholic practitioner base across a range of sects in China not recognized by the state. Typically, such Christians practice in family and friend groups in private settings or in "underground" churches hidden from the public eye.[499] By contrast with the country's

[498] Kaimin (2012); Dunn (2009), p. 101.

[499] For a broad overview of Christianity under communism in China, see Lian, Xi. *Redeemed by fire: The rise of popular Christianity in modern China*. Yale University Press, 2010.

Muslim population, the government in Beijing is only occasionally concerned with suppressing such activities.[500] A range of scholars note that this is likely because few of China's Christian communities exhibit extreme sectarian behavior that the government could link to social discontent.[501]

Paranoia about EL is strong among China's Christian communities because EL cells are demonstrably interested in conversion from within the broader faith over atheistic indoctrination. Though the group will certainly attempt to recruit members from the general population at times, the main thrust of EL proselytizing occurs through the infiltration of non-EL churches.[502] Tactics have included slow efforts to subvert entire hidden Christian communities to the EL cause through increasing exposure to Zhao and Yang's version of the gospel. More often, EL members directly interact with other Christians through kidnappings, beatings, torture and various forms of blackmail.

By contrast, Eastern Lightning's experience with government opposition aligns with that of Falun Gong. Though the suppression of Eastern Lightning has been less severe than is that of Falun Gong – perhaps due to the much smaller membership of the group – the government in Beijing maintains that EL is an "evil cult" and various state officials have labeled EL as "another Falun Gong."[503] The group has been officially banned since 1995.[504] In particular, the Chinese government began to more heavily

---

[500] Lian (2010), p. 8.
[501] Ibid, pp. 15-17.
[502] Dunn (2007), pp. 451-453.
[503] Xinhua, 7 August 2006.
[504] *"Gonganbu guanyu chajin qudi 'huhanpai' deng xiejiao zuzhi de qingkuang ji gongzuo yijian"* 公安部关于禁取"呼喊派"等邪教的情况及工作意 [Opinion of the Ministry of Public

crackdown on EL in 1998 after eight small violent protests that broke out in Henan province.[505] In recent years, the government has stepped up efforts to locate group members. These efforts have led to more than 1,500 arrests. Several practitioners were jailed or executed between 2012 and 2017 in response to violent attacks, notably the murder of a woman in a McDonalds.[506]

Beijing's cyber suppression of Eastern Lightning has been less focused than has the campaign against Falun Gong. Falun Gong is presented as a unique existential threat to the Chinese state and authorities – notably the 6-10 Office super-agency set up by the PRC to end dissident threats – hold the destabilization and destruction of the group as a sine qua non.[507] By contrast, the 6-10 Office focuses on Eastern Lightning and organizations – for instance, those linked with Xinjiang or Tibetan separatism – as minor digital threats.[508] In reality, most suppression of Eastern Lightning comes in the form of direct monitoring and sporadic cyber attacks on group websites.[509] There is, nevertheless, a tactical similarity in the way that China treats Falun Gong and groups like EL. For the 6-10 Office, the goal is to create a net of observation that allows full knowledge of dissident activities such that the government can craft its suppression campaign towards achieving the most beneficial results (i.e. retaining full control of timing of arrests,

---

Security on the circumstances and work related to investigating and stamping out cults such as the "Shouters"].

[505] Zhang Dakai, *Pouxi xiejiao zuzhi "Dongfang shandian"* "" [Analyzing the cult "Eastern Lightning"], p. 7.

[506] Carrie Gracie (13 August 2014). "The Chinese cult that kills 'demons'". BBC. Retrieved 8 April 2017.

[507] See Gutmann, Ethan. "Hacker nation: China's cyber assault." *World Affairs*, 2010, pp. 70-79

[508] Ibid, p. 75.

[509] Dunn (2007), p. 458.

preventing assembly, etc.).[510] For an unauthorized organization like EL, creation of such a net can be difficult, particularly as EL maintains a limited Web presence based in Western countries and advocates their theology through physical means (direct proselytizing, pamphlets or newspapers). Moreover, again likely because of the scope of the organization, Beijing's actions taken against EL online have largely been restricted to monitoring activities and not disruption.

To some degree, EL's experience with state suppression fits the trend set in the Falun Gong case. With such restrained suppression, it is perhaps of little wonder that there has been no apparent impetus to enhance group circumventive capabilities. Likewise, as heightened social opposition manifests in this case, it is unsurprising that the group has not felt the need to slip the "net" and employ ICT to reach a broader audience. Since the group's focus on other elements of the Christian community in China has particularly involved interactions with more mainstream "underground" house churches, there has been relatively limited advertisement of group activities in police reports or publications. Since these sects operate without government approval, the incentive to avoid state involvement provides a further cover for Eastern Lightning's activities and produces a distinct disconnect between member activities and general sentiment on EL in the population at large.

[510] Gutmann (2010), p. 74.

10.5. Conclusion

The analysis presented in this chapter reinforces previous chapters' suggestion that revisionism *indirectly* produces antagonism. Just as before, the preceding sections note that there is a strong relationship between revisionism, the way objectives are articulated by key decision-makers, and the way in which groups interact with proxies that employ ICT antagonistically. Again, a revisionist agenda clearly appears to (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone shady and criminal behavior among fringe members. This theory explains variation in the experiences of the five organizations described in Chapters 6 through 10 on a number of fronts. Moreover, focus on group objectives itself provides more mechanical insight as to the direct causes of choices to antagonize than do other variables. Cases examined in both Germany and China have certainly demonstrated that there is a correlative link between support for an organization and the group's propensity to the use of ICT for circumvention or disruption. But evidence suggests that elements of a given organization respond to changes in how objectives are articulated – in direct statements and the condition of support from group leadership – in determining whether or not to act antagonistically. The preceding chapters also indicate that national-level context *does* dictate the terms of subversive activism and a group's use of ICT for all manner of activism. This itself is an important point that has a number of implications – to be discussed in Chapter 12's discussion of research implications and

next steps – for the budding research programs on cyber repression and the spread of cyber "arms" in the form of developing markets for toolkits of activism and antagonism.

Chapter 11
Case Study Conclusion: Analysis and Further Steps

Christopher E. Whyte

The content of the five cases presented in Chapters 6 through 10 suggest that there is a strong relationship between revisionism and the way in which groups interact with proxies that employ ICT antagonistically. Having said this, the narrative approach to understanding digital antagonism in the preceding chapters focused on determining the variable strength of different possible explanations and elucidating the viability of different mechanisms that cause variation on the dependent variable. Here, there remains need to further assess the findings of the preceding empirical chapters when taken together. Thus, this chapter is devoted to outlining evidence across the five cases presented in Chapters 6 through 10 that corroborates the theory suggested in Chapter 4. This chapter also discusses the impact of national-level conditions and describes remaining shortcomings of the research design in aid of future scholarly efforts. In preparation for these tasks, the next section summarizes the findings of the preceding case chapters and outlines the general argument that follows on from them.

11.1. What the Cases Say About Subversives and Digital Antagonism

What prompts decision-making amongst subversive actors to retain emphasis on strategies of antagonism whilst attempting to digitally engage the public in some cases, but not in others? As the case analyses of groups in China and Germany show, this narrative regarding subversive groups' uses of ICT for both activism and antagonism oversimplifies in its description of general trends. In many ways, such an oversimplification is inevitable insofar as subversive actors as a category of non-state belligerents are immensely diverse (as is the repertoire of digital antagonism available to such actors). But case analyses reveal much about the common features of experiences with ICT had by different subversive groups in world affairs such that a unique story about the relationship between core and peripheral elements of subversive actors emerges.

Before discussing these features, it is worthwhile revisiting those expectations had regarding the experiences of different groups as based on the results of Chapter 4's quantitative analysis (see Table 11.1):

Table 11.1. Summary expectations and findings across primary independent variables for case studies in Chapters 6, 7, 8, 9 and 10.

Group	Eastern Lightning	Civic Passion	Falun Gong	NPD	Die Linspartei
Type of Agenda	Idiosyncratic	Limited > Maximalist	Limited	Maximalist	Maximalist > Limited
Nature of Grievance	Non-Structural	Structural	Non-Structural	Structural	Structural
Permissive (Summary)	No	Mixed	No	Yes	Yes
Regime Type	Autocracy	Autocracy	Autocracy	Full Democracy	Full Democracy
Regime Durability	High	High	High	High	High
Contestation	Repressed Competition	Repressed Competition	Repressed Competition	High	High
Type of Structure	Bureaucratic (Pyramid)	Weak Bureaucratic	Mixed All-Channel	Hub-and-Spoke	Bureaucratic
Criminal History	Yes	No	Yes	Yes	No
Foreign Sponsors	No	No	Yes	No	No
Gov't Inquiry	Yes	No	Yes	Yes	No
Expectations	Minimal or no incidence of digital antagonism	Some incidence of digital antagonism	Minimal or no incidence of digital antagonism	Occasional incidence of digital antagonism	Pronounced incidence of digital antagonism
Findings	No incidence of digital antagonism	Punctuated incidence of digital antagonism	Consistent low-level incidence of digital antagonism	Punctuated incidence of digital antagonism	Punctuated incidence of digital antagonism

As noted in previous chapters, the dependent variable is only loosely dichotomous insofar as the data employed in Chapter 4 is episodic. There is no basic assumption of ICT usage for antagonism across the entire lifespan of a subversive campaign. Rather, the assumption bound up in the puzzle is that such employments will emerge in line with the evolution or appearance of distinct driving characteristics of subversive organizations or the environment in which they operate. My expectations on the degree to which dependent variable variation should occur across cases were therefore based on observation of variation across a range of different independent variables. Where multiple conditions appeared to vary in line with the predictive results of Chapter 4, I held a strong expectation that digital antagonism would be completely absent or markedly prominent in the experiences of a given organization. Where conditions were mixed, I held the expectation that groups would have a mixed set of ICT experiences conditioned on the main explanatory variable highlighted in Chapter 4 – the nature of group grievances.

Table 11.1 above outlines group-specific case conditions and expectations. Of the groups studied, I found that four generally conformed to my expectations. In the case of Eastern Lightning, the expectation that no interest in structural revisionism and the maintenance of an idiosyncratic portfolio of aims fits with the lack of observation of digital antagonism. Likewise, Civic Passion, the NPD and Die Linke were guilty of digital antagonism roughly in line with expectations. Only the case of Falun Gong, taken as a whole, contradicts expectations.

And yet, the story emerging from each case is more nuanced than these general conditions suggest. With Civic Passion, the NPD and Die Linke, antagonistic employments of ICT have been concentrated in specific periods of time. In each case, variation on the dependent variable is limited to periods following organization fragmentation or consolidation efforts. Evidence from each case, which will be further addressed in sections below, suggests that cyber antagonism varies directly with the permissiveness of the organization's broader membership sphere and degree of permissiveness is largely determined by how group leaders (1) express their objectives and (2) formalize their aims in group policy. With the three cases mentioned above, antagonism occurs directly in line with changes in such dynamics. With Eastern Lightning, an idiosyncratic guiding ideology and incentive structure diminishes both the ability and desire of members to antagonize online. And with Falun Gong, the unique diaspora dynamics of the movement produce an unexpected result wherein antagonism is common, but emerges solely from peripheral members and leaders based abroad.

Given these results, it sees clear that revisionist agendas (1) incentivize the development of free agents that antagonize and (2) produce a willingness to condone shady and criminal behavior among fringe members. Specifically, where a group turns from participatory approaches, both group leaders and peripheral elements are incentivized to condone and undertake antagonism. For leaders, fringe operations remain largely deniable, present as a unique set of options for mitigating the gains of sociopolitical opponents and offer opportunities for growth beyond those that accompany

legitimate political participation. For peripheral elements in such a situation, digital antagonism is a cheap and arguably effective way for advancing a cause without (1) running the risk of harming efforts to garner broad public support or (2) running into the kind of significant law enforcement opposition to civil disobedience that often, offline, leads to arrests and negative publicity.

11.2. Corroborating Evidence

Case studies are useful for illustrating theory that emerges from quantitative testing and discovering key mechanisms through process tracing. As such, though case narratives can reveal the necessary nuance to draw a more detailed picture of action and reaction as it pertains to the dependent variable, analysis of specific features of different cases is invariably required to validate the emerging argument and discount alternative explanations. As such, I ask this section what else we might expect to see in these cases given the argument above.

11.2.1. The Link Between Greater Revisionism and Greater Antagonism

Up until here, cases study analysis of the NPD and Die Linke in Germany and Falun Gong, Civic Passion and Eastern Lightning has outlined suggested a plausible causal mechanism for incidence of digital antagonism among sub-elements and proxy actors with clear membership affiliation to subversive entities. Changes in strategic objectives are reflected in group structures and new direction creates incentives for free agents antagonism. The case sections above show how macro changes in party direction

and staunch refusal to adopt participatory approaches to revision are linked with different measures of digital antagonism. But what else might we expect to see if articulation of strategic direction in statements and party organization is the main mechanical cause of variation?

Direct Encouragement. One clear sign of the link between shifting strategic direction and changes in the antagonistic tendencies for the broader organization would be direct statements of either encouragement or discouragement. For our purposes, where the far left and far right in Germany target one another for attention, for recruitment purposes and for philosophical reasons, changes in the responsiveness of either the NPD or Die Linke to antagonism in line with the narrative described above would signal support for the theory.

Such statements exist in both cases. With Die Linke, according to Patton, party doctrine shifted in a major fashion in 2004-2005 from active encouragement of antagonism in countering the far right to one of public denouncement of the NPD and related groups as antithetical to modern German society.[511] Members and affiliates of PDS broadly protested performances by several neo-Nazi punk bands in 1997 and 1998 in Saxony and Brandenburg, for instance. More than simply protesting the shows, PDS's Zimmer and several others made public statements through October of '97 holding that members should "resist fascism" and "take all measures to expel" neo-Nazi influences from Germany. Resulting clashes between band supporters and protesters turned violent, with

[511] Caiani and Parenti (2016).

riot police eventually breaking up fighting that produced a dozen serious injuries in Dresden. Five Left Party members were among those arrested for inciting crowds to push past policemen separating the groups.[512] Similar incidents occurred in Magdeburg when NPD officials visited prior to state elections in 1998, 2000 and 2002, with Voigt and several other leftist spokesmen coming under fire for the perceived invitation to violence in their statements.[513] And active encouragement of antagonism on the part of the organized far left has not always been simply rhetorical. Die Linkspartei officials refused to comment on website defacements by far right organizations in 1998 and 2001.[514] Combined with subsequent denial of service attacks on a range of far right sites – more than 18 of which were linked to the NPD – this non-acknowledgment led to media coverage of a "private war" fought at the fringes of German politics.[515]

By contrast, Die Linke spokesmen and officials have rarely made such remarks following the 2005 elections. Indeed, party doctrine emphasizes calling attention to antagonism by either far right or other extremist elements (*including* other far left wingers) as public nuisances. Specifically, Gysi, Lafontaine and others denounced spamming of NPD content in emails in 2009 prior to state elections as "propaganda unbecoming" a "so-called political party" and widely panned the NPD's alleged use of

[512] 2000 Annual Report of the Office for the Protection of the Constitution, p. 7.
[513] "Bundesverfassungsgericht verbietet Überwachung von Bodo Ramelow". tagesspiegel.de. Retrieved 7 April, 2017.
[514] Patton, (2011).
[515] Ibid.

private demographic data as a "crime to bolster" the case of the federal government to ban the NPD.[516]

With the NPD, newfound freedom of operation and rising vocal support among a minority of Germans (particularly in the former East Germany) in the 1990s saw a renaissance of pushback against the violence of fringe affiliates and resort to legal process to stake a claim to legitimacy. In the cases of neo-Nazi band performances above, the NPD sponsored legal action against specific members of the resulting protests for hate crime targeting (charges were thrown out, though sentencing on other charges went forward) and directly petitioned police to deny permits to anti-performance protests.[517] However, such recourse to official channels has diminished in recent years. Of particular interest is a chain of events following the 2005 elections that saw the NPD drop below the 5% threshold across most of Germany's states. Despite great gains in three eastern states, diminished draws elsewhere drastically reduced the visibility of the party in national politics. In the months that followed, Udo Pastörs decried the losses for a range of reasons and stated that the NPD must "fall back on core community support" to continue the "people's movement."[518] Between six and nine months later, Pastörs twice urged supporters to "resist leftist pigs"[519] protesting far right social groups putting on shows. The police were not petitioned in either instance.[520] The next year, in March, skinhead social groups met communist vandalism in Western Pomerania with localized

[516] Ibid.
[517] See Caiani and Parenti (2016).
[518] Ibid.
[519] "Germany seeks to ban far-right party". *3 News NZ*. 6 December 2012.
[520] Caiani and Parenti (2016).

protest. That protest resulted in three arrests for arson.[521] Whereas the NPD had vocally denounced such acts as late as 2002,[522] no statements were forthcoming. Members (not officials) of the NPD published support opinions in three local papers over the next two weeks. This trend has continued to this day. For the first time in 2009, the NPD scheduled support rallies in direct proximity to Die Linke and Green Party town hall events.[523] Three of six resulted in street fighting, for which Frank Franz blamed liberal supporters.[524] In short, though the use of violence is rejected at an official level, there has been a clear trend towards tacit acknowledgement of the deviant actions of members in the lack of executive-level announcement and in changes in rhetorical messaging that has increasingly emphasized non-participation.

Similar trends also exist with the Chinese organizations. With Falun Gong, antagonism has manifested in direct reference to changes in the position and nature of group leadership. The group's early use of ICT antagonistically was largely, but not entirely, incidental. In the wake of the group's banning in the later 1990s, the group principally continued to use the web to publish content on teachings and on limited advocacy goals (namely aimed at stopping repression by state authorities). Authoritarian upgrading of the censorship apparatus in China over the next several years saw a large number of takedowns and more than 225 arrests for "subversive" publication and illegal

[521] Ibid.
[522] Ibid.
[523] Ibid.
[524] Ibid.

attempts to organize for seditious purposes.[525] As of 2000, in the wake of this enhanced digital censorship, Falun Gong member pamphlets began advising on the "privating of exercises,"[526] even going so far as to encouraging practitioners in Wuhan to "only discuss aerobics sessions generally" in email and physical media. This practice changed radically in 2003-2004 with the widespread adoption of Dynaweb/Freegate and the reemergence of exiled leaders operating websites hosted (mostly) in the United States. Alongside language denouncing "CCP brutality" and "unreasonable oppression" for Falun Gong members, web postings guided members in China to best practices for circumventing Beijing's digital controls.

With Eastern Lightning, clear evidence that adherents receive direct discouragement comes in the form of the cult's strict behavior guidelines and requirements on tithing. Members are instructed to convert others and are monetarily rewarded for doing so. However, converts must be fully initiated prior to such rewards. Thus, digital activities are far less effective in terms of returns on time invested. Moreover, members are explicitly denied access to personal mobile devices. In short, EL has clear rules of action that focus members on the expansion of the cult among Christian communities in China and safeguard the group from undue focus by explicitly gimping the ability and incentive of members to become free agents.

Finally, with Civic Passion, direct connections between decision-makers and arms of the group that antagonize are evident in the loss and subsequent reappearance of

[525] Tong (2009).
[526] Found at http://web.archive.org/web/http://www.clearwisdom.net/3/sio/39097318.

high-level leadership the group suffered in 2015-2016. Clear executive direction in the lead up to and during Umbrella not only gave supporters ownership of specific protest tasks (preventing detrimental antagonism, much in the same way EL does); it also explicitly denounced the hactivism of others as deleterious to civil negotiations with Beijing.[527] The same kind of executive direction has recently reappeared in the return of Wong and others to lead the party, ending a period of relative disarray and civil disobedience (including digital disobedience) with a new set of goals characterized by the desire to transition away from social activism to moderate participationism.

The Changing Shape of Proxies. Another sign in support of the narrative above would be changes in the shape of those group elements most guilty of antagonism in reaction to changes in organization agenda. With Die Linke, several elements closely linked to violence by members have been disbanded and reabsorbed into other component parts of the party following group restructuring in 2005.[528] Specifically, according to federal reporting,[529] three neo-Marxist outfits linked to WASG, to arson in protest clashes in 1998 and to website defacements following electoral upsets in 2002 were defunct by 2009. Analysis suggested that lead members of each had been redistributed into "seven regional recruitment committees" focused on expanding the Left Party's roll count in historically underperforming areas.[530]

---

[527] See Kwong, Ying-Ho. "The Dynamics of Mainstream and Internet Alternative Media in Hong Kong: A Case Study of the Umbrella Movement+." *International Journal of China Studies* 6.3, 2015, p. 273.
[528] Patton, (2011).
[529] 2007 Annual Report of the Office for the Protection of the Constitution, p. 40.
[530] Ibid.

With the NPD, about half of the party-linked ICT employments and no less than 7 non-digital criminal acts between 2005's redistribution of votes and 2014 were undertaken by "new" neo-Nazi/fascist groups operating either in partnership with the NPD or to spread NPD content.[531] In reality, these groups are composed on members with long histories of interaction with the NPD and with other related neo-Nazi outfits, many of which have undertaken no active role in campaign efforts since 2009. Moreover, arrest of several members of these "new" groups suggests that the far right fringe has seen a geographic redistribution of activists from eastern Germany to western states.[532] In short, at least several of the right's most outspoken propaganda mouthpieces and coordinators have left now-defunct groups linked to the NPD to join newly formed, often antagonistic ones in areas where the NPD has dramatically lost support and visibility (thanks to the loss of parliamentary legitimacy). The clear suggestion here is that NPD campaign strategy for beginning the "people's front" has shifted in the wake of electoral defeats and that party (and fringe) infrastructure increasingly reflects a minimally-participatory mode of citizen engagement.

With the two cases in China where there is evidence of digital antagonism across the lifespan of the organizations, there is also evidence of changes in the shape of group elements most closely associated with such ICT usage in conjunction with variation on the dependent variable. Falun Gong's initial use of ICT for illegal purposes, as noted in Chapter 8, was a holdover from the legitimate web presence maintained in websites and

[531] 2014 Annual Report of the Office for the Protection of the Constitution, pp. 35-56.
[532] Ibid. p. 53.

online forums prior to the group's banning in the late 1990s. In reality, the group did little to utilize the web in their resistance to government repression through the early 2000s (i.e. most protest was arranged locally and through existing practice groups). And the removal of then-illicit Falun Gong web content occurred in line with Beijing's rapid investment in the apparatus of digital censorship and wasn't linked to any notable attempt to contest the government's digital crackdown. The group's later development and use of circumvention tools like Dynaweb, however, followed directly from the formation of Falun Gong practice groups centered on exile members in the United States, Canada and elsewhere. Perhaps more clearly than is the case for other groups covered in the project, these peripheral elements shifted the organization's understanding of the potential of online contention and became the clear source for disruption and circumvention tools for the group writ large.

With Civic Passion, digital antagonism emerged from the loss of central direction at the end of the Umbrella movement. Specifically, during that time, various members splintered into sub-groups that attached themselves to more radical elements of the Umbrella coalition.[533] Though evidence on the perpetrators of specific defacements and cyber attacks undertaken during that period is generally non-specific on which elements of the Passion organization were guilty of antagonism, the relatively decentralized nature of the group relative to a few driving individuals clearly suggests that the removal of

[533] See Kwong, Ying-Ho. "The Dynamics of Mainstream and Internet Alternative Media in Hong Kong: A Case Study of the Umbrella Movement." *International Journal of China Studies* 6.3, 2015, p. 274.

core leaders was akin to a complete loss of direction for membership. At this time, remaining member sub-groups were forced to take cues from their environment and other pro-democracy organizations previously affiliated with Umbrella. This period includes the only incidents of digital antagonism by Passion members and is distinct from the period that followed with return of group leaders like Wong Yueng-tat.

11.2.2. Other Possible Explanations

There appears to be distinct support for the argument outlined above and in past chapters. But what other factors might come to bear on incidence of digital antagonism by organizations and their derivative units? Across the cases, the primary variation on the independent variable side of the equation was with group objectives and political content. However, various groups exhibit many of the same tendencies and characteristics across the range of alternative explanatory categories outlined in earlier chapters. I consider the most relevant alternative explanatory factors here.

One possible explanation for use of ICT disruptively lies with path dependent involvement in criminal enterprise. As the argument goes, either executive-level condoning of criminal acts or the existence of criminally minded members path dependently improves the chances that organizations will take their antagonism online. In Germany, both Die Linke and the NPD have extensive histories that link them to criminal activism (though neither has demonstrable links to organized crime or to economic crime). Over the course of their lives, the Left Party and the NPD have seen the arrest of more than 2,000 members and innumerable individuals that linked to their

respective causes.[534] The question is whether or not this fact mechanically explains incidence of digital antagonism over time, specifically the recession of Die Linke's association with such acts and the NPD's continuing association. The case details outlined above suggest that this is likely not the case. The originators of ICT disruption for both organizations certainly *are* some of the main culprits of the most visible criminal acts linked with both groups over the past few decades (Geraer Dialog/Sozialistischer Dialog, shared members with Deutsche Kommunistische Partei, etc.).[535] But the case of Die Linke particularly is difficult to explain via such a blanket assumption about embedded criminality. Organizers of the Dialog sub-group, for instance, have regularly since 2005 been censured or accused of criminal intent related to incitement of violence by members (scheduling protests for the same location and time as far right ones, etc.).[536] And yet, this stands in stark contrast with actions linked to what was a dissident WASG element before 2005 in that members were charged with arson, property theft, physical assault and, in at least one instance, website vandalism.[537] Why the shift away from such criminality on most fronts but maintenance of emphasis on limited forms of antagonism? More than simply having experience in criminal enterprise, the streamlining and reorganization of the party movement in line with a reconsideration of objectives provides the strongest mechanical explanation of the new shape of behavior.

[534] 1998 Annual Report of the Office for the Protection of the Constitution.
[535] Ibid.
[536] Patton, (2011).
[537] Ibid.

Unlike in Germany, where both organizations investigated had strong links to criminal activism going back decades, none of the three groups discussed in China have links with criminal enterprise. To clarify, the Chinese government maintains limited accusations of involvement in criminal embezzlement and advocacy of crimes that disrupt the peace in the case of all three groups. Moreover, the publication of material outlining group objectives and philosophy has, in the case of all three, been deemed illicit or has been the target of government disruption attacks. EL's proselytizing is illegal, as is mention of Falun Gong's version of *qigong*, and Civic Passion has variously been censored for anti-state speech regularly since 2014. However, in the traditional sense, none of these organizations has connection with criminal enterprise.

Another possible explanation contends that the permissiveness of a given political system acts as a modulating influence on the behavioral inclinations of subversive groups. This explanation – along with the notion that use of ICT disruptively in the German case stems from the specific ability of Germans to access such tools – will be considered in part in the section below on multi-country context. However, initial analysis suggests that a highly permissive political and legal regime does not strongly restrain criminal behavior by countercultural entities (see Table 11.1 above). Even beyond ICT usage, the extensive repertoire of criminal incitement and hate messaging practiced by the NPD particularly demonstrates that systemic tolerance certainly doesn't have a strong mitigating effect. The question is whether or not it tempers the

expectations of subversives in a meaningful way and dictates the approach taken in engaging the population (i.e. through participatory means vs. revolutionary ones).

Yet another possible explanation lies with the nature of opposition facing a given subversive organization. To some degree, of course, the nature of support is arguably linked to decision a group might make to approach transformation via involvement in the current political process or not. There is some correlative evidence, primarily with the German cases, to suggest that these factors affect group actions that ultimately produce greater or lesser antagonism. Increased police investigation of the NPD and affiliates in the past five years does fit with the falling popularity of the party and rising focus on encouraging civic misbehavior. Likewise, one might easily argue that surging support for Die Linke after 2005 matches the sudden moratorium on illicit and disruptive activities but far left affiliates. And yet the notion that tolerance for such acts rests solely on observation of national support (or the support of influential sponsors) is a tenuous one, in some respects. Rising NPD popularity and falling involvement in criminal activism in the early 2000s corresponds with a series of groundbreaking attempts to ban the organization in cases brought by the government to the Constitutional Court. And, as noted above, Die Linke's surging popularity in electoral results in 2005 and 2009 did not *actually* reflect votes taken from other political parties so much as it meant a consolidation of the broad left-wing fringe. Likewise, neither group in this case benefit broadly from foreign support. Thus, in terms of mechanisms, while the perception that there might be value in good behavior might have influenced

group decision-making on both fronts there is little evidence to suggest that such an understanding of the national environment manifested as anything more than an incentive to actualize meaningful organizational changes. Moreover, the experiences of Falun Gong, where digital antagonism appears to be a unique artifact of foreign-based peripheral member agency, suggest that there is no mechanical connection here. And particularly given the default experience of subversive groups as unpopular and under close scrutiny, there is furthermore little reason to think that modulations of support matter as much as does self-defined notions of participation vs. revision.

11.3. Access & Opposition: Does Country-Level Variation Matter?

Does the permissiveness of national-level conditions help explain the propensity of subversive activists in using ICT antagonistically? In previous sections and chapters, this has been discussed in several separate veins. Does support for an organization or direct opposition to it, whether expressed by the public or in government persecution, matter? Additionally, does the nature of a given political system as legally and culturally more permissive of countercultural organizations affect group strategy? It is also important note that, though the case studies in this dissertation project are not designed to allow for testing on this front, the relative opportunities a group or its members have to develop the toolkit of digital antagonism might affect tactical choices. Here, the question is really about the interaction of market development (i.e. the availability of talent and tools, which these cases do not observe variation of) and market restrictions

(i.e. any act taken by the government to restrict the development of talent or access to tools).

A possible way to explain propensity to use ICT disruptively lies with the nature of opposition facing a given subversive organization. With the groups studied above, results reflect a mixed bag. Certainly, broad-scoped opposition to Eastern Lightning corresponds with the lack of focus on digital antagonism. However, there is no apparent connection between directives from group leadership and the practices of organization arms that suggests some reaction to popular opposition is mechanically responsible for restraint in this regard. Moreover, EL absolutely can be said to be guilty of other forms of antagonism in the form of targeted kidnappings, torture and blackmail for purposes of conversion. With Falun Gong, an organization that is not broadly seen as fundamentally objectionable amongst the public, direct and strict government opposition alongside limited use of ICT circumventively actually flies in the face of expectations set in Chapter 3. Direct opposition should impel a wariness of antagonism and further ostracization, but that does not seem to be the case here. And with Civic Passion, perceived governmental opposition and diminished popular support after the dissolution of Umbrella led to free agent antagonism through 2016. Just as with Falun Gong, Passion's experience suggests no connection in line with expectations regarding subversive responses to lacking support and presents no more compelling a mechanical reason for incidence of antagonism than does the absence of authority that thereafter demonstrably affected group behavior.

The same mixed bag result is true with the German groups studied in Chapters 6 and 7. Particularly given that the party's post-2005 electoral surges reflect a redistribution of leftist support rather than an expansion of the traditional voter base, it is not uniquely apparent that Die Linke's receding experience with antagonism on all fronts stems from higher levels of public support. With the NPD, however, diminishing support and direct investigation by the government does parallel an apparent lessening of efforts to restrain antagonism on the part of leadership. However, particularly given the fact that Die Linke's surging popularity emerged from a direct result of internal actions taken to consolidate and streamline party agenda, it is not immediately clear that conditions of support and opposition themselves compel ICT antagonism. Such conditions may reinforce courses of action being taken and may constitute an incentive to rethink group objectives, but case evidence suggests that they are mechanically secondary to the actual outputs of reorganization efforts.

Another possible explanation contends that the permissiveness of a given political system acts as a modulating influence on the behavioral inclinations of subversive groups. At face value, it seems clear that the format of engagement and activism differs for groups in Germany and those in China directly based on the structure of political process. In Germany, two organizations that are professedly counter-hegemonic nevertheless participate in the democratic process. True, there is distinct variation over time and the experience of both groups has historically been characterized by efforts by mainstream political parties to run far left/right influences out of politics. But both the

NPD and Die Linke, regardless of the state of popular support for either, are able to choose participation even if eventual objectives dictate structural transformation or overthrow. Indeed, Germans that object to one or both extremes of political advocacy have fought in court and have engaged in protests for the right of such groups to be full-fledged members of civil society. In China, government restrictions on what is seen to be extreme advocacy are incredibly severe. Falun Gong and EL are outlawed organizations and could not participate freely even if such an approach were desirable to members. Even with Civic Passion, arrest of members with questionable cause is common and the original charter statement made in 2012 even emphasizes social activism over party operation because prevailing systems are "biased against native" participation.[538] Thus, it seems reasonable to suggest that basic legal and political conditions *do* shape campaign tactics. Moreover, it seems reasonable to suggest that such conditions affect the tactical decision to antagonize at any level. Greater willingness to antagonize legitimate political operators, after all, is a logical extension of the diminished propensity to participate in repressive systems and is roughly synonymous with the narrative above that links group objectives to political action.

Finally, do the relative opportunities a group or its members have to develop the toolkit of digital antagonism affect tactical choices? Again, these case studies are not designed with variation on the availability of talent and tools in mind. Both Germany and China are advanced economies wherein the average consumer has extensive access to

[538] See Ip, Kelly, Phneah, Jeraldine and NectarGan, "Undampened". *The Standard*, 5 June 2013.

sophisticated hardware and software across a range of formats. In both countries, citizen use of the Internet is above 55%. Both boast advanced technology sectors with globally known industry brands – like Huawei and Siemens – that lead development on mobile devices, superconductors and more. And both offer exceptional educational access to computer science and engineering programs as part of an effort to maintain the integrity and vitality of the national innovation economy. Given this, it is impossible to offer a simple assessment of whether or not digital antagonism exists across some cases in these countries *only* because subversives have greater access to technology than do contemporaries in less developed countries.

However, the cases outlined in Chapters 6 through 10 *do* offer further support for the hypothesis – evidence in support of which was presented in Chapter 4 – that relatively less codification of monitoring, investigative and censorship abilities on the part of the government relative to high national levels of access to the means for digital antagonism produces freer use of ICTs for circumvention or disruption. Such support exists on two fronts. First, the rise of a sophisticated government censorship regime in China *has* had a clear effect on choices made to engage in disobedience online. The case of Falun Gong perhaps emphasizes this point most clearly. In the late 1990s, Falun Gong maintained a strong web presence in the form of dozens of websites. In the two years following the group's banning, Falun Gong members maintained these websites and, though some arrests were made in connection with continued publication of group materials, even expanded web activities within China to blogging and photo journalism

of ongoing suppression efforts. The development of the Great Firewall in 2002 and subsequent actions to rapidly cleanse the national cyber environment of mention of Falun Gong, however, successfully drove the group from the domestic Internet. As Li noted in 2003, the ability of Falun Gong practitioners to "peacefully gather" was "increasingly tenuous because of communications' crackdowns" on the part of the Chinese government. Even today, Falun Gong's extensive use of ICT pivots entirely on the support of exiled members and foreign sympathizers. Dynaweb, Freegate, hosting in foreign servers and more are outputs of members operating beyond the traditional reach of the Chinese government. And there is further evidence of this link between government abilities and antagonism in the experience of anti-fascist organizations rapidly expanding to help federal authorities in Germany crack down on hate speech on NPD and other websites. In Germany, the federal government is constitutionally limited in its ability to surveil and monitor the actions of private citizens employing encryption or requiring community entry credentials. This has given rise to a cottage industry of activists that aims to inform the government of violations of federal law in content published on such sites – the full scope of which remains unmapped and unmonitored by authorities – by inciting violence and more.

11.4. Directions for Future Inquiry

The next chapter concludes this dissertation project by briefly recapping the main argument and discussing implications for both scholarship and policy. In doing so, it outlines the significance of the project's findings and places both the data collection

effort and the theory in the context of research programs across the cyber conflict, terrorism studies, political communications and social movement sub-fields of study. First, however, I consider directions for future inquiry as it pertains specifically to this topic. What might advanced versions of this project look like? What information would enhance the analysis of previous chapters? And how might scholars validate the arguments made herein regarding the relationship between core and peripheral group elements.

11.4.1. Data Collection

Data collected in this project for the purposes of large-N testing and analysis followed emerging standards in the field of cyber conflict studies for cataloguing different kinds of antagonistic digital actions. The dataset that resulted from my efforts herein produced unique knowledge about the repertoires of digital antagonism maintained by subversive activists. Overall, it seems reasonable to think that other studies of non-state actors would benefit from following a similar approach scheme of collecting data on digital actions conditioned on close examination of common actor operations.

Data efforts might be improved, however, on two fronts – relating to (1) severity and (2) intention. Part of the difficulty in studying something as subjective as digital antagonism is the inherently subjective way in which the researchers must categorize different basic techniques. In reality, many web technologies – arguably most – are inherently dual use in that the user's employment of them is equally likely to be benevolent or malicious. Following the coding approach suggested herein – again, where

coding follows close understanding of actor aims and preferred methods – allows for data collection that mutes the limitations of basic technique identification. However, the resulting data must still be assessed subjectively. This project's identification of techniques most regularly employed by subversive groups – labeled *information enrichment* techniques or operations in previous chapters – is based on understanding of common features of those techniques. Cyber attacks that involve malware tend to be more severe than are website defacements, and the former type of action is generally more about sending a message than about actual disruption.

However, the fact of the matter is that while this dynamic is generally accurate, it is not always so. Cyber attacks of varying sophistication can be used to coerce targets and send messages in the same way that content manipulations might. For instance, an attacker might gain access to a system without achieving an effect (such as stealing information or restricting legitimate access) in order to demonstrate an ability to hack effectively (typically called "burning a vulnerability"). Future data collection might control for this spectrum of possible actions and generally provide more nuance in efforts to outline repertoires of digital antagonism among non-state actors by coding for severity and intention. Specifically, coding of cyber attacks might be parsed out to more closely record elements of the attacker lifecycle – i.e. efforts to gain access to networks, to generically achieve a disruptive or criminal goal and to achieve a primary objective. Regarding intention, coding might follow emerging procedures in the field for classifying the aims of different kinds of cyber attack. Though most procedures have been designed

with state actors in mind, there are few reasons that such coding schemes – which aim to capture disruptive, degrading and espionage operations of various kinds – cannot be employed with non-state actors. As is the case with data collection on state cyber conflict actions, the primary obstacle facing researchers with such an effort lies with data availability. Absent access to classified or proprietary information, reporting of different antagonistic ICT employments is often absent the granularity needed to record effectively over so many nuanced categories.

11.4.2. The Study of Group Proxies

Naturally, next steps with this project and with advanced versions of this project will want to focus on the relationship between core and peripheral elements of subversion non-state actors. There are two tasks involved in doing so. First, future efforts would do well to expand data collection parameters to better speak to this relationship, the significance of which to scholarship is discussed in Chapter 12. To more effectively test the nature of the link between different ICT behaviors and proxies, future work should take steps to find better and alternative ways to measure the role and actions of proxies. This is not an easy task.

Alternative approaches to studying proxies in a quantitative setting would essentially attempt to validate the strong positive results for highly decentralized organizations in Chapter 4's analysis. The result that high levels of decentralization predict digital antagonism – a finding that was not expected – implies that high independence of peripheral elements of organizations is linked to free agent antagonism

online. This dynamic appears to be borne out in case study analyses wherein the expression of aims and methods dictates the propensity for fringe elements to "defect" from behavior we would otherwise expect. However, it is not clear what it is about fringe elements that make them more or less likely to develop cyber conflict capabilities or to employ them.

To both expand the current study and to look to the question of what prompts individuals (or sub-groups) linked with a group to gain experience in cyber intrusion techniques, future work should consider the collection of a range of information around non-state actors. From the start, it is necessary to retain focus on specific non-state groups. Though future efforts may wish to expand the scope of study to include contentious non-state actors beyond subversives, it is critical to retain information regarding the relationship between core and periphery elements of particular non-state actors. Moreover, there are strong arguments for retaining the focus on episodic incident data collection. Non-state campaigns and operations are not ubiquitous over the course of a non-state actor's lifespan. Thus, to best understand proxies, it is necessary to maintain focus on events and conditions at specific points in time. Not only does this allow for a more granular approach to examining such actors, but it also leaves open the possibility of conducting advanced statistical tests, such as panel regression models or fuzzy/crisp set testing on specific attacks.

More specifically, data collection on proxy elements of non-state actors should rely on a model understanding of group structure that incorporates the presence of

proxies as more or less directly under the control of group executives. This layer of nuance would be a new condition beyond functional differentiation (or not) wherein peripheral elements are operationalized by the possibility for un-directed support an organization. In quantitative testing, such a variable could take a number of forms, from an additional typology of group structure to simple dummy variables for different formats of proxy.

11.4.3. Validating the Argument: Core Signaling and Peripheral Reactions

The second task involved in better understanding the relationship between core and peripheral elements of subversive campaigns is to more specifically attempt to validate the dynamic described in the theory of this dissertation project. Specifically, future work should attempt to better assess the notion that expressions of preferred approaches motivate peripheral antagonists and to flesh out what it is about such expressions that particularly motivates member deviation from expectations.

Naturally, such an effort involves better description of different types of proxy actors that operate within the sphere of influence of a non-state actor. But it also involves a closer look at expressions of approach by leaders. What is it about statements made by executives that either restrains or motivates antagonistic behavior by members? Is explicit direction required or is implication enough? Does a leader have to demonstrate resolve to effectively constrain peripheral elements of the subversive movement? Or are the statements of societal opponents a determining feature of whether or not proxies are inclined to take matters into their own hands? In answering these

questions, there is great potential in the ability of content analysis approaches to construct data useful to the task of examining the relationship between leadership communications and proxy behavior.

Chapter 12
Conclusion

Christopher E. Whyte

This dissertation project has addressed a specific puzzle about the way in which subversive actors utilize ICT in their campaigns. In attempting to fly under the radar, ICTs provide actors abilities to hide, obfuscate and clandestinely organize in preparation for a subversive campaign. Once in the public limelight, ICTs continue to provide subversive groups new and enhanced abilities to coordinate, activate and mobilize in their attempt to affect sociopolitical transformation. In line with the move that successful subversive actors make from counterculture to mainstream voice, group usage of ICTs invariably transitions from emphasis on strategies of subterfuge to those of digital activism. This tendency is evident in a range of modern cases of attempted subversion and makes a great deal of sense. Activist strategies are logical outgrowths of a situation in which a group suddenly finds itself relevant to mainstream popular discourse. Renouncement of techniques and strategies that might have once aided the clandestine operation of a group makes particular sense, as such activities often invite government scrutiny and threaten to link a subversive cause with a shady past in the public eye. But the fact of the matter is that many subversive groups enduringly "keep

one foot in the shadows" – i.e. they continue to engage in digital antagonism that involves shady online activities alongside the digital activism that characterizes the later stages of a subversive campaign.

In the preceding chapters, I presented strong evidence that incidence of digital antagonism is tied to the nature and expression of an organization's grievances. In the quantitative analysis, grievances explicitly focused on affecting structural revision (not simply policy modification) appeared to strongly predict group employment of ICT for antagonistic, disruptive purposes. Moreover, structural revisionists – particularly those with maximalist agendas – appeared clearly more likely to escalate their use of cyberspace to more disruptive formats of interaction, including malware employments, tailored distributed denial of services (DDoS) attacks and direct, unauthorized tampering with hardware. And such groups are more likely to target government or military assets directly and to employ ICT disruptively even where there is a clear precedent of prosecution of such actions.

I have argued herein that structural grievances are closely tied to a willingness to condone criminality. In this way, revisionism *indirectly* produces antagonism. Far from seeing evidence of explicit executive-level direction of hacking or circumventive efforts, Chapters 6 through 10 suggest that there is a strong relationship between revisionism and the way in which groups interact with peripheral elements of their movement that employ ICT antagonistically. Across cases, the sources of web tools and the initiative to disrupt regularly stems from extended elements of subversive organizations.

Moreover, patterns of digital antagonism change directly in line with significant shifts in subversive groups' stated approach to transformation. Participatory rhetoric and emphasis on methods of achieving change that involve participation in extant political processes mute incentives for peripheral subversive elements to undertake acts of civil disobedience online. Specifically, in attempting to enhance the perception and prospects of a subversive cause through participationism, leaders are incentivized to explicitly denounce such acts and to veto, where possible, any antagonistic operation that does not meet strict threshold criteria for deniability (such as low-level encryption to hid intra-organization communication or actions taken against unpopular societal opponents, such as occasionally occurs in relations between Germany's far right and far left parties). Where a group turns from participatory approaches, however, both group leaders and peripheral elements are incentivized to antagonize. For leaders, fringe operations remain largely deniable, present as a unique set of options for mitigating the gains of sociopolitical opponents and offer opportunities for growth beyond those that accompany legitimate political participation. For peripheral elements in such a situation, digital antagonism is a cheap and arguably effective way for advancing a cause without (1) running the risk of harming efforts to garner broad public support or (2) running into the kind of significant law enforcement opposition to civil disobedience that often, offline, leads to arrests and negative publicity. In short, expressions of approach to a given subversive effort act as signaling mechanisms that dictate the probability that peripheral elements of a movement will act antagonistically.

This argument and the gathered evidence it emerges from hold a number of implications for both scholarly research programs and the efforts of policy practitioners. This concluding chapter briefly outlines several such implications and indicates the scope of future work in this vein. Of note, this concluding chapter is circumspect in describing its implications for both scholarship and policy. In reality, this project is significant because it has taken broad strokes concepts and expectations, added evidence and offered first-of-its-kind assessments of subversive group behavior. As is so often the case with such projects, the main value of the effort lies in new direction for research.

12.1. Blurred Lines: Criminality and the Digital Age

A primary takeaway of this dissertation project is that subversive non-state actors are willing to use ICT criminally quite often. A third of those groups studied in Chapter 4's quantitative analysis have used ICT for antagonism over their lifespan. Among these groups, the most common uses of web technologies are unsophisticated. Subversive activists disrupt, circumvent and hide non-digital criminal activities via the use of low-intensity techniques. Most are off-the-shelf. Many – encryption, the use of botnets, etc. – are unique specifically because of the way they emphasize the anonymity of the user. Moreover, a sizable number are questionably prosecutable. And, given the quantitative finding in Chapter 4 regarding heightened probability of antagonism by actors operating in mismatch technology adoption environments, it seems that this fact is known to subversives on at least some level.

All evidence suggests that subversive groups are highly opportunistic when it comes to the use of information technologies. Further, all evidence supports a narrative of increased criminality amongst belligerent non-state actors following the information revolution. Where the toolkit of digital antagonism entails access to low-risk ways of harassing opponents, reaching new audiences and harnessing resources beyond the reach of conventional approaches, radical non-state actors are faced with less firm incentives to avoid criminality in their campaigns. Though discussed further in the concluding sections below, this is in itself a significant finding for the broader research program on non-state actors and cyber conflict worthy of singular mention. Government agencies and institutions of democracy across the globe are more likely to encounter non-state antagonism affected via use of web technologies than they might have been to see criminality through conventional means among such groups in eras past. At the highest level, this means that governments and inter-governmental agencies should redouble efforts to streamline and align approaches to prosecution and evidentiary standards around the world. At the same time, national security researchers would do well to better theorize and test different approaches to deterring non-state political cyber crime. To do this, we need to better understand the determinants of non-state actor decision-making, a task which this project has made headway with and which the next sections use to describe specific future tasks in detail.

12.2. Implications for Scholarship and Analysis

I argue that there are two main areas in which this project holds serious implications for research programs in political science and international relations (IR) – (1) the program on subversion and information warfare in IR and, more specifically, (2) the study of non-state proxies as an important element of international cyber conflict. This is not to say that there are not implications in other veins. Indeed, elements of this project speak to a great number of research efforts on the contours of social movements in the digital age and the use of cyber tools by non-state actors beyond subversives, among others. Moreover, the project speaks to challenges for homeland security efforts in democratic states. I address the latter below and argue of the former that the primary contribution of this study for scholarship is to drive better understanding in the two specific areas noted above.

12.2.1 The Study of Subversion and Non-State Behavior

Subversion is one of the most common sociopolitical phenomena in human history. It is also one of the most complex. And yet, despite its regular occurrence across societal experiences and the challenges bound up in problematizing and generalizing on such a phenomenon, it is remarkably understudied. As noted in this project's introductory chapters, scholarship advancing understanding of subversive actors and efforts is not only thin on the ground, but also tends to arise in response to highly specific manifestations of the thing. Going back fifty years, the major inspiration for such scholarship was the specter of global communist subversion during the first half of

the Cold War. More recently, scholars have begun to revisit the topic in the context of various global movements that espouse specifically subversive objectives, including anti-globalization and fundamental Islam. However, until now there has been little in the way of large-scale empirical efforts to flesh out and analyze specific elements of the phenomena as it manifests in the behavior of non-state actors around the world.

As noted in preceding chapters, the challenge that scholarship on subversion faces is the retention of appropriate conceptual clarity when studying subversion by actors that aren't principally interested in ideational transformation. A lot of work suffers from the use of theoretical frameworks adapted from terrorism studies, insurgency examinations and more that conflate tactical subversive acts by belligerents with subversive intent. Such frameworks have some merit, but they don't provide scholars interested in subversion with a clear mechanical set of expectations about how subversive actors should operate. This project steps in to update and expand the conceptual foundations available for scholars interested in studying subversion.

Specifically, this dissertation demonstrates the existence of a unique conceptual and empirical dynamic amongst subversive non-state dissidence organizations, namely that most antagonism is muted. With ICT, efforts to circumvent state authority and to disrupt societal forces (broadly writ) is largely constituted of low-intensity tricks and techniques designed to improve the environment in which more conventional persuasive efforts take place. Broadly, this offers challenges for legal efforts to constrain disruptive subversive activities, for the efforts of law enforcement in attempting to deter criminal

actions and for the work of intelligence organizations interested in decoupling counterculture from more violent extremism. This dynamic also suggests that the challenge of ensuring security whilst maintaining respect for privacy in democratic states is extremely acute. Where antagonism is limited and occurs in the shadows, the onus on law enforcement to reach further into private space will be greater. This is discussed briefly again in the next section on the policy significance of this work.

Perhaps more conceptually significant than the basic empirical finding regarding categories of digital antagonism, this project adds nuance to the limited body of work on subversive actors in world affairs in describing the relative volatility of many groups. Where antagonism characterized parts of a particular group's campaign, this dissertation found that understanding of the relationship between core and peripheral elements of the organization was needed in order to explain variation. This finding suggests, as one might expect of a category of non-state actor as diverse as subversives, that there is limited utility in trying to predict subversive behavior via blanket understanding of the cause of a given group. In reality, understanding tactical choices requires comprehension of complex interactions in group structure, national context and the expression of group objectives.

There remains a broad range of questions to be addressed by scholars interested in subversion. In particular, project findings add a new dimension to a hypothesis commonly found in studies that focus on subversive actors today, namely that the information revolution presents challenges for groups in the form of a more mobile

membership base. As a result, in an attempt to retain otherwise transitory sympathizers, groups often become more cause-oriented in their activist efforts. The results of this project support the notion that ICT present new opportunities for subversive groups. They also, however, suggest that digital antagonism manifests more often than not among fringe elements and that group leaders might need to worry about free agents among members. Particularly where groups attempt to push their cause in the public eye to retain membership, subversives might face additional threats to group prospects in the bad behavior of their adherents.

12.2.2 Non-State Proxies and Cyber Conflict

There also remain open questions to be answered about the shape of non-state subversion as it pertains to proxy actors. This project is particularly significant because it provides a basis for assessing the behavior of subversive groups and their proxies in the context of both state actors and other kinds of non-state actors. With state actors that attempt to subvert as an aid to broader foreign policy goals, to what degree do digital tactics and techniques overlap with those observed to be common amongst subversives? And, since this research also validates the notion that rhetoric triggers proxy action, it seems clear fruitful work might be done on the relationship between proxy behavior and state cyber campaigns. How do states control their proxies? In particular, how do states trigger and restrain proxy actors that act patriotically – i.e. in service to a cause and not for money – in hacking?

Moreover, can we use what we know of state-based subversion to further our understanding of non-state actors? Do subversive groups also encourage trolls? If so, when and how? Do subversives encourage disinformation on the periphery of mainstream debates so as to manipulate the information environment? The findings of this project suggest that the tools of subversion include those commonly employed by Russia and other states in information campaigns in recent years, but further study of specific campaigns is required. In essence, a deeper dive into actual tactical toolkit of subversives beyond the tools themselves is needed, and this project provides a foundation from which such investigations might be possible.

With other kinds of non-state actors, the results of this project suggest that examination of proxies of terrorist groups – i.e. of individuals and self-constructed sub-groups that aim to aid terrorist agendas, not traditional terrorist cells – is a fruitful avenue for research. In particular, this project's results suggest that such proxy actors should be looked at more closely in quantitative and formal analyses. Looking at terrorist proxies like this is not common in such efforts and, though there are number of efforts to expand research in this vein linked with the transnational terrorism of groups like ISIS, study of less formal proxy elements of a given organization's campaign might elucidate information to practitioners. Indeed, thinking about more distributed elements of a terrorist campaign seems important particularly in the context of transnational movements/groups like ISIS, where the group's aims are arguably more subversive than a traditional terrorist organization.

12.3. Implications for Policy

This is dissertation's puzzle, research design and results further emphasize enduring challenges faced by both national authorities and the international community. In particular, the results' focus on low-intensity digital antagonism by non-state subversives and the prominent role of proxy elements in generating contention online speak (as mentioned above) to the enduring issue faced by democratic states in balancing privacy and security. Inevitably, the harder-to-detect antagonistic actions are, the more law enforcement and intelligence organizations will feel the need to reach further into the private spheres of operation of citizens, companies and communities. Of course, this result and suggestion is not particularly groundbreaking. But findings do, at least, suggest possible opportunities for law enforcement agencies in the ability to focus on the correlates of non-traditional proxies of dissentious elements of society. Better understanding of signaling that occurs between extremist organizations and their followers, as is forwarded in this project, stands to better inform incident prediction and response efforts. Future work on the correlates of digital antagonism among proxies – i.e. the sources of technical training, technology acquisition, etc. – might offer more precise tools for pre-empting non-state cyber threats and blunting the claws of subversive groups without impinging on the free speech of dissidents.

Much as has been the case with past works on subversion in the digital age, this project's puzzle and approach also emphasize the degree to which there are limited institutions in place in international affairs for determining the responsibility to

troubleshoot the kinds of low-intensity, non-economic cyber disobedience described in previous chapters. The international community faces challenges of coordination and cooperation particularly because of the conflation of various issues bound up in problematizing subversive efforts. Again, subversive is contextual. One country's struggle against extremism might invoke concern over civil liberties denial and human rights abuse among other members of the international community. Moreover, some non-state subversives are themselves proxies for states, and it is rarely clear where links to non-state groups end and links to states begin. Given these issues, where does jurisdiction lie for investigating criminal antagonism and setting standards of response to extreme activities? Again, as noted in the sections above, this project's focus on the relationships between leadership of non-state organizations and peripheral elements suggests common space within which international agreements might focus on combating those elements of subversion that are criminal in nature.

12.4. Conclusion

One problem with studying subversion and with approaching an empirical study of subversive actors in the way this project has done is that the unit of analysis is in no way uniform. Subversive organizations can take every shape and, in the global sense, *are* organized around every kind of ideological position one might imagine. In short, across most conceivable "common" attributes, subversive actors are amorphous and best understood in context. Given this, a social scientist would likely not be considered off base if they asserted that the shape of subversion as a sociopolitical phenomenon is most

approachable from an interpretive perspective – i.e. from a qualitative perspective that holds unique context as a unique barrier to comparative analysis.

A final observation emerging from this dissertation project, however, has to be not only that subversion is assessable given an appropriately specific research design, but that decentralization and diffusion are actually critical when it comes to explaining variation in subversive behavior in the digital age. Not only do the results of this project reveal information about subversive actors and their use of ICT for the first time; they also indicate that peripheral, distributed elements of subversive non-state actors are armed for dissidence and disruption today in a way they weren't in the past. Most disruptive actors studied herein have no real connection to more traditional forms of crime and results suggest that digital antagonism is particularly in evidence where (1) societal adoption of ICT is high and (2) government regulation of the digital domain is limited. Indeed, if anything, the results of this project demonstrate above all else that the information revolution itself has underwritten and driven the development of new modes of non-state contention in world affairs. To be sure, this project – which answers one specific question – falls at the crossroads of a series of exciting research areas and there are many complicated questions to address in new work to come. But the final note must be that the premise and findings of this project dramatically reinforce the notion that the transformative effect of the information revolution – something that is often taken for granted in this kind of research – has meaningfully altered the shape of contention in world politics.

Reference List

'Russian trolls spread government propaganda', Al Jazeera, 11 August 2015 (http://www.aljazeera.com/news/2015/08/russian-trolls-internet-government-propaganda-150811205218686.html).

'This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists', Stopfake, 13 July 2015, (http://www.stopfake.org/en/this-is-how-pro-russia-trolls-manipulate-finns-online-check-the-list-of-forums-favored-by-propagandists/).

"【專訪】鄭松泰：黃洋達退出熱血公民　熱血公民撤出社運　加強社區服務　下月政黨化". *Stand News*. 5 January 2017.

"Bundesverfassungsgericht verbietet Überwachung von Bodo Ramelow". tagesspiegel.de. Retrieved 7 April, 2017.

"Commission on Strategic Development: Hong Kong's Relationship with the Central Authorities/the Mainland," *Central Policy Unit. Hong Kong Government*. 26 May 2014.

"Emanzipatorische Linke". Emanzipatorische-linke.de. Retrieved 6 April 2017.

"German politicians seek way to bankrupt 'neo-Nazi' NPD", Ben Knight. Deutsche Welle. January 20, 2017.

"Germany seeks to ban far-right party". *3 News NZ*. 6 December 2012.

"Gonganbu guanyu chajin qudi 'huhanpai' deng xiejiao zuzhi de qingkuang ji gongzuo yijian" 公安部关于禁取"呼喊派"等邪教的情况及工作意 [Opinion of the Ministry of Public Security on the circumstances and work related to investigating and stamping out cults such as the "Shouters"].

"Hacks and Highlights of the Chaos Communication Congress," *Tech the Future*, 20 August 2014.

"Hong Kong's angry young millennials: an interview with Joshua Wong," *Open Democracy*, 1 November 2015; and "黃洋達辭任熱血領導 黃毓民：樹敵多累選情". *AM730*, 6 September 2016.

"Kabinett beschließt Netzsperren gegen Kinderpornos" (German) (Cabinet approves blocking against child pornography), Pressestelle Bundesministerium für Wirtschaft und Technologie (Press Office Federal Ministry for Economics and Technology), 22 April 2009.

"Linkspartei diskutiert über Lötzsch-Nachfolge". tagesschau.de, 2012.

"New German government reaches key internet security agreements", Neil King, Deutsche Welle, 15 October 2009.

"New Hacktivism: From Electronic Civil Disobedience to Mixed Reality Performance". *Hemispheric Institute of Performance and Politics at NYU*, 2009.

"NPD – einzige ernstzunehmende nationale Kraft!". npd.de. 28 September 2009.

"Out with the old: Two big-name pan-democrats ousted in tight district council election races". *South China Morning Post*. 23 November 2015.

"Report of the Verfassungsschutz". Verfassungsschutz.de. April 19, 2014.

"Significant Terrorist Incidents, 1961-2003: A Brief Chronology". *Office of the Historian: Bureau of Public Affairs*. United States Department of State. Retrieved 9 April 2017.

"黃洋達辭任熱血領導 黃毓民：樹敵多累選情". *AM730*. 6 September 2016.

"A brief discussion of *falun gong*," *Minghui*.

"China Bolsters Censorship Tactics on the Internet," *San Jose Mercury News*, 19 September 2000.

"China Tightens Internet Restrictions," Associated Press, 7 November 2000.

"Demands on *falun dafa* guidance stations" (4/20/1994).

"Ending the party ... with thought power?," SCMP, 12 June 2014.

"Falun gong zhenshi di gushi" ("The real story of *falun gong*") 14 August 1999.

"German Internet blocking law to be withdrawn," EDRi-gram newsletter, European Digital Rights, 6 April 2011.

"Huangyan mengbi buliao xueliang di yanjing"("Lies cannot deceive bright eyes"); "Suowei shijie mori" ("So-called end of the world")

"Insurgents 'Inside Iraqi Police,'" *BBC News,* September 21 2005.

"Norms for *falun dafa* guidance counsellors" (n.d.).

"On Important Matters, Practitioners Must Watch the Position of Minghui Net," <http://www.clearwisdom.ca/eng/2000/July/16/AW071600 1.html>.

"Organisers say 510,000 people take to the streets for July 1 march," *South China Morning Post*, 1 July 2014.

"passiontimes.hk brutally attacked by 200,000,000 requests per second," *Passion Times*, 16 November 2014.

"Protesters storm Baghdad's Green Zone again, dozens hurt," Thompson Reuters, May 20, 2016.

"Pussy Riot Convicted: Moscow Court Website Hacked 'By Anonymous' In Retaliation," Huffington Post, August 21, 2012.

"Pussy Riot court website up after hack attack," *BBC*, August 21, 2012.

"Pussy Riot Supporters Hack Court's Website," *The Telegraph*, August 21, 2012.

"Radical Hong Kong group Civic Passion to become 'moderate' political party," *South China Morning Post*, January 6, 2017.

"Regulations on propagating the doctrine and method for *falun dafa* disciples" (4/25/1994).

"Subversion and Terrorism: Understanding and Countering the Threat," in Memorial Institute for the Prevention of Terrorism, *MIPT Terrorism Annual,* Oklahoma City, Okla., 2006.

"The crackdown on Falun Gong and other so-called *heretical organizations*," Amnesty International, 23 March 2000.

"The critical masses: Officials increasingly ask people a once taboo question: what they think," *The Economist*, April 11, 2015.

"The critical masses: Officials increasingly ask people a once taboo question: what they think," *The Economist*, April 11, 2015.

"The Law in Hizb ut Tahrir Lawsuits: Present But Not Present!" TheKhalifah, April 10, 2015.

"What *falun dafa* practitioners ought to know" (n.d.).

(2003 [2000]) Announcement from the first division of the Shijiazhuang Public Security Bureau. Chinese Law and Government 36(2).

1998 Annual Report of the Office for the Protection of the Constitution.

2001 Annual Report of the Office for the Protection of the Constitution.

2005 Annual Report of the Office for the Protection of the Constitution, p. 17.

2007 Annual Report of the Office for the Protection of the Constitution.

2009 Annual Report of the Office for the Protection of the Constitution.

2011 Annual Report of the Office for the Protection of the Constitution.

2014 Annual Report of the Office for the Protection of the Constitution.

Abrahms, Max. "What terrorists really want: Terrorist motives and counterterrorism strategy." *International Security* 32.4, 2008: 78-105.

Abrahms, Max. "Why terrorism does not work." *International Security* 31.2, 2006.

Ackermann, Robert: *Warum die NPD keinen Erfolg haben kann – Organisation, Programm und Kommunikation einer rechtsextremen Partei.* Budrich, Opladen 2012.

Adams, James, "Virtual Defense," *Foreign Affairs*, Vol. 80, No. 3 (May/June 2001).

Ahern Jr, T.J.., "Determinants of Foreign Coverage in Newspapers," in R.L. Stevenson and D.L. Shaw (eds) *Foreign News and the New World Information Order*, Ames: Iowa State University Press, 1984.

Albright, David, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges At the Natanz Enrichment Plant?" Institute for Science and International Security (22 December 2010) pp. 3–4.

Allen-Robertson, J. and D. Beer, "Mobile Ideas: Tracking a Concept through Time and Space." *Mobilities* Vol. 5, No. 4, pp. 529–545, 2010.

Allison, Graham and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, New York: Addision-Wesley Longman, 1999.

Allison, Graham T., "Conceptual Models and the Cuban Missile Crisis," *American Political Science Review*, Vol. 63, No. 3 (September 1969), pp. 689-718.

apabiz e. V.: *Die NPD – Eine Handreichung zu Programm, Struktur, Personal und Hintergründen.* Zweite, aktualisierte Auflage. 2008.

Aro, Jessikka, 'Yle Kioski Traces the Origins of Russian Social Media Propaganda – Never-before-seen Material from the Troll Factory', *Yle*, 20 February 2015 (http://kioski.yle.fi/omat/at-the-origins-of-russian-propaganda).

Arquilla, John and David Ronfeldt. "The Advent of Netwar." *Networks and* Netwars. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica 2001.

Arquilla, John and David Ronfeldt. "What Next For Networks and Netwars?" *Networks and Netwars*. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica 2001.

Asal, Victor, and Joseph K. Young. "Battling abroad: Why some organizations are likely targets of foreign counterterrorism." *Civil Wars* 14.2, 2012: 272-287.

Assange, Julian, "The Curious Origins of Political Hacktivism". *CounterPunch*, 2006.

Bambauer, Derek E., et al., "Internet filtering in China in 2004-2005: A country study," 2005.

Bamman, David, Brendan O'Connor, Noah A. Smith Censorship and deletion practices in Chinese social media firstmonday.org Volume 17, Number 3–5 March 2012.

Bandurski, David, "China's Guerilla War for the Web," *Far Eastern Economic Review*, July 2008.

Bapat, Navin A. "The Escalation of Terrorism: Microlevel Violence and Interstate Conflict." *International Interactions* 40.4, 2014: 568-578.

Bapat, Navin A. "The Sponsorship Dilemma: State Support for Militant Insurgency." 2007.

Barber, Elizabeth, "Hong Kong Police Arrest Prominent Radicals in Home Raids," TIME, December 10, 2014.

Barno, David and Nora Bensahel, "Fighting and Winning in the 'Grey Zone,'" *War on the Rocks*, May 19, 2015.

Barno, David, "The Shadow Wars of the 21st Century," *War on the Rocks*, July 23, 2014.

Beam, Christopher, "The Uglier Side of the Hong Kong Protests," *New Republic*, October 2014.

Beck, Colin J. "The contribution of social movement theory to understanding terrorism." *Sociology Compass* 2.5, 2008: 1565-1581.

Beijing wanbao, 7 August 1999.

Beilenson, Laurence, *Power Through Subversion*, Washington, D.C.: Public Affairs Press, 1972.

Beissinger, Mark R., *Nationalist Mobilization and the Collapse of the Soviet State* (Cambridge: Cambridge University Press, 2002.

Bell, Mark R., and Taylor C. Boas. "Falun Gong and the Internet: Evangelism, community, and struggle for survival." *Nova Religio: The Journal of Alternative and Emergent Religions* 6.2, 2003, pp. 277-293.

Benjamin Penny, "The Past, Present and Future of Falun Gong," A lecture by Harold White Fellow, Benjamin Penny, at the National Library of Australia, Canberra, 2001.

Bennett, Lance and Shanto Iyengar, "A New Era of Minimal Effects? The Changing Foundations of Political Communication," *Journal of Communication*, Vol. 58, No. 4 (2008) pp. 707-731.

Bennett, Lance W., "The Personalization of Politics Political Identity, Social Media, and Changing Patterns of Participation." *The Annals of the American Academy of Political and Social Science,* Vol. 644, No. 1, pp. 20–39, 2012.

Bennett, William, "Where Did Eastern Lightnings Leaders Come From?" ChinaSource, April 2, 2014.

Berger, J., The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion. *Perspectives On Terrorism, 9*(4), 2015.

Berger, M., "The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion" (2015).

Bernat, Jose, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016.

Bessant, Judith. "The political in the age of the digital: Propositions for empirical investigation." *Politics* 34.1, 2014: 39.

Betz, David, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *Journal of Strategic Studies*, Vol. 35, No. 5 (October 2012), pp. 689–711.

Beyer, Jessica L. "The emergence of a freedom of information movement: Anonymous, WikiLeaks, the Pirate party, and Iceland." *Journal of Computer-Mediated Communication* 19.2, 2014: 141-154.

Bezmenov, Yuri, "Soviet Subversion of Western Society," Lecture on Subversion, 1983.

Bimber, Bruce, "The Internet and Political Transformation: Populism, Community and Accelerated Pluralism," *Polity*, 31 (1), 1998, pp. 133-160.

Bimber, Bruce, *Information and American Democracy* Cambridge: Cambridge University Press, 2003.

Blackstock, Paul W., *The Strategy of Subversion: Manipulating the Politics of Other Nations*, Quadrangle Books, 1964.

Bohara, Alok K., Neil J. Mitchell, and Mani Nepal. "Opportunity, democracy, and the exchange of political violence: A subnational analysis of conflict in Nepal." *Journal of conflict resolution* 50.1, 2006: 108-128.

Borkowicz, Jacek. "Pussy Riot and Cyber-Orthodoxy." New Eastern Europe 4.3, 2012: 37-44.

Brandstetter, Marc: *Die NPD unter Udo Voigt. Organisation. Ideologie. Strategie*, Nomos Verlag, Baden-Baden, 2013.

Brenner, Susan, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law & Criminology*, 97/2, 2007, 379–475.

Briggs, Rachel and Ross Frenett, 'Foreign fighters, the challenge of counter-narratives', Policy Brief, London: Institute for Strategic Dialogue, 2014.

Buckley, Chris and Alan Wong, "*Factions Seeking Escalation Put Pressure on Hong Kong Protest*," New York Times, November 24, 2014.

Buckley, Chris and Wong, Alan, "Pro-Democracy Movement's Vote in Hong Kong Abruptly Called Off". *New York Times,* 26 October 2014.

Butsenko, Anton, 'Тролли из Ольгино переехали в новый четырехэтажный офис на Савушкина' [Trolls from Olgino move to a new four-storey office on Savushkina Street], *Delovoy* Peterburg, 28 October 2014 (http://www.dp.ru/103iph/).

Byman, Daniel. *Deadly connections: States that sponsor terrorism*. Cambridge University Press, 2005.

Caiani, Manuela and Parenti, Linda, *European and American Extreme Right Groups and the Internet*, Routledge, 2016, p. 43.

Carr ,J., The Myth of the CIA and the Trans-Siberian Pipeline Explosion, 2012.

Carr, Jeffrey, Inside Cyber Warfare Sebastopol, CA: O'Reilly Media, 2010; Reveron, Derek, "An Introduction to National Security and Cyberspace." In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Derek Reveron, Ed., Washington, DC: Georgetown University Press, 3– 20., 2012.

Caverley, Jonathan D., et al. "Military Technology and the Duration of Civil Conflict".

Chaffee, S. & M. Metzger, M., "The end of mass communication," *Mass Communications and Society*, No. *4*, pp. 365-79, 2001.

Chan, Conrad, Anthony Dao, Justin Hou, Tony Jin, Calvin Tuong, "German Censorship Policy," 2011.

Chan, Kevin, "Chinese shoppers latest target of Hong Kong protest anger". *USA Today*, 2 March 2015.

Chapin, Wesley D., *Germany for the Germans?*. Greenwood Publishing Group, 1997.

Chase, Michael S., and James C. Mulvenon. *You've got dissent! Chinese dissident use of the Internet and Beijing's counter-strategies*. Rand Corporation, 2002.

Chenoweth, Erica, and Maria J. Stephan. *Why civil resistance works: The strategic logic of nonviolent conflict*. Columbia University Press, 2011.

Chenoweth, Erica. "Terrorism and democracy." *Annual Review of Political Science* 16, 2013: 355-378.

China Anti-Cult Association, *Shipo xiejiao "quannengshen"* 破邪教"全能神" [Seeing through the "Almighty God" cult], http://zt.kaiwind.com/a/qns/shipin/2013/0124/284.html.

Ching, Julia, "The Falun Gong: Religious and Political Implications," *American Asian Review*, Vol. XIX, no. 4, Winter 2001.

Choucri, Nazli, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press, 2012)

Christensen, Christian. "Discourses of technology and liberation: State aid to net activists in an era of "Twitter Revolutions"." *The Communication Review* 14.3, 2011, pp. 233-253.

Clark, David D. and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010).

Clarke, Richard A. and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010).

Clayton, Richard, *Anonymity and Traceability in Cyberspace*, vol. 653, Technical Report, Cambridge: Univ. of Cambridge Computer Laboratory 2005.

Coleman, Gabriella. "Anonymous and the Politics of Leaking." *Beyond WikiLeaks*. Palgrave Macmillan UK, 2013. 209-228.

Connolly, Kate in Erfurt and Berlin, "Die Linke party wins German votes by standing out from crowd," *The Guardian*, 2012.

Cornish, Paul, David Livingstone, Dave Clemente and Claire York, "On Cyber Warfare," Chatham House (November 2010).

Cox, Christopher, "Digital Repertoires: Non-State Actors and ICTs," *The Osprey Journal of Idea and Inquiry*, Paper 57, 2006.

Cox, Robert W. *Production, power, and world order: Social forces in the making of history*. Vol. 1. Columbia University Press, 1987.

Cox, Robert W., "Gramsci, Hegemony and International Relations," *Millennium Journal of International Affairs*, 12(2), 1987.

Crenshaw, Martha. "The psychology of terrorism: An agenda for the 21st century." *Political psychology* 21.2, 2000: 405-420.

Cronin, Audrey Kurth, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*, Princeton University Press, 2011.

Dahan, Michael. "Hacking for the Homeland: Patriotic Hackers Versus Hacktivists." *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013*. Academic Conferences Limited, 2013.

Danzig, Richard. *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. 2014.

Davenport, Christian. "The promise of democratic pacification: An empirical assessment." *International Studies Quarterly* 48.3, 2004: 539-560.

David Ownby, *Falun Gong and the Future of China*. New York, NY: Oxford University Press, 2008.

De Mesquita, Bruce Bueno, *The logic of political survival*, MIT Press, 2005.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, Mass.: MIT Press.

Deibert, Ronald, and Rafal Rohozinski. "Liberation vs. control: The future of cyberspace." *Journal of Democracy* 21.4 (2010): 43-57.

Diamond, Larry, and Marc F. Plattner. *Liberation technology: Social media and the struggle for democracy*. JHU Press, 2012.

Diamond, Larry. "Liberation technology." *Journal of Democracy* 21.3 (2010): 69-83.

DoD; Joint Education and Doctrine Division, November 2010.

Dongsheng, Wu, Xiejiaode mimi: dangdai Zhongguo xiejiao juhe jizhi yanjiu (English title: The secrecy of evil cult – A study on the regime of evil cult assembly in today's China), Beijing: Shehui kexue wenxian chubanshe, 2005.

Dunn, Emily C. "'Cult," Church, and the CCP: Introducing Eastern Lightning." *Modern China* 35.1, 2009, pp. 96-119.

Dunn, Emily C., Netizens of Heaven: Contesting Orthodoxies on the Chinese Protestant Web, *Asian Studies Review*, 31:4, 2007, pp. 447-458.

Dupree, J.D., "International Communication, View from a Window on the World," *Gazette* Vol. 17, pp. 224-235, 1971.

Earl, Jennifer and Katrina Kimport, *Digitally Enabled Social Change* (Cambridge: MIT Press, 2011).

Efroni, Zohar, "German Court Orders to Block Wikipedia.de Due to Offending Article," *Center for Internet and Society Blog*, Stanford University Law School, 16 November 2008

Elo, Kimmo, "The Left Party and the Long-Term Developments of the German Party System". *German Politics and Society*. **26** (88), 2008, pp. 53–58.

ENCURVE, LLC. "Hacktivism and Politically Motivated Computer Crime," 2008.

Enders, Walter, and Todd Sandler (2002). Patterns of Transnational Terrorism, 1970–1999: Alternative Time- Series Estimates. *International Studies Quarterly 46*(2), 145.

Eriksson, Johan and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: The (IR)relevant Theory?" *International Political Science Review*, Vol. 27, No. 3 (July 2006), pp. 221–244

Eubank, William Lee, and Leonard Weinberg. "Does democracy encourage terrorism?." *Terrorism and Political Violence* 6.4, 1994: 417-435.

Faison, Seth, "In Beijing: A Roar of Silent Protestors". *The New York Times*, 27 April 1999.

Fletcher, Owen, "China Clamps Down on Internet Ahead of 60th Anniversary," IDG News Service, 25 September 2009; available at *www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html*.

Forney, Matthew, Jesus is back, and she's Chinese. Time 158:8, 2001. Available at http://www.time.com/time/world/article/0,8599,181681,00.html.

Fujian ribao, 5 August 1999.

Galtung, J. & M. Ruge, "The structure of foreign news the presentation of the Congo, Cuba and Cyprus Crises in four Norwegian newspapers," *Journal of Peace Research*, 1965.

Galtung, Johan, "Positive and negative peace," *School of Social Science, Auckland University of Technology*, *30*, pp.23-26.

Gapova, Elena. "Becoming Visible in The Digital Age: The class and media dimensions of the Pussy Riot affair." *Feminist Media Studies* 15.1, 2015: 18-35.

Gartzke, Erik, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73.

Gates, S., & Podder, S., Social Media, Recruitment, Allegiance and the Islamic State. *Perspectives On Terrorism, 9*(4), 2015.

Gehrett, Anne, Vice-President of Law Enforcement Program, CACI. Personal Interview, July 2004 Gehrett 2004.

George A.L. and Bennett A, Case Studies and Theory Development in the Social Sciences, Cambridge, MA: Belfer Center for International Affairs, Harvard University, 2004.

Germano, Judith and Zachary Goldman, *After the Breach: Cybersecurity Liability Risk*, The Center on Law and Security, New York University School of Law (2014).

Germano, Judith, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, The Center on Law and Security, New York University School of Law (October 2014).

Gilboa, Eytan, "The CNN Effect: The Search for a Communication Theory of International Relations," *Political Communication*, Vol. 22, No. 1, pp. 27-44, 2005.

Gill, S. and D. Law, "Global Hegemony and the Structural Power of Capital," *International Studies Quarterly*, 33-475, 1989.

Gilpin, Robert. *The political economy of international relations*. Princeton University Press, 2016.

Goddard, Stacie E., and Daniel H. Nexon. "The Dynamics of Global Power Politics: A Framework for Analysis." *Journal of Global Security Studies* 1.1, 2016: 4-18.

Goldstein, Avery, and Guobin Yang. *The Internet, Social Media, and a Changing China*. University of Pennsylvania Press, 2016.

Gordon, Bennett, "Iranian Protesters, Web Censors, and the Falun Gong," UTNE Reader, September 4, 2009.

Gracie, Carrie (13 August 2014). "The Chinese cult that kills 'demons'". BBC. Retrieved 8 April 2017.

Greenhow, C. and B. Robelia, "Informal Learning and Identity Formation in Online Social Networks." *Learning, Media and Technology* Vol. 34, No. 2, pp. 119–140, 2009.

Grossman, Taylor, and Amy B. Zegart. "The Problem of Warning: Homeland Security and the Evolution of Terrorism Advisory Systems." 2015.

Guangming ribao, 13 August 1999.

Guangming ribao, 3 August 1999.

Guo, Luke, Dangxin! "Dongfang shandian" yudang zhengzai liyong QQ laqun, 3 March 2006. Available at http://bbs.loves7.com/viewthread.php?tid1/423353, accessed 6 April 2017.

Gutmann, Ethan. "Hacker nation: China's cyber assault." *World Affairs*, 2010, pp. 70-79.

Haas, Mark L., The Ideological Origins of Great Power Politics, 1789-1989 (Ithaca, NY: Cornell University Press, 2005.

Haerbin ribao, 1 August 1999.

Hairen, Zong, "Zhu Rongji zai yijiujiujiu nian" ("Zhu Rongji in 1999").

Han, Sam, and Kamaludeen Mohamed Nasir. *Digital culture and religion in Asia*. Vol. 4. Routledge, 2015, p. 53.

Hartley, Matt. "How a Canadian cracked the great firewall of China". The Globe and Mail, 3 Oct 2008.

Healey, Jason (eds.), *A Fierce Domain: Conflict in Cyberspace 1986– 2012*, Washington, DC: Cyber Conflict Studies Association, 2013;.

Heilig, Dominic, Mapping the European Left: Socialist Parties in the EU, Rosa Luxemburg Stiftung, April 2016.

Hindman, Matthew. *The myth of digital democracy*. Princeton University Press, 2008.

Hjorth, Larissa, and Olivia Khoo, eds. *Routledge Handbook of New Media in Asia*. Routledge, 2015.

Hochschild, Jennifer L. and John H. Mollenkopf (2009). *Bringing Outsiders in: Transatlantic Perspectives on Immigrant Political Incorporation*. Cornell University Press.

Hoffman, Bruce, *Inside Terrorism*, Columbia University Press, 2006.

Holsti, K. J., Peace and War: *Armed Conflicts and International Order 1648-1989*, New York: Cambridge University Press, 1991

Hong Kong Voice of Democracy, "Chinese Government Blocked E-Mails During Falun Gong Crackdown," <http://www.democracy.org.hk/EN/jul1999/mainland 18.htm>.

http://digital-activism.org/projects/GDADSs/.

http://frank-franz.de/.

http://web.archive.org/web/http://www.clearwisdom.net/3/sio/39097318.

https://www.ccc.de/en/.

https://www.landtag-mv.de/index.php?strg=3_45&modStrg=5&baseID=45&memID=101.

Huang, Bi Yun. *Analyzing a social movement's use of Internet: Resource mobilization, new social movement theories and the case of Falun Gong*. Indiana University, 2009.

Hudson, Alan. "NGOs' transnational advocacy networks: from 'legitimacy'to 'political responsibility'?." *Global networks* 1.4, 2001: 331-352.

Hughes, Christopher R. "Google and the great firewall." *Survival* 52.2, 2010, pp. 19-26; and Ziccardi, Giovanni. *Resistance, liberation technology and human rights in the digital age*. Vol. 7. Springer Science & Business Media, 2012.

Hui, Victoria Tin-bor. "The protests and beyond." *Journal of Democracy* 26.2, 2015, pp. 111-121.

Hunt, Katie, "China arrests 1,000 members of banned religious cult 'Eastern Lightning'" *CNN*, August 20, 2014.

Imlay, Talbot and Monica Duffy Toft (eds.), *The Fog of Peace and War Planning: Military and Strategic Planning under Uncertainty*, New York: Routledge 2006.

Inspectors General, *Interagency Assessment of Iraq Police Training,* Washington, D.C.: U.S. Department of State and U.S. Department of Defense, July 2005.

International Crisis Group (ICG), *Radical Islam in Central Asia: Responding to Hizb ut-Tahrir,* Asia Report No. 58, June 30, 2003

Ip, Kelly, Phneah, Jeraldine and NectarGan, "Undampened". *The Standard*, 5 June 2013.

Jacobs, Andrew, "Chatter of Doomsday Makes Beijing Nervous". *The New York Times*, December 19, 2012.

Jardine, Eric. *The Insurgent's Dilemma: A Theory of Mobilization and Conflict Outcome*. Diss. Carleton University Ottawa, 2014.

Jensen, Benjami, Ryan Maness and Brandon Valeriano, "Cyber Victor: The Efficacy of Cyber Coercion," Working Paper, 2016.

Jessop, Bob. "A neo-Gramscian approach to the regulation of urban regimes: accumulation strategies, hegemonic projects, and governance." *Reconstructing urban regime theory: regulating urban politics in a global economy* 5 (1997): 1-74.

Johnson, Ian, "The Survival of Falun Dafa Rests on Beepers and Faith," *Wall Street Journal*, 25 August 2000.

Johnsson, Stefan. "China: The Silence Behind the Wall." *Information Warfare*, 2013.

Joint Analysis Report 16-20296A, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, December 29, 2016.

Jones, Seth G., and Martin C. Libicki. *How terrorist groups end: Lessons for countering al Qa'ida*. Rand Corporation, 2008.

Jordan, Lisa, and Peter Van Tuijl. "Political responsibility in transnational NGO advocacy." *World development* 28.12, 2000: 2051-2065.

Jordan, Tim, and Paul A. Taylor. *Hacktivism and cyberwars: Rebels with a cause?*. Psychology Press, 2004.

Junio, Timothy J., "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conoict Debate," *Journal of Strategic Studies*, Vol. 36, No. 1 (February 2013), pp. 125–133.

Kahin, Audrey and George Kahin, *Subversion as Foreign Policy: The Secret Eisenhower and Dulles Debacle in Indonesia*, New Press, 1995.

Kaimin, Jonathan, "China arrests 500 followers of religious cult over Mayan apocalypse rumours," *The Guardian*, December 19, 2012.

Kamat, Sangeeta. "NGOs and the new democracy." *Harvard International Review* 25.1, 2003.

Kang-chung, Ng, "Radical Hong Kong group Civic Passion to become "moderate" political party," ViewHK, 6 January 2017.

Karagiannis, Emmanuel, and Clark McCauley, "Hizb ut-Tahrir al-Islami: Evaluating the Threat Posed by a Radical Islamic Group That Remains Nonviolent," *Terrorism and Political Violence,* Vol. 18, 2006.

Karamay, Josh, "Blogger Describes Xinjiang as an 'Internet Prison,'" BBC News, 3 February 2010; available at *http://news.bbc.co.uk/2/hi/asia-pacific/8492224.stm.*

Karapin, Roger. "Far-Right Parties and the Construction of Immigration Issues in Germany." *Shadows over Europe*. Palgrave Macmillan US, 2002, pp. 187-219.

Karatzogianni, Athina. *The politics of cyberconflict*. Routledge, 2006.

Katsiaficas, George. "The subversion of politics: European autonomous movements and the decolonization of everyday life." *Atlantic Highlands, NJ: Humanities Press*, 1997.

Katz, Mark N., *Revolutions and Revolutionary Waves*, New York: Palgrave Macmillan, 1999.

Keck, Margaret E., and Kathryn Sikkink. *Activists beyond borders: Advocacy networks in international politics*. Cornell University Press, 2014.

Kello, Lucas, "The Meaning of the Cyber Revolution: Perils to Theory and State- craft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40.

Keohane, Robert O. *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press, 2005.

Khamidov, Alisher "Countering the Call: The US, Hizb-ut-Tahrir, and Religious Extremism in Central Asia," Washington, D.C.: Saban Center for Middle East Policy, Brookings Institution, Analysis Paper No. 4, July 2003.

Kilberg, Joshua. "A basic model explaining terrorist group organizational structure." *Studies in Conflict & Terrorism* 35.11, 2012: 810-830.

Kilberg, Joshua. *Organizing for destruction: How organizational structure affects terrorist group behaviour*. Diss. Carleton University Ottawa, 2011.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107.02, 2013, pp. 326-343.

Kiruthiga, A., S. Bose, and N. Buvaneswari. "An experimental simulation of hub-spoke terrorist organizational structure." *Advances in Natural and Applied Sciences* 9.9 SE, 2015: 41-45

Kitson, Frank, *Low intensity operations: subversion, insurgency, peacekeeping,* Harrisburg PA: Stackpole Books, 1971.

Klausen, Jytte, "Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38 no.1 (2015): 1-22.

Klein, Adam G. "Vigilante media: Unveiling Anonymous and the hacktivist persona in the global press." *Communication Monographs* 82.3, 2015: 379-401.

Koesel, Karrie J., and Valerie J. Bunce. "Putin, Popular Protests, and Political Trajectories in Russia: A Comparative Perspective." *Post-Soviet Affairs* 28.4, 2012: 403-423.

Kosseff, Jeff. "The hazards of cyber-vigilantism." *Computer Law & Security Review* 32.4, 2016: 642-649.

Krapp, Peter, *Noise Channels: Glitch and Error in Digital Culture*, University of Minnesota Press, 2011.

Kutolowski, "The Role of Clear Wisdom Net in My Cultivation."

Kwong, Ying-Ho. "The Dynamics of Mainstream and Internet Alternative Media in Hong Kong: A Case Study of the Umbrella Movement+." *International Journal of China Studies* 6.3, 2015, p. 273.

Lam, Oiwan, "China: Blue Dam Activated," *Global Voices Advocacy,* 13 September 2009; available at *http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated.*

Lam, Oiwan, "China: More than 100 Thousand Websites Shut Down," *Global Voices Advocacy,* 3 February 2010; available at *http://advocacy.globalvoicesonline. org/2010/02/03/china-more-than-100-thousand-websites-shut-down.*

Lang, Jochen. "Policy Implementation in a Multi-Level System: The Dynamics of Domestic." *Linking EU and National Governance*, 2003.

Langner, Ralph, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group (November 2013).

Lathem, Niles, "Qaeda Claim: We 'Infiltrated' UAE Government," *New York Post,* February 25 2006.

Lawrence, T.E., *Seven Pillars of Wisdom*, 1922.

Lee, Alice YL, and Ka Wan Ting. "Media and information praxis of young activists in the Umbrella Movement." *Chinese Journal of Communication* 8.4, 2015, pp. 376-392.

Lee, Francis LF, and Joseph Man Chan. "Digital media activities and mode of participation in a protest campaign: A study of the Umbrella Movement." *Information, Communication & Society* 19.1, 2016.

Lee, Francis LF. "Social movement as civic education: Communication activities and understanding of civil disobedience in the Umbrella Movement." *Chinese Journal of Communication* 8.4, 2015, pp. 393-411.

Lee, Martin A. *The Beast Reawakens: Fascism's Resurgence from Hitler's Spymasters to Today's Neo-Nazi Groups and Right-Wing Extremists*. Routledge, 2013.

Lee, Terrence, "Anti-communist news site Passion Times banned from China's Apple App Store". *Tech in Asia*, 11 November 2014.

Leigh, David, Luke Harding, and Charles Arthur. *Wikileaks: inside Julian Assange's war on secrecy*. PublicAffairs, 2011, p. 183.

Lemieux, Anthony .F., and Victor Asal. 2010 "Grievance, social dominance orientation, and authoritarianism in the choice and justification of terror versus protest."Dynamics of Asymmetric Conflict 3 (3):194-207.

Lewis, James and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, 22 July 2013).

Lian, Xi. *Redeemed by fire: The rise of popular Christianity in modern China*. Yale University Press, 2010.

Libicki, Martin *Conquest in Cyber- space: National Security and Information Warfare*;;

Liff, Adam P., "Cyberwar: A New 'Absolute Weapon?' The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401–428.

Lindsay, Jon R. and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in Greenhill, Kelly and Peter Krause (eds.), *The Power to Hurt: Coercion in the Modern World,* 2016.

Lindsay, Jon R. and Erik Gartzke, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2 (2015) pp. 316-348.

Lindsay, Jon R. and Stephen Haggard, "North Korea and the Sony Hack: Exporting Instability Through Cyberspace," East-West Center, 2015.

Lindsay, Jon R., "Stuxnet and the limits of cyber warfare." *Security Studies*, Vol. 22, No. 3 (2013) pp. 365-404.

Lindsay, Jon R., "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3 (Winter 2014/15) pp. 7-47.

Lindsay, Jon R., Tai Ming Cheung and Derek Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford: Oxford University Press, 2015.

Lo, Barry Hashimoto, and Dan Reiter, "Ensuring Peace: Foreign-Imposed Regime Change and Postwar Peace Duration, 1914-2001," International Organization 62 (2008), 717-36.

Lo, Sonny Shiu-Hing, *Hong Kong's indigenous democracy: Origins, evolution and contentions*, Springer, 2016.

Luhn, Alec, 'Game of trolls: the hip digi-kids helping Putin's fight for online supremacy', *Guardian*, 18 August 2015 (http://www.theguardian.com/world/2015/aug/18/trolls-putin-russia-savchuk).

Lynch, Marc. "After Egypt: The limits and promise of online challenges to the authoritarian Arab state." *Perspectives on politics* 9.02 (2011): 301-310.

Lysenko and Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." 2013.

Lysenko and Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." 2013.

Lysenko, Volodymyr, and Barbara Endicott-Popovsky. "Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia." *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013*. Academic Conferences Limited, 2013.

MacDonald, Paul K. "'Retribution Must Succeed Rebellion": The Colonial Origins of Counterinsurgency Failure." *International Organization* 67.02, 2013: 253-286.

MacKinnon, Rebecca. "China's" networked authoritarianism"." *Journal of Democracy* 22.2 (2011): 32-46.

MacKinnon, Rebecca. "China's" networked authoritarianism"." *Journal of Democracy* 22.2, 2011, pp. 32-46.

Madsen, Richard, "Understanding Falun Gong," *Current History* 99, no. 638, September 2000, pp. 243-247.

Manjikian, Mary M., "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly*, Vol. 54, No. 2 (June 2010), pp. 381–401.

Marighella, Carlos, *Minimanual of the Urban Guerrilla,* 1969.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho, "Stuxnet under the Microscope," eset, white paper (20 January 2011).

Matthes, Jörg, and Matthias Kohring. "The content analysis of media frames: Toward improving reliability and validity." *Journal of communication* 58.2 (2008): 258-279.

Mazarr, Michael, "Struggle in the Grey Zone and World Order," *War on the Rocks*, December 22, 2015.

McConnell, Mike, "Cyberwar is the New Atomic Age," *New Perspectives Quarterly,* Vol. 26, No. 3 (Summer 2009) pp. 72–77.

McCormick, Gordon H., "Terrorist Decision Making," *Annual Review of Political Science,* Vol. 6, 2003.

McDonough, Frank. *Opposition and resistance in Nazi Germany*. Cambridge, UK: Cambridge University Press, 2001.

McFaul, Michael, 'What's it like to be hated by the Russian internet?', *Guardian*, 26 May 2015 (http://www.theguardian.com/world/2015/may/26/russia-internet-hated)

McFaul, Michael. *Russia's unfinished revolution: political change from Gorbachev to Putin*. Cornell University Press, 2015.

McGowan, Lee. *The radical right in Germany: 1870 to the present*. Routledge, 2014.

Mclelland, Mark. "Internet Domains between China and India: Beyond Anglophone Paradigms." *Asian Studies Review* 31.4, 2007, pp. 387-395.

McMichael, Polly. "Defining Pussy Riot musically: Performance and authenticity in new media." *Digital Icons: Studies in Russian, Eurasian and Central European New Media* 9 (2013): 99-113.

Melinda Liu, "The Great Firewall of China," *Newsweek*, int. ed., 11 October 1999, <http://discuss.washingtonpost.com/nw-srv/issue/15_99b/printed/int/wb/ov1315 1.htm>.

Miegel, Fredrik, and Tobias Olsson. "Civic Passion: A Cultural Approach to the "Political"." *Television & New Media* 14.1, 2013, pp. 5-19.

Miller, Andrew. "Perfect Opposition: On Putin and Pussy Riot." *Juncture* 19.3, 2012: 205-207.

Mingxia and Shiping Hua (eds.), "The battle between the Chinese government and the falun gong," *Chinese Law and Government*, September-October 1999.

Minzner, Carl, "Social Instability in China: and Causes, Consequences, and Implications," Center for Strategic and International Studies, December 2006, available at http://csis.org/files/attachments/061205_Minzner.pdf, accessed March 29, 2017.

Molnar, Andrew R., *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare,* Washington, D.C.: Special Operations Research Office, November 1963.

Morais, Richard C. "China's Fight With Falun Gong", *Forbes*, 9 February 2006; and Associated Press, *China Dissidents Thwarted on Net*. Retrieved 10 April 2017.

Morozov, Evgeny. *The net delusion: The dark side of Internet freedom*. PublicAffairs, 2012.

Mosher, Stacy and Chine Chan, "Reviewing a Quarter Century of Political Crime," *China Rights Forum* no. 2, 2003.

Mudde, Cas, “Germany wants to ban the neo-Nazis of the NPD again, but why now?” *The Guardian*, March 4, 2016.

Mudde, Cas. "The far right and the European elections." *Current History* 113.761, 2014.

Nanfang ribao, 18 March 1999.

Neues Deutschland, 20/21 August 2005.

Newman, Edward. "Exploring the “root causes” of terrorism." *Studies in Conflict & Terrorism* 29.8, 2006: 749-772.

Ng, Kang-chung (May 4, 2016). "Pro-independence Hong Kong radicals start recruiting youth corps for 'military' summer camp". *South China Morning Post*. Retrieved December 6, 2016.

NPD party programme (in German) http://npd.de/inhalte/daten/dateiablage/br_parteiprogramm_a4.pdf.

Nye, Joseph, “Cyber Power,” (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010).

O'Reilly, Kenneth, Hoover and the Unamericans: The FBI, HUAC, and the Red Menace. Temple University Press, 1983.

O’Brien, Kevin J. and Lianjian Li, *Rightful Resistance in Rural China,* New York: Cambridge University Press, 2006.

O’Brien, Kevin J., “Spam attack linked to German election,” *New York Times*, May 19, 2005.

Olson, Eric, “America’s Not Ready for Today’s Gray Wars,” *DefenseOne*, December 10, 2015.

Ortega y Gasset, Jose, *Invertebrate Spain*, Howard Fertif, 1974.

Ortmann, Stephan. "The umbrella movement and Hong Kong's protracted democratization process." *Asian Affairs* 46.1, 2015, pp. 32-50.

Owen, John, *The Clash of Ideas in World Politics: Transnational Networks, States, and Regime Change, 1510-2010*, Princeton University Press, 2010.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009).

Palmer, David A. (2007). *9. Falun Gong challenges the CCP. Qigong fever: body, science, and utopia in China*. Columbia University Press.

Palmer, David, *Qigong Fever: Body, Science and Utopia in China*. New York, NY: Columbia University Press, 2007.

Parvin, Manoucher, "Economic Determinants of Political Unrest: An Econometric Approach," *Journal of Conflict Resolution* 17:2 (June 1973): 271-96.

Patton, David F.. *Out of the East: From PDS to Left Party in Unified Germany*, State University of New York Press; 2011.

Pearson, Frederic S., Isil Akbulut, and Marie Olson Lounsbery. "Group Structure and Intergroup Relations in Global Terror Networks: Further Explorations." *Terrorism and Political Violence*, 2015: 1-23.

Peter Davies, Derek Lynch, *The Routledge companion to fascism and the far right*, Psychology Press, 2002, pp. 319.

Peterson, Dale, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, Vol. 36, No. 1 (February 2013), pp. 120–124.

Philippsberg, Robert: *Die Strategie der NPD: Regionale Umsetzung in Ost- und Westdeutschland.* Baden-Baden 2009.

Phillips, Tom and Eric Cheung, "Hong Kong elections: anti-Beijing activists gain foothold in power," *The Guardian*, September 5, 2016.

Pike, Douglas, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam,* Cambridge, Mass., and London: MIT Press, 1966.

Pomerantsev, Peter and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York, NY: The Institute of Modern Russia, 2014.

Porter, Noah. *Falun Gong in the United States: an ethnographic study*. Universal-Publishers, 2003.

Prados, John, "Impatience, Illusion, and Asymmetry: Intelligence in Vietnam," in Marc Jason Gilbert, ed., *Why the North Won the Vietnam War,* New York: Palgrave, 2002.

Prozorov, Sergei. "Pussy Riot and the politics of profanation: Parody, performativity, veridiction." *Political Studies* 62.4, 2014: 766-783.

Quercia, D., L. Capra, and J. Crowcroft, "The Social World of Twitter: Topics, Geography, and Emotions." *Proceedings of the Sixth International Conference on Weblogs and Social Media*, Dublin: Palo Alto, CA: AAAI Press, 2012.

Rahimi, Babak. "Internet and Political Activism in Post-Revolutionary Iran." *The Handbook of Media and Mass Communication Theory* (2014): 907-928.

Rahimi, Babak. "Vahid Online: Post-2009 Iran and the Politics of Citizen Media Convergence." *Social Sciences* 5.4 (2016): 77.

Rath, Robert, "The politics behind Hong Kong's Pikachu protests," ZAM.

Rattray, Gregory J., *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001); Scott Borg, "Economically Complex Cyberattacks," *IEEE Security and Privacy Magazine*, Vol. 3, No. 6 (November/December 2005), pp. 64–67.

Renmin ribao (*People's Daily*), 15 August 1999.

Renmin ribao, 11 August 1999.

Renmin ribao, 13 August 1999.

Renmin ribao, 23 July 1999; "A brief discussion on *falun gong*."

Renmin ribao, 4 August 1999.

Renmin ribao, 5 August 1999.

Renmin ribao, 7, 8 August 1999.

Research Department, Ministry of Public Security, "Li Hongzhi."

Resolution on Opposing Evil Cults and Resisting Heretical Beliefs, Amity News Service 11:5/6, 2002. Available at http://www.amitynewsservice.org/page.php?page1/4674.

Reveron, Derek, "An Introduction to National Security and Cyberspace." In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Derek Reveron, Ed., Washington, DC: Georgetown University Press, 3– 20., 2012.

Ricchiardi, Sherry. *Supporting Internet Freedom: The Case of Iran*. Center for International Media Assistance, 2014.

Richard Madsen, "Understanding Falun Gong," *Current History* 99, no. 638, September 2000, pp. 243-247.

Rid, Thomas and Ben Buchanan, "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2, 2015: 4–37.

Rid, Thomas, "Think Again: Cyberwar," *Foreign Policy*, Vol. 192 (March/April 2012), pp. 80–84.

Rid, Thomas, and Peter McBurney, "Cyber Weapons." The RUSI Journal 157 (1): 6– 13, 2012.

Rid, Thomas, *Cyber War Will Not Take Place*, Oxford University Press, 2013.

Robert W. Cox, "Social Forces, States and World Orders" in Keohane, Robert Owen. *Neorealism and its Critics*. Columbia University Press, 1986.

Roberts, H. (n.d.). The Evolving Landscape of Internet Control. Berkman Center for Internet & Society.

Robertson, Graeme B. "Managing society: protest, civil society, and regime in Putin's Russia." *Slavic Review*, 2009: 528-547.

Robins, K., Cyberspace and the World We Live in. *Body & Society*, *1,* 3-4, 2015, 135-155.

Ronfeldt, David, and John Arquilla. "Networks, netwars and the fight for the future." *First Monday* 6.10, 2001.

Rosenau, William, "Subversion and Insurgency," RAND Counterinsurgency Study, Paper 2, Santa Monica, California: RAND Corporation, 2007.

Ross, Jeffrey Ian. "Beyond the conceptualization of terrorism: A psychological-structural model of the causes of this activity." 1999.

Ross, Jeffrey Ian. "Structural causes of oppositional political terrorism: Towards a causal model." Journal of Peace Research 30.3, 1993: 317-329.

Salehyan, Idean. "Transnational rebels: Neighboring states as sanctuary for rebel groups." *World Politics* 59.02, 2007: 217-242.

Sanger, David E., *The Reckoning: How President Obama Has Changed the Force of American Power*, New York: Crown, 2012.

Sataline, Suzanne, "Meet the Man Who Wants to Make Hong Kong a City-State". *Foreign Policy*, 18 May 2015.

Sauter, Molly, *The Coming Swarm: DDoS Actions, Hactivism and Civil Disobedience on the Internet*, Bloomsbury: New York, 2014.

Schattkowsky, R., Separatism in the Eastern Provinces of the German Reich at the End of the First World War. *Journal of Contemporary History*, *29*(2), 1994, pp.305-324.

Schechter, Danny, *Falun Gong's challenge to China: spiritual practice or 'evil cult'?.* Akashic Books, November 2001.

Schedler, Andreas. *The politics of uncertainty: Sustaining and subverting electoral authoritarianism*. OUP Oxford, 2013.

Schmid, Alex P. "Terrorism and democracy." *Terrorism and Political Violence* 4.4, 1992: 14-25.

Scholl, Inge. *The White Rose: Munich, 1942–1943*. Wesleyan University Press, 2011.

Schuler, Catherine. "Reinventing the show trial: Putin and Pussy Riot." *Anthropology, Theatre, and Development*. Palgrave Macmillan UK, 2015. 286-302.

SCIO, "The Internet in China."

Sechrist, Michael, "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems," in *Science, Technology, & Public Policy Program*

Discussion Paper Series, Cambridge, MA: Explorations in Cyber International Relations Project at Belfer Center for Science and International Affairs, 2012.

Selznick, Philip, *The Organizational Weapon: A Study of Bolshevik Strategy and Tactics,* New York: McGraw- Hill Book Company, Inc., 1952.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes, 2013.

Shanthi Kalathil, "A Thousand Websites Almost Bloom," *Asian Wall Street Journal*, 29 August 2000.

Shantz, Jeff and Tomblin, Jordon, *Cyber Disobedience: Re://Presenting Online Anarchy*, John Hunt Publishing, 2014.

Sharafutdinova, Gulnaz. "The Pussy Riot affair and Putin's démarche from sovereign democracy to sovereign morality." *Nationalities Papers* 42.4, 2014: 615-621.

Shea, Matt, "The Cult Who Kidnaps Christians and Is at War with the Chinese Government," VICE, July 21, 2013.

Smith, James Morton, *Freedom's Fetters: The Alien and Sedition Laws and American Civil Liberties*. Ithaca NY: Cornell University Press, 1956.

Smith, Jessica Malekos, "Twilight Zone Conflicts: Employing Gray Tactics in Cyber Operations," *Small Wars Journal*, 2016.

Snidal, Duncan. "The limits of hegemonic stability theory." *International organization* 39.04 (1985): 579-614.

Spiegel, Mickey (2002). *Dangerous Meditation: China's Campaign Against Falungong*. Human Rights Watch.

Spjut, R. J. "Defining Subversion". *British Journal of Law and Society*, 1979, **6** (2): 254–261.

Staniland, Paul. "Organizing insurgency: Networks, resources, and rebellion in south asia." *International Security* 37.1, 2012: 142-177.

Stefanidis, Anthony, Amy Cotnoir , Arie Croitoru , Andrew Crooks , Matthew Rice & Jacek Radzikowski, "Demarcating new boundaries: mapping virtual polycentric communities through social media content," *Cartography and Geographic Information Science*, Vol. 40, No. 2, pp. 116-129, 2013.

Steger, Isabella, "Two years after the Occupy protests, Hong Kong's pro-democracy parties are their own worst enemy," QZ, September 1, 2016.

Steinmetz, Kevin F. *Hacked: A Radical Approach to Hacker Culture and Crime*. NYU Press, 2016.

Stephan, Maria J., and Erica Chenoweth. "Why civil resistance works: The strategic logic of nonviolent conflict." *International security* 33.1, 2008: 7-44.

Stone, Brad, and David Barboza. "Scaling the digital wall in China." *New York Times* 16, 2010.

Stone, Geoffrey R. *Perilous Times: Free Speech in Wartime from The Sedition Act of 1798 to the War on Terrorism*, W.W. Norton, 2004.

Storch, Leonid. "The Pussy Riot Case: Anti-Westernism in the Paradigm of the Beilis Trial." *Russian Politics & Law* 51.6, 2013: 8-44.

Strange, Susan. "The persistent myth of lost hegemony." *International organization* 41.04 (1987): 551-574.

Streit über Präsidentenwahl: Linke verteidigt Anti-Gauck-Kurs, Spiegel Online, 1 July 2010.

Sullivan, Jonathan. "The Power of the Internet in China: Citizen Activism Online Guobin Yang New York: Columbia University Press, 2009.

Symantec, "Advanced persistent threats: How they work," 2014.

Takhteyev, Y., A. Gruzd, and B. Wellman, "Geography of Twitter Networks." *Social Networks* Vol. 34, No. 1, pp. 73–81, 2012.

Tang, Gary. "Mobilization by images: TV screen and mediated instant grievances in the Umbrella Movement." *Chinese Journal of Communication* 8.4, 2015, pp. 338-355.

Tanner, Murray Scot, "China Rethinks Unrest," *The Washington Quarterly* 27:3, Summer 2004, pp. 138.

Tchermalykh, Nataliya. "Will Pussy Riot Dance on# Euromaidan? New Dissidence, Civic Disobedience and Cyber-Mythology in the Post-Soviet Context." Religion and Gender 4.2, 2014: 215-220.

Thapa, Ganga B., and Jan Sharma. "From insurgency to democracy: The challenges of peace and democracy-building in Nepal." *International Political Science Review* 30.2, 2009: 205-219.

Thaxton, Ralph A., *Catastrophe and Contention in Rural China: Mao's Great Leap Forward Famine and the Origins of Righteous Resistance in Da Fo Village,* New York, Cambridge University Press, 2008.

The Dui Hua Foundation, "Dialogue," 34, Winter 2009, p. 7 and the Dui Hua Foundation, "Dialogue," 35, Spring 2009, p. 2.

The Dui Hua Foundation, "Statistics on Political Crimes in the People's Republic of China," Volume 3, Occasional Publications, no. 23, (December 2006, p. 11.

The Dui Hua Foundation, *Reference Materials on China's Criminal Justice System*, Volume 2, June 2009, pp. 23-26.

Thomas, Kelly A. "Falun Gong: an analysis of China's national security concerns." *Pac. Rim L. & Pol'y J.* 10, 2000, p. 471.

Thompson, John, *Other People's Wars: A Review of Overseas Terrorism in Canada,* Toronto, Ontario, Canada: Mackenzie Institute, 2003.

Thornton, Patricia M. "Manufacturing dissent in transnational China: boomerang, backfire or spectacle?." *Popular Contention in China*, 2008.

Thornton, Patricia M. (2003) The new cybersects: Resistance and repression in the reform era, in E. J. Perry and M. Selden (eds), Chinese society: Change, conflict and resistance. 2nd edition, pp. 247–70 (London/New York: RoutledgeCurzon).

Tong, James (2009). *Revenge of the Forbidden City: The Suppression of Falungong in China, 1999-2005*. New York, NY: Oxford University Press.

Tong, James. "An organizational analysis of the Falun Gong: Structure, communications, financing." *The China Quarterly* 171, 2002, pp. 636-660.

Toren, Peter, "A Report on Prosecutions under the Economic Espionage Act," paper presented at the American Intellectual Property Law Association annual meeting, Trade Secret Law Summit, Washington, D.C. (October 23, 2012).

Trinquier, Roger, *Modern Warfare: A French View of Counterinsurgency*, Pall Mall Press, 1964.

Tsang, Emily; Sung, Timmy; Chan, Samuel, "Split within Occupy deepens as splinter group challenges leadership". *South China Morning Post*, 21 November 2014.

Tsui, Lokman. "The coming colonization of Hong Kong cyberspace: government responses to the use of new technologies by the umbrella movement." *Chinese Journal of Communication* 8.4, 2015, pp. 1-9.

Tweed, David, "Hong Kong Independence Goes From Fringe Cause to Contender," *Bloomberg*, February 25, 2016.

U.S. Central Intelligence Agency (CIA), Directorate of Intelligence, "The Vulnerability of Non-Communist Groups in South Vietnam to Political Subversion," record 31052, CIA Collection, May 27, 1966.

U.S. Information Service, Office of Policy and Research, "The Viet Cong: The United Front Technique," R- 13-67, Record 128321, Douglas Pike Collection: Unit 06—Democratic Republic of Vietnam, April 20, 1967.

U.S. Marine Corps Intelligence Activity, *The Urban Threat: Guerrilla and Terrorist Organizations,* n.d. 1999.

Unerman, Jeffrey, and Brendan O'Dwyer. "Theorising accountability for NGO advocacy." *Accounting, Auditing & Accountability Journal* 19.3, 2006: 349-376.

Vaishnav, Chintan and Nazli Choucri and David D. Clark, *Cyber International Relations as an Integrated System*, MIT Political Science Department Research Paper No. 2012-16 (June 14, 2012).

Valeriano, Brandon and Ryan Maness, "A Theory of Cyber Espionage for the Intelligence Community," EMC Conference Paper (2013).

Valeriano, Brandon; Maness, Ryan C., *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford University Press, 2015.

van den Berge, Wietse, and Koningin Julianaplein. "Analyzing Middle Eastern Armed Non-State Actors' Foreign Policy." *Global Security Studies* 7.3 2016.

Van Dijk, Jan. *The network society*. Sage Publications, 2012.

Varon, Jeremy, *Bringing the War Home: The Weather Underground, the Red Army Faction, and Revolutionary Violence in the Sixties and Seventies,* Berkeley, Los Angeles, and London: University of California Press, 2004.

Vidino, Lorenzo. "The Muslim Brotherhood's Conquest of Europe." *Middle East Quarterly*, 2005.

Vidino, Lorenzo. *The new Muslim brotherhood in the West*. Columbia University Press, 2010.

Villeneuve, Nart, "Breaching Trust: An Analysis of Surveillance and Security Prac- tices on China's TOM-Skype Platform," Open Net Initiative and Information Warfare Monitor, October 2008; available at: *www.nartv.org/mirror/breachingtrust.pdf*

Von Mering, Sabine, and Timothy Wyman McCarty. *Right-wing radicalism today: perspectives from Europe and the US*. Routledge, 2013.

Voronina, Olga G. "Pussy Riot Steal the Stage in the Moscow Cathedral of Christ the Saviour: Punk Prayer on Trial Online and in Court." *Digital Icons: Studies in Russian, Eurasian and Central European New Media* 9 (2013): 69-85.

Votel, Joseph, *Statement before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities,* March 18, 2015.

Vuori, Juha A. *Critical Security and Chinese Politics: The Anti-Falungong Campaign*. Routledge, 2014, pp. 38-45.

Walt, Stephen M., *Revolution and War*, Ithaca, NY: Cornell University Press, 1996.

Walton, Greg. *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*. Rights & Democracy, 2001.

Webster, Frank. *Theories of the information society*. Routledge, 2014.

Wedeman, Andrew. "Enemies of the state: mass incidents and subversion in China." (2009), p. 10.

Weggemans, Daan, Edwin Bakker and Peter Grol, "Who are they and Why do they go? The Radicalisation and Preparatory Processes of Dutch Jihadist Fighters," *Perspectives on Terrorism* 8 no. 4 (2014): 104.

Weimann, Gabriel, *How Modern Terrorism Uses the Internet,* Washington, D.C.: United States Institute of Peace, Special Report No. 116, March 2004.

Weimann, Gabriel, *How Modern Terrorism Uses the Internet,* Washington, D.C.: United States Institute of Peace, Special Report No. 116, March 2004.

Weiss, Jessica Chen. *Powerful patriots: nationalist protest in China's foreign relations*. Oxford University Press, 2014.

Wheeler, David A. and Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, Alexandria, VA: Institute for Defense Analysis, 2003.

Whyte, Christopher, "Dissecting the Digital World: Old Questions, New Answers," *International Studies Review*, Forthcoming.

Whyte, Christopher, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy*, 35:2, 2015, pp. 93-102.

Whyte, Christopher, "Power and Predation in Cyberspace," *Strategic Studies Quarterly*, Vol. 9, No. 1 (Spring 2015) pp. 100-118.

Wodak, Ruth. *Right-wing populism in Europe: Politics and discourse*. A&C Black, 2013.

Wu, Dennis, "Investigating the Determinants of International News Flow," *International Communication Gazette*, Vol. 60, No. 6, pp. 493-512, 1998.

Xia, Bill. "The Coming Crash Of The Matrix." *China Rights Forum*. Vol. 3. 2004.

Xinhua, 21 October 1999.

Xinhua, 27 October 2001.

Xinhua, Beijing, 21 October 1999.

Xinhua, Beijing, 27 October 2001.

Xu, Beina. "Media censorship in China." Council on Foreign Relations 25, 2014;

Yablokov, Ilya. "Pussy Riot as agent provocateur: conspiracy theories and the media construction of nation in Putin's Russia." *Nationalities Papers* 42.4, 2014: 622-636.

Yang, Guobin. "Internet activism & the party-state in China." *Daedalus* 143.2 (2014): 110-123;

Yang, Guobin. *The power of the Internet in China: Citizen activism online*. Columbia University Press, 2009.

Young Sr, Aaron M., and David H. Gray. "Insurgency, guerilla warfare and terrorism: Conflict and its application for the future." *Global Security Studies* 2.4, 2011: 65-76.

Yu, Haiqing, "The new living-room war: Media campaigns and Falun Gong," 2004.

Zaihua, Wang 王在, "Quannengshenjiao mudi shi tuifan zhengfu jian 'shen de guodu'" 全能神教目的是推翻政府建“神的國度” [The goal of the Church of the Almighty God is to overthrow the government and establish "The Kingdom of God"], China Central Television 中国中央台, December 22, 2012.

Zanini, Michele and Sean J.A. Edwards. “The Networking of Terror in the Information Age.” *Networks and Netwars*. in Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica, 2001.

Zelin, A., Picture Or It Didn’t Happen: A Snapshot of the Islamic State’s Official Media Output. *Perspectives On Terrorism, 9*(4), 2015.

Zetter, Kim, “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History,” Wired Threat Level Blog, 11 July 2011, http://www.wired.com/ threatlevel/2011/07/how- digital- detectives- deciphered- stuxnet.

Zhang Dakai, *Pouxi xiejiao zuzhi "Dongfang shandian"* "" [Analyzing the cult "Eastern Lightning"].

Zhejiang Gong’an Nianjian (浙江公安年)

Zicht, Wilko. "Wahlergebnisse" (in German). Wahlrecht.de. 2014.

Biography

Christopher Whyte received a BA in International Relations and Economics from the College of William & Mary and an MA in Political Science from George Mason University. His research interests include a range of international security topics related to the use of information technology in war and peace, political communication and cybersecurity doctrine/policy. His scholarly and analytic work on cyber conflict and trends in international politics scholarship has appeared or is forthcoming in several publications including *International Studies Quarterly*, *International Studies Review*, *Strategic Studies Quarterly*, *Orbis*, *Comparative Strategy*, *New Media & Society*, *Foreign Policy* and *The National Interest*. He is also co-author of a forthcoming Routledge volume on international security and cyberspace, entitled *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Upon completion of his Doctor of Philosophy in Political Science degree in 2017, he will begin as Assistant Professor in the L. Douglas Wilder School of Policy and Government at Virginia Commonwealth University.