CYBER MERCENARIES

Cyber Mercenaries explores the secretive relationships between states and hackers. As cyberspace has emerged as the new frontier for geopolitics, states have become entrepreneurial in their sponsorship, deployment, and exploitation of hackers as proxies to project power. Such modern-day mercenaries and privateers can impose significant harm undermining global security, stability, and human rights. These state-hacker relationships therefore raise important questions about the control, authority, and use of offensive cyber capabilities. While different countries pursue different models for their proxy relationships, they face the common challenge of balancing the benefits of these relationships with their costs and the potential risks of escalation. This book examines case studies in the United States, Iran, Syria, Russia, and China for the purpose of establishing a framework to better understand and manage the impact and risks of cyber proxies on global politics.

Tim Maurer co-directs the Cyber Policy Initiative at the Carnegie Endowment for International Peace. He is a member of several US track 1.5 cyber dialogues and the Freedom Online Coalition's cybersecurity working group. He co-chaired the Advisory Board of the 2015 Global Conference on CyberSpace, participated in the Global Commission on Internet Governance, and supported the confidence-building work of the OSCE. His work has been published by *Foreign Policy*, *The Washington Post*, *TIME*, *Jane's Intelligence Review*, *CNN*, *Slate*, *Lawfare*, and other academic and media venues. He holds a Master's in Public Policy from the Harvard Kennedy School.

Cyber Mercenaries

THE STATE, HACKERS, AND POWER

TIM MAURER
Carnegie Endowment for International Peace

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107127609
DOI: 10.1017/9781316422724

First published 2018

Printed in the United States of America by Sheridan Books, Inc.

A catalogue record for this publication is available from the British Library.

ISBN 978-1-107-12760-9 Hardback
ISBN 978-1-107-56686-6 Paperback

Contents

Figures

Preface

At first glance, Kiev in the summer of 2015 seemed like an odd place to investigate the relationship between hackers and the state. It was a beautiful July weekend and people were out on the streets and in the parks. You could hardly tell that the country was at war. Not the old kind of war, the one with a declaration of war and soldiers in uniform. This was a war of the twenty-first century, where "little green men," as the locals called the unmarked foreign agents, had appeared in the country to exploit local tensions and to escalate them into a bigger conflict.[1] Over a year had passed since the eastern part of Ukraine had fallen into the hands of pro-Russian fighters, but the capital was relatively peaceful except for occasional violence, such as the deadly clashes in front of parliament that occurred in between my two research trips to Kiev.[2] Nevertheless, the situation felt a bit surreal when I arrived at what looked like an old industrial complex a few miles south of the center of town to meet Eugene Dokukin, the self-declared commander of the Ukrainian Cyber Forces, one of Ukraine's most prominent hacktivist groups.[3] In contrast to the pro-Russian fighters in eastern Ukraine, who were an old kind of proxy, Dokukin and his cadre of followers were a new kind of proxy, adding a new dimension to an already intricate conflict.

Originally, my plan was to meet Mr Dokukin at a café near my hotel in central Kiev. However, a few days prior to our planned meeting, he changed his mind. He said that he had been planning to go to a classical concert and suggested we meet there instead. Based on our previous exchanges online, it seemed probable that he would cancel if I did not accept his change of plans, so I ventured to the location he provided. What looked like an old industrial complex turned out to be the historical Dovzhenko Film Studios, created in 1928 and named after one of the most important Ukrainian filmmakers, Alexander Dovzhenko.[4] Once I had found my way through the maze of old buildings, I eventually got to an amphitheater of sorts where some

I thank the Cooperative Cyber Defence Centre of Excellence for granting permission to include material in this section from Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, (Tallinn: NATO CCD COE Publications, 2015), available at https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html.

200 people, mostly families, had gathered to listen to classical music in the afternoon sun. After watching this scene at the birthplace of Ukrainian cinema for several minutes, I noticed a man making a movie of a more modern sort – standing with his back turned to the orchestra, he held an iPod in his hand, recording me on video as he passed by. A text message a few minutes later confirmed my suspicion that it was Dokukin. We spent the next hour walking in circles around the concert site with the classical music playing in the background, while Dokukin explained why he decided to form the Ukrainian Cyber Forces a year earlier, how they were structured, and his relationship with the government.

The 32-year-old Dokukin shared with me how he had used social media to start recruiting a group of (unpaid) volunteers angered by the Kremlin's aggressive actions. Over the previous months, their number had fluctuated from several dozens to a few hundred, and primarily included ordinary people without a technical background. They were based not only in Ukraine but also abroad – for example in Germany and the UK, highlighting the transnational character of many of these hacktivist groups.[5] Together, they carried out a series of activities, ranging from the unauthorized monitoring of CCTV cameras and troop movements in eastern Ukraine, to reporting separatist activities to Web companies such as PayPal in an effort to shut down the separatists' accounts, to launching distributed denial of service (DDoS) attacks against websites and leaking sensitive documents from the Russian Ministry of the Interior that revealed details about separatists in eastern Ukraine being paid by Russian authorities.[6]

Dokukin shared information about the group's actions with the media and the government, but there was no evidence that the government coordinated with or supported him financially or otherwise.[7] Dokukin told another interviewer that the Ukrainian Cyber Forces work independently, unlike Russian hackers with ties to the Russian FSB (the Russian Federal Security Service, the successor organization to the KGB).[8] The Ukrainian security services were certainly aware of the group's activities given Dokukin's media interviews.[9] And while the government could interfere and stop Dokukin's and the group's activities, it was turning a blind eye instead.

Why did I become interested in proxy actors in the first place? When I started working on this book in 2013, the debate over whether there could be a cyber war was in full swing.[10] But there was something puzzling: the debate was state-centric, while the media was full of reports about the significant role non-state actors play in this field, including private companies such as Gamma International and Vupen, hacktivist groups from Anonymous to the Syrian Electronic Army, and cyber criminals operating with impunity from different hotspots around the world.[11] These reports were telling a different story in the shadow of the debate about whether cyber war will or will not take place, a story in which non-state actors have become increasingly active in cyberspace. States are only one subset of a larger group of actors with significant offensive cyber capabilities.[12] In fact, the US Secret

Service agent Ari Baranoff stated in 2014 that "Many of the [non-state] actors that we look at on a daily and weekly basis have capabilities that actually exceed the capabilities of most nation-states."[13]

I became particularly interested in the capabilities of these actors and the dynamic relationship between them and the state in peacetime, in wartime, and in the increasingly blurry space in between. How have these new global coercive cyber capabilities become organized?[14] How do states use actors detached from the state to project power? And how do states that aspire to a monopoly over the legitimate use of force pursue these efforts in the context of offensive cyber operations? Looking back, my conversation with Dokukin was more than a bit surreal. Yet it was similar to other stories I experienced during the three-year research for this book, which took me to more than a dozen countries around the world, including China, South Korea, Mongolia, India, Israel, France, and the United States.

Between the origin of this book and its release, a lot has changed. The last twelve months alone have been full of noteworthy events that have raised greater awareness of this dynamic field generally and of proxies specifically. In March 2016, the US government unsealed two indictments against seven Iranian hackers and three members of the Syrian Electronic Army with details about their relationship to the Iranian and Syrian governments respectively.[15] A year later, another indictment shed light on the relationship between the FSB and hackers in Russia.[16] Meanwhile, in May 2016, US Cyber Command awarded a contract of USD 460 million to six private security companies that included assisting with offensive cyber operations.[17] In China, the government has been actively supporting cyber militias at universities and companies during the past several years.[18] A member of Russia's State Duma has openly acknowledged that the Nashi youth movement was mobilized to support the DDoS attack that flooded and crashed the websites of the Estonian government in 2007.[19] A hacker in a Colombian prison boasted in an interview with *Bloomberg Businessweek* that he had been hired by political campaigns in various Latin American countries,[20] and the hack of the Italy-based company Hacking Team shed light on a globalized market of cyber capabilities.[21]

These examples not only illustrate how states outsource certain functions to non-state agents but also shed light on the much murkier reality in which states cultivate loose relationships with actors that are not formally part of the state, yet work to its benefit. This is an under-appreciated phenomenon. To capture this reality and to compare states' behavior globally, the concept of proxy relationships is useful. I define *cyber proxies* as intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary. This broad definition covers the phenomenon of states committing to support specific proxies as well as states omitting to take certain actions and turning a blind eye to a non-state actor's malicious actions.[22] Most states will use a variety of proxies with differing relationships, so the focus of this book is rather on a state's broader *modus operandi* and the organization of proxy relationships generally.

I argue that projecting coercive power through cyberspace is not only a state-centric affair but often a dynamic interplay between the state and actors detached from the state. This raises important questions over control, authority, and the legitimacy of the use of cyber capabilities. For example, states use these proxies for a wide variety of purposes not limited to projecting power abroad; in both Russia and Iran, reports about government-supported hackers targeting dissidents predate reports about such proxies hitting targets abroad. Moreover, states' proxy relationships range across a spectrum: from delegation to orchestration and sanctioning. *Delegation* describes proxies held on a tight state leash and under the state's effective control. *Orchestration* applies to proxies on a looser leash with the state but usually sharing strong ideational bonds with the state and receiving funding or tools. And the concept of *sanctioning* (approving or permitting) builds on the concept of "passive support" developed by counterterrorism scholars to describe situations where a state is aware of the activity of a non-state actor but turns a blind eye towards it and indirectly benefits from its actions. Nevertheless, while countries pursue different models for proxy relationships and have different doctrines for the use of coercive cyber power, they also face a common challenge and have an interest in balancing the benefits of proxy relationships with the cost and increased risk of escalation.

What I learned in Ukraine was also remarkable for another reason. My questions focused on offensive cyber operations and their role in the conflict in Ukraine, namely those targeting critical infrastructure. Yet, in most interviews, the conversation would quickly turn away from these type of actions; interviewees seemed less concerned about the impact of cyber operations on the military outcome and much more concerned about the impact of information operations on the broader political outcome. In view of the Russian operation targeting the 2016 US presidential election, the Ukrainians were clearly ahead of their time. I left Ukraine with answers to some of my original research questions but also with new questions and an increasingly gnawing concern. What if the focus on the military dimension of offensive cyber operations and the long discussion about cyber war obscured other potential ways in which international stability can be and is being undermined through offensive cyber operations? Why focus on the use of offensive cyber operations during a military conflict if cyber capabilities can be used to help empower politicians that would make such an escalation less likely? This implies that the relevance of proxies lies not only in their ability to cause harm but also in their ability to wield power more broadly.

Some of my conversations with experts helped crystallize the multiple dimensions of cyber capabilities. In May 2016, a Google employee and I discussed the changing media landscape, how some governments actively plant false information, and what this means for companies like Google. When I mentioned my research and what I had learned about Dokukin and his volunteers, the Google employee's immediate reaction was that these were "the kind of grass roots actors that are needed to counter

government-sponsored information operations."[23] Through his lens, Dokukin was essentially an important guardian for the media and of the effort to present a verifiable truth in the face of intentionally spread false information and rumors. Others, including Dokukin himself, saw the Ukrainian cyber forces through more of a militaristic lens. It is reminiscent of the famous story of the group of blind men touching an elephant to understand what it is but each only touching a single part.

These different perspectives are an important reminder of how much terminology matters in this field. Activities funded through the US State Department's "Internet Freedom" program are labeled "cyber terrorism" by Iran's communications minister. What Russia and China view as information "threats" are considered content and a protected human right in many other countries. This explains why international cybersecurity negotiations are indirectly also a battle over human rights. Or, to use a historical analogy, whereas the negotiations for the landmark 1975 Helsinki Accords had a track focusing on security and one focusing on human rights,[24] today's cybersecurity negotiations essentially combine these two baskets, and some states are unwilling to separate them.[25] These different perspectives shape which actors are perceived as proxies and also pose conceptual challenges and special escalatory risks. Since, analytically, I strive to incorporate global perspectives, my discussion of proxies' activities and their political effects is broader in scope than that of other scholars[26] and not limited to proxy actors causing disruptive and destructive effects. At the same time, I reject some governments' implied moral equivalency that leads them, for example, to equate expressing public support for a peaceful protest in another country with using an aggressive influence operation against that state.

This book stands on the shoulders of giants in numerous different fields; the literature ranges from international relations to international law, communications studies, and the still-nascent cybersecurity scholarship spread across different academic disciplines. I also reviewed reports from nontraditional sources, including reports by cybersecurity companies and nonprofit organizations such as the Citizen Lab. Corporate reports come with obvious additional risks regarding quality, bias, and verifiability. Their inclusion therefore depended on technical details, considerations of possible alternative explanations, and vetting by other experts. Some new data is included based on qualitative, semi-structured expert interviews. Given significant data limitations, I rely on historical narrative and an illustrative case study approach. In my view, there is simply not enough data publicly available to date to allow for robust, comparative quantitative analyses testing hypotheses across countries. The phenomenon of cyber proxies is still relatively new, usually hidden behind a shroud of secrecy, and information is often shared only off the record. I therefore focus on developing a framework for analyzing cyber proxies that will inform future empirical research and allow for the study of changes over time. When analyses of the same incident contradict each other, as in the case of the Georgian-Russian war in 2008, I present what I consider to be the most accurate account based on my analysis of the literature and interviews. In light of the pace at which this field

is changing and new literature published, it is also worth mentioning that I only include publications available as of November 2016, when the manuscript was submitted for review (with the exception, in light of their importance, of the indictment of the Russian nationals by the US government and the information about Guccifer 2.0 that became available between the submission and publication).

I hope this book will reach several audiences. There is a growing demand from academia, with a proliferating number of courses, and even degree programs, now dedicated to the Internet and cybersecurity. There also remains a significant gap in the international relations context between traditional concepts and the study of cyberspace. Professors and students alike will ideally find this publication a useful contribution to their scholarship, syllabi, and thinking. Working at the Carnegie Endowment for International Peace, a global think tank dedicated to informing policy through quality research, I also hope that policymakers will find value in the analysis presented here. The proposed frameworks present tools that may help them think through and structure the world of cyber proxies, its implications, and how to manage it. Last but not least, cybersecurity is no longer an obscure topic that requires alarmist books to raise attention. By Christmas 2014, the geopolitics of cybersecurity had entered people's living rooms when the US president went in front of television cameras to accuse North Korea of hacking Sony and to reassure the American people that there were no secret North Korean sleeper cells waiting to attack moviegoers. So, this book is also written for a general audience that does not follow cybersecurity news on a daily basis but is generally curious.

The first part of this book focuses on the main argument that it is important to focus on proxies as well as states and that proxies are capable of causing significant harm. Chapter 1 explores cyber proxies' power and what their capabilities are likely used for, as well as the implications of the attribution problem, the challenge of attributing a malicious cyber action to its source. The second chapter outlines the analytical frameworks helpful in the study of cyber proxies, including a review of the various manifestations of proxy relationships throughout history, ranging from privateers to Italy's condottieri, satellite states, militias, and spies for hire. It also draws on insights from organizational and institutional theory to discuss the underlying conditions that allow proxy relationships to exist in the first place. Chapter 3 provides an overview of the geopolitics of cyber power and the different perspectives of Russia, China, Iran, and the United States. These countries are also the focus of case studies in the second part of the book (Chapters 4–7), which describe in detail the different types of proxy relationships. This part underscores the second main argument of the book that how states use cyber proxies is not very different from how states have used conventional proxies. What is new, and is the third main take-away from this book, is the diffusion of reach, which allows state and non-state actors to cause effects remotely across vast distances through offensive cyber operations.

The implications of cyber proxies and how to effectively manage them is the focus of the third and final part of the book. Chapter 8 reviews the utility of international

law and its nuanced distinctions for taking action against malicious activity by a cyber proxy. Chapter 9 discusses the different approaches for managing proxies held on a tighter leash as well as those on a loose leash. This is of interest not only for academic scholarship but also for practitioners and policymakers. Recent arrests of members of the hacktivist group Anonymous in the United States and Europe, as well as China's arrests of hackers as part of the government's overall anti-corruption campaign,[27] illustrate efforts to punish those whose malicious activity is not considered legitimate in the eyes of the state. The US government's recent unsealing of indictments represents another attempt to create a deterrent effect by exposing and shaming foreign nations who keep proxies on a looser leash. Finally, Chapter 10 summarizes the findings and conclusions and outlines some suggestions for future research.

Acknowledgments

Writing a book takes a long time, sometimes longer than the author's time with a single institution. I am therefore particularly grateful to the Carnegie Endowment for International Peace, which I joined in the autumn of 2015, for giving me the time to finish writing it. I still remember the first conversation with my new colleague, Ariel "Eli" Levite, over breakfast and his comment about studying cyberspace not for the sake of studying cyberspace but for what cyberspace can tell us about the changing world writ large, a perspective that's particularly influenced my writing in the final stages of this book. I thank George Perkovich for his support in words and in action that was crucial to get me across the finish line and for inspiring me along the way. A particular gem I have come to treasure at the Carnegie Endowment is its in-house library and its staff, who were tremendously helpful and whose research assistance I have greatly appreciated.

This book would not exist without Peter Bergen, Vice President at New America and Director of its International Security Program. It was his early encouragement at the beginning of 2013 that led me to embark on this adventure. Thank you. I also owe gratitude to New America and its inspiring leader Anne-Marie Slaughter for providing an environment for my project to succeed. I thank Peter Singer for his active support and open door as well as Ian Wallace and Robert Morgus for their team spirit and my former colleagues at New America's Open Technology Institute. John Berger at Cambridge University Press also deserves a special acknowledgment for his belief in this project from the start.

Professor Robert Axelrod and Professor John Ciorciari at the University of Michigan's Gerald R. Ford School of Public Policy provided me with a second home that became a most welcome escape and refuge from the constant buzz and meetings in Washington, DC, especially during the summer of 2016 as I was finishing this book. The regular luncheons with Bob often had me scurrying for a pen or my phone to note down a historical precedent or analogy he mentioned in the midst of a conversation about the latest cyber incident of the day. I am grateful to both for the physical second home and the intellectual community they have provided,

which extends to people like Professor Alex Halderman at the University of Michigan's computer science department and its impressive group of PhD students, including Nadiya Kostyuk, Benjamin VanderSloot, and Drew Springall.

I am also indebted intellectually and grateful personally for the mentorship and friendship of a number of people who were sharing their thoughts and advice with me even before this book project started. Professor Joseph Nye, Jr, offered thoughtful feedback on my writings when I first started to focus on this field back in 2010. Professor Martha Finnemore and Professor Duncan Hollis have become particularly important sounding boards growing out of the MIT/Harvard cyber norms community during the past few years. I am particularly indebted to Thorsten Benner, Director of the Global Public Policy Institute, for reasons too numerous to recount here. They all have taken time out of their busy schedules above and beyond what could be expected, and have offered feedback, advice, and criticisms throughout several projects during the past years, including this book.

My thanks also go to Jason Healey at Columbia University's School for International and Public Affairs and the group of scholars that convened for a workshop focusing on proxy actors and cybersecurity in July 2016, who provided me with an opportunity to present my work. Professor Nicholas Tsagourias and Dr. Russell Buchan at the University of Sheffield have my gratitude for inviting me to present at their conference in the autumn of 2015, and for publishing my first article on this subject in Oxford's *Journal for Conflict and Security Law*, alongside a series of articles by international law experts discussing the question of state and individual criminal responsibility and non-state actors in the context of cyberspace. I would also like to thank Kenneth Geers. Not only did he include my short article based on my two research trips to Kiev in his edited volume on cyber operations during the conflict in Ukraine, but he also made the trips so much more enjoyable by sharing his knowledge of the local culture and history.

While I deserve the blame for all errors and inaccuracies in this book, its particularly well written and interesting parts exist thanks to those who reviewed the manuscript and shared their invaluable feedback. These include Martha Finnemore, Duncan Hollis, and Joseph Nye, as well as Matthew Noyes, Max Smeets, Matan Chorev, and George Perkovich. They were all incredibly generous with their time and responses. In addition, I am thankful to Beau Woods, Collin Anderson, Adam Segal, and Nigel Inkster for reviewing specific sections focusing on the capabilities of non-state actors, Iran and China respectively. I owe a particular debt to Isabella Furth and Jonathan Diamond for their assistance with the final manuscript. Finally, I would like to thank the two anonymous reviewers who provided very helpful comments.

Most importantly, I am indebted to the many people who were willing to speak with me as part of the research for this book. During the past three years, I had the privilege of speaking with over four dozen experts from more than a dozen countries on three continents who shared their thoughts, experience, and expertise. Many are

referenced in the book by name, others preferred their contributions to be anonymous, and others asked me not to mention them at all. They include white-hat and black-hat hackers as well as former and current officials in the law enforcement and intelligence communities. The list ranges from experts in the private sector, academia, think tanks, and government, as well as computer emergency response teams, security research communities, and journalists. They are what makes this book unique. They helped me separate the wheat from the chaff in the existing literature and often provided additional details and information for this comprehensive account of proxies and cyberspace. Thanks to people like them, publications like this are possible, even on topics that are rather difficult to research.

Last but not least, I would like to thank Eli Sugarman and the William and Flora Hewlett Foundation for having made my research possible. The foundation's Cyber Initiative has become an important source enabling scholars in the United States and abroad to pursue their activities, and the foundation's commitment to general operating support stands out in an increasingly challenging funding environment. Many of the people I have met and interviewed for this book have not remained one-time contacts but have become part of a growing global network of cybersecurity scholars. Additional thanks go to the hosts of the various conferences where I have been invited to speak and participate during the past few years, which often enabled me to add a few more days in the respective country to interview local experts for my book.

Special thanks are reserved for my family and friends who made all of this possible with their support, patience, and understanding. You know who you are and how deeply grateful I am.

Abbreviations

APT	advanced persistent threat
ASEAN	Association of Southeast Asian Nations
CEO	chief executive officer (of a corporation)
CERT	computer emergency response team
CIA	Central Intelligence Agency of the United States
DARPA	Defense Advanced Research Projects Agency (of the United States)
DDoS	distributed denial of service
DoD	Department of Defense (US)
FBI	Federal Bureau of Investigation (of the United States)
FSB	Federal Security Service (of the Russian Federation)
G20	Group of Twenty
G7	Group of Seven
GCHQ	Government Communications Headquarters (of the UK)
GRU	General Staff Main Intelligence Directorate (of the Russian Federation)
ICBM	intercontinental ballistic missile
ICT	information and communications technology
IRA	Irish Republican Army
ISP	Internet service provider
IT	information technology
KGB	Committee for State Security (of the Soviet Union)
MIT	Massachusetts Institute of Technology
NATO	North Atlantic Treaty Organization
NCPH	Network Crack Program Hacker
NGO	non-governmental organization
NSA	National Security Agency (of the United States)
NTRO	National Technical Research Organization (of India)
PLA	People's Liberation Army (of China)
PMC	private military companies
PSC	private security companies
PSMC	private security and military companies

SBU	Security Service of Ukraine
SCADA	supervisory control and data acquisition
SORM	System for Operative Investigative Activities (in Russia)
UN	United Nations
UNGGE	United Nations Group of Governmental Experts
US	United States of America
USD	United States dollars