SSI
STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH~WISDOM

CYBERSPACE: MALEVOLENT ACTORS, CRIMINAL OPPORTUNITIES, AND STRATEGIC COMPETITION

Phil Williams
Dighton Fiddner
Editors

The emergence and evolution of cyberspace have contributed to globalization, the creation of a new global commons, the rapid spread of knowledge and ideas, the development of global markets for local products, and the empowerment of individuals and small groups. Yet, cyberspace also creates new opportunities for criminality, provides new avenues for terrorist recruitment, and adds a new playing field upon which geopolitical rivalry among great and not-so-great powers plays itself out. The dependence of societies on cyberspace also creates new vulnerabilities. At the same time that cyberspace has brought new potential and promise, it has also become a domain in which malevolent actors pursue selfish interests, spy, steal, extort, bully, and stalk.

What makes this development all the more problematic is that cyberspace is constantly evolving. Accordingly, this book has three parts: the first focuses on cyberspace itself; the second on some of the major forms of malevolence or threats that have become one of cyberspace's defining characteristics; and the third on possible responses to these threats. Each section focuses on conceptual and analytic issues as well as the implications for policy and strategy.

Dighton Fiddner describes the nature and structure of cyberspace and teases out some of the ramifications for security. Fiddner also argues that cyberspace is first and foremost a strategic domain—a sphere of activity, concern, or function—similar in some respects to the traditional land, air, sea, and space domains. If cyberspace is a fifth, separate, and independent strategic domain, however, it is structured and operates differently than the other four traditional domains. Moreover, cyberspace superposes the other four strategic domains and, as such, can have a direct causal and catalytic effect on activity that occurs within them.

The novelty of cyberspace is also highlighted by Nazli Choucri, who identifies seven disconnects between traditional and familiar conditions and current realities. As a result, old ways of visualizing the pursuit of political and/or economic power have been rendered passé, if not obsolete, by diffuse, decentralized, diverse, and different types of interactions. One of the difficulties recognized by Choucri, but more fully elucidated by Rick Hutley in Chapter 4, is that cyberspace itself is constantly morphing and expanding as a result of a continuing exponential explosion of technological innovation that has brought both immense benefits and new threats. A cohesive, holistic architecture that addresses security as a foundational design element is essential to respond to these threats.

Cyberspace, as Jeff Boleng and Colin Clarke discuss in Chapter 5, has also created a "new 'Net" in urban areas in the developing world. The new 'Net has emerged in large part through the proliferation of feature phones (rather than smartphones), a trend that has contributed to the creation of a new type of information environment. Information generated and consumed on these mobile devices is largely composed of multilingual text jargon, voice, images, and videos, especially 6-second vines. The creation and sharing of information in this new environment is staggering. It is also disconcerting, not only because of the likelihood of failing cities but also because U.S. military forces might have to engage in contingen-

cies in a range of unstable and chaotic urban environments, where the information environment adds further complexity.

The threats that arise in cyberspace are the subject of Part II of this book. Not all threats are equal, however. In Chapter 6, Michael Kenney concludes that the threat of cyberterrorism is greatly exaggerated. The most immediate online threat from terrorists lies in their ability to exploit the Internet to raise funds, research targets, and recruit supporters, rather than engage in cyberterrorism. The skill with which the Islamic State has used Twitter to spread its message, to mobilize support, and to flaunt its victories underlines the arguments presented in Kenney's chapter. As he notes, cyberterrorism might well occur in the future, but at present, online crime, hacktivism, and cyberwarfare are more pressing virtual dangers.

Timothy Thomas, in Chapter 7, "China's Reconnaissance and System Sabotage Activities: Supporting Information Deterrence," examines how and why the Chinese so aggressively probe and enter global networks. His chapter goes beyond simply describing the cyberactivities that China employs to gain an advantage in economics, business, military competition, and political bargaining, to elucidating the Chinese use of cyberactivities for truly strategic purposes, including the use of what Thomas terms "strategic digital reconnaissance." The chapter provides an important guide to China's thinking on cyberconflict.

In Chapter 8, Stephen Blank argues that Russia also views actions and policies in cyberspace as part of a more comprehensive strategy. This strategy consists of cyberwar, economic sanctions, domestic and international public information campaigns, the manipulation of youth organizations or criminal gangs, and the penetration of key sectors of the economy and subversion of politicians. These strategies become a surrogate for large-scale military capabilities that are unavailable or simply not usable. The Russian experience in both Estonia and Georgia indicates that Moscow operationalized strategic information war to achieve victory by paralyzing a target country's social infrastructure networks, i.e., its central nervous system.

In addition to threats in cyberspace that emanate from geopolitical competition and the pursuit of power and security in the fifth domain, there are other forms of malevolence linked to the profit motive. Cybercrime has become pervasive, simultaneously exploiting, challenging, and eroding the use of cyberspace for commerce and business. In Chapter 9, Shawn Hoard, Jeffrey Carasiti, and Edward Masten consider how cyberspace has not only facilitated new ways of carrying out old crimes, but also has created criminal opportunities, including new methods of money laundering. The chapter contains a series of highly illuminating case studies that provide strong support for the notion that cybercrime has become a major threat in its own right.

A less obvious set of threats targets the nongovermental-organization community and humanitarian initiatives in crises and conflicts. As Ronald Deibert and John Scott-Railton point out in Chapter 10, social media have penetrated armed conflict just as they have penetrated most others aspects of life. Humanitarian groups, aid organizations, and conflict-prevention and peace-building bodies use crowd-sourced maps to anticipate, predict, and respond to crises and organized violence. Yet, there is a growing risk to digital humanitarianism, as armed groups also become adept at exploiting digital technologies. As the chapter emphasizes, those who exploit cyberspace for humanitarian reasons can also be threatened by cyberspace.

Isaac Porche discusses the same theme in Chapter 11. His emphasis that automobiles have a cybersecurity risk is both compelling and disturbing. The vulnerabilities of automobiles stem from the abundance of software, computers, and networks that can be used to disable a vehicle or to override the commands of the driver, with potentially disastrous consequences. Using some very plausible scenarios, Porche highlights the extent of the risks involved not only in the automobiles themselves but also in the transportation infrastructure (traffic lights, for example), which is also susceptible to both degradation and manipulation.

Having examined the challenges and threats in cyberspace, this book considers a variety of responses, with the authors suggesting that some of the most favored options being pursued by the United States are poorly conceived and ultimately inadequate and ill-suited to the tasks at hand. In Chapter 12, "Reflections on Cyberspace," Martin Libicki considers the possibility of cyberdeterrence as a major option for the United States and concludes that, for several reasons, it is still not an effective option.

In Chapter 13, Davis Bobrow comes to a similar conclusion, albeit by a very different route. In Bobrow's view, much of U.S. cyberpolicy has been driven by the experience of Pearl Harbor and subsequently the development of nuclear strategy. Bobrow challenges the wisdom of these dominant frames and emphasizes the dissimilarity between nuclear weapons and cybertechnologies. Rather like Bobrow, in Chapter 14, Rob van Kranenburg postulates that the existing models of thinking about cybersecurity are

not necessarily the most appropriate or useful. Emphasizing the emerging Internet of Things, he advocates constructing a "new conceptual space," with new notions of privacy, security, assets, risks, and threats. In Chapter 15, Benoît Morel offers another critique of existing approaches to cyberspace. He also examines whether the United States should seek cyber-arms-control agreements at either a bilateral or multilateral level. His answer is a clear no. In Morel's view, there needs to be a real change in culture so that cybersecurity is integral.

Instead of focusing on government responses to malevolence in cyberspace, Kelsey Ida, in Chapter 16, suggests there might be bottom-up emergent responses, particularly to transnational organized crime. She argues that bottom-up regulation by "digilantes" is not far-fetched, and that we have already seen some evidence of this. The prevalence of cybercrime also provides the background against which Timothy Shimeall, in Chapter 17, considers how to distinguish between different kinds of attacks in cyberspace and the ways certain groups might move from crime to war. In addition to providing considerable technical details about the shifts, Shimeall also begins the process of identifying those attacks that constitute acts of cyberwar.

These acts are the starting point for Phil Williams's discussion of crisis management in Chapter 18. Williams first distinguishes between crises that begin in cyberspace with a major cyberattack and those that are precipitated by events in the real world but are played out in cyberspace as an additional and important strategic domain. He then elucidates some of the dangers and provides a set of recommendations to enhance the capacity for crisis management, both in cyberspace and in a cybered world. The notion of a "cybered" crisis is an extension of the idea of cybered warfare developed in Chapter 19 by Chris Demchak, who argues that contemporary conflict is now "cybered conflict." Yet, the response to this and the shape of the emerging "'Cyber-Westphalia' interstate system" remains uncertain. Nevertheless, Demchak identifies three major possibilities: (1) fractious states with varying degrees of cyberpower; (2) a system dominated by the rise of an illiberal superpower; and (3) a system of technologically integrated regional alliances of like-minded, like-structured, or like-threatened nations. Which of these scenarios becomes dominant will do much to determine the future of malevolence in cyberspace. Some of the same underlying themes are evident in Dighton Fiddner's concluding Chapter 20. Fiddner looks at the complex interrelationship between the physical sphere and cyberspace and how different forms and levels of governance and security operate at the individual, state, and global levels. He also emphasizes that cybersecurity is not a technical issue but one that involves fundamental policy, strategy, great-power relations, global commerce and financial stability, and personal privacy and the safety of personal information. He concludes by noting that, since cyberspace is an emergent phenomenon that is constantly changing, approaches to cybersecurity need to be equally dynamic and adaptable and, therefore, have to be both bottom-up and top-down.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *www.StrategicStudiesInstitute.army.mil.*

*****

This Publication

SSI Website

USAWC Website