GEORGETOWN UNIVERSITY PRESS

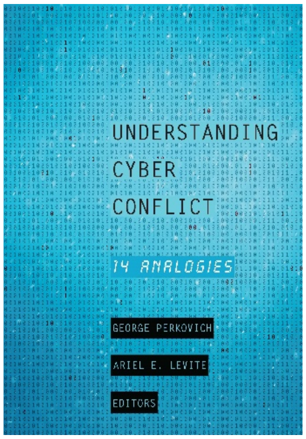
Introduction

George Perkovich and Ariel E. Levite

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



UNDERSTANDING
CYBER
CONFLICT

14 ANALOGIES

GEORGE PERKOVICH
ARIEL E. LEVITE
EDITORS

Introduction

GEORGE PERKOVICH AND ARIEL E. LEVITE

In extensive conversations with senior civilian and military cyber policymakers in the United States, the United Kingdom, France, Canada, Israel, Russia, and China, the editors of this volume heard repeatedly that these individuals and their counterparts in government frequently invoke historical analogies—aptly and inaptly—as they struggle to manage new technologies. The cyber domain is new to most senior officials. Cyber capabilities have unique properties. Experience with them in conflict thus far has been limited. Consequently, it is difficult to make confident judgments about their effects and escalatory potential. Moreover, the range of adversaries and behaviors that policymakers and experts must strive to dissuade, deter, or defeat in and through cyberspace is unprecedented: massive-scale thievery, political subversion, terrorism, covert operations, and open warfare. In such circumstances the human mind naturally pulls up analogies from the past to guide thinking and acting amid the new.

One of our interlocutors, in early 2014, recommended that we read *Cyber Analogies*, a collection of essays edited by Emily O. Goldman of US Cyber Command and John Arquilla of the US Naval Postgraduate School.[1] We took this advice and found that, indeed, those essays sharpened our thinking about differences and similarities between cyber and previous military technologies and episodes. Goldman and Arquilla encouraged us to extend the exploration of analogies, with an eye toward adding examples and perspectives that would be pertinent to readers beyond the United States. The result is the present volume, which includes four revised essays from their collection, plus ten chapters that we commissioned to explore additional analogies.

Human beings think, learn, and communicate through analogies. We use analogies—naturally, often without trying—to familiarize that which is new. As Richard E. Neustadt and Ernest R. May recorded in their classic study, *Thinking in Time*, policymakers and pundits regularly invoke analogies as they struggle to make sense of and affect new situations, often without adequate reflection.[2] This practice occurs now regarding the cyber world, which is evolving with an ever-quickening pace. For people who were born in this era, the benefits and risks that flow from the enhancement and distribution of information and communications technologies are more familiar than the earlier technologies, episodes, and policy challenges to which elders analogize. Young readers may know how hacktivists operate and how cyber attacks brought Estonia to a standstill in 2007, but they may be less familiar with the eighteenth- and nineteenth-century privateering at sea that resembles the challenges posed by proxy actors in cyberspace. Cybersecurity professionals may be convinced that the speed of offensive attacks will require automated defensive responses, but they may be unaware of how governments wrestled internally over the pre-delegation of authority to launch nuclear weapons under attack. Curricula today in courses on history, political science, international relations theory, and security studies still derive from pre–cyber era experiences; relatively few explore whether and how the cyber era may be similar or different. So, too, the strategies, policies, and institutions that governments use to manage dual-use technologies today generally predate the World Wide Web. Therefore, analogies across eras can be instructive for the young as well as for the not-so-young.

Variations in culture, ideology, and circumstances affect how audiences perceive and understand analogies. The authors of this volume are American, British, Israeli, and Swiss. The analogies to which they compare cyber technology and the challenges arising from it tend to be especially meaningful in their countries and, probably, in the West more broadly. We have tried throughout to keep the aperture wide enough to invite readers with different backgrounds to consider whether observations and analyses offered here do or do not apply more broadly. Moreover, readers from other locales and perspectives may gain insight from considering how these well-informed Western authors think about the given topic even if it differs from their perspective. In any case, the Cyber Policy Initiative of the Carnegie Endowment for International Peace hopes subsequently to build on the present volume and invite authors from other countries and perspectives to write about analogies that may be especially important to them.

Learning from analogies requires great care. Analogies can mislead as well as inform. Indeed, their educational value stems in no small part from identifying where, when, and how an analogy does not work well. Differences between technologies, effects, and historical, political, and strategic circumstances are as important to understand as similarities are. For example, today one must take particular care in analyzing which attributes of the nuclear era carry forward into the cyber era and which do not, and what the implications of confusion on this score could be.

Stanley Spangler, a professor of national security affairs at the US Naval War College, noted in 1991 that "virtually every postwar American president has been influenced by parallels drawn from the 1930s when Great Britain and France failed to react soon enough and strongly enough to halt [Adolf] Hitler."[3] President Lyndon Johnson, for example, declared, "Surrender in Vietnam [would not] bring peace, because we learned from Hitler at Munich that success only feeds the appetite of aggression."[4] Ironically, in ensuing decades the Vietnam War itself became a frequently used analogy in American debates over military intervention in other distant lands. In the 2015 debate over the Joint Comprehensive Plan of Action, which was negotiated to resolve the crisis over Iran's nuclear program, critics made countless references to the Munich Pact of 1938 and Neville Chamberlain, while proponents invoked the need to avoid repeating the 2003 war in Iraq. The Iran debate of 2015, like the Vietnam debate, demonstrated the risk that analogies can be a flawed substitute for actual knowledge of the past and the present and for critical thinking about both. Nevertheless, people ineluctably employ analogies to conceptualize and manage new circumstances. Thus, it is necessary and salutary to examine analogies carefully and to search for what is apt and inapt in them.

We have organized the essays (and analogies) in this volume into three groups. The first section, "What Are Cyber Weapons Like?," examines the characteristics of cyber capabilities and how their use for intelligence gathering, signaling, and precision strikes compares with pertinent earlier technologies for such missions. The second section, "What Might Cyber Wars Be Like?," explores how insights from episodes of political warfare, preventive force, and all-out war since the early nineteenth century could apply or not apply to cyber conflict in the twenty-first century. The final section, "What Are Preventing and Managing Cyber Conflict Like?," suggests what insights that states seeking to civilize cyberspace might draw from earlier experiences in managing threatening actors and technologies. We introduce the essays here accordingly.

What Are Cyber Weapons Like?

The cyber domain—and its associated hardware, software, and human resources issues—is constantly growing and evolving. Information and communications technologies can serve manifold peaceful and coercive purposes in addition to providing legal and illegal means of generating wealth. In the context of interstate conflict alone, hundreds of analogies could be drawn and analyzed between cyber weapons and their predecessors. Capabilities and plans exist and are being developed further to use cyber assets in large-scale, combined-arms military campaigns. Cyber operations could be conducted to cause massive disruption and, indirectly, significant human casualties. A literature is already emerging on these larger-scale capabilities and scenarios.[5] Essays in the second and third sections of this volume explore whether and how technologies and practices central to World Wars I and II and the management of nuclear deterrence offer insights to the conduct and prevention of cyber warfare.

Here, in this first section, we focus on analogues to less destructive capabilities. In an era when all-out warfare among major powers may be deterred by nuclear weapons, among other factors, and global dependence on networked information and telecommunications technologies creates unprecedented vulnerabilities, the instruments of stealth, speed, and precision that can be controlled from great distances will be particularly salient as states compete to influence each other in the coming years. These applications pertain to intelligence gathering, covert operations, "political warfare," and relatively low-intensity, precise offensive actions. Such activities are especially germane to operations in the gray zone between declared war and peace, when large numbers of boots on the ground are not envisioned but exercising covert influence and coercive power is deemed expedient or necessary.

"What we call cyber is intelligence in an important sense," Michael Warner writes in the first chapter. "Intelligence activities and cyberspace operations can look quite similar." Warner, the US Cyber Command's historian, describes how cyber capabilities have been applied rather straightforwardly to serve the functions of spying and counter-spying that human agents have performed for millennia. "The main difference," he notes, "is the scale that can be exploited" by cyber techniques. Similarly, the use of cyber capabilities to conduct covert operations and to inform the planning and conduct of military operations builds on methods developed through the advent of the telegraph and radio in the nineteenth and twentieth centuries. The similarities here extend to the importance of cryptography and counter-cryptography to facilitate offensive and defensive missions. A key difference in the cyber era is that previously "the devices that secured and transmitted information did not also store it." Today, however, past, current, and future data are vulnerable to spies and eavesdroppers in unprecedented ways. This raises several questions that Warner examines: Will cyber espionage be more likely to cause conflict than traditional spying has done? What can responsible states do to gain the benefits of more fulsome intelligence collection while minimizing the risks to international stability and their own reputations, as well as to the brand value of companies whose products they exploit?

"No one has ever been killed by a cyber capability," write Lt. Gen. Robert Schmidle, Michael Sulmeyer, and Ben Buchanan in their chapter, "Nonlethal Weapons and Cyber Capabilities." Schmidle, the deputy commander of US Cyber Command from 2010 to 2012, and Sulmeyer, formerly the director for plans and operations for cyber policy at the Office of the Secretary of Defense, have been deeply involved in US military cyber policymaking. Buchanan is a postdoctoral fellow at the Cyber Security Project in Harvard University's Belfer Center for Science and International Affairs. Their chapter analogizes cyber capabilities to nonlethal weapons that the United States and other states have developed for decades. The Department of Defense defines *nonlethal weapons*—such as pepper spray, spike strips to puncture tires of vehicles, rubber bullets, flash bangs, electronic jamming devices, and lasers—as "weapons, devices, and munitions that are explicitly designed and primarily employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the target area of environment."[6] In a first-of-its-kind analysis, the authors compare and contrast potential utilities of nonlethal weapons and cyber capabilities in four ways: their ability to incapacitate, the reduced collateral damage they inflict, the reversibility of their effects, and their ability to deter. Schmidle, Sulmeyer, and Buchanan also address an interesting paradox: Why have US defense officials been particularly reluctant to approve the use of nonlethal capabilities, and can this reluctance be expected to continue, in the United States and in other states?

Moving up the ladder of coercive power, James M. Acton, a physicist and the codirector of the Nuclear Policy Program at the Carnegie Endowment for International Peace, explores the analogy between precision-guided munitions (PGMs) and cyber weapons. The development of PGMs—"guided gravity bombs and cruise missiles, in particular—has had profound implications for warfare," Acton begins. "Such weapons tend to cause much less collateral damage than their unguided predecessors do, and because they can remain effective when used from a distance, they can also reduce casualties sustained by the attacker. Thus, PGMs have altered national-level decision-making by lowering the political threshold for the use of force and by slowing the likely loss of public support during a sustained military campaign."

Cyber weapons may extend the militarily, politically, and morally attractive logic and functionality of PGMs. Cyber weapons offer the potential of "exquisite precision" in terms of targets and effects, although this potential may be very difficult for many actors to achieve in practice. They involve "minimal risk to the lives of the service personnel who 'deliver' them" and are "likely to cause fewer civilian casualties than even the most carefully designed and executed kinetic attack." As a result of these attributes, cyber weapons "could further lower the threshold for the use of force." At the same time, the effective use of cyber weapons requires sophisticated intelligence, surveillance and reconnaissance, and time-sensitive battle damage assessment. As with PGMs, it also remains questionable whether cyber weapons can accomplish larger, strategic political-military objectives. From all this the fundamental question arises of whether cyber weapons will augment deterrence of military conflict or make conflict more likely.

Drones, or unmanned aircraft used to surveil and precisely strike targets on the ground, have been celebrated and reviled since their use by the United States became an open secret in the mid-2000s. Armed drones are a form of PGM. What has made them more controversial, and perhaps more analogous to cyber weapons, are both the secrecy that for a long time shrouded the decision-making surrounding their use and the perception that their operators' immunity from physical harm lowers inhibitions on their use. David E. Sanger, the *New York Times*' chief Washington correspondent and author of *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, explores this analogy.

Sanger begins by recounting how outgoing-president George W. Bush told President-elect Barack Obama "there were two programs he would be foolish to abandon"—the drone program and a super-secret program called Operation Olympic Games, which was designing an offensive cyber operation to disable centrifuges in Iran's nuclear enrichment facility at Natanz. In the years that followed, Obama famously (or infamously to some) intensified the use of attack drones and authorized what became known as the Stuxnet attack on Iran. As Donald Trump stamps his imprint on US policy, he will need to grapple with the moral, legal, and strategic issues that these two types of weapons raise. What targets in what locations and under what circumstances are legitimate not only for the United States but for others too? What degree of confidence can realistically be attained that effects of cyber attacks (and drone strikes) will be limited to legitimate targets and will not cause unintended harm, or “collateral damage”? Many observers argue that drone strikes have incited escalatory revenge. Can cyber capabilities enhance deterrence of terrorism and other forms of aggression without this counterproductive effect? Sanger unpacks these issues by comparing and contrasting the nature and effects of drone and cyber attacks, and by drawing on the experience with drones, he considers how secrecy regarding cyber techniques and operations may affect prospects of governing them nationally and internationally.

What Might Cyber Conflicts Be Like?

The present conflicts in Ukraine, the Islamic State of Iraq and Syria operating in both states, and the cyber-abetted interference in the 2016 US presidential campaign may characterize prevalent challenges to peace and security in the twenty-first century, at least in cyberspace. At the same time, of course, the recent escalation in tensions between Russia and the West, and between China and its US-backed neighbors in East Asia, underscores the enduring importance of historical major power conflicts in continuing to shape perceptions and political discourse in the East and the West. Thus, the chapters in this section explore analogies from a wide span of history to draw implications for a range of confrontations and conflict contingencies that cyber-capable states may face and in which cyber operations may play a role.

In his chapter, Stephen Blank, of the American Foreign Policy Council, describes how Russia’s contemporary use of offensive cyber operations against Estonia (2007), Georgia (2008), and Ukraine (2014–15) is not merely analogous but also a direct continuance of the strategy and practice of Soviet subversion of neighboring states. He writes, “Tactics and strategies developed and employed during the Soviet period have served as a foundation for establishing new strategies that incorporate some of the century-old Leninist repertoire and new trends like IW [information warfare], as defined by Moscow, for the conduct of continuous political warfare against hostile targets.”

In describing the conduct of IW and cyber attacks in Estonia, Georgia, and Ukraine, Blank reports that Russia’s aim was to “instill a feeling of constant political and economic insecurity among the target state’s population” while testing whether and how European security institutions and the United States would respond. In Georgia and Ukraine, attackers believed to be linked to the Russian state penetrated and placed malware in electricity supply systems. When the Georgian conflict ended early, without Western intervention, no decision to execute destructive cyber attacks was made. In Ukraine, nationalists sabotaged electricity supply lines to (Russia-annexed) Crimea in November 2015 and cut off power there. Russian retaliation, prepared well in advance, was executed four weeks later in the form of a sophisticated, measured cyber attack that shut down three regional electric power distribution companies. Thus, as Blank details, cyber capabilities provide Russian actors with a spectrum of relatively inexpensive and risk-mitigating coercive instruments to impose Russian interests on adversaries below the threshold of violence that would prompt military escalation, especially by Western powers. "Russia has already engaged its adversaries in information warfare," Blank concludes, "thus, its adversaries must understand and learn from it for their own security."

Moving up the ladder of force, many assessments posit that offensive cyber operations would optimally be undertaken secretly, before armed warfare has commenced, to impair an opponent's capacity to fight or to create facts on the ground that could motivate an opponent to stand down. In "An Ounce of (Virtual) Prevention?," John Arquilla, the chair of defense analysis at the US Naval Postgraduate School, considers how the use of preventive force in the Napoleonic Wars and leading up to World War I may hold insights for the cyber era. Arquilla describes how the British navy in 1801 and 1807 conducted attacks on the Danish fleet, the coastal artillery emplacements, and the city of Copenhagen to prevent Denmark from colluding with Napoleon in closing the Baltic Sea to British trade. While the British attacks accomplished their tactical and strategic objectives, the exercise of preventive force also motivated Germany in the late nineteenth and early twentieth centuries to build up its navy to deny Britain the option of preventive force. Fast forwarding a hundred years, Arquilla analogizes that the Stuxnet cyber attack conducted by the United States and Israel against Iran's centrifuge program not only successfully slowed Iran's acquisition of enriched uranium but also may have spurred Iran and future potential nuclear proliferators to take defensive measures that will make counter-proliferation more difficult in the future. Ultimately, Arquilla concludes, twenty-first-century states are likely to see cyber techniques and operations as useful for preventive force—including against terrorist groups—and will therefore compete offensively and defensively in this type of conflict.

Francis J. Gavin, an international historian and director of the Henry A. Kissinger Center for Global Affairs at the School of Advanced International Studies at Johns Hopkins University, addresses the issue of war instigation from a different angle, assessing whether and how the technology of railroads drove Germany, France, the United Kingdom, and Russia into World War I. Early historiography on the war posited that the European great powers' reliance on railways to transport military forces to their borders placed a premium on deploying their forces before their adversaries did. Ambiguities about the purpose of mobilization—either offensive or defensive—exacerbated crisis dynamics. Moreover, the logistics of railway mobilization made it difficult to pause or reverse once it started. Consequently, according to early historiography, once mobilization began, it acquired too much momentum to be stopped in the amount of time that the complicated diplomacy to prevent war would have required.

Modern historians have corrected the overly simplistic determinism of the railway narrative, yet, as Gavin notes, this work has not prevented the notion of technological determinism from influencing conceptions of cyber warfare. Nor should it necessarily. Indeed, the military implications of major, globally infused dual-use technologies can and should be analyzed independently. Comparing their similarities and differences with prior technologies can be helpful in this regard.

In Gavin's view, rail and especially cyber technologies are more facilitating technologies than they are instruments for killing adversaries, destroying their military assets, and occupying their territory. Both rail and cyber technology quickly spread around much of the world because they were vital to national and international economies, even as they also serve military purposes. The economic indispensability of these technologies complicates efforts to control their military or other coercive uses. Both technologies condense the effects of space and time, making the world smaller and faster, which, in turn, dramatically increase the pressures on decision-making during a crisis.

Yet, as Gavin analyzes, differences between cyber technology and railways may be most instructive. In any case, looking from 1914 to the future of potential cyber conflict, a portentous question is whether states in tense regions possess the "institutional capacities . . . to deal with massively increased amounts of information coming from a variety of different sources and in an environment where cyber attacks might be oriented toward degrading and blinding" decision-making capabilities.

World War I offers another analogy to potential cyber warfare in the twenty-first century, as the British historian Nicholas A. Lambert considers in "Brits-Krieg: The Strategy of Economic Warfare." Lambert, the Class of 1957 Chair in Naval Heritage (2016–17) at the US Naval Academy, fascinatingly describes how the advent of the telegraph and undersea cables enabled an unprecedented, global movement of goods, money, knowledge, and information that transformed international commerce. In earlier eras, traders purchased and stockpiled large amounts of goods. In the newly globalized system, traders relied on processes such as just-in-time delivery, credit-based purchase, and transfer of goods, all underpinned by new information technology. Britain was the hub of much of this global trade and finance. Realizing this, a few strategists in the Admiralty began in 1901 to consider how, in a time of war, Britain could leverage its dominant naval and commercial position to halt global trade and thereby cause a quick and devastating economic shock to an adversary's economy and society, in this case Germany's. Unlike the interdiction of ships and the preventive and attrition bombing of military-economic assets, "the British aim" would be "far higher: . . . delivering an incapacitating 'knock-down' blow that would obviate the need for less intense but more prolonged types of war."

In the cyber era, an analogous act would be to use "cyber means as a weapon of mass destruction or disruption, targeting an enemy's economic confidence as well as its infrastructure, with the aim of causing enemy civilians to put political pressure on their government." For example, a sophisticated actor could corrupt the integrity of data and the processing algorithms in one or more major financial institutions in ways that would profoundly undermine the confidence on which modern international commerce depends. Yet, as Lambert recounts, the United Kingdom's application of economic warfare at the onset of war in 1914 was so effective that it ultimately backfired and had to be abandoned. Trade plummeted, and with it went the well-being of British traders, financiers, and labor. “As the scale of the economic devastation [in the United Kingdom] became increasingly apparent, domestic interest groups became ever more vocal in clamoring for relief and lobbying for special exceptions, and neutrals [countries] howled in outrage at collateral damage to their interests.” Soon, “political commitment to the strategy began to crumble; more and more exceptions to the published rules were granted, thereby further undermining the effectives of economic warfare.” In October 1914, the government aborted the strategy. Readers can easily imagine how in the globalized, digitally intertwined world of today, a strategy to cause massive economic disruption through cyber attack could pose similar challenges. Not only would the intended object of the attack suffer enormously but so too would the attacking state if its labor force, employers, and treasury were dependent on global trade and finance. Lambert’s conclusion details some of these possible challenges and ways of anticipating them.

Pearl Harbor presents the most frequently deployed analogy to cyber warfare, at least in US discourse. In October 2012 Secretary of Defense Leon Panetta warned of a possible “cyber Pearl Harbor,” saying a malicious actor could launch devastating cyber attacks to “paralyze and shock the nation and create a new, profound sense of vulnerability.”[7] Since then, cyber Pearl Harbor has become a recurring motif for officials, journalists, and experts warning of the dangers of a massive surprise cyber attack, especially in the United States. The image invoked is of a bolt-from-the-blue attack that catches defenders by surprise. Yet Emily O. Goldman, the director of the US Cyber Command–National Security Agency Combined Action Group, and Michael Warner clarify in chapter 9 that Pearl Harbor was not a surprise. “The United States was exercising coercive power to contest Japan’s occupation of China and other Asian states, and Washington expected war. Pearl Harbor was a logical, if misguided, result of Imperial Japan’s long-term strategy to expand its Pacific empire and blunt the United States’ effort to stop it.” Faulty American analysis and communication of intelligence data, and mistaken assumptions that the adversary (Japan) would calculate the risks of attacking as American personnel did, produced the sense of surprise. This observation makes what happened at Pearl Harbor even more salient for the United States and perhaps others today. Insofar as weaker actors embroiled in confrontations with powerful states may calculate, correctly or incorrectly, that a surprise cyber attack could temporarily weaken their adversary’s political resolve and military capability, they may see such an attack as the least bad alternative. By creating a fait accompli, with relatively few casualties on both sides, they could shift the burden of escalation to the stronger party to choose war rather than compromise. Goldman and Warner conclude that the United States and other states whose militaries, economies, and societies are extremely reliant on cyber capabilities should both increase their vigilance and create resilience in their military cyber networks. Unlike the case of Pearl Harbor, the vectors of attack could be located not only in military networks but also through privately owned and managed networks. This possibility greatly complicates the challenge of detecting, defending against, and responding to attack.

What Are Preventing and Managing Cyber Conflict Like?

Capabilities to conduct cyber information warfare, criminal activities (including terrorism), covert operations, and preventive military force are spreading faster than the international community's capacity to establish agreed rules for managing them. This is normal; all major disruptive technologies have emerged and created challenges that states have then struggled for years and decades to regulate. These management struggles have been waged first on a national basis and then later, if at all, internationally. Cyber capabilities may emerge and evolve faster, and spread more extensively and quickly, than have antecedents such as nuclear power plants and weapons, air transportation, radio, and so on. Moreover, cyber capabilities are less geographically bounded than preceding technologies are. Nevertheless, the inherent interests of states and societies dictate that norms and rules for managing these new capabilities must be proposed, negotiated, and ultimately agreed on, even if their enforcement will be imperfect. Otherwise, the dangers and costs of threatening activities will be too severe for most states and societies to bear.

States have already begun to address the complexities of regulating the underlying technologies of cyberspace, including the Internet's infrastructure. The struggle to establish rules for cyber capabilities and activities is intertwined with a broader, ongoing struggle over the governance of the Internet and the nature of sovereignty in cyberspace. This plays out in various formal bodies, such as the International Telecommunications Union, nongovernmental organizations including the Internet Corporation for Assigned Names and Numbers, and multistakeholder groups including the Internet Governance Forum. More tentatively, informal and formal efforts at various levels have begun to develop norms for the use of cyber weapons and the conduct of cyber conflict. Most notably they come from such groups as the G20 (or Group of Twenty), the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and the participants in the *Tallinn Manual on the International Law Applicable to Cyber Warfare* project. Clear, internationally agreed-on rules remain elusive, but unilateral and multilateral initiatives can begin to reduce the risks of unrestrained cyber conflict. These efforts can be enlightened by past experiences in managing threats to national and international security.

In the first essay in this section, Steven E. Miller, the director of the International Security Program at Harvard University's Belfer Center for Science and International Affairs, compares essential features of the nuclear era with those emerging in the cyber era. Miller notes that the nuclear age emerged publicly in 1945 with ferocious suddenness as nuclear weapons were detonated over Hiroshima and Nagasaki. The technology was born through secrecy, was militarized, and was tightly controlled—first by one government, the United States, and then by another, the Soviet Union. Civilian applications of the technology came later and never lived up to the advertisements of its progenitors. In contrast, cyber technology, notwithstanding its origination in the US defense establishment, quickly and widely took root and spread through commercial channels. Countless, often unpredicted, civilian applications of the technology have fueled economic growth and affected the lives of billions of people who have become dependent on them. Thus, the nature, purposes, and stakeholders associated with cyber technology are profoundly different than those associated with nuclear weapons and with civilian applications of nuclear technology. In this context, Miller considers whether and how the four central "pillars" of the nuclear order—"deterrence, damage limitation, arms control, and nonproliferation"—may be useful or not in managing cyber threats.

Miller's essay provides a segue to the next three essays in this section, which explore key facets of the defensive challenge. John Arquilla, in "From Pearl Harbor to the 'Harbor Lights,'" leads off the discussion of analogues to defending against cyber attack and conflict. Arquilla illuminates some of the sometimes surprising difficulties in reducing the vulnerabilities of civilian and defense networks. He recounts how the United States for three months *after* Pearl Harbor failed to "turn off" the lights in the country's coastal cities and harbors at night. As a result, German U-boats easily identified the eastern coastline, lurked off open anchorages and undefended harbors, and inflicted enormous casualties and destruction. Once the order to darken the coasts was implemented, along with other defensive measures, the German navy significantly reduced its operations in US waters. Arquilla likens the US failure to dim the harbor lights to the ongoing, inadequate government and private sector policies and actions to make their computers, networks, and data less accessible to attackers, and he suggests ways to redress these liabilities.

One of the growing policy conundrums in cyberspace is whether and how states and legitimate non-state entities should be permitted to actively defend themselves against intrusion and attack. Passive defenses such as encryption, firewalls, authentication mechanisms, and the like do not carry risks of international crisis. But some "active" cyber defenses that in some cases could harm another country raise serious risks and challenges. Intervention in an adversary's networks or computers that causes serious economic harm to an innocent entity in another country or that (unintentionally) impedes another state's national intelligence collection and defenses, could make the active defender liable to economic and criminal penalties or worse. Dorothy E. Denning and Bradley J. Strawser, professors at the US Naval Postgraduate School, explore the ethical and legal issues arising from active defense by analogizing air defense to active cyber defense. They focus mainly on state-conducted defensive actions while recognizing that such cyber actions by businesses and other legitimate non-state actors, although entirely plausible, pose additional complications.

To set up the analogy, Denning and Strawser describe a range of active defenses deployed against air and missile threats. Among them are aircraft, which the United States and the United Kingdom have deployed since September 11, 2001, to defend against hijacked aircraft; missile defense weapons, such as the Patriot surface-to-air system used in the Gulf War in 1991; other rocket and missile defense weapons, such as Israel's Iron Dome; and electronic warfare.

The authors then summarize some possible forms of active cyber defense and ask several questions about each to assess their ethical implications.

The development of missile-carried nuclear weapons in the 1950s confronted American (and Soviet and UK) authorities with an existential problem—that is, how to preserve political control over these forces when evolving technology and threats narrowed the time to respond to a nuclear attack. President Dwight D. Eisenhower's response in 1959 was to grant military commanders the authority to use nuclear weapons under carefully prescribed conditions. Peter Feaver, a professor of political science and public policy at Duke University, and Kenneth Geers, an ambassador with the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of excellence and a senior fellow at the Atlantic Council, reflect on how this challenge and the US response to it may be analogous to challenges posed by potential cyber warfare.

Three features of nuclear war motivated the adoption of nuclear predelegation: "the speed with which a nuclear attack could occur, the surprise that could be achieved, and the specialized nature of the technology (that meant only certain cadres could receive sufficient training to be battle competent)." While cyber war does not pose the civilization-ending threat that global thermonuclear war does, it may impose similar challenges on the management of cyber weapons (offensive and defensive). Feaver and Geers expertly unpack these challenges and the possible solutions to them.

The final chapter in this section explores a different and necessary way of reducing cyber threats—curtailing the operations of hostile private actors that operate as proxies of states or with state toleration. The analogy here is to naval privateering between the thirteenth and nineteenth centuries. Written by Florian Egloff of the Cyber Studies Programme at the University of Oxford, "Cybersecurity and the Age of Privateering" chronicles how governments commissioned privately owned vessels in wartime to operate against their adversaries' trade and in peacetime to attack merchants' ships in reprisal for harms attributed to a nation and to capture goods of equal value.

Analogies to the cyber domain abound here. Several states recently have used or allowed hackers and criminal organizations to conduct cybercrime and cyber-enabled espionage against adversarial states and economic interests. This practice is analogous to privateering and piracy. Meanwhile, if a state lacks the capacity to defend the cyber domain and obtain redress for harmful cyber activities, then the users are largely left to protect themselves. Naturally, private companies, like the earlier naval merchants, are now debating with governments the advisability of issuing letters of marque that would allow companies to counterattack against cyberespionage and theft. Of course, as Egloff discusses, the myriad state and non-state actors and interests at play in the cyber domain, and the pace of technological change, mean that ordering this space will be exceptionally difficult and will take considerable time. He offers a thought-provoking framework for understanding differences and similarities in the naval and cyber domains and how this understanding could inform efforts to secure cyberspace.

Each of these chapters is valuable and instructive in its own right. Together, as we describe in the conclusion, they suggest insights into the challenges that cyber capabilities and operations pose to individual states and the international community. We expect that this work will stimulate readers to think of additional analogies that could augment their understanding of cyber capabilities and operations, as well as policies to manage them in ways that reduce conflict and enhance international well-being. It would be especially welcome if scholars, journalists, and officials from non-Western countries were to elucidate analogies from their own technological and historical experiences to the cyber era, for the unprecedented benefits of cyber technology are the relative ease and affordability of its global dissemination. To realize its benefits, and to minimize the technology's destructive potential, the widest possible range of societies and states must learn to steward it wisely. The authors here seek to contribute to this outcome and encourage others to do the same.

Notes

1. Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014), 5.

2. Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision-Makers* (New York: Free Press, 1986).

3. Stanley E. Spangler, *Force and Accommodation in World Politics* (Maxwell Air Force Base, AL: Air University Press, 1991), 52.

4. Ibid., 62.

5. See, for example, Joseph Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011); Andrew Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), http://csbaonline.org/research/publications/cyber_warfare_a_nuclear_option; and Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2012).

6. Ashton B. Carter, "DOD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy," Number 3000.03E (Washington, DC: Department of Defense, April 25, 2013), 12, http://www.dtic.mil/whs/directives/corres/pdf/300003p.pdf.

7. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattacks on U.S.," *New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.