7 Cybersecurity's Uncertain Battleground

Michael Hayden, former head of the Central Intelligence Agency (CIA), once remarked about cybersecurity that "rarely has something been so important and so talked about with less clarity and less understanding."[1] In large part this is because neither those who have carried out a cyberattack nor the attack's victims are anxious to reveal many details. Attackers do not wish to publicly admit responsibility and become the target for reprisals or have their capabilities known. Victims fear that in providing details of a successful attack they will reveal what information has been compromised or alert others to weaknesses in their systems, thereby inviting further attacks. For example, the March–April 2010 cyberattack on computers used by Iran to produce nuclear power, about which we will have much more to say later, was only uncovered in June 2010. The United States and Israel are generally considered to have perpetrated the attack, but neither has officially assumed responsibility and Iran has not confirmed the extent of the damage done.

Cyberthreats—dangers to the security of a country's electronic and computer-related activities that result in the unwanted manipulation of data or compromise operating systems—used to be the stuff of science fiction novels or the imagination. And in many regards they still are. One forecaster of world politics recently presented a detailed account of a twenty-first-century world war started by Japan that began with a cyberattack in outer space against the United States.[2] Japan lost. But today cyberthreats are also very real.

On June 8, 2013, U.S. president Barack Obama and Chinese president Xi Jinping met in California for a get-to-know-you retreat that was part of an overall effort by the two governments to define their relationship with one another in an era in which Chinese economic and military power is on the rise and the United States is facing increasing domestic and global limitations on its exercise of power. While the meeting was described as cordial and productive, with each side promising to work with the other to solve common problems, the talks contained a dark underside. President Obama voiced concerns over industrial espionage and cases of computer hacking linked to China. He pointedly observed that this continued cyberactivity

could become "a very difficult problem" and an "inhibitor" to the development of good relations.[3]

Obama's warning was not entirely unexpected. In the months preceding the meeting, complaints about Chinese cyberattacks on the United States had become more direct and vehement, with an editorial by *The New York Times* asserting that "both nations need to take steps to avoid an all-out cyberwar."[4] In early April, without directly mentioning China, the Pentagon announced that it would increase spending for cyberoperations from $3.9 billion to $4.7 billion in the 2014 defense budget, with the majority of that increase going toward developing greater offensive capabilities. Later that month U.S. and Chinese military leaders held their highest-level talks in nearly two years, and a senior Chinese general observed that the consequences of a major cyberattack "may be as serious as a nuclear bomb."[5] Then, in early May, the Obama administration publicly charged China's military with mounting attacks on U.S. government and private sector computer systems in an effort to obtain "military capabilities that could be exploited during a crisis."[6] Chinese officials denied involvement in any attacks directed at the United States and countered that "China has repeatedly said that we resolutely oppose all forms of hacker attacks."[7]

Growing evidence pointed to the conclusion that U.S. concern about Chinese cyberattacks was well founded.[8] Ten major American energy firms had been the target of cyberattacks that provided China with valuable information about oil production technologies and potentially saved it years of research. Pentagon officials have asserted that over the past six years, "Chinese computer spies raided the data banks of almost every major U.S. defense contractor."[9] Among the weapons systems now believed to have been compromised in some way due to cyberattacks were the Patriot missile system, the Black Hawk helicopter, and the F-35 Joint Strike Fighter.[10] Other U.S. computer systems that have been compromised include that of the National Aeronautics and Space Agency (NASA); State Department computer networks, especially those at the Bureau of East Asian and Pacific Affairs; U.S. Naval War College computers, possibly those involved with running war games; the e-mail system of the Office of the Secretary of Defense; and computers at the Oak Ridge National Lab, which is run by the Department of Energy.

The U.S. government is not the only target of Chinese cyberattacks. The private sector has been hit hard as well. Chinese hacking is estimated to cost the American economy more than $300 billion per year. Coca-Cola fell victim after it failed to acquire a Chinese juice company. Google has been the target of several attacks, presumably because dissident political groups in China have used it as a method of communication. *The New York Times* came under attack probably for its reporting on political events in China. Cyberattacks have the potential to build on one another. When the computers at the security services firm RSA were compromised, the Chinese hackers also gained access to Lockheed Martin, a major defense subcontractor.

Box 7.1

Case Summary

Cyberthreats have emerged as the newest security problem facing states, and great uncertainty exists over how to both define and respond to them. The most significant issues surround cyberwarfare. Unilateral, regional, and global responses to cyberthreats are being explored.

Global Context

Debates over how to respond to cyberthreats and promote cybersecurity are taking place in an international system undergoing rapid change as a result of globalization. State monopolies on key power resources and the importance of state boundaries are disappearing as globalization has created an international system in which cyberspace has become a new and uncharted arena for conflict and competition.

Key actors

- United States
- China
- Russia
- Iran
- Israel

Motives

- Russia has used cyberpower as part of its military and political strategy to secure its borders as well as for economic and domestic political reasons.
- China is a major source of cyber-related espionage and cybercrime; many of its cyberattacks are conducted to add to its military power, speed the growth of its economy, and control political dissidents.
- The United States, Israel, and Iran have all been linked to stand-alone cyberattacks that reflect their national and regional security interests; for the United States and Israel, that includes preventing Iran from acquiring an operational nuclear capability.
- All states are concerned with the lack of international norms and rules governing the use of cyberpower and have begun to explore national and international strategies for dealing with cyberthreats.

Concepts

- Information and international relations
- Military strategy
- Nature of war
- Technology and international relations

Were the story to stop here, the United States would appear to be the victim seeking justice, and to some extent this is true. The emerging cybersecurity case study, however, also contains evidence of the United States

as an aggressor. Along with Israel, the United States has been linked to the Stuxnet virus that attacked Iran's computer system. The Obama administration also considered but ultimately rejected using cyberattack capabilities in helping to remove Muammar Gaddafi from power during Libya's uprising during the Arab Spring. Russia and Iran have also been linked to cyberattacks, as have scores of criminals and hacktivists (political and social groups) located around the world. By one estimate, over thirty countries have created cyberunits within their militaries.

In this chapter we will travel down a pathway of conflict and cooperation that is far less well defined than those we encounter in other case studies. As a result, when it comes to cybersecurity, policymakers, analysts, and the public at large find themselves trying to understand both the problems they face and the direction the path they are travelling is taking them. The resulting uncertainty of how to proceed greatly expands the room for disagreement over what is feasible and what is desirable when formulating cybersecurity policy.

We will begin moving down the pathway of cybersecurity conflict and cooperation by first outlining the dimensions of the problem and defining key terms. We then examine in more detail key cyberattacks that have brought us to this point in time. We next consider how the United States and others are thinking about cybersecurity and conclude by speculating what directions the cybersecurity pathway may take in the future. Our Concept Focus looks at a current method used by strategists to characterize different levels of cyberattacks. The Spotlight section examines Russia and China as rising cyber superpowers.

The Nature of the Cybersecurity Problem

Policymakers often look to what has worked in the past for guidance in solving new policy problems. In the case of cybersecurity threats, this has led to warnings of cyber-Pearl Harbors and cyber-9/11s. In developing cybersecurity strategies, the historical analogy most frequently relied upon is the development and use of nuclear weapons. The nuclear era ushered in a new age of military strategy and redefined power relations among states. The cyberpower era is expected to do the same.

Tempting as historical analogies might be, however, they are also potentially dangerous because the pathways of present and future conflict and cooperation are not likely to duplicate any single road already travelled. For instance, nuclear weapons are immensely destructive in their own right, but cyberweapons are not. They cannot destroy buildings or kill large numbers of people in an instant. They do their damage by crippling computers, blocking communications, and manipulating information.

Despite these differences, there are similarities between nuclear technology and cybertechnology.[11] Most important is the fact that nuclear technology changed and developed over time and nuclear offensive and defensive strategies changed with it. As with nuclear arms control efforts, we may see periods in which most states agree on the nature of the problem

of cyberthreats and the consequences of inaction but lack the cooperation to prevent unwanted futures from occurring.

Another approach to understanding cybersecurity is to break it down into four component parts: cyberspace, cyberpower, cyberthreats, and cyberstrategy. Cyberspace, along with air, sea, land, and space, is now accepted by strategic planners as one of five geographical domains for war and peace. Although it was created by the Pentagon to provide a secure means of communication for the military, early civilian advocates believed that the Internet would be a force for cooperation and mutual benefit.[12] Unlike the other four domains, cyberspace is a human creation. Land, sea, space, and air would still exist without human activity, but cyberspace came into existence as a result of manmade technological innovations. It is the physical infrastructure of networked computers, cellular technologies, fiber optic cables, and space-based communications that link people together. Because of its manmade nature, the boundaries and properties of cyberspace as a domain of policymaking are capable of undergoing far greater and more rapid changes in character than are land, sea, air, and space domains, thus complicating the development and execution of cybersecurity policies. As one commentator has noted, "Nothing is final in cyberspace."[13]

Box 7.2

Concept Focus

Cyberthreat Conflict Ladder

A common method employed by strategists and military observers to assess the range of threats and security challenges facing a country is to create a threat contingency ladder with the most threatening scenarios at the top and the least threatening at the bottom. The idea of a conflict ladder is not meant to suggest that conflicts move up or down one rung at a time. It is designed to help organize thinking and prioritize problems. As we have noted, concepts such as cyberwarfare, cyberthreats and cybersecurity are far from precise and lend themselves to multiple interpretations. Below is one possible way to think about the range of cybersecurity challenges and threats that a country could face.

Types of Cybersecurity Threats

THREAT	DESCRIPTION
15. Full-Range First-Strike Cyberattack	A widespread, offensive attack carried out against military, economic, and societal targets
a. stand-alone attack	
b. as part of coordinated military attack	Damage: temporary, although if accompanied by military attacks, it could be extensive

(Continued)

(Continued)

THREAT	DESCRIPTION
14. Selective First-Strike Cyberattack a. stand-alone attack b. as part of coordinated military attack	An offensive attack carried out against a limited set of societal targets Damage: temporary and not extensive unless accompanied by military attacks
13. Full-Range Preemptive Cyberattack a. stand-alone attack b. as part of coordinated military attack	A widespread, offensive strike in self-defense against military, economic, and societal targets; carried out in anticipation of imminent war Damage: temporary, but could be extensive if accompanied by military attacks
12. Selective Preemptive Cyberattack a. stand-alone attack b. as part of coordinated military attack	An offensive, self-defense strike with a limited target set Damage: temporary and not extensive, although more significant damage would occur if accompanied by military attacks
11. Full-Range Retaliatory Cyberattack a. stand-alone attack b. as part of coordinated military attack	A widespread strike against military, economic, and societal targets carried out in response to an adversary's attack Damage: temporary, but could be extensive if accompanied by military attacks
10. Selective Retaliatory Cyberattack a. stand-alone attack b. as part of coordinated military attack	A strike against a limited set of targets carried out after an adversary has attacked Damage: temporary and not extensive unless accompanied by military attacks
9. Full-Range International Terrorist Cyberattack	An offensive strike delivered by a centrally organized terrorist group(s) Damage: extensive but temporary; no military component
8. Selective International Terrorist Cyberattack	An offensive strike, most likely delivered by a single terrorist cell or loose alliance of cells Damage: limited but temporary; no military component
7. Symbolic Cyberattack	A statement attack intended as a warning to an adversary of further action—cyber and military—should tensions continue or undesirable policies not change

THREAT	DESCRIPTION
6. Crisis Management Cyberattack	An attack by states outside of a conflict for the purpose of stabilizing a crisis situation and allowing for the restoration of civil order and regional security
5. Sabotage Cyberattack	Carried out either as stand-alone activities designed to weaken an enemy or an attack in conjunction with a planned military maneuver designed to defeat the enemy
4. Espionage Cyberattack	An attack aimed at obtaining otherwise secret national security information from an adversary that is carried out by government and military agencies or civilians working in alliance with state officials
3. Criminal Cyberattack	An attack aimed at gaining information that will lead to a financial profit
2. Hacktivist Cyberattack	An attack initiated by political and social groups as part of a global campaign to advance their cause
1. Mischief Cyberattack	A recreational and isolated cyberattack carried out by individuals with no political or financial motive

Source: Compiled by the author.

Cyberpower, at its most elementary level, is information used in order to inflict harm, persuade, or more generally gain an advantage. Unlike traditional military technologies that achieve their objectives through the physical destruction of a target, information power achieves its objectives by temporarily capturing its target and providing it with misleading or false information that reduces its effectiveness. Cyberattacks gain entry into networks by exploiting previously unknown computer vulnerabilities known as zero days. Typically, these zero days are identified by individuals who, in return for their silence, sell their discovery. Software firms seeking to protect their products by fixing the vulnerability before it became known were once the primary purchasers of this information. Today, governments play a major role as they seek to protect their military systems from attack and create an inventory of vulnerabilities that can be used against adversaries on short notice. For example, the Stuxnet virus that attacked Iran's nuclear processing system made use of four or five zero days to gain entry into the system.

Cyberweapons are attractive instruments of influence because in their most generic form they can literally be purchased off the shelf at affordable prices and delivered via messages to personal computers or through portable thumb drives.[14] The cyberweapons employed against Iran's nuclear capability in March or April 2010 were virtually identical to those employed by cybercriminals seeking to ferret out secret information from companies or government offices. For example, in 2011, as a result of Operation Ghost Glick, the FBI arrested six Estonians and charged them with running an Internet fraud scheme that operated in over 100 countries and infected more than 4 million computers. By infecting the computers with a virus, the hackers were able to manipulate Internet advertising and steal $14 million in illegitimate fees.[15]

Cyberthreats and risks, from a national security policy perspective, come in two forms. The first are risks and threats to the infrastructure of cyberspace. Virtually all individuals, corporations, and governments face these risks and threats and are concerned about protecting computers and other information-processing systems from being covertly captured, disrupted, disabled, or deceived. The second set of risks and threats involve the information that flows through cyberspace, which is perceived and evaluated to different degrees. For authoritarian political systems, the information in cyberspace may be a potentially serious threat to their ability to rule. It may also seriously harm a country's economy through its ability to influence investment, savings, and purchasing decisions. Finally, information in cyberspace may be seen as threatening fundamental societal values, as is often perceived to be the case with child pornography.

The fourth and final dimension to cybersecurity is cyberstrategy. Strategy is the lynchpin that unites policy goals with tactics. Tactics without strategy means winning the war and losing the peace. Wars are fought for political purposes that go beyond simply defeating the enemy. Failing that, wars, even if they are won on the battlefield, can be lost. Pearl Harbor was a tremendous military success for Japan, but it did not prevent that country from losing World War II. One of the major critiques of cyberstrategic thinking is that it is overly concerned with tactics and not strategy. Too much emphasis is given to what cyberpower can and might do, without adequate attention paid to whether or not its use will make a country more secure or whether its side effects might create even greater security threats in the future.

Military strategists have no agreed-upon answers regarding the strategic effectiveness of cyberpower. Three major areas of disagreement exist, and the chosen conclusions will help determine the nature of the cybersecurity pathway that countries travel in the coming decades. The first area of dispute is over whether or not cyberweapons can be used defensively. For some, given the speed and stealth of cyberpower, there is no effective defense against it. Cyberweapons are by their very nature first-strike weapons. Advocates of defense argue that while offense has the advantage now, this may not be the case in the long run since cybertechnology is in its infancy and will mature, change, and stabilize over time.

The second debate is over whether cyberweapons can be used alone—that is, can a war in which only cyberweapons are used be fought and won? The low cost, relative ease of use, and covert nature of cyberattacks make them attractive weapons of choice that are sought by military establishments around the world. At the same time, critics ask what country is likely to surrender or abandon its position simply as a result of a cyberattack. From this perspective, cyberweapons are valuable only when used in conjunction with other weapons systems.

The third and most finely tuned debate is over the possibility of cyberdeterrence, a concept that gained great prominence with the advent of nuclear weapons. Deterrence seeks to prevent a country from taking unwanted actions by threatening an immediate and unacceptable level of retaliation. Threatening like retaliation for a cyberattack has become a standard part of the language of cyberstrategy. Yet problems exist in carrying out this

Timeline

Cybersecurity Attacks

1998	U.S. Defense Department computers are penetrated by hackers.
1999	Hackers target NATO computers in response to the NATO bombing of Kosovo.
2001	Russian hackers penetrate U.S. Defense Department computers.
2007	Estonia suffers a cyberattack linked to Russia.
2008	Georgia suffers a cyberattack as part of military conflict with Russia.
2009	A cyberattack linked to China attacks computers used by supporters of the Dalai Lama.
2010	The United States and Israel are linked to the Stuxnet virus that attacks Iranian computers used in its nuclear weapons program.
2011	The Obama administration releases its International Strategy for Cybersecurity.
	The London Conference on Cyberspace is held.
2012	Iran undergoes a second cyberattack linked to Israel.
	Saudi Aramco oil company suffers a cyberattack linked to Iran.
	The Pentagon announces Plan X, designed to give the United States the ability to launch retaliatory or preemptive cyberattacks
2013	President Obama and Chinese leader Xi Jinping meet and discuss cybersecurity issues.

strategy, the most profound of which is the difficulty of detecting who was behind an attack. Simply because the attack came from country X does not mean the government of country X was responsible for it. Without firm proof, a retaliatory action can turn into an offensive act of war.

Problem Setting and Origins: The Beginning of Cyberwarfare

The exact date at which cyberconflict became an important aspect of world politics is subject to debate. Numerous starting dates exist to choose from. In 1998 computers believed to be in the United Arab Emirates succeeded in penetrating the Defense Department's security system (later it was discovered the computers were in fact controlled by teenagers in Israel and California). In 1999 NATO's computer system was overwhelmed by hackers protesting the NATO bombing in Kosovo. In 2001 Russian hackers penetrated Defense Department computers in what are referred to as the Moonlight Maze attacks. Some treat the 2007 cyberattacks on Estonia as the beginning of a new era in warfare, while others say the notable date is for yet a different attack or has in fact not yet even occurred. In this section we examine these and other examples of cyberconflict that mark the pathway of conflict and cooperation policymakers find themselves on today. They are significant as much for the questions they raised as for what actually happened.

The cyberattacks on Estonia began on April 27, 2007, and continued into mid-May. The spark that ignited these attacks was the decision to relocate a bronze statue of a Russian soldier from the center of Tallinn, Estonia's capital, to a war cemetery. Russians saw the statue as commemorating the sacrifices made in fighting Nazi Germany during World War II, but Estonians considered it to be a symbol of Soviet-enforced communist rule. Rioting by ethnic Russians living in Estonia and by Nashi, the government-sponsored youth group in Russia, broke out over the statue's relocation. The Russian government protested the action and then put in place a series of limited economic reprisals such as cutting railroad service between the two countries.

At the same time, a flood of junk e-mail was sent to parliamentary Web sites in Estonia as well as those of the president and prime minister. In the following weeks, newspaper and broadcasting Web sites crashed, online access to Estonia's largest bank was blocked, telephone exchanges were attacked, and Web sites were defaced with cybergraffiti and Russian propaganda. On May 5 Estonia announced the attacks had originated in Russia, which denied responsibility. However, it is generally held that the attacks could not have been carried out without the approval and support of the Russian government. Among those known to have participated in the attacks were individuals affiliated with Nashi and "script kiddies," individuals located around the world who followed Russian-language chat rooms, which provided information on how to attack Estonian Web sites.

The key question raised by the cyberattacks on Estonia was how the event should be classified. The question is significant because how it is defined legitimizes some responses and places others off limits. Initial accounts referred to it as a cyber-riot. Estonians officials took a more somber view, arguing that these cyberattacks were no different from a physical attack on their country.

The following year cyberattacks surfaced as part of a traditional military operation. On August 8, 2008, Russian troops invaded Georgia, an independent country on its borders that had been part of the Soviet Union. The invasion was the culmination of growing tensions between Georgia and Russia over South Ossetia, a breakaway province of Georgia containing large numbers of ethnic Russians. On August 7 Georgia sent troops into South Ossetia in an effort to reestablish control over it. Russia retaliated by invading Georgia and quickly overran the country.

In carrying out its military operation, Russia also engaged in a two-phase cyberoffensive, the goal of which was to isolate and silence Georgia.[16] In the first phase, Russian hackers unleashed a brute force denial-of-service attack. Unlike a semantic attack, which targets specific software systems, a brute attack seeks to overwhelm the target by increasing Internet traffic to the target to a point where its system fails. Groups of computers known as botnets that have had their command and control systems infected are taken over and used for this purpose. In the Georgian brute force attack, the botnets used were linked to Russian criminal organizations. In the second phase of the cyberoffensive, Russia concentrated its efforts on a more specific set of Web sites used by businesses, financial firms, Western media outlets, and educational institutions. CNN, for example, was hit with over 300,000 e-mails from individuals supporting the Russian invasion. The primary sources of cyberactivity in this phase were Russian "patriotic hackers," many of whom were members of Nashi and other youth movements. As with the Estonia cyberattack, they received guidance and instruction from Web sites such as StopGeorgia on how to launch denial-of-service attacks to the point where a user-friendly button (FLOOD) was made available to them. Evidence suggests that these sites were overseen by professionals who sought to counter Georgia's efforts to repair the damage done or to block the attack. A key question the Georgian attacks raised was the definition of neutrality in a cyberconflict. How were other states supposed to respond, especially since Russia denied responsibility for the cyberattacks? Moreover, was there any form of global responsibility to aid the victims of a cyberattack?

Another milestone in cyberwarfare occurred in 2010 with Operation Olympic Games. [17] Beginning in 2007, during George W. Bush's administration, the United States and Israel began working together with the goal of finding a means of crippling Iran's efforts to obtain nuclear capability. A secondary goal for the United States was to convince Israel that war with Iran would not be necessary to achieve this, thus averting the possibility of a

widening and escalating conflict in the Middle East. The tool used to achieve this objective became known as Stuxnet. Five different organizations in Iran were identified for attack, with the Natanz uranium enrichment facility being the primary one. After the Stuxnet attacks, Iran confirmed that about 30,000 IP addresses had been infected. Evidence points to a reduction in the number of operational enrichment centrifuges in Iran from some 4,700 to 3,900 and a reduction in operational capacity at Nantz of 30 percent.

Stuxnet's objective was to penetrate and attack Iran's nuclear industrial control systems through a multistep process. First, it exploited several previously unknown vulnerabilities (referred to as zero-day exploits) in the Windows operating system. It then used stolen digital certificates to target specific industrial codes made by Siemens. By capturing the Siemens industrial codes, Stuxnet was able to issue instructions to computers controlling the uranium enrichment centrifuges to change the speed of the centrifuges and break them. The virus is initially attached to a host via a USB drive or other removable device. Once present, it self-replicates, infecting other local networks of computers that might not be connected to the Internet and sending information back to its operators.

Stuxnet's significance to the future of cyberconflict is found in several different issues surrounding its use. First, it was a preventive attack. There was no significant rise in tensions and war was not imminent. According to conventional international laws of war, a preemptive attack, striking first in self-defense when war is about to happen, is justified. A preventive attack is not. Second, it produced directed and limited damage. Stuxnet did not silence Iran nor cripple its entire cyberspace as the attacks on Estonia and Georgia sought to accomplish. Third, the damage done was repairable and more limited than early public accounts suggested, leading to questions about the wisdom of the attacks.

In May 2012 a second U.S.-Israeli cyberattack on Iran occurred. It also was developed as part of Olympic Games. Known as Flame, its primary purpose was intelligence gathering. Masquerading as a Windows updating program, Flame can activate computer microphones and cameras, take screenshots, log keyboard strokes, get location data, and send and receive commands, making it a valuable tool for constructing future attacks. It is estimated that 1,000 computers in Iran were infected. Other infected targets were found in Syria, Sudan, and the West Bank. Flame was discovered after Iran was hit with a series of cyberattacks on its oil fields. These attacks were apparently organized and carried out by Israel without U.S. knowledge.

Suspicion focused on Iran itself as the source of a cyberattack uncovered in 2012. The target was Saudi Aramco, Saudi Arabia's national oil and gas company.[18] The virus, referred to as Shamoon, did not cause any physical damage to Saudi Arabia's oil production facilities and has been described as relatively amateurish, but it did affect Saudi Aramco's business operations by randomly destroying drilling and oil production data. It took the company two weeks to fix the problem. Iran officially denied any involvement in the Shamoon attacks. Unlike the earlier attacks surveyed in this

case study, this attack had the potential for disrupting the global economy if Saudi Aramco's oil production had been severely damaged. The question raised then became whether the potential scope of the consequences of the cyberattack changed the manner in which other states could and should respond to it.

To date, no significant act of cyberwarfare can be included in this overview of cyber-related events, although fears of cyberterrorism occupy a prominent place in both public and governmental rhetoric on cybersecurity.[19] Instead, the most common form of cyberwarfare by al-Qaeda, Hamas, and other extremist groups has been the release of videos calling for an electronic jihad.

Problem Definition and Response: Coordinating and Structuring a Strategy

The United States undertook several initiatives in 2011 to address the problems of cybersecurity.[20] In May the Obama administration released its International Strategy for Cyberspace. Its conceptual starting point is that cyberspace is a global commons that cannot become the possession of any one country or set of countries. The United States' ultimate objective is defined as an open and secure information and communications infrastructure that supports international trade, strengthens international security, and fosters the free flow of ideas. According to this strategy document, the United States believes that these goals can be achieved through the application of long-standing international norms of peaceful behavior and behavior that is permitted during conflict. The United States does not see cyberspace as requiring the creation of new norms or as having made existing norms obsolete. The strategy reaffirms that "when warranted the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. . . . We reserve the right to use all necessary means . . . as appropriate and consistent with applicable international law in order to defend our Nation, our allies, our partners, and our interests."

Two months later, the Government Accountability Office (GAO) released its study on the Defense Department's efforts to bolster U.S. cyberdefenses. The GAO acknowledged the immense scope of this challenge, noting that the Pentagon possessed over 7 million computer devices, linking together more than 10,000 networks. The primary finding of the GAO's report was that the Defense Department lacked both a coherent command structure to coordinate its cybersecurity efforts or a coherent strategic doctrine to guide planning and assess the resources needed to succeed in cyberdefense.

Two concrete steps have been taken to address these concerns. The first was the creation of the U.S. Cyber Command in 2010. It is charged with the direction of Defense Department information networks for conducting a full spectrum of cyberspace activities in all domains, thereby ensuring the United States and its allies freedom of action in cyberspace and denying such use to U.S. adversaries. Responsibility for federal civilian information

networks rests with the Department of Homeland Security. Second, in October 2012 the Pentagon announced the start up of Plan X by the Pentagon's Department's Defense Advanced Research Projects Agency (DARPA), an organization established in 1958 in order to ensure that the United States would have a technological edge over any adversary and to prevent a surprise technological attack.[21] The conventional strategy for protecting information networks is to build firewalls around them to thwart any attack. Plan X is a five-year, $100 million research program designed to create a global map of cyberspace that will provide military commanders with the ability to identify and track threats continuously and allow them to retaliate or preemptively attack cybertargets instantly using preplanned scenarios.

The Defense Department issued a report to Congress in November 2012 detailing its cyberstrategy policy. The report noted that a cyberattack had to be of "significant" scale in order to justify a retaliatory strike, but it did not present specifics on at what point an attack moved from being an annoyance or limited engagement to qualifying as an action meriting a response. It was also silent on when that response should entail the use of military force and, should that be the case, at what point the provisions of the War Powers Resolution requiring that the president obtain the consent of Congress became relevant.[22]

Efforts to address cybersecurity issues have also taken place at the international level.[23] In 2010 the United Nations Group of Governmental Experts, in this case diplomats and military officers from cyberstates, issued a report titled "Developments in the Field of Information and Telecommunications in the Context of International Security," which called upon states to undertake confidence-building and risk-reduction measures in order to protect critical national and international information infrastructures. This group has continued to meet on ways to improve cybersecurity.

The following year Russia and China jointly introduced a proposal to the United Nations General Assembly calling for a code of conduct among cyberstates. The objective was to keep cyberspace from becoming a battleground, prevent a cyber arms race, and promote dialogue as a means of settling cyber-related disputes. A key aspect of this proposed code was the right of states to protect their information space from attacks and sabotage. Later in the same UN meeting, Russia introduced the separate Convention on International Information Security. The wording and spirit of the codes raised concern by observers that what one country defined as cyberspace sabotage might strike another as a legitimate exercise of free speech.

These concerns were very much in evidence at the 2011 London Conference on Cyberspace, which was attended by government officials from sixty countries, including Russia and China, and representatives from the private sector. Although the conference officially focused on cyberattacks and cybercrime, the discussion quickly turned to questions of free speech, with one participant asserting that the threat to the Internet was not cybercriminals but misguided or overreaching government policy. U.S.

and British officials urged that governments not use cybersecurity as an excuse for censorship and warned against the dangers of a "repressive global code."[24]

Whereas Russia and China have sought the establishment of global codes of conduct, the United States and many of its allies have looked to regional organizations as the most appropriate site for developing such standards of behavior.[25] Primary attention has focused on the Organization for Security and Cooperation in Europe (OSCE). Now with almost sixty members, the OSCE was established during the Cold War as an organization dedicated to conflict reduction and risk management. Cybersecurity issues are seen as a logical next step for this organization due to its long experience in dealing with Cold War conventional and military security issues. ASEAN (the Association of Southeast Asian Nations) is viewed as the logical partner organization for addressing cybersecurity concerns among Asian states. Other regional and international organizations have also directed their attention to cybersecurity issues. Three of the most prominent are the Group of 8 (G8), the European Union, and NATO.

Box 7.3

Spotlight

Russia and China: Cyber Superpowers

China's approach to cybersecurity encompasses a full range of activity.[26] The first major Chinese statement regarding the military uses of cyberpower came in 1998 with the publication of *Unlimited Warfare*, which argued that U.S. military dependence on information and communication technology was a weakness that China could exploit. Today, Chinese military thinking integrates electronic warfare and cyberwarfare into the concept of information confrontation, and there are special units within the People's Liberation Army dedicated to carrying out hacking operations. Political dissidents are a prime target of Chinese cyber-related espionage operations. While many blogs are tolerated by the Chinese government, especially those on foreign affairs that are highly nationalist in tone, blogs on democracy, religion, and Tibet tend to be taken down. Ghost Net, discovered in 2009, was a cybersystem suspected of being linked to the Chinese government that targeted the computer systems used by supporters of the Dalai Lama. It infected 1,200 computers in 103 countries.

The popular perception is that Chinese hacking is highly sophisticated, but in fact much of it is considered to be rather sloppy and easily detected. Cyberattacks from China tend to occur only from 9:00 a.m. to 5 p.m., Beijing time; hackers do not hide their activity very well; and many attacks are noisy because they are carried out by multiple hackers in search of the same information. This stands in contrast to Russia, where hacking occurs 24/7 and is harder to identify as a result of carefully scripted targeting of sites.

(Continued)

(Continued)

Finally, China also engages in cyber-related sabotage. "Patriot hackers" (private citizens who are believed to act with the encouragement of the government) have attacked en masse the Web sites of organizations such as CNN for its reporting on riots in Tibet in 2008. Additionally, the Chinese government has blocked Internet access in parts of China by establishing firewalls and gateway controls that prevent IP addresses from getting through.

Russian thinking on the military uses of cyberpower has several dimensions. As evidenced by its operation against Georgia, the Russian military embraces an offensive strategy that emphasizes informational warfare to achieve political objectives, but it is also developing plans for regional cyberdefense systems. It is a major source of cyber-related espionage, with motivation being an important distinguishing feature separating the Russian and Chinese efforts.[27] In China the profit motive is very much present but exists alongside an organized effort by the Chinese government to obtain secret information from foreign businesses in order to strengthen China's world military and economic standing. In Russia the profit motive is far more pronounced. A recent example was uncovered in 2013 when four Russians and one Ukrainian were charged with stealing 160 million credit card numbers between 2005 and 2008. One of the leading Russian crime organizations is the Russian Business Network (RBN), which is said to be responsible for about 40 percent of all global cybercrime committed in 2007. The net worth of its efforts that year was put at over $100 billion. RBN is also the reported to be the world's largest spammer, accounting for 20 percent of all spam in 2008. It was also involved in Russia's cyberattack on Georgia in 2008.

Russian authorities have employed many of the same techniques used on Georgia and Estonia against their domestic opponents. Some of the prominent voices that have been subject to cyber-related sabotage are involved with Russia's anticorruption movement, such as Alexei Navalny's blog site; the People's Freedom Party, which was set to post an anti-Putin report on LiveJournal; and opposition leaders' Web sites that were hit on the eve of the 2012 Duma elections.

Countries are considered to be military superpowers because of the range of weapons they possess and their ability to inflict harm. So it is with cyber superpowers. Russia and China, along with the United States, have a far more extensive range of cyberweapons at their disposal than do most countries. As the China and Russia cases illustrate, one important difference between conventional military superpowers and cyber superpowers is that cyber superpowers need not rely on the military to exercise their influence. They can work through patriot hackers, criminals, and private citizens, making it very difficult to assign responsibility for their actions and thus clouding retaliatory efforts as well as arms control undertakings.

Problem Evolution and Development: A Pathway under Construction

Unlike many other case studies in this book, our overview of the cybersecurity pathway of conflict and cooperation being travelled has brought us to the present. We have not seen the next wave of conflicts that will allow

us to judge whether cyberdefenses or deterrence work or whether certain forms of cyberweapons will be used more often than others. Much more than those studied in our other cases, the cybersecurity pathway is under construction. In this it very much resembles the period right after World War II when strategists began to struggle with understanding the power and limits of nuclear weapons as an instrument of foreign policy. Those debates lasted into the 1960s before a consensus on nuclear strategy was developed. Rather than speculate on the direction that the cybersecurity pathway will take, we will identify four of the leading possibilities under discussion.

The two end points of the debate are that (1) cyberwar has fundamentally changed the nature of war and (2) while it is a new tactic, at the strategic level nothing has changed. The possibility that cyberwar will usher in a new era of warfare was put forward a decade before the attacks on Estonia, Georgia, and Iran.[28] This position argues that managing, obtaining, and denying information is a potentially transformative strategic asset whose full realization will require reorganizing military structures from ones based on hierarchy to ones organized around networks. Cyberwar is also seen as requiring a change in military doctrine so that political and psychological factors are fully integrated with the military aspects of war. The definition of the boundaries of a battlefield, what constitutes an attack, and how to define victory and defeat are three elements of military doctrine which will need to be reconsidered.

At the opposite end of the spectrum is the view that cyberwar is business as usual.[29] Proponents of this belief argue that cyberweapons, while swift and covert, are not deadly. Scenarios built around catastrophic damage done by the stand-alone use of cyberweapons are not found to be persuasive. Instead of being rooted in transformative information power, cyberpower is here treated as just information. Military strategy is unchanged by cyberpower and the fascination with new technologies should not obscure that. Cyberpower is just another weapon.

In between these two positions can be found two others of note. In one perspective cyberwar is seen as an extension of the Cold War, and thus the debate over the extent to which cyberpower has altered the nature of warfare is off target. Just as in the Cold War, we are not likely to see major confrontations between opposing global powers. Instead, we will see indirect conflicts, local wars, and wars fought by proxies.[30] These wars may become commonplace and will include cyberpower, but it will be used in a limited and constrained fashion so as not to provoke the anger of the global powers. Cyber-related subversion and espionage will flourish and cyberstates will routinely deny their involvement in these disputes.

The final alternative future sees cyberpower as being transformative in its impact on military strategy, but not in the way in which the first perspective we introduced in this section views it. Here cyberwar is transformative not because of the damage it can do, which is seen as temporary in nature, but by the uncertainty it creates in other states.[31] Accordingly, the target of a cyberattack is not the adversary's information systems but the adversary's

confidence in the ability of its information systems to engage in successful offensive or defensive action. Without such confidence, there is no reason to go forward with developing a cyberwar capability. The development of such an offensive capability by the United States would not dissuade Russia or China from moving forward to develop cyberpower capabilities, nor would it eliminate the problems of cybercrime and cyberhacking, but it would serve as an effective deterrent to the majority of the world's countries from obtaining a cyber-related military capability.

Conclusion: An Evolving Cyberthreat

The cybersecurity pathway we have explored began with an overview discussion of the different component parts of cybersecurity and moved to an examination of key cyberwar incidents that elevated cybersecurity from an abstract problem to a concrete national security issue. We then looked at efforts by countries and international organizations to create cybersecurity strategies and place limits on cyberconflicts. As we noted in our look into future developments, although much has transpired, cybersecurity is still in its formative period and uncertainty exists over the future direction it may take.

Regardless of which direction the cybersecurity pathway takes, elements of conflict and cooperation will be present. Particularly challenging for countries as they continue on this journey will likely be the higher-than-usual degree of suspicion and uncertainty that will surround their interactions (both peaceful and conflictual ones). Suspicion grows out of the stealth nature of cyberattacks and the difficulty of assigning responsibility for them: Who really is an ally and who is an enemy? Uncertainty grows out of the newness of cyberattacks. Will cyber arms control really work? How much damage will a cyberattack produce and how quickly will the enemy recover from it?

Case Analysis

1. In our discussion, we noted that the cybersecurity pathway was under construction. Rank in order of likelihood and desirability the four possible directions the cybersecurity pathway might develop. Justify and compare your rankings.
2. Does China, Russia, or the United States represent the greatest cyberthreat to global security? Why?
3. What would you include in a code of conduct for cyberspace? What would you want excluded?
4. Are separate national, regional, or global efforts the best way to go in making cyberspace secure?

5. Should different rules govern cyberspace as it exists in the global commons and within national state boundaries?
6. At what point in the cyberthreat conflict ladder do we cross over to cyberwar?
7. In looking at the cybersecurity pathway, which cyberattack is most relevant for thinking about the future: Estonia, Georgia, or Iran? Why?
8. Assume that you are the national security advisor and have been asked to develop a cyberstrategy for the United States. What are the key issues that must be addressed in this document? What is your position on them?

Suggested Readings

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming." *Comparative Strategy* 12, no. 2 (1993): 141–165. This is an early classic statement of the conflict-transforming potential of cyberpower.

Deibert, Ronald, and Rafal Rohozinski. "Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4, no. 1 (2010), 15–32. This article provides a conceptual overview of the concept of cybersecurity and the debates over its meaning and implications.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle Barracks, PA: U.S. Army War College Press, 2013. This work argues that concerns with the uniqueness and destructive potential of cyberpower are overstated.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011): 41–60. Klimburg presents an overview of the concept of cyberpower and discusses Russian, Chinese, and U.S. cyberpower resources and polices.

Nye, Joseph S., Jr. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38. Nye presents a balanced account of the parallels and dissimilarities between strategic thinking for nuclear weapons and cyberweapons

Rudner, Martin. "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge." *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (2013): 453–481. This article presents an overview of threats from international terrorism, state-sponsored terrorism, malevolent hacking, and insider threats.

Web Resources

Center for Strategic and International Studies, http://csis.org/category/topics/technology/cybersecurity. This bipartisan nonprofit organization presents an overview on policy, research, and news coverage on cybersecurity.

CyberDomain Security and Operations, U.S. Department of Defense, www.defense.gov/home/features/2013/0713_cyberdomain. Access articles, speeches, news, and more from this DOD site, including links to U.S. Cyber Command.

Royal United Services Institute, www.rusi.org. Explore research, analysis, and publications from this independent think tank based in the UK.

Strategic Studies Institute, U.S. Army War College, www.strategicstudiesinstitute.army.mil/. Access research, analysis, and other publications on a range of security topics, including cybersecurity.

U.S. Department of Homeland Security, www.dhs.gov/topic/cybersecurity. The DHS provides an overview on cybersecurity, U.S. policy, privacy, and more.

Comprehensive National Cybersecurity Initiative, the White House, www.whitehouse.gov/cyber security/comprehensive-national-cyber security-initiative. Read the Comprehensive Cybersecurity Initiative presented by the White House and explore related White House blog posts.