JANUARY 2018

Rethinking Cybersecurity

Strategy, Mass Effect, and States

AUTHOR
James Andrew Lewis

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Report of the
CSIS TECHNOLOGY PROGRAM

JANUARY 2018

Rethinking Cybersecurity

Strategy, Mass Effect, and States

AUTHOR
James Andrew Lewis

A Report of the
CSIS TECHNOLOGY POLICY PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report and associated events were made possible by a generous grant from the Smith Richardson Foundation.

ISBN: 978-1-4422-8051-9 (pb); 978-1-4422-8052-6 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

Contents

Introduction: Security for the Digital Revolution

Despite all the attention, cyberspace is far from secure. Why this is so reflects conceptual weaknesses as much as imperfect technologies. Two questions highlight shortcomings in the discussion of cybersecurity. The first is why, after more than two decades, we have not seen anything like a cyber Pearl Harbor, cyber 9/11, or cyber catastrophe, despite constant warnings. The second is why, despite the increasing quantity of recommendations, there has been so little improvement, even when these recommendations are implemented.

These questions share an answer: the concepts underlying cybersecurity are an aggregation of ideas conceived in a different time, based on millennial expectations about governance and international security. Similarly, the internet of the 1990s has become "cyber," a portmanteau term that encompassed the broad range of global economic, political, and military activities transformed by the revolution created by digital technologies.

If our perceptions of the nature of cybersecurity are skewed, so are our defenses. This report examines the accuracy of our perceptions of cybersecurity. It attempts to embed the problem of cyber attack (not crime or espionage) in the context of larger strategic calculations and effects. It argues that policies and perceptions of cybersecurity are determined by factors external to cyberspace, such as political trends affecting relations among states, by thinking on the role of government, and by public attitudes toward risk.

We can begin to approach the problem of cybersecurity by defining attack. While public usage calls every malicious action in cyberspace an attack, it is more accurate to define attacks as those actions using cyber techniques or tools for violence or coercion to achieve political effect. This places espionage and crime in a separate discussion (while noting that some states use crime for political ends and rampant espionage creates a deep sense of concern among states).[1]

Cyber attack does not threaten crippling surprise or existential risk. This means that the incentives for improvement that might motivate governments and companies are, in fact, much smaller than we assume. Nor is cyber attack random and unpredictable. It reflects national policies for coercion and crime. Grounding policy in a more objective appreciation of risk and intent is a first step toward better security.

[1] Colin S. Gray, "The Product: Strategic Effect," chap. 5 in *The Strategy Bridge: Theory for Practice* (New York: Oxford University Press, 2010), http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199579662.001.0001/acprof-9780199579662.

01

Outdated Ideas Guide Cybersecurity

Ideas from the 1990s still shape cybersecurity policy, but they are inadequate for a very different international environment. They reflect the ideas and aspirations of a different time. Cyberspace is a new terrain for conflict and it has not been well-mapped, but just as medieval cartographers were hampered by their belief that the earth was flat, cybersecurity is hampered by inaccurate beliefs about opponents and risk.

The driving principle of the internet's commercialization was that technology should be as untrammeled as possible. This helped to enable the rapid growth of globally connected networks, but it was predicated on a much less risky world where nations appeared to be in accord on democratic governance and market economies. Russia and China would be partners and friends, not opponents, in a liberal world order led by an unchallenged United States. However, many of the core concepts that shape our understanding of cybersecurity deserve reexamination. They are:

- The end of the Cold War began (to quote Francis Fukuyama) the "universalization of Western liberal democracy as the final form of human government."
- Governance is a shared responsibility. A new model of governance that substitutes a global stakeholder community for the traditional Westphalian model is best for this new space and will provide public goods.
- Cyberspace is borderless
- State and nonstate actors have equivalent capabilities for attack; nonstate actors are as powerful as states in cyberspace
- The greatest risks for cybersecurity come from potentially catastrophic attacks on critical infrastructure by terrorist or hostile states.
- Attribution is difficult.
- Self-interest will lead private actors to improve cybersecurity

This is not the world we are in today. What we face now is rejection of American hegemony and the liberal world order developed after 1945 and the appearance of assertive challengers who see cyber operations as a tool for gaining influence at the expense of the United States and its allies. In this environment, the old approach no longer works. Nonstate actors organized into a multistakeholder community provided light governance that did not get in the way of growth but also created the "Wild West" environment that nations have been quick to exploit and where

crime is largely unhindered. Imperfect software sold without liability quickened adoption and implementation, but contained many vulnerabilities that today make cyberspace a hacker's paradise. This minimalist approach was right for the creation of cyberspace, but it is time for change.

Initial policies for cybersecurity focused on terrorist cyber attacks on critical infrastructure—the famous "Cyber Pearl Harbor" of the 1990s, now modernized by some to "Cyber 9/11." People still talk about this although in more than 20 years, it has never happened. There have been only a handful of real attacks carried out by state actors that have been focused on a specific target, and limited in duration and effect.

Interviews with executives at leading internet companies found that they believe they are offering services that expanded democracy and allowed the best in humanity to be expressed, views entirely consistent with the beliefs of the 1990s. This unguarded optimism created an opportunity, however, for states and criminals to exploit the new media for political and criminal effect. Our infrastructure-centric view of cybersecurity was unprepared for this. The scope of cybersecurity needs to be broadened to include a range of malicious actions not envisioned in the 1990s.

Perceptions of the appropriate role for government in cybersecurity are also shaped by the powerful ideologies of the internet, which grew out of the millennial views of the relationship between citizen and state. In this view, civil society and the private sector would assume greater responsibility for supplying public goods, such as governance, and the Westphalian arrangement of international relations would decline in importance.[2] Yet the Westphalian system remains robust and largely intact and some observers ask whether the woeful state of cybersecurity reflects market failure, the inability of the market to deliver security. The market cannot inflict painful consequences on a sovereign state when it misbehaves. Policy reflects the failure to recognize the centrality of the state in offensive action and in enforcement, making cybersecurity a matter for international politics more than private action.

The history of cybersecurity policy in the United States reflects these conceptual shortcomings. Initial efforts were the domain of technologists, network operators, and administrators. Cybersecurity is still shaped by its network administrator heritage, with system administrators defending their own networks and perhaps forming ad hoc alliances to coordinate defenses. A focus solely on defending network is inadequate, however, in the face of well-resourced foreign opponents who face little or no risk of penalty. It creates a fragmented and reactive defense that provides opportunity and the initiative to attackers.

The Clinton administration's decision to commercialize the internet was implemented by two working groups. The first was the Secure Public Networks Working group, which focused on encryption policy and lawful access. The thinking was that if there was widespread use of encryption to protect data and authenticate users, this would provide online security. There was the problem of law enforcement access to encrypted traffic and the struggles over key

[2] James B. Stewart, "As a Guru, Ayn Rand May Have Limits: Ask Travis Kalanick," *New York Times*, July 13, 2017, https://www.nytimes.com/2017/07/13/business/ayn-rand-business-politics-uber-kalanick.html?rref=collection%2Fsectioncollection%2Ftechnology.

management and public key encryption that ultimately led to the decisions (despite resistance from the FBI and National Security Agency) to release strong encryption for public use.

Had the rapidly growing number of internet users chosen to use encryption for data and authentication, the security problems of the internet would have been much smaller, but at that time, encryption products were complicated to use, slowed performance, and in any case, the risks of online activity were generally under-appreciated in the initial years of internet growth.

The second working group was the e-Commerce working group, which actually laid the foundations of internet policy. It established five principles to guide government action in the development of electronic commerce in its foundational report, "The Framework for Global Electronic Commerce." These included principles that the private sector should lead and the internet should not be regulated, relying instead on industry self-regulation and private-sector leadership where possible; that undue restrictions on electronic commerce should be avoided and government should avoid imposing regulations; that governmental involvement should support and enforce a "predictable, minimalist, consistent and simple legal environment" and be limited to the protections for "intellectual property and privacy, prevent fraud, foster transparency, and facilitate dispute" to reflect "the needs of the new electronic age."[3]

The internet's commercialization was disconnected from larger discussions of international security. The Bush and Clinton administrations undertook a series of reviews to reexamine the challenges to American security after the Cold War. At the end of the Cold War, U.S. analysts reassessed the changing nature of threats to the United States, and a series of influential studies emphasized the risk of asymmetric attacks and the vulnerabilities of critical infrastructure and information technologies. These reports identified the principal sources of asymmetric threats to U.S. security as weapons of mass destruction and threats to the American "homeland"—its population and critical infrastructure—but information systems and the communications infrastructure were viewed as a specific area of vulnerability.

The first such report, issued by the Joint Security Commission in 1994, called the security of information systems and networks "the major security challenge of this decade and possibly the next century." This was followed by a 1996 Defense Science Board "Report on Information Warfare," which warned that national security increasingly relied on interdependent infrastructures that were vulnerable to cyber attack, and called for "extraordinary action" to defend against information warfare. A specially convened National Defense Panel's 1997 report concluded that asymmetric threats to the United States were increasing and becoming potentially more damaging. It emphasized that the United States would need to prevent a range of attacks targeted at the American population and economic infrastructure, including cyber terrorism.[4]

The most influential statement for cybersecurity was the 1997 Report of the Presidential Commission on Critical Infrastructure Protection (the Marsh Report), which provided the basis

[3] Office of the Press Secretary, *A Framework for Global Electronic Commerce: Executive Summary* (Washington, DC: White House, September 1997, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html.
[4] For another influential report, see National Commission on Terrorism, *Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism* (Washington, DC: GPO, June 2000), https://fas.org/irp/threat/commission.html.

for U.S. efforts to protect critical infrastructure. Many of the ideas that still guide cybersecurity—cyber Pearl Harbor, private-sector ownership of critical infrastructure, Information Sharing and Analysis Centers, public-private partnership—date from the Executive Order developed in response to the March Commission (EO 13010).

These reports did not foresee the challenges that would emerge from jihad, Russian revanchism, and China's aspirations, nor how opponents would take advantage of the global internet to damage the United States. To the extent to which they considered what we would now regard as cybersecurity, the reports emphasized asymmetric cyber attacks against critical infrastructures. This does not accurately reflect how cyber operations are used by our opponents, whose primary efforts have concentrated on espionage and crime and whose most damaging action have manipulated information online to achieve harmful political effect.

The focus on asymmetric attacks on critical infrastructure began to shift in 2007, when a series of damaging penetrations of major U.S. agencies by a foreign intelligence service capped a decade of Russian and Chinese intelligence successes in cyberspace against U.S. agencies and companies. In response, the Bush administration introduced the "Comprehensive National Cybersecurity Initiative" (CNCI) in September 2008.[5] While not comprehensive (the CNCI lacked an international strategy, for example) and so highly classified that at first it could not be shared with allies or companies, and despite its emphasis on actions to secure federal networks, the CNCI marked a major change in U.S. policy, with the abandonment of an ad hoc, market-based approach to cybersecurity.

The CNCI shape this second generation of cybersecurity policy. It called for improved federal organization, standards (for government networks), strengthening information sharing, developing a strategy for expanding research and the cyber workforce, and planning for the "coordination and application of offensive capabilities to defend U.S. information systems." While the CNCI came too late in the Bush administration to be implemented, many of its elements were carried over into the Obama administration. The CNCI raised the idea of a federal responsibility, in partnership with privately owned critical infrastructure companies, for improving the security of their networks. The Obama administration continued many of the CNCI initiatives and added a strong international element (an area where there was less contention over the role of government), and expanding transparency on offensive capabilities.

We now face a very different international security environment. The fear of nonstate actors launching crippling asymmetric attacks against critical infrastructures, expounded in the early 1990s, is wrong. Our most dangerous opponents are other nation-states. America's attackers in cyberspace are nation-states, not terrorists—Russia, China, Iran, and North Korea. They have the capabilities, the resources, and the intent to use cyber capabilities to damage the United States and its allies. They are ultimately responsible (either through their own actions or by inaction, failing to take steps against those who target the West) for the majority of harmful cyber actions. These opponents do not seek "cyber catastrophe." They use espionage, coercion, and crime to advance their aims (the most important of which is now the dismantling of the U.S.-led world order created after 1945).

[5] White House, "National Security Presidential Directive/NSPD-54," January 8, 2008, https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

U.S. politics also played a role in focusing cybersecurity on critical infrastructure protection. Tech companies—in the second Clinton administration and again in the 2012 legislative battle over cybersecurity regulation—were very eager to avoid being controlled in any way. Focusing cybersecurity on critical infrastructure was the path of least resistance for policymakers. A minimalist approach was the right policy for building the internet and for a time when international relations seemed to be heading to a cooperative rather than conflictual environment, but revisiting this decision is crucial for better cybersecurity.

02

States Are the Most Dangerous Actors

The primary source of risk in cybersecurity comes from conflict between states. For Russia and China, a questioning of the legitimacy of democratic institutions, the challenge to transatlantic hegemony, the politics of criminal states, and China's pursuit of economic power motivate the constant barrage of damaging cyber actions. For the United States and its allies, untrammeled espionage, even if justified, creates a sense of vulnerability among our opponents and allies.

Governments are the most dangerous and most active attackers in cyberspace. States remain the most powerful actors in the international system. States retain a monopoly on violence; those who disagree with this have likely not experienced the full range of violent capabilities available to a powerful state. That states usually choose not to use these capabilities reflect both prudence and, in the West, a certain timidity over the application of armed force.

Simply put, the primary threat comes from hostile states that seek to gain advantage from coercive actions in cyberspace. It is this sense that cyber attacks are destabilizing—not because of physical damage but because of the uncertainty they create, the inadequacy of existing policy tools and concepts, and a lack of clarity on how existing state practices applies to cyberspace, all compounded by an absence of effective defenses.

The most dangerous and damaging attacks required resources and engineering knowledge that are beyond the capabilities of nonstate actors, and those who possess such capabilities consider their use in the context of some larger strategy to achieve national goals. Precision and predictability—always desirable in offensive operations in order to provide assured effect and economy of force—suggest that the risk of collateral damage is smaller than we assume, and with this, so is the risk of indiscriminate or mass effect.

State Use of Cyber Attack Is Consistent with Larger Strategic Aims

Based on a review of state actions to date, cyber operations give countries a new way to implement existing policies rather than leading them to adopt new policy or strategies. State opponents use cyber techniques in ways consistent with their national strategies and objectives. But for now, cyber may be best explained as an addition to the existing portfolio of tools available to nations.

Cyber operations are ideal for achieving the strategic effect our opponents seek in this new environment. How nations use cyber techniques will be determined by their larger needs and interests, by their strategies, experience, and institutions, and by their tolerance for risk. Cyber operations provide unparalleled access to targets, and the only constraint on attackers is the risk of retaliation—a risk they manage by avoiding actions that would provoke a damaging response.

This is done by staying below an implicit threshold on what can be considered the use of force in cyberspace.

The reality of cyber attack differs greatly from our fears. Analysts place a range of hypothetical threats, often accompanied by extreme consequences, before the public without considering the probability of occurrence or the likelihood that opponents will choose a course of action that does not advance their strategic aims and creates grave risk of damaging escalation. Our opponents' goals are not to carry out a cyber 9/11. While there have been many opponent probes of critical infrastructure facilities in numerous countries, the number of malicious cyber actions that caused physical damage can be counted on one hand. While opponents have probed critical infrastructure networks, there is no indication that they are for the purposes of the kind of crippling strategic attacks against critical infrastructure that dominated planning in the Second World War or the Cold War.

Similarly, the popular idea that opponents use cyber techniques to inflict cumulative economic harm is not supported by evidence. Economic warfare has always been part of conflict, but there are no examples of a country seeking to imperceptibly harm the economy of an opponent. The United States engaged in economic warfare during the Cold War, and still uses sanctions as a tool of foreign power, but few if any other nations do the same. The intent of cyber espionage is to gain market or technological advantage. Coercive actions against government agencies or companies are intended to intimidate. Terrorists do not seek to inflict economic damage. The difficulty of wreaking real harm on large, interconnected economies is usually ignored.

Economic warfare in cyberspace is ascribed to China, but China's cyber doctrine has three elements: control of cyberspace to preserve party rule and political stability, espionage (both commercial and military), and preparation for disruptive acts to damage an opponent's weapons, military information systems, and command and control. "Strategic" uses, such as striking civilian infrastructure in the opponent's homeland, appear to be a lower priority and are an adjunct to nuclear strikes as part of China's strategic deterrence. Chinese officials seem more concerned about accelerating China's growth rather than some long-term effort to undermine the American economy.[6] The 2015 agreement with the United States served Chinese interests by centralizing tasking authority in Beijing and ending People's Liberation Army (PLA) "freelancing" against commercial targets.

The Russians specialize in coercion, financial crime, and creating harmful cognitive effect—the ability to manipulate emotions and decisionmaking. Under their 2010 military doctrine on disruptive information operations (part of what they call "New Generation Warfare"). Russians want confusion, not physical damage. Iran and North Korea use cyber actions against American banks or entertainment companies like Sony or the Sands Casino, but their goal is political coercion, not destruction.

None of these countries talk about death by 1000 cuts or attacking critical infrastructure to

[6] James A. Lewis, "Economic Warfare in Cyberspace," in *Special Report: China's cyberpower* (Barton, ACT: Australian Strategic Policy Institute, November 2014), http://sdsc.bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-03/sr74_china_cyberpower.pdf.

produce a cyber Pearl Harbor or any of the other scenarios that dominate the media. The few disruptive attacks on critical infrastructure have focused almost exclusively on the energy sector. Major financial institutions face a high degree of risk but in most cases, the attackers' intent is to extract money. There have been cases of service disruption and data erasure, but these have been limited in scope. Denial-of-service attacks against banks impede services and may be costly to the targeted bank, but do not have a major effect on the national economy. In all of these actions, there is a line that countries have been unwilling to cross.

When our opponents decided to challenge American "hegemony," they developed strategies to circumvent the risks of retaliation or escalation by ensuring that their actions stayed below the use-of-force threshold—an imprecise threshold, roughly defined by international law, but usually considered to involve actions that produce destruction or casualties. Almost all cyber attacks fall below this threshold, including, crime, espionage, and politically coercive acts. This explains why the decades-long quest to rebuild Cold War deterrence in cyberspace has been fruitless.

It also explains why we have not seen the dreaded cyber Pearl Harbor or other predicted catastrophes. Opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return. States are the only actors who can carry out catastrophic cyber attacks and they are very unlikely to do so in a strategic environment that seeks to gain advantage without engaging in armed conflict. Decisions on targets and attack make sense only when embedded in their larger strategic calculations regarding how best to fight with the United States.

There have been thousands of incidents of cybercrime and cyber espionage, but only a handful of true attacks, where the intent was not to extract information or money, but to disrupt and, in a few cases, destroy. From these incidents, we can extract a more accurate picture of risk. The salient incidents are the cyber operations against Iran's nuclear weapons facility (Stuxnet), Iran's actions against Aramco and leading American banks, North Korean interference with Sony and with South Korean banks and television stations, and Russian actions against Estonia, Ukrainian power facilities, Canal 5 (television network in France), and the 2016 U.S. presidential elections. Cyber attacks are not random. All of these incidents have been part of larger geopolitical conflicts involving Iran, Korea, and the Ukraine, or Russia's contest with the United States and NATO.

There are commonalities in each attack. All were undertaken by state actors or proxy forces to achieve the attacking state's policy objectives. Only two caused tangible damage; the rest created coercive effect, intended to create confusion and psychological pressure through fear, uncertainty, and embarrassment. In no instance were there deaths or casualties. In two decades of cyber attacks, there has never been a single casualty. This alone should give pause to the doomsayers. Nor has there been widespread collateral damage.

Electrical grids and power generation are a central concern for cybersecurity.[7] We have two

[7] An interesting examination of vulnerability and how it may be overstated can be found in Yang Yang, Takashi Nishikawa, and Adilson E. Motter, "Small vulnerable sets determine large network cascades in power grids," *Science* 358, issue 6365 (November 17, 2017), http://science.sciencemag.org/content/358/6365/eaan3184.

examples of such attacks in the Russian interference with Ukrainian power facilities. If we look at these from a strategic or political rather than technical point of view, the damage was temporary, lasting only a few hours. The Russians could have done more, perhaps, but they chose not to; they were sending a signal to the Ukrainians: "see what we can do."

There are unique features to these Ukrainian incidents. Russia had an advantage in its familiarity with the Ukrainian facilities from when Ukraine was part of the Soviet Union, but some researchers believe that the malware could be adjusted for use against other facilities. Russia and Ukraine are in a low-level war and have launched far more destructive and fatal artillery assaults against the civilian population, providing precedent and justification for a far more damaging cyber assault. This was the ideal scenario for "catastrophic" action, but the Russians chose not to do this. Their actions were not the ham-handed strategic bombing of the past but a surgical operation intended to produce psychological effect more than damage.

Stuxnet caused physical damage, but only to its specific target. There was no collateral damage outside the facility. Stuxnet was a complex, sophisticated, multipart attack requiring both engineering and programming skills, but also advanced espionage capabilities. It is best thought of as a destructive payload that affected only its specified target and a delivery vehicle, which was found on many computers around the world (allegedly the result of a programming error) but caused no damage. Stuxnet was a precise attack, the cyber equivalent of a precision-guided munition (PGM).

The actions against Estonia and leading U.S. banks used denial-of-service attacks. These do not involve gaining access to the target network, but flooding the receiving computers with data to overwhelm their ability to receive incoming traffic. It is a cyber equivalent of a noisy demonstration outside the front doors and intended to cause psychological pressure rather than damage. The effect of the Estonian attack is routinely exaggerated as crippling, when in fact it only restricted access to some banking and government services. Losing access to ATMs for foreign exchange transactions is not an existential threat.

North Korea's use of cyber operations has been to achieve coercive effect to support its strategic and diplomatic goals, not to cause physical damage or destruction. North Korea may lack the capability to cause destruction through cyber means. In some instances, banking data was erased and broadcast services were disrupted. Conversations with South Korean officials show they regarded these actions as political, intended for the North's leaders to signal defiance and hostility to the South.

Iran's efforts against Aramco (and RasGas) rendered thousands of computer hard drives unusable. The Iranians might have also been able to damage refinery control systems but were either unaware they had gained access to those systems or chose not to do so. The Aramco incident may have been for punishment or signaling, sending a warning and demonstrating Iranian capabilities.

All of the most significant cyber incidents—those that most closely resemble attacks—were carried out by state actors in support of their larger strategic aims. In each of these cases, states used precise, limited action to achieve political effect, not mass destruction or catastrophe. The attacks were carefully calculated and designed. All were violations of sovereignty; a few caused

tangible damage, while others produced intangible effect (erasing data) and coercive action. Even those attackers who were very capable chose to exercise restraint.

03

Misperception and Mirror Imaging

If something that is widely feared has never happened, it is useful to ask why, despite all evidence to the contrary, people fear it. There have been no attacks on critical infrastructure because states, who have the ability to carry out such attacks, have no interest in doing so without strategic justification, and because nonstate actors, who might be tempted to undertake such actions, lack the capabilities. Why people fear these attacks has to do with outdated concepts, changing social attitudes toward risk, and "mirror imaging."

Mirror Imaging the Threat

"Mirror Imaging" is a term intelligence analysts use for assuming that your opponents will act and think as you would. Mirror imaging meant that America has been caught off guard repeatedly, most recently when Russia hacked the Democratic National Committee, purloined emails, and then leaked them to create political turmoil. The Russians had used this tactic against opponents. The Russian action probably did not change the election outcome, but it certainly created uproar and confusion—and that was the Russian goal.

Neither the United States nor its allies know how to respond to this kind of attack. If this had been an attack that damaged critical infrastructure, the United States would have known what to do and it would have known how international law would apply. We need to be similarly prepared to respond to cyber actions intended to disrupt data or create cognitive effect. Coming up with such responses will not be easy—this is a new kind of conflict that does not fit the mold of military action, and opponents will be less bound by the rules designed to govern conventional armed conflict between states.

Does this mean we should stop trying to make American critical infrastructure a more difficult target for potential attackers to disrupt or damage? Of course not. We have seen Russia and Iran interfere with critical infrastructure as a way to intimidate, and they have (along with China) engaged in reconnoitering U.S. infrastructure to find vulnerabilities that could be used in conflict. A world that is more dependent on cyber-enabled devices and connectivity will require a different strategy to ensure public safety and security. This broader cybersecurity strategy will need to go beyond the critical infrastructure concepts created at the end of the twentieth century. Countries will need a full-spectrum cyber defense that looks at how to defend against information operations and state-sponsored cybercrime as well as possible attacks on critical infrastructure. The focus should be on the broader goal of protecting data from manipulation and developing punitive responses for attacks.

Risk in cybersecurity comes from larger political changes: a questioning of the legitimacy of democratic institutions; the pursuit of globalization and the ease of transborder access; the

challenge to transatlantic hegemony; and the politics of criminal states and China's pursuit of economic power. Cyber is the tool by which the tensions engendered by these changes are expressed. This is a very different environment from the one we expected at the start of the cyber age, and our policies would be more effective if they took this into account.

We can identify two sets of actual risk and two opportunities that could affect the strategic position of the United States. The first is the possibility that an opponent could use cyber attack to inflict massive harm on the United States. This could include crippling attacks on critical infrastructure or the military. The second is the possibility of long-term economy harm through the theft of intellectual property. This affects not only the domestic economy but the technological leadership that has been crucial to U.S. military strength. A less-examined risk (until recently) is the ability to produce cognitive effect in the American population, to affect popular attitude and beliefs, create turmoil and undercut support.

Truly damaging cyber attacks are a tool reserved for states. Covert or deniable actions that fall below the threshold of the use of force will appeal to them. Catastrophic attacks, especially against nuclear powers, will not. Even in armed conflict between two major powers, the goal of minimizing existential risk to the survival of the state will constrain them. No opponent wants a war that will lead to their destruction or prove so costly as to exhaust the state. Why then does the fear of catastrophe and cyber Pearl Harbor retain such salience?

Misperception of Cyber Risk

Everyone has seen depictions of violence and warfare, portraying explosions, shootings, rockets, and even nuclear explosions, but very few have seen a credible depiction of a cyber attack, making it difficult to conceptualize this new form of warfare. The lack of knowledge provides an ample canvas for our fears. There are many examples that point to an increasingly risk-averse America, including exaggerated fears of disease, shortages of essential resources, and decreased willingness to take business risk.[8] Our fears do not map to the reality of risk.

Americans became used to thinking in terms of catastrophe and massive strategic attacks during the Cold War. Nuclear war did not occur—partially through luck, partially as a result of defensive strategies that blended diplomacy and military power, and partially because of a reluctance among the possessors of nuclear weapons to unleash holocaust. The United States and its opponents shared (in private) a conviction that strategic nuclear war was unwinnable and perhaps unsurvivable. The ideas of nuclear war have carried over into cybersecurity with the use of the terminology of nuclear strategy and a lingering sense of vulnerability. However, cyber attack is not comparable to nuclear war in destructive effect or consequences.[9]

The Y2K episode contributed to the sense of cyber vulnerability. Y2K predicted disruptive computer failures at the turn of the century because of programming flaws in commercial

[8] Ben Casselman, "Risk-Averse Culture Infects U.S. Workers, Entrepreneurs," *Wall Street Journal*, June 2, 2013. https://www.wsj.com/articles/SB10001424127887324031404578481162903760052.
[9] For a review of the literature on social aspects of increased fear, see Frank Furedi, "The only thing we have to fear is the 'culture of fear' itself," Spiked, April 4, 2007, http://www.spiked-online.com/newsite/article/3053#.Wa6aZsaQzyM.

software. The effort to prevent Y2K, involving public-private partnerships, information sharing, and international collaboration, has become something of a template for cybersecurity. Ultimately, Y2K had no noticeable effect, but the idea that a single, systemic vulnerability could produce mass disruption became part of the lore of cybersecurity.

The attacks of 9/11 profoundly affected American perceptions of risk.[10] An embarrassing surprise attack by a tiny force cost 3,000 lives and produced the dramatic destruction of two large, symbolic buildings, accompanied by immense harm to the Pentagon. These images were replayed constantly on television, reinforcing the sense of vulnerability. Since 2001, the United States has become a more risk-averse society. These fears have been transferred to our perceptions of cyber attack,[11] and distort analysis and policymaking.

Reporting in the media distorts attitudes toward risk.[12] The media overemphasize hazards. For example, the recent "Wannacry" ransomware attack was called a crippling global cyber attack. Wannacry affected several hundred thousand systems, but this is out of a population of more than a billion connected devices. Media sensationalism is reinforced by public relations efforts, where companies find it advantageous to announce dramatic cyber attacks. In 2009, in response to the Conficker worm, the chief executive of a cybersecurity company announced in a major newspaper, "If you're looking for a digital Pearl Harbor, we now have the Japanese ships steaming toward us on the horizon."[13] An emphasis on violence and risk helps sell products and papers, and affects both policy and research.

The psychology of risk shapes cybersecurity.[14] The chances of an airplane crash are miniscule (perhaps 1 in 11 million), but if that airplane crashes the chances of dying in that crash is perhaps 1 in 20. The extreme outcome distorts our sense of what is an otherwise low-probability event. If our analysis of cyber attacks goes immediately to the extreme and we assume maximum effect, it leads to the kind of analysis that warns we risk "a global disaster sparked by cyber-attacks."[15]

How we collect information on cyber risk and how we assess its probability also alters our perception of risk. Cyber attacks have become front-page news, but the consequences are overstated, creating an atmosphere where the perception of risk is exaggerated. Cyber attacks have produced no deaths, no physical destruction, and have cost the economy only a fraction

---

[10] Nicholas L. Carnagey and Craig A. Anderson, "Changes in Attitudes Towards War and Violence after September 11, 2001," *Aggressive Behavior* 33, issue 2 (March/April 2007), 118–129, http://public.psych.iastate.edu/caa/abstracts/2005-2009/07CA.pdf.

[11] This is in part because many of the analysts who turned to cybersecurity were schooled in nuclear warfare.

[12] Paul Slovic and Elke U. Weber, "Perception of Risk Posed by Extreme Events" (paper presented at Risk Management Strategies in an Uncertain World, Palisades, NY, April 12–13, 2002), https://www.scribd.com/document/55025108/Slovic-P-2002-Perception-of-Risk-Posed-by-Extreme-Events.

[13] John Markoff, "Worm Infects Millions of Computers Worldwide," *New York Times*, January 22, 2009, http://www.nytimes.com/2009/01/23/technology/internet/23worm.html.

[14] Eugenia Cheng, "The Logic of Our Fear of Flying," *Wall Street Journal*, February 10, 2017, https://www.wsj.com/articles/the-logic-of-our-fear-of-flying-1486738105.

[15] Andrew Griffin, "Cyber Attacks on Satellites Could Spark Global Catastrophe, Experts Warn," *Independent,* September 21, 2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/cyber-attacks-on-satellites-could-spark-global-catastrophe-experts-warn-a7321361.html. See also Josephine Wolff, "How Would the U.S. Respond to a Nightmare Cyber Attack? The Danger of Overreaction Is Real," *Scientific American*, July 23, 2013, https://www.scientificamerican.com/article/how-would-us-respond-nightmare-cyber-attack/.

of a percent of national income. The real damage from cyber attack is political, with the effect on confidence in government and on relations between states, encouraging a sense of instability and unease that increases as our dependency on networked devices grows, but this is neither measured nor reported upon.

We overestimate the risk of cyber attack, and we misidentify the most likely targets. While the idea of nonstate actors launching a paralyzing cyber attack against critical infrastructures remains central to much of the discussion of cybersecurity, the majority of cyber incidents involve espionage, crime, or coercion by state actors and their proxies. A focus on protecting critical infrastructure led opponents to find other ways to inflict harm. That this has happened repeatedly reflects both the complexity of the terrain to be defended and the difficulty of agreeing to how to defend it.

The long-term trend is to undermine public confidence in online activities at a time when these activities are expanding. There is a clear erosion of confidence that creates economic harm and may erode stability.[16] But this long-term erosion, while damaging and a serious public policy problem, is not a crisis or a catastrophe.

[16] Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," Pew Research Center, January 26, 2017, http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

04

Cyber Operations and Interstate Conflict

International relations are being reshaped by the confluence of several powerful trends, some created by new technologies, some by the powerful reaction to American hegemony, and some from the fraying of the international order created after 1945. In contrast to sunny millennial optimism, efforts to improve cybersecurity must be designed for a period where, for an unknown duration, there will be increased conflict as states challenge the liberal postwar order. We are at the end of a sustained period of strategic stability[17] and conflict, albeit at low levels, will be the norm. Conflict between states will take new forms and cyber operations will be an important part of this. They are ideal for the new strategic environment, given their opacity, the lack of clear norms, and inadequate defenses.

Opponent actions that stay below this threshold inhabit a "gray area," that is neither peace nor war, where the United States and its allies, unable to use military force in response, have so far been stymied in designing and articulated an effective reply. Opponents will exploit gray areas in international law to coerce without triggering armed conflict. Deterrence will be more difficult in this opaque environment, and we will see increased use by our opponents of coercive acts that fall below thresholds for the use of force or armed attack.

The future of armed conflict is that major powers will try to avoid armed confrontation. Wars between big, heavily armed states are expensive and risky, particularly if they have nuclear weapons. The major powers will not renounce the use of force and coercion—Russia, the United States, China, Iran, North Korea, and others use force or the threat of force all the time—but they will try to avoid war with each other. If major powers do stumble into conventional war, cyber attacks will be a part of the fighting, but the real nature of cyber conflict involves something other than warfare and lacks the sharp discontinuity between war and peace. The experience of the last decade suggests that the norm for interstate conflict will be increasingly continuous and not kinetic.

Cyber techniques are a new way to exercise national power. Opponents will exploit gray areas in international law and practice to do damage without triggering armed conflict. Cyber operations are an important part of the new strategic environment where the United States has advantages in its ability to conduct military and espionage operations and disadvantages in its weak cyber defenses.

This will not be a new "Cold War"—the world is too interconnected for that, nor will it be World War Three. Even without nuclear weapons, major combat operations against an advanced opponent are risky and expensive. Cyber operations give countries a new way to implement existing policies rather than leading to new policies or significant shifts in strategy. There are no

[17] Stability means there is no incentive for a country to seek change through force or coercion.

examples of a nation acquiring cyber capabilities and then abruptly changing its strategy. In fact, the benefit of cyber operations is that coercion can be applied while minimizing the risk of armed response. Deterrence will become harder and impossible in some conflictual situations, and we will see increased use of coercive acts that fall below the existing threshold for the use of force or armed attack.

Military Use of Cyber Attack

The first known cyber attacks used for coercive effect took place during the Serbian campaign of the late 1990s. These were primitive actions and were more like harassing pranks than military assaults. Since then, there have been perhaps a half dozen publicly known incidents that rise to the level of attack and can be used to assess effect. A review of these known incidents suggests that the scope and risk of damage in cyber attack has been overstated. We can put cyber attacks in perspective by measuring the effect on income, national power, and public confidence.

Cyber attack will be used to shape the battlefield in advantageous ways by manipulating information to shape opponent perceptions and decisions. Trickery, ruse, and stratagem have always been part of the commander's portfolio. Genghis Khan pretended to retreat to lure opponents into ambush. Eisenhower used inflatable tanks and radio signals that mimicked a huge force to persuade the Germans he would invade somewhere other than Normandy. Cyberspace creates a new dimension for this age-old military technique.

The most likely targets of cyber attack in armed conflict are weapons, sensors, and communications, not critical infrastructure. Many major U.S. weapons systems have been hacked, including aircraft, drones, air and missile defense systems, and naval vessels. What has been done to the United States is also likely to have been done to others. Leading cyber powers have undertaken operations to gain access to opponent weapon systems software, to understand their operational limits, perhaps to copy them, and to provide the possibility to interfere with their operations in combat. A cyber attack may produce obvious damage, but a sophisticated attacker would avoid a noticeable failure and instead interfere with performance just enough to degrade it.

Tampering with opponent weapons and sensors is an important military objective. Corrupting weapon software prior or during battle would significantly degrade performance. Illicit access to the software could take place during production, or when the weapon is temporarily connected to a network. In the field, radars provide a useful entry point, even if the radar is not attached to the internet. Radars receive a signal, process it, and then pass it through a dedicated network to another system, operator, or weapon. A signal transmitted to a radar receiver could introduce malicious code or data that could degrade sensors, weapons, or command systems. Cyberwarfare will blend electronic warfare and its exploitation of opponent signals with cyber attack and the disruption of opponent software programs and computer systems to produce damage and effect that go far beyond conventional electronic warfare.

In conflicts involving advanced powers, we should expect to see cyber attack combined with electronic warfare, antisatellite attacks, informational campaigns, and other unconventional

tactics and weapons. Cyber, jamming, and kinetic attacks against space assets have been tested by several nations, and other countries are developing antisatellite operations that rely on cyber attack to degrade space services (such as navigation or communications). Opponent intent will be to degrade the American "informational advantage," to degrade communications and intelligence, surveillance, and reconnaissance (ISR) assets and capabilities, in order to damage decisionmaking and operations.

Civilian infrastructure is not the most likely target. While there is extensive literature on the effect of cyber attacks on critical infrastructure, this discussion is often disconnected from realities of conflict and based on abstract and hypothetical scenarios. The reason to attack critical infrastructure is to disrupt military-industrial capabilities. In a long war, this may provide advantage. Some also argue that cyber attack against critical infrastructure will lead to political chaos, just as early theorists of air power incorrectly assumed that bombing would lead to panic. However, conflicts, particularly involving great powers, will be not "to the death." They will be fought with forces already in existence, and using supplies and munitions already built. Disrupting industrial capacity will not change the outcome of a conflict. Disrupting logistics for resupply would be useful, but such attacks will also focus on military targets or commercial services under contract to the military rather than purely civilian targets not involved in the conflict. In nuclear parlance, cyber attacks are likely to be "counterforce" rather than "counter value."

The attacks on Aramco, Sony, various South Korean entities, Canal 5, and the Sands Casino generally resemble each other in technique, delivery, and effect. Each required only moderately advanced skills and relied on variants of black-market malware, meaning they could be duplicated by attackers with moderately advanced skills and resources. This has not happened. Nor, in each case, was there any collateral damage. These were not random acts by unknown assailants but state actions intended to intimidate while avoiding the use of force or causing physical damage or destruction. We can expect our opponents—Russia, China, Iran, and North Korea—to continue to experiment with intrusion to manipulate data and interfere with services as they seek to maximize their national goals, but they will do this in the context of their national strategies and objectives, their perception of risk in the international strategic environment, and their desire to avoid armed conflict.

Stuxnet involved precise targeting that resulted in limited collateral damage. The attack itself had two elements: the "delivery vehicle," which spread to system around the world, and the "payload," which affected only centrifuges in an Iranian nuclear facility. Despite hyperbolic predictions that Stuxnet had opened "Pandora's box" for cyber war—since the spread of the delivery vehicle malware around the world (apparently a programming error) made its code readily available for copying—the attack has never been duplicated. These predictions were wrong. Stuxnet used both a deep knowledge of industrial control systems and advanced tradecraft for acquisition and insertion of the malware that most states and all nonstate actors are unable to duplicate. The attack was precise, elegant, and unrepeatable.

Another attack known to have caused physical damage involved an unnamed German steel mill. This attack used a conventional delivery vehicle (apparently a phishing ploy). The malware was able to spread from the business network to the industrial control systems, leading to the loss of

control of a blast furnace and causing major damage to the plant. However, there was no collateral damage. German authorities investigating the attack said that the attack itself required a deep understanding if industrial control systems. While the delivery mechanism is commonly used by cyber criminals and could easily be duplicated, the same is not true for the 'payload" that did the actual damage.

Cyber as a "Weapon"

We often talk about cyber weapons but the analogy is imprecise. Calling cyber attack a weapon is an easy shorthand, but it is inaccurate. Opponents will use cyber techniques to deliver effect on target, but it is too limiting to confine ourselves to kinetic parallels in predicting this effect. If we use conventional measurements of weapons' effectiveness, the cyber "weapon" provides precision capabilities and has long range and high speed, but effect and consequences can vary in both duration and damage depending on the attacker's intent.

It may be better to think of cyber attack as an "exploit" rather than a "weapon," a combination of tactics and technologies to penetrate opponent systems and achieve the desired effect, whether this is crime, espionage, or disruption. The most damaging cyber attacks have a high degree of precision. The trend in weapons development for the last several decades has been away from broad, indiscriminate effects and toward greater precision in striking specific, intended targets. Commanders prefer precision weapons because they provide economy of force and greater predictability of effect.

In this, we can think of cyber attacks as a kind of digital precision-guided munition, unlikely to have indiscriminate effect. A cyber weapon must usually be tailored for the specific network or device it is targeting, and by "tailor" we mean code written specifically to exploit a vulnerability in the programs the target network or device is running. System configuration can vary widely, limiting the effectiveness of a cyber attack designed for one system but used against another. Some kinds of cyber attacks, such as the destruction of servers or other network devices, or of critical infrastructure providing service to a broad population, pose greater risk of collateral damage, but these only provide limited military advantage.

One implication of this is that the benefits of "entanglement" can be overstated. Entanglement is the idea that opponents will be deterred from launching cyber attacks because they will experience harm as well as the target. But since the most damaging weapons are also the most precise, entanglement will not restrict their use. For better or worse, the leading cyber powers have gained enough experience and skill through practical experience in the last decade that they are unlikely to make mistakes in targeting.

Cyber attacks are designed to exploit a particular configuration and set of vulnerabilities in the target computer system. Attacks on critical infrastructure require "adversaries to become intimately aware of the process being automated and the engineering decisions and design of…the system."[18] Attackers target systems through a sequence of efforts that enables access

[18] Michael J. Assante and Robert M. Lee, *The Industrial Control System Cyber Kill Chain* (Bethesda, MD: SANS Institute, October 2015), https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

and provides the information to create effect. A cyber attack requires a sequence of efforts to enable access and provide "targeting" information before the "attack" is launched. Attacks have several stages: gaining access, reconnaissance to identify target vulnerabilities, developing code tailored to damage or disrupt, delivering the software "payload," and then "triggering" it—all without being detected. An attack requires more than a single breach.

A major attack can take several months to prepare and involves reconnaissance of the target network, "weapons" development (writing or modifying code to damage or disrupt, affect, circumvent defenses if they exist), probing the target network and inserting and executing the attack. While disruptive software is widely available in cyber black markets, the ability to launch damaging cyber attacks is limited to only a few countries. Even if the sophistication of black-market software increases, the rationale for its use will not change, meaning that even if more countries acquire some increased level of cyber capability, they are unlikely to go on the rampage.

The most damaging attacks have been carried out by well-organized and resourced state actors.[19] This pattern is consistent across damaging cyber attacks. Groups like ISIS or al Qaeda have not launched damaging cyber attacks and there is no evidence that they have acquired or are acquiring these capabilities. Every year for more than a decade, there have been predictions that terrorist groups would turn to cyber attack. The law of averages suggests that eventually this may be right, but for now cyber conflict falls outside nonstate capabilities.

Once the attack has been carried out, an astute defender can close vulnerabilities. This may limit the useful life of an exploit, creating what some call "single use" attacks. "Single use" assumes opponents will react and take defensive action; this is not always true in the civilian world, where known vulnerabilities can persist for months or years. Additionally, the software that runs industrial control systems or other hardware can be difficult to patch or modify to eliminate known vulnerabilities. In these circumstance, far from being single use, cyber exploits are often reused, sometimes after slight modification. Attackers, however, do not know if they will have other opportunities and the least-risk approach is to strike first. The greatest benefit of damaging cyber attack could come in the opening phase of conflict. The tempo and duration of conflict also affects use. In a short, intense conflict, early single use may be best, but the preferred targets will not be critical infrastructure. Disrupting command and control, logistics, and weapons performance in the opening states of conflict may provide immediate and irreversible benefit by placing an opponent at a disadvantage from which they may be unable to recover. In contrast, disrupting infrastructure will not reduce combat capabilities or provide immediate battlefield advantage, and the effects of disrupting infrastructure may not appear in time to change the outcome of a conflict.

Future conflicts between states will not involve "total war." They will be limited in intensity and scope, given their cost and the risk of escalation, reducing the value of mass attack on civilian targets. Drawn-out counterinsurgency operations in Iraq and Afghanistan (or the civil wars in Libya and Syria) have involved a minimal use of force against irregular forces. Disrupting millions

[19] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Bethesda, MD: SANS Industrial Control Systems, March 2016), https://ics.sans.org/media /E-ISAC_SANS_Ukraine_DUC_5.pdf.

of consumer devices might produce only marginal and short-lived military advantage, perhaps slowing mobilization (noting that it is no longer 1914 when war required mass mobilization of civilians). Attacks that disrupted logistics support or the supply chain of key expendable munitions could be attractive but this would not require the kind of mass attack against the general economy used in the past. An attack that disabled software for an entire class of weapons (such as an F-35 or Patriot) would produce military advantage, but would not harm critical infrastructure or other civilian targets.

Mass Effect

We need to distinguish strategic effect from mass effect, as the two are not the same. Cyber attacks could produce mass effect against a number of targets, but the strategic benefit from these actions is doubtful. It is possible to achieve certain kinds of mass effect through cyber attack—the early history of cyber incidents is replete with worms that infected millions of machines. Early hackers sought to make public statements to win the admiration of their peers. These early efforts at mass effect achieved this notoriety, but it did not produce strategic benefit or criminal returns.

The ghost of these early global network infections haunts cybersecurity, but as software products and cyber defenses have slowly improved, and as law enforcement has been able to penalize hackers, these simple mass attacks also became more difficult and dangerous for the kind of hackers who would be attracted to carrying them out. These sprawling incidents like Love Bug or the Morris Worm that produced largely annoyance are increasingly a thing of the past. Their modern equivalent is ransomware, which can be spread virally and affect thousands of machines. So far, ransomware attacks have been criminal in intent. These programs encrypt data on a victim's computer and demand a payment for decryption. Some examples, such as disruption at a global shipping company, suggest that ransomware could be used in conflict.

Many kinds of cyber attacks—such as the destruction of network devices or of critical infrastructure providing service to a broad population—provide only limited strategic advantage. Malware that exploited a shared vulnerability in consumer software to erase data or disrupt functionality could have mass effect, as could an attack aimed at disrupting core internet infrastructure. But in neither case is it clear that such an attack would produce military or political benefit, making it more of an annoyance than an ultimate weapon. Recent ransomware attacks have had mass effect, but produced neither catastrophe nor strategic benefit, given their relatively brief duration and the difficulty of translating the disruption into physical effect. None of these attacks changed the fundamental balance of power between victim and attacker and would serve only to increase, however slightly, the risk of countermeasure or retaliation.

Mass effect could be produced by attacks on specific targets, such as interfering with a control software to trigger a regional blackout similar to the (accidental) 2003 Northeast blackout, or recreating the 2010 "flash crash" for financial networks. The military benefits of this kind of mass disruption are difficult to calculate and rely on a string of worst-case assumptions about public reaction and interdependence. These "panic in the streets" scenarios mirror the 1930s expectations about aerial bombardment leading to riots and political collapse when in fact nothing of the kind occurred. States are unlikely to engage in these minimally destructive mass

attacks as they would not degrade an opponent's military capabilities and would almost certainly provoke a damaging response.

The spread of cyber-enabled devices (the "internet of things," or IoT) increases the possibility of mass effect and even fatalities. However, to create a large number of fatalities, hackers would need to exploit simultaneously a flaw in critical systems found in multiple devices. This poses operational challenges in planning, implementation, and coordination that decrease the likelihood of occurrence. A series of improbably scenarios—hackers adjust thermostats or ovens to cause houses to burst into flame, or force all cars to stop at once—have been advanced, but these do not deliver strategic benefit. If it were possible to affect a large number of medical devices simultaneously, it might produce fatalities, but the military advantage from this is small since the affected population would be the elderly, the weak, or the sick. Given their lack of value for strategic objectives and their political implications, such mass attacks are unlikely to appeal to any state.

An attacker could seek mass effect by attacking the global financial network or the internet infrastructure—large global networks where an attack affects thousands or millions of targets simultaneously—but only in the most improbable scenario would this kind of mass attack lead to an opponent's defeat or impede his ability to retaliate. It would be unappealing to our opponents to engage in actions that are provocative but do not produces victory or reduce the risk of retaliation. The usual argument is that these attacks would create panic or turmoil and rests on a set of dubious assumptions about how societies respond to attack.

Russia and China are unlikely to attack the financial infrastructure as it would be akin to breaking their own piggy-bank. For others, it would create a powerful and most likely fatal reaction from the international community Attacking the internet backbone would be appealing only if an attacker were confident in their ability to operate national networks independent of the internet (a goal that China and Iran are pursuing). In all instances, an attacker would need to be confident that it could avoid or withstand retaliation and decide that systemic disruption would produce long-term advantage.

An attacker would also need to be confident that the victim would not be able to retaliate and that it could avoid or withstand any retaliation. These would be bold assumptions about a nuclear-armed power. In these circumstance, perhaps the only likely attacker who might be tempted would be North Korea, since it has the least to lose, but broad global attacks do not fit with North Korea's strategy of regional provocations to support coercive diplomacy.

There is no doubt that many computer networks are very vulnerable to attack, but a high degree of network or computer vulnerability, while creating great risk for an individual company, does not translate into a strategic vulnerability that degrades national security, given the difficulties of launching simultaneous, perfect attacks and the ability of a target to react and respond to limit damage. Analyses oriented on technical vulnerabilities miss the bigger picture. From a strategic or military perspective, attacks that do not degrade national capabilities are not significant and, as they will not cripple an opponent, do not reduce the risk of retaliation and escalation.

A massive cyber attack that would have even a chance of crippling a developed nation would require intense preparation and extensive resources beyond the scope of all but three or four

nations. Even then, a cyber attack would not produce the same effect as nuclear or conventional strikes; cyber "weapons" are not as damaging and some targets may not experience full damage. One lesson from strategic bombing is that "no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary."[20] The need for persistence will affect an opponent's calculation of risk: a single cyber attack will not be crippling, and a series of attacks invites retaliation.

Recognizing this lets us set limits for the coercive effect of threatening a cyber attack. The target, if not given to hysteria, may well calculate that they would not only survive a cyber attack (in contrast to a nuclear attack) but would be able to continue to use their military forces and be able to restore economic activity. Of all the possible strikes—missile, air, ground forces—cyber may be the least threatening of these options if target countries have made minimal steps to prepare their defensive response.

This helps explain why cyber terrorism is unlikely. Cyber attacks do not produce the political and psychological effects desired by terrorists and which they expect their acts of violence to produce.[21] Groups like ISIS or al Qaeda have not launched damaging cyber attacks, and there is no evidence that they have these capabilities. Cyber attacks are unappealing, in that they produce little in the way of violence. Every year for more than a decade, there have been predictions that terrorist groups would turn to cyber attack. The law of averages suggests that eventually this may change, but for now cyber conflict falls outside nonstate capabilities.

Similar constraints militate against cybercriminals becoming attackers. They have some capability, though not enough, and no intent. They hack to gain money and are eager to avoid determined pursuit. The extensive toolsets sold on the black market are designed to gain access and extract value. The release of NSA tools by an unidentified third party was most likely part of a larger Russian information warfare campaign aimed at the United States rather than inadvertent release, and so far, the damage from this release, in strategic or macroeconomic terms, has been minimal. It is interesting to note that while Russia uses cybercriminal groups as proxy forces (most notably in Estonia and Georgia), the most significant Russian cyber actions in the last few years have been carried out by government services, either the FSB (Federal Security Service) or the GRU (Russian Military Intelligence).

Techno-anarchist groups also lack the capability but might be more likely to acquire it. The trajectory of the group "Anonymous"—dramatic, but relatively inconsequential hacks (accompanied by heavy public relations efforts), then intense law-enforcement activity, followed by the collapse of the group and imprisonment of its leaders—suggests that if tempted, anarchist groups would have only brief initial success.

Damaging attacks required skill levels not generally available to private actors. Since the most damaging attacks have been the most precise, this suggests that those skilled enough to deliver such attacks are also skilled enough (and concerned enough) to avoid collateral damage as they contemplate designing an attack. This likely reflects the requirement to tailor damaging attacks

[20] U.S. Strategic Bombing Survey, 1945 European War, http://www.anesi.com/ussbs02.htm.
[21] "Do terrorists really think they're going to win?," BBC, November 25, 2015, http://www.bbc.com/news/magazine-34909636.

to target specific software and systems—the best cyber weapons are "bespoke," designed to damage a specific target with little or no chance of indiscriminate effects.

Cyber powers have command and control structure to prevent inadvertent use. If anything, there has been a degree of caution in the use of the new tools. With somewhat less confidence, we can also assume that these cyber powers ensure that the design of their attacks minimizes the risk of collateral damage that could escalate any conflict. They could intentionally launch a series of cyber attacks that could have destabilizing effect, but so far, cyber powers have largely avoided incidents that could produce escalation or military conflict. Tripping into inadvertent cyber war is unlikely.

Clausewitz warned that war does not consist of a single, instantaneous blow but of course, in strategic nuclear war, it did. Nuclear war produced the "catastrophic" effect now attributed to cyber attack, and in contemplating the nuclear threat, our thinking about resilience and strategic benefit have been distorted. The concept of catastrophe has been diluted to the point of absurdity. In 1990, catastrophe meant the deaths of tens of millions of people and the complete destruction of cities in less than an hour. Now, it means going without lights for a few days.

Achieving Strategic Effect

Mass effect and strategic effect were wedded in the mid-twentieth century when militaries acquired that ability to inflict massive damage from the air. We need to disengage mass effect and strategic effect, however, if we are to better understand the use of cyber attack. Strategic effect requires crippling an opponent's military forces or economy, or perhaps creating political chaos. Strategic effect makes it difficult for an opponent to continue resistance, usually as the result of physical destruction or damage. What is new in cyber conflict is the pursuit of long-term strategic effect by undermining an opponent's political institutions and ability to govern. While cyber operations can provide valuable military effect at the tactical or operational level, strategic effects come from political operations, not through mimicking kinetic attack on critical infrastructures. Concern about catastrophic attack is overstated because of both operational difficulties in creating catastrophe and because of strategic considerations that make it unlikely that opponents will begin a major war.

Most cyber incident are not attacks. Most are criminal acts, usually fraud or theft, and accomplished without violence. The difficulty in defining what qualifies as a cyber attack makes it difficult to apply the existing remedies found in international law. This lack of precision has brought tremendous confusion to the discussion of cyber war," and it is helpful, drawing on the UN Charter, to consider the concepts of use-of-force (Article 2/4) and armed attack (Article 51).

Very few cyber incidents qualify as the use of force. Most of what we call cyber attacks involve theft or manipulation of data. Sustained attacks to cripple economies, like the strategic bombing of World War II, are also unlikely—the discussion of cyber attack too often ignores both changes in the nature of warfare and larger geopolitical environment. A broad attack on civilian targets in the homeland of a nuclear-armed state creates existential risk of the attacker.

Many cyber incidents, such as the actions against Estonia in 2007, were coercive acts intended to intimidate but did not involve the use of force or cause damage or destruction. There is a gray area in the definition of the use of force—if an attack erases data or software, there is destruction, albeit of an intangible object. Deciding whether a "gray area" incident qualifies as an attack involves measuring the scope, duration, and effect of the data and service disruption.

Straightforward measures allow us to assess the strategic effect of cyber incidents, by measuring the effect on income, national power, and public confidence in the targeted state. The most important of these measures is to gauge whether a cyber incident reduces military power or economic performance. Another would be to ask if there is tangible damage, either in human casualties or in destruction. Finally, we need to assess "cognitive effect," the use of cyber techniques by opponents to create political damage. A standard for strategic effect would be an action that threatens "territorial integrity and political independence" of a state. Focusing our analysis on strategic effect allows us to distinguish between incidents that are damaging to the victim and those that pose serious risk to states.[22]

The simplest definition of strategic effect would be that one side is compelled to cease resistance and make the preponderance of concessions in any conflict termination. Strategic effect could also be gaining significant advantage over an opponent that makes them less able to resist in future conflict and more likely to make concessions. The most extreme case would be that the defeated state no longer survives. Cyber attacks' value at an operation level is unquestionable, but except against the most pusillanimous opponent, it will not produce strategic effect.

Cyber actions that disrupt military command systems could have strategic effect in armed conflict by reducing the overall capacity of an opponent to resist, but attacks on civilian economic targets or critical infrastructure against even moderate-sized states might not be effective. We no longer rely on huge conscript arms and mobilization of entire national economies, nor are wars likely to involve prolonged bouts of intense conflict. Interconnected global supply chains are also harder to disrupt.

One essential aspect of this limitation is the inherent resilience of even less-developed economies. Resilience is often overlooked, so it deserves particular emphasis. If there is to be victory, what must be destroyed is not infrastructure but an opponent's will to resist. In this, the Russian doctrine focusing on producing cognitive effect may be more astute than traditional military strategies that seek to destroy industrial capabilities. Let us consider one example.

In the 1980s, the United States engaged in a covert war with a small Marxist state. Using proxy forces, it attacked the electric grid and the nation's only oil refinery. It occupied large areas of territory. It mined the only major harbor, assaulted local police and security forces, and made its displeasure known in a variety of other ways. The Marxist state was not popular with many of its citizens, and it relied to a considerable degree on force against much of its own population to maintain its hold on power. This created a steady supply of recruits for the American proxy force and created a degree of sympathy within country for U.S. actions. This was not a developed economy, and the war led to blackouts, fuel shortages, the collapse of manufacturing, and (in

[22] Gray, "The Strategy Bridge: Theory for Practice" Oxford Scholarship Online, September 2010.

combination with Marxist economic policies) a drastic fall in income. But despite inflicting considerable harm, it took nearly a decade to dislodge the rulers. No cyber attack could match these effects and it is wishful thinking to ascribe powers equal to strategic bombing or nuclear weapon to cyber attack. It is harder to defeat a nation than it looks.

The nuclear precedent, conscious or not, strongly influences thinking about cybersecurity and the effect of cyber attack. For example, a recent report asserted that "Large scale cyber-attack…could cause chaos by disrupting the flow of electricity, money, communications, fuel, and water."[23] This assertion raises two issues: the feasibility of such an attack and the likelihood that such disruptions would lead to "chaos."

The assumption that service disruptions will produce chaos is very doubtful. Nothing of the kind happened in the aerial attacks of the 1940s or afterwards. Instead, the result was a stiffening of resistance. The evidence for chaos from disruption points to other variables than the effect of the attack. The 2003 blackout of the Northeast United States did not produce chaos. Hurricane Katrina did, Hurricane Sandy did not. In reviewing these natural disasters, the key variable for determining the likelihood of chaos is strength of governance.[24] A competent government can muster the resources and support to maintain control in the face of disruption. Seeking to create crippling political chaos would succeed only against an incompetent government incapable of taking the steps needed to preserve order.

Fragile societies (like Czarist Russia) may collapse, as could societies under the immense pressure of prolonged war, like Wilhelmine Germany, but in most cases in the last 60 years the response of the victim to such attacks is anger, increased resistance, and a desire for retribution. An astute attacker would seek to avoid creating such resistance. Violence (or the threat of violence) to achieve a political end. The goal is not only to eliminate opponent capabilities, but to convince opponents to no longer resist. Violence is not random but serves some larger purpose. This is the lens through which we should view cyber attack.

Can cyber attacks put at risk the survival of the state?[25] The immediate answer is no. Advanced cyber attacks, such as those damaging military command or critical infrastructures, are likely to be used by an attacker the same way they would use any other weapon. This implies a high degree of caution for cyber attacks outside of armed conflict. Coercive acts that stay below a level that is likely to trigger retaliation will be more attractive to opponents. The ability to use cyber operations to create political turmoil is a better way to strategic effect than attacking critical infrastructure.

---

[23] Defense Science Board Task Force on Cyber Deterrence, *2017 Cyber Attack Deterrence: Developing Scalable Strategic Cyber Capabilities, Resilience of U.S. Nuclear Weapons, Attribution* (Washington, DC: Department of Defense, February 2017), 2, https://www.amazon.com/2017-Cyber-Attack-Deterrence-Capabilities/dp/1520777469.
[24] James A. Lewis, "Critical Infrastructure Protection and Cyber Terrorism: Mass Destruction or Mass Annoyance?," in *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, ed. Anja Dalgaard-Nielsen and Daniel Hamilton (New York: Routledge, 2006).
[25] "The bottom line of security is survival [of the state]." Barry Buzan, "New Patterns of Global Security in the Twenty-First Century," *International Affairs* 67, no. 3 (July 1991): 431–51.

05

Political and Strategic Constraints on Cyber Attack

Analysts began speaking of a cyber Pearl Harbor in the early 1990s. In this scenario, computer attacks on critical infrastructures would produce catastrophe. Concern over this kind of event provided the impetus for the 1998 Marsh Report and reappeared as recently as a 2017 Defense Science Board Report. A cyber Pearl Harbor has not occurred, not because a tactically damage surprise attack is impossible, but because the opponents capable of such attacks chose not to launch them.

This international security environment imposes strategic and political constraints on the use of cyber attack. To say that Russia has developed new "cyber weapons" that can cause a massive disruption to the electric grid should be unsurprising. Russia already has such weapons. They are called atomic bombs. Understanding why the Russians, even under Putin, are reluctant to use atomic bombs can help our assessment of cyber catastrophe and opponent decisionmaking.

Nuclear weapons are complex, expensive instruments. They provide certainty in their destructive capabilities, but states are reluctant to use them. This reflects both a fear of retaliation and also implicit understandings that guide state thinking on nuclear weapons, the most important of which may be an unwillingness to be the first to use a nuclear weapon in a conflict.

Tacit norms and the risk of retaliation reduce the likelihood of nuclear attack.[26] These norms grow from a general repugnance created by nuclear weapons' immense destructive effect, whose horror is increased by fears over lingering radiation that could spread beyond the victim's territory. These are truly horrible weapons. If we contrast cyber attack and nuclear weapons, we can ask if the less-horrific nature of cyber attack, their relative cheapness compared to strategic nuclear forces, and the prospective (albeit decreasing) advantage of covertness make it more likely that our opponents will choose to use cyber attacks. While the nuclear precedent provides a flawed guide for understanding cybersecurity, it is useful for considering how nations make strategic decisions about entering into conflict with another state.

The context for such decisions has changed markedly. The wars of the last century pitted great powers against each other in existential conflicts involving mass mobilization, global scope, and long duration. These will not be repeated. They include massive attacks on critical infrastructure,

[26] There is a larger debate over the strategic context for North Korean decisions, but as long as the Kim Jon-un regime believes that nuclear use would create an existential threat that it would be unlikely to survive, it will seek to use its nuclear arsenal for symbolic and coercive purposes.

which make little sense outside of existential conflict. Nuclear weapons have reduced the chances of major war between nuclear-armed powers and their allies. Even conventional war may be too costly in most circumstances. The constraints of cost and destructiveness create caution, but also create a space for actions that fall below the threshold of armed attack, a space for which cyber operations are ideally suited.

Future armed conflicts are likely to be localized, not all-out affairs, given their cost and the risk of escalation to the point that could threaten the existence of the state. The drawn-out operations against insurgents in Iraq and Afghanistan and the civil wars in Libya and Syria do not pose existential threats to major powers nor do they involve the use of overwhelming force to achieve conclusive victory. These conflicts may be protracted but inconclusive and involve limited forces rather than the full range of national capabilities. Additionally, most of America's opponents have regional objectives and will seek to avoid escalating conflict by attacking the U.S. homeland. In some scenarios, an attacker may miscalculate that an attack on specific civilian critical infrastructure would be justified. Turning off the electricity in Pearl Harbor, Washington, or Brussels at the onset of conflict might seem justified, even though such actions would be unlikely to degrade U.S. or NATO military capabilities. The attacks on critical infrastructure hypothesized by many analyses are more likely to appear as too risky to foreign opponents, of limited benefit to their goals, and perhaps irrelevant in terms of achieving the desired strategic outcomes of undermining U.S. hegemony and building regional dominance without armed conflict with the West.

The Ukrainian power disruption points to how states might use attacks on critical infrastructure—not as a massive blow intended to produce crippling effect, but as a demonstration intended to warn an opponent. The attacks on the Ukrainian power grid were intended as a signal, something demonstrated by the fact that these disruptions were not sustained. A widespread disruption of long duration would not be seen as a signal but as an escalation of the conflict. Interference with critical infrastructure is more likely to be of short duration and reversible, to signal and punish while avoiding escalation.

State opponents—Russia, Iran, China, North Korea—weigh the benefits of cyber attack against the risk of retaliation. They likely calculate that a cyber attack on civilian critical infrastructure would not degrade the major opponent's ability to retaliate forcefully or violently. Opponent efforts are designed to avoid U.S. retaliation by staying below the threshold of what could be considered an armed attack, use of force is an implicit threshold opponents are unwilling to cross. Cyber attacks are not horrible in effect, and norms do not militate against their use, but there is a parallel to nuclear weapons in that the risk of retaliation constrains potential attackers and shapes their calculation or the risk and benefits of cyber attack.

If it was possible to use a cyber attack to simultaneously cripple strategic forces and launch a massive attack on critical infrastructure, an opponent might be tempted, but this would require a high degree of certainty that all strategic delivery systems could be taken offline by a cyber attack. This is unlikely, and it is more probable that a cyber attack will not be 100 percent effective. Some targeted weapons or systems will still operate. Saying that the United States can only shoot 50 missiles at your capital instead of 100 is not much of a comfort. In a larger armed

conflict, this kind of reduction in enemy tactical capabilities can be valuable, but if the goal is to attack without fear of retaliation, it is insufficient.

This upper bound on cyber attack is affected by the likelihood of attribution. If an attacker was confident that it could avoid having the attack attributed to it, the risk of retaliation would be reduced, making some attacks more attractive. Uncertainty about attribution capabilities, particularly American capabilities, combined with uncertainty about the effectiveness of cyber attack, creates caution. Public expressions of uncertainty about attribution are not shared by opponents, who know when they have been caught. Over the last decade, the United States has made a major effort to improve its attribution capabilities and has succeeded to the point where no opponent can be confident about anonymity and this, if linked to truly credible threats to impose consequences, may finally produce the cyber deterrence so long sought by the United States.

The implicit threshold governing cyber attack is the line between force and coercion. With very few exceptions, states have avoided cyber actions that could be judged as the use of force, based on international understandings on what actions qualify as the use of force or armed attack. Opponents have engaged in cyber actions below this implicit threshold with impunity, but they are reluctant to cross it for fear of creating a situation that they cannot control. In this, cyber incidents are more like border incursions or bandit raids than attacks.

Public sources suggest that at least seven countries have used cyber tools for coercive purposes. However, they have been careful to avoid anything that could be interpreted as the use of force, and they have avoided physical destruction or casualties. This suggests that countries prefer actions that advance their strategic goals without creating unmanageable risk of escalation into armed conflict. Opponents calculate the advantage they would gain from an attack against the potential cost. Miscalculation is possible, but if anything, opponents appear more likely to overestimate the risk of retaliation.

A cyber attack that would produce strategic effect greatly increases the risk of retaliation that could put the existence of the state or its current government at risk. Catastrophe scenarios assume that opponents will calculate mass attack against civilian targets in the United States would not trigger retaliation, an assumption that is likely to strike opponents as improbable. A cyber attack that minimizes the risk of retaliation will seek to avoid mass effect, particularly if this effect is irreversible or of long duration. States will develop cyber techniques that produce coercive effect and political advantage without crossing thresholds that could lead to a forceful response.

Opponents will weigh the operational benefit from a cyber attack against the risk of escalation in considering what targets to attack. One factor that weighs upon all of them is the immense capacity of the United States to inflict punishment and judging from their behavior, Russia, China, Iran, and North Korea's strategies will seek to minimize or avoid the risk of U.S. retaliation. In this, they are comforted by a belief in U.S. strategic clumsiness, which makes coercive operations that stay below the threshold of the use of force more attractive. Cyber attack is ideal for this, if used against the right targets—those that provide political or military benefit while minimizing the risk of escalation.

A Case Study in Constraint: North Korea

The heightened tension over North Korea's (DPRK) missile and nuclear weapons programs, combined with growing DPRK cyber capabilities and their occasional use for coercion or theft, has led some analysts to conclude that the North is preparing to launch a catastrophic cyber attack against the U.S. financial system or electrical grid. A sophisticated analysis would attempt to place this decision by the DPRK's leader in a larger strategic context. Several assumptions guide this analysis. First, the primary objective of the North Korean state and the Kim family is regime survival. Someone who is worshiped as a god-king by millions, controls immense personal wealth, and has unchecked power will be loath to put this at risk.

North Korea is both cautious and cunning in its use of force, including cyber attacks. It is willing to take provocative actions that flout international law and norms, but these have been limited in scope and effect, intended to shape and advance North Korea's diplomatic agenda vis-à-vis South Korea (ROK) and the United States. These actions also serve to reinforce the regime's narrative among its domestic population of an encircled North, an evil but defeatable hegemon, and heroic resistance. Its policy goals, in addition to regime survival, are to create political conditions that would cause the United States to leave the peninsula, disrupt the U.S.-Japan alliance, and improve its position in the region. It uses threats and provocative actions not to attack opponents but to manipulate opinion among ROK and Japanese leaders on the utility of alliance with the United States and the benefits of concessions to the North.

North Korean cyber capabilities, while improving, still have not reached the level that would allow them to duplicate the effect produced by Stuxnet or the Russian attack on a Ukrainian power facility. The DPRK can disrupt data and services using variants of malware available on the cybercrime black market and could likely produce a result similar to the Iranian attack against Aramco (and there may be a link between the DPRK and Iran in developing cyber capabilities). The North has been successful only against poorly protected targets (of which there are many), suggesting that there is a relatively low ceiling for its cyber attack capabilities.

In general, it is not in the North's interest to start a war with the United States, since the Kim regime would not survive. The DPRK's nuclear program is driven by fears of regime change, and Kim does not wish to share the fate of Saddam Hussein or Muammar Gaddafi, dragged from their hiding places and killed. The North will use violent rhetoric and low-level provocation to shape U.S. and ROK policies and to advance its policy goals while seeking to avoid armed conflict.

North Korean cyber attacks against a hardened target, like the U.S. military, would not degrade U.S. retaliatory capabilities sufficiently to ensure regime survival. Attacks on critical infrastructure in the United States would also not degrade U.S. military capabilities. A major cyber attack by the North on civilian targets in the American homeland would likely be interpreted by the United States as justifying a violent response. In no instance would a major cyber attack against the United States leave North Korea better off militarily or increase its chances of survival.

The North does engage in cyber reconnaissance, and there is an extensive discussion of the hypothetical risk that espionage could be confused for the precursor to attack. However,

reconnaissance itself is not indicative of attack preparations unless it is accompanied by an increased tempo of reconnaissance activities and changes in military posture and readiness level. To date, the North has not miscalculated how much it can get away with in its provocations and it is hard to see why this would change, absent some extreme situation, to a point where a suicidal attack would make sense.

The North's isolation and ideology increase the risk that it could miscalculate how much it could get away with in a provocative action against the United States, but the risk of miscalculation is counterbalanced by the North's assessment of U.S. capabilities (including its ability to attribute the source of an attack) and intentions. The current U.S. administration is more volatile than its predecessor and this provides a degree of protection.

In extremis, if regime survival was in jeopardy, the North might be tempted to try a major cyber attack against civilian infrastructure, but this calculation would be shaped by the expectations of Korean leaders on how this would affect the condition of conflict termination. Using major cyber attacks to improve the conditions to conflict termination to make them more favorable to the North would be a desperate strategy and the effect of a cyber attack against the United States might be to worsen the terms of conflict termination rather than improve them. In any case, *in extremis* attacks would occur only after major armed conflict had begun.

The alternative scenario, that North Korea is a crazed opponent eager to attack the United States and possessing destructive cyber capabilities. This is cartoonish and not supported by the North's pattern of behavior seen since Kim Jong-un assumed power. Cyber attack is not *sui generis*, but another tool for a state to advance its larger strategic interests and it is in this strategic context that we are best able to assess the risk of catastrophic North Korean cyber attacks.

06

Rethinking the Principles for Cybersecurity

Cybersecurity rests on an intellectual foundation created more than two decades ago. Its core concepts reflect the assumptions of the 1990s about the future of international relations, threats to national security, and evolution of governance in a digitally connected world, but they are inadequate for understanding the problem of cybersecurity as it has actually evolved. A more accurate set of concepts upon which to base policy are:

- Many technology users still neglect to take the most basic protective measures, and the widespread use of pirated software in some countries amplifies the costs of neglect. Absent incentives (either market or regulatory) this will not change.

- Improvements in technology can shift the nature of attacks, but cannot prevent them and confer advantage equally to defender and attacker.

- States are the most powerful actors in cyberspace and dominate offense. Private defenses are overmatched by state opponents. Nonstate actors, unless they are proxies of a state, lack the tools to achieve strategic effect from cyber attack.

- Governments see cyberspace as a largely unconstrained space for action, and a few governments actively support cyber criminals. The actions of greatest concern have involved espionage, crime, and political coercion—not attacks on critical infrastructure.

- Our opponents reject universal political values and seek to remake the U.S.-centric international order, emphasizing sovereignty in cyberspace, and use cyber actions as an ideal tool for this new conflict.

- Cyberspace has borders and states (both democracies and authoritarians) are developing technologies that let them assert sovereign control and define boundaries; this will reshape the environment for security.

- Attribution is increasingly easy, particularly when dealing with repeated attacks. This creates the potential for changing opponent calculation of the risk of an attack in ways favorable to the defender.

- Cyber attacks cannot produce catastrophic results, nor is it a decisive weapon that can determine the outcome of a conflict. We can dismiss the idea that terrorist or nonstate actors will launch massive and damaging cyber attacks.

- The use of cyber attacks will stay below the threshold of the use of force, in order to avoid escalation to larger and more damaging conflicts. States will avoid destructive attacks on critical infrastructure and instead prefer to use the manipulation of data and opinion to achieve coercive effect.

From Critical Infrastructure to Cognitive Effect

Perceptions of cyber attack are shaped by the precedents of strategic bombing and nuclear war. We need to move away from kinetic precedents in explaining cyber conflict. Strategic bombing sought to destroy critical infrastructure using mass attacks to reduce an opponent's ability to resist. Much of the thinking on cybersecurity assumes that current opponents will also target critical infrastructure, duplicating aerial bombardment or nuclear attack through cyber means, but the rationale for massive crippling attacks on critical infrastructure no longer exists. Strategic bombing was linked to a theory of how to achieve victory by destroying the economic and political underpinnings of an opponent's war effort. Cyber attacks against critical infrastructure would not have the same effect, making them unattractive to those states capable of carrying them out.

Strategic bombing, using conventional munitions, even of the most savage kind, did not lead opponents to surrender or cease military operations. In contrast, nuclear weapons create existential risk. At the height of superpower nuclear deployments, an all-out (or "strategic") exchange would have killed hundreds of millions and destroyed entire cities in minutes. Even clashes between adversaries' conventional forces or the limited use of nuclear weapons brought unacceptable risks of escalation to an all-out exchange. The demonstrably existential risks created by strategic nuclear weapons created a perilous stability in the global contest between the victors of the Second World War.

The golden age of nuclear strategy began in the mid-1950s and its central concepts—escalation management and deterrence—were established by the 1970s. Policy and strategy were driven by technological change. In the case of cyber attack, technological and political change has outstripped the conceptual framework applied to American strategy. Efforts to force cyber attack into nuclear paradigms create analytical imprecision.

Nuclear war threatened catastrophe, but the pursuit of similarly catastrophic cyber attack is unlikely to appeal to our opponents. They will prefer alternative techniques. Cyber attack can shape the battlespace, enhance surprise, and create new fields for maneuver, but a massive attack against a nuclear power runs the risk of generating an unsustainably damaging response. Opponents will seek to avoid this risk. Cyber operations provide a new way to achieve military and perhaps strategic advantage, but this will not come from some cyber equivalent of the mass bomber raids of World War II. We need concepts that capture the cognitive and informational aspects that will dominate cyber conflict in the future.

While cyber attacks can produce effects similar to kinetic weapons, their intangible effects can be more important. There is an informational and cognitive element involving the manipulation of information and decisionmaking that is more likely to produce strategic effect and place opponents at a disadvantage. This cognitive approach will challenge conventional, kinetic-

oriented strategies, but it is not a new concept, with the classics of strategy emphasizing the importance of affecting opponent thinking and will as "the ultimate determinants in war." The political and psychological effects of cyberspace technologies provide an ideal vehicle for creating psychological effect in both domestic audiences and foreign opponents, allowing opponents to manipulate how and when decisions are made.

Cyber operations provide a new way to use force, to coerce, or to gain intelligence advantage, but the aspect of cyber as an instrument of national power that is least appreciated is its cognitive and informational capacity. Cyber is most useful in creating uncertainty among opponents. An astute opponent might only need to affect a limited penetration to create a high degree of uncertainty, recognizing that using an easily detectable penetration to create uncertainty and fear would hamper the ability to carry out more damaging penetrations—the target might move to a heightened state of defense as a result.

The targets in cyber conflict will be data, algorithms, and cognition, not just critical infrastructures. Data manipulation and interfering with algorithms are both ways to affect directly decisionmaking and achieve cognitive effect (where the friction of war and politics is expanded to make an opponent weaker and more vulnerable).

The error of any fixed defense is in constructing powerful obstacles to block an opponent's expected line of attack; opponents attack elsewhere. As we focus on protecting critical infrastructure, our opponents found other ways to inflict harm and gain advantage. That this has happened repeatedly reflects the complexity of the terrain to be defended in cyberspace, and also the difficulty of agreeing to how to defend this terrain when the discussion is shaped by outdated concepts regarding the role of governments and the nature of international conflict.

Better cybersecurity in critical infrastructure is necessary, but not sufficient. The two most damaging attacks against the United States (Sony and the Democratic National Committee) did not target infrastructure. As our use of the internet reshapes how we think and affects human cognition, and as machines increasingly obtain the ability to make decision based on advanced, self-learning algorithms, the new emphasis in cybersecurity will be to defend against the manipulation of thought processes, data, and emotion to achieve cognitive effect.

Technology Will Not Save Us

The phrase "technology changes too fast" is a slogan devised in the 1990s to avoid regulation, but when it comes to cybersecurity it may be more accurate to say that technology does not change fast enough. One fundamental problem for security is that the network and computing technologies we use are still relatively primitive. They contain many vulnerabilities and even more vulnerabilities are created when these systems are linked together. This asymmetry between defense and offense is exacerbated by the scale of what must be defended—millions of machines with millions of lines of code that may contain an exploitable error—and because the incentives for attackers to discover vulnerabilities is much greater than the incentive for producers to find and fix them. This asymmetry will not change for some time.

Technologies that benefit defenders also benefit attackers. We can expect improvements in the defensive technology, driven by the trends that shape the larger IT market place, such as data analytics, artificial intelligence, and cloud services, as well as novel technologies for monitoring, isolating threats, using virtual spaces, and better controlling data. The problem with relying on technological advances to improve cybersecurity is that they work just as well to improve attacks, especially for the advanced hackers found in government agencies and leading cybercrime groups. There is no silver bullet for cybersecurity and a "Cyber Manhattan Project"[27] to build new technologies will not work. Solutions must be found in strategy, policy, and the actions that derive from them.

The industrial revolution made technological change a factor in conflict and competition among states, producing a constant back and forth in the balance between offense and defense, with new technologies bringing advantage to one side, forcing the other to adjust tactics, operations, and weapons. In cyberspace, the technological advantage lies with the attacker. This has been the case for cybersecurity, but it need not remain this way. Having the best technology does not ensure superiority if the thinking on how to use that technology is outdated.

Rebalancing Public and Private Action

A minimal role for government, which grew out of the millennial views of the relationship between citizen and state, has been part of the ideology of the internet from the start.[28] These millennial beliefs now serve to hamper policymaking. The central questions for policy are how to shape private actions to improve cybersecurity, how to do this in a way that does not impose undue burdens and costs or stifle innovation, and how to best use the "instruments of public power." The answer will vary from country to country, but countries that develop effective and efficient models for the government's role in cybersecurity will have an advantage in a digital world.

Cybercrime is an example of the need for a new approach. It is transnational, putting the best cybercriminals out of the reach of national law enforcement. Cybercrime hides behind sovereign immunity, making it impossible to arrest and convict criminals unless they leave their sanctuary. Sanctuary and state support allow some of these groups to develop or acquire truly advanced capabilities and these sanctuary states use cybercriminals for political purposes. As long as a few countries provide sanctuary for cybercriminals and use them as proxies (or in some cases, use state employees as cybercriminals), there will be only limited progress in reducing cybercrime. Companies must defend themselves against it, but lowering the crime rate requires governmental actions

The United States relies on a blend of voluntary action, market forces, public-private partnerships, and regulation for cybersecurity, but the interplay between public and private action is more complex than in the past. The innovators in national cybersecurity policy have moved to different organization models, creating new cyber-specific agencies, clarifying and

[27] Marc Goodman, "We Need a Manhattan Project for Cyber Security," *Wired*, January 21, 2015, https://www.wired.com/2015/01/we-need-a-manhattan-project-for-cyber-security/.
[28] Stewart, "As a Guru, Ayn Rand May Have Limits."

limiting that new agency's responsibilities to work the private sector to respond to incidents and improve defenses. Other countries are also more assertive in intervening when there is an incident at a company or in requiring companies to keep the government informant on breaches and other incidents.

Defense in the Gray Zone

The need to revise our understandings on the appropriate roles for the private sector and government are one challenge for any reconceptualization of cybersecurity. How we think about our relations with other states also needs to change from one based on an assumption of cooperation to one based on an assumption of conflict. The crux of the cybersecurity problem is international—foreign governments are the most dangerous attackers and are skillful in using cyber techniques in ways that damage the United States and its allies without creating the risk of traditional warfare.

We will see increased use by our opponents of coercive acts that fall below implicit thresholds for the use of force or armed attack. Opponent actions that stay below this threshold inhabit a "gray area," which is neither peace nor war, where the United States and its allies, unable to use military force in response, have so far been stymied in designing an articulated and effective reply. The benefit of cyber operations is that coercion can be applied while minimizing the risk of armed response. Opponents will exploit gray areas in international law to coerce without triggering armed conflict. Deterrence will be more difficult in this opaque environment. Deterrence will become harder and impossible in some conflictual situations, and we will see increased use of coercive acts that fall below the existing threshold for the use of force or armed attack.

Progress in international negotiations on cybersecurity remains slow. This is unlikely to change absent some truly compelling global crisis (creating existential threat for national survival, such as occurred in the Cuban Missile Crisis). There has been endorsement of general norms by UN member states, the most important of which embed cyber attack in the existing framework of international law, including the law of armed conflict. However, significant disagreements have emerged in the last two years (reflecting the general deterioration of the international security environment). In the absence of an existential threat from cyber, progress on reaching broader agreement on stability and security is unlikely, given the more confrontational policies adopted by Russia and China in the last few years.

This new security environment creates a much more complex landscape for negotiation. A more finely graded diplomatic strategy could take advantage of public statements and private messages of retaliation to affect opponent calculations. To warn potential opponents and to reassure the American public, the president should make a public statement that clearly lays out that the United States would respond forcefully, using cyber means, to incidents where a foreign power used cyber operations against the United States for coercive effect.

Agreement on norms will not change opponent behavior unless opponents believe the norms have teeth. Adversaries do not fear the consequences of malicious cyber action. The United States and its allies need to change this opponent assessment that the risk of committing

below-the-threshold use-of-force cyber operations is acceptable by imposing consequences for malicious action. A few retaliatory actions to show that the threat of counteraction was serious would reset the boundaries of the permissible for opponents.

To be clear, this means that a defensive effort is inadequate for better cybersecurity—a strategy that does not impose consequences on attackers is inadequate—and the United States and its allies will need to retaliate for cyber attacks. There is some risk that this could lead to an escalation of conflict, but the alternative is to continue to endure constant malicious cyber action. In any case, given the desire of our opponents to avoid direct armed conflict with the United States, the risk of escalation by opponents to retaliatory cyber attacks is low. There is reason, judging from the effect of sanctions on Russia, Iran, North Korea, and China, to expect that retaliatory acts below the use-of-force threshold can have this effect without escalation or tit-for-tat exchanges.

Imposing consequences is legitimate under state practice and international law, and a norm adopted by the 2015 Group of Governmental Experts (GGE), which holds states responsible for actions taken from their territory even if they are not the parties undertaking the action. An example would be if a country found its ships being raided by pirates who had a base in a neighboring country, it could ask the hosting nation to close the pirate base and try the pirates. If the hosting country refused, the victim nation could go to the Security Council or invoke its right to self-defense to take action against the pirates. For cybersecurity, if the location of the attacker can be determined, a country could request assistance. If the hosting country was incapable of taking action, the victim country could offer a joint action or build capacity in the hosting nation. If the host country refused to cooperate in good faith, imposing consequences would be legitimate. The victim country would need to be willing to share compelling evidence and the host country would need to demonstrate a good-faith effort to find the perpetrators.

The current administration's policy is to seek bilateral agreements with like-minded nations on consequences for malicious cyber actions that contravene the norms agreed to by the UN Group of Government Experts (GGE). These GGE reports define the nature of malicious cyber action by placing them in the context of existing international law and state practice, and lay out the responsibilities of states for taking action against cyber attacks. The intent is to link norms to deterrence, by demonstrating that there will be consequences for norms violations. The focus of the effort is not on creating new norms, but on implementing and enforcing existing norms. This approach has some support among key allies, but implementation will be challenging.

First, agreement to collaboratively impose consequences will require agreement on the level of attribution needed to assign culpability. Many allies will not accept a simple assertion by the United States that it knows the source of an attack, and the United States may be reluctant to share the methods by which it made its determination. States will be reluctant to impose consequences on another nation in the absence of compelling information that justifies their actions. Recurrent calls for an institution (like the International Atomic Energy Agency [IAEA]) to conduct impartial investigations into cyber attacks and identify their source discount the certainty that any such institution would face insurmountable political problems. The desire to have an impartial body of experts examine cyber attacks and determine who is responsible is

understandable, but these proposals underestimate the difficulty of creating an impartial process.

To be effective, a policy of imposing consequences for malicious cyber actions needs to be part of a larger diplomatic strategy for cybersecurity if it is not to become a series of tit-for-tat exchanges. First, there should be a public doctrine that makes clear that an attacked state will respond in a manner consistent with international law. This public doctrine should lay out general thresholds that will trigger response and identify the degree of proportionality that will apply, making clear that responses will be roughly proportional and use the full range of countermeasures (retaliatory actions that do not involve the use of force) available to the United States. Third, the policy should be coordinated with allies, and the recent development of a "Cyber Diplomatic Toolkit" by the European Union offers an opportunity for coordinated action.

Agreement on consequences requires agreement on a portfolio of appropriate responses. Efforts to use indictments and sanctions can be effective tools for dissuasion and there is scope for the United States to work with the European Union and it new "toolbox" of responses, which allows for the imposition of sanctions by the European Union in response to malicious cyber activities.[29] Consequences that go beyond such countermeasures (i.e., actions that stay below the threshold of use of force) may be seen as disproportionate and may not win support from allies or the broader international community. The United States and its allies need to develop a range of new responses that include responses that are painful, but reversible and temporary and that do not involve the use of force

Indictments and sanctions can be effective, but when there is sufficient confidence in the attribution of culpability, the most effective response may be a proportional counter action using cyber techniques to reduce the chance of escalation. Even warning adversaries of the adoption of a new policy of retaliation could have a beneficial effect. It may seem counterintuitive to say that a more active approach could produce stability, but there are precedents from arms control to support this. Stretching historical precedent, we could even look back to the response to the Barbary pirates, where limited naval action ultimately led to treaties ending pirate attacks.

Consequences will have more effect if they are multilateral and in every previous effort to establish norms and consequences, the United States has taken a multilateral approach. The issues, whether in a bilateral or multilateral format, will be agreeing on the level of evidence necessary to identify a violation of norms and agreement on suitable consequences. The focal point for agreement among likeminded nations should be on the multilateral imposition of consequences for norms violations, the level of evidence required for this, and the nature of an appropriate consequence. For other nations, the immediate negotiating goal should be clear understandings of what those norms are and what would be considered violations that would trigger the imposition of consequences, while the long-term goal should expand the circle of

[29] Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?," European Union Institute for Security Studies, July 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_24_Cyber_sanctions.pdf.

likeminded to leading, eventually, so some kind of formal consensus on the nature of responsible state behavior in cyberspace.

Concern about escalation should not lead to timidity or indecision. This is a contest of wills and our opponents will use threats to bluff us into continued inaction. However, the same political constraints on the conduct of warfare that hamper the U.S. ability to respond to opponent cyber actions using its military forces will also hamper them. For a better defense, the West will need to become more comfortable in operating in the "gray zone" that our opponents now inhabit. Escalation is managed by clarity in messaging and by diplomatic engagement (either direct or indirect) with the attacker. The goal is to change opponent thinking about the utility of cyber attack at levels below the use of force and to reshape the negotiating environment; no one will negotiate (or stop) if they do not believe there is risk, and cyber attackers believe that as long as they stay below the threshold of the use of force, cyber attack is risk free.

Imposing consequences for malicious cyber action enters difficult terrain when it comes to considering how to respond to the use of action to create cognitive effect. States have considerable practice in deciding what is a reasonable and proportional response for kinetic actions, but not for cyber actions that fall in the gray area created by this new kind of conflict.

07

Moving to a New Paradigm

Cybersecurity is a child of the 1990s. The technological and ideological views that dominated much of the discussion of cybersecurity are inadequate for effective policy. Progress requires us to take into account a more conflictive international environment, albeit conflict that does not meet the expectation of the twentieth century. It also requires a more forceful role of the state in defense, accompanied by experimentation with new models for cybersecurity governance.

We need to broaden our definition of cybersecurity to expand the scope of cybersecurity to look at its informational and cognitive aspects. Whether we call it "cyber" or "digital revolution," every aspect of social and economic activity has a cyber component in ways not expected in the 1990s offering broad scope for malicious action. Technological and political changes are reshaping cyberspace and the ways that people interact with it. The old distinctions between cybersecurity, internet governance, and privacy are disappearing as digital technologies play an increasingly central role in society and business. Our concept of cybersecurity must expand to defend this new environment.

It takes time for new technologies to reshape how we wage and think about conflict. It took two decades to develop effective doctrine for tanks and aircraft carriers, and we are at the early stages of developing concepts for cognitive effect. Nations will experiment, tactics and technologies will change, and our cyber defenses must be ready for this.

Cybersecurity is a central part of this challenge to governance and stability that comes from the digital revolution that is "beginning to transform the structure and organization of society and communities in deep ways."[30] Change will be slow absent some crisis that threatens the existence of states, but our actions can begin to reshape the cyber's environment in positive ways. To improve cybersecurity, we need to change the ideas that underpin it. Effective policy requires a new conceptual framework to understand and respond to the digitization of governance and conflict, and to counter our enemies as they are and not as we once expected them to be.

[30] Philip Zelikow, "Is the World Slouching Toward a Grave Systemic Crisis?," *Atlantic*, August 11, 2017, https://www.theatlantic.com/international/archive/2017/08/zelikow-system-crisis/536205/.

About the Author

James Andrew Lewis is a senior vice president at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes a broad range of assignments. He led the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civilian and military technologies. He worked on presidential policies for arms transfers, commercial space remote sensing, on policies to secure and commercialize the internet, and on encryption and lawful access to communications. He was the Commerce Department lead for national security and espionage related to high-technology trade with China.

Lewis was the rapporteur for the UN Group of Government Experts on Information Security for the successful 2010, 2013, and 2015 sessions. He has led long-running Track 1.5 discussions on cybersecurity with the China Institutes of Contemporary International Relations. Lewis has authored numerous publications since coming to CSIS on a broad array of topics, including innovation, space, information technology, globalization, deterrence, and surveillance. He was the director for CSIS's Commission on Cybersecurity for the 44th Presidency. He has testified numerous times before Congress. Lewis's current research examines the effect of technology on warfare and how the internet has changed politics. He received his Ph.D. from the University of Chicago.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.**csis**.org

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

4501 Forbes Boulevard
Lanham, MD 20706
301 459 3366 | www.**rowman**.com