Nuclear Lessons for Cyber Security?

Nuclear Lessons for Cyber Security?

Joseph S. Nye Jr.

Identifying "revolutions in military affairs" is arbitrary, but some inflection points in technological change are larger than others: for example, the gunpowder revolution in early modern Europe, the industrial revolution of the nineteenth century, the second industrial revolution of the early twentieth century, and the nuclear revolution in the middle of the last century.[1] In this century, we can add the information revolution that has produced today's extremely rapid growth of cyberspace. Earlier revolutions in information technology, such as Gutenberg's printing press, also had profound political effects, but the current revolution can be traced to Moore's law and the thousand-fold decrease in the costs of computing power that occurred in the last quarter of the twentieth century.

Political leaders and analysts are only beginning to come to terms with this transformative technology. Until now, the issue of cyber security has largely been the domain of computer experts and specialists. When the Internet was created 40 years ago, this small community was like a virtual village of people who knew each other, and they designed an open system with little attention to security. While the Internet is not new, the commercial Web is less than two decades old, and it has exploded from a few million users in the early 1990s to some two billion users today. This burgeoning interdependence has created great opportunities and great vulnerabilities, which strategists do not yet fully comprehend. As Gen Michael Hayden, former director of the CIA says, "Rarely has something been so important and so talked about with less clarity and less apparent understanding [than cyber security]. . . . I have sat in *very* small group meetings in Washington . . . unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of *any* decision we might make."[2]

Joseph S. Nye Jr. is the University Distinguished Service Professor and former dean of Harvard's Kennedy School of Government. He received his bachelor's degree summa cum laude from Princeton, attended Oxford University as a Rhodes Scholar, and earned a PhD in political science from Harvard. He has served as assistant secretary of defense for international security affairs, chair of the National Intelligence Council, and a deputy undersecretary of state. He is best known for developing and expounding on the term *soft power* in a number of articles and books.

Governments learn slowly from knowledge, study, and experience, and learning occurs internationally when new knowledge gradually redefines the content of national interests and leads to new policies.[3] For example, the United States and the Soviet Union took decades to learn how to adapt and respond to the prior revolution in military affairs—nuclear technology after 1945. As we try to make sense of our halting responses to the current cyber revolution, are there any lessons we can learn from our responses to the prior technological transformation? In comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy. After a short overview of the problem of cyber security in the next section, I will suggest several general lessons and then discuss a number of international lessons that can be learned from the nuclear experience. While the two technologies are vastly different, as I will argue below, there are nonetheless useful comparisons one can make of the ways in which governments learn to respond to technological revolutions.

Cyberspace in Perspective

Cyber is a prefix standing for computer and electromagnetic spectrum–related activities. The cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign jurisdiction and control. This aspect of the Internet is not a traditional "commons." It also has a virtual or informational layer with increasing economic returns to scale and political practices that make jurisdictional control difficult. Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer. Cyber power can produce preferred outcomes *within* cyberspace or in other domains *outside* cyberspace. By analogy, sea power refers to the use of resources in the oceans domain to win naval battles on the oceans, but it also includes the ability to use the oceans to influence

battles, commerce, and opinions on land. Likewise, the same analogy can be applied to airpower.

The cyber domain is a complex man-made environment. Unlike atoms, human adversaries are purposeful and intelligent. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off by throwing a switch. It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier task forces and submarine fleets create enormous barriers to entry and make it possible to speak of American naval dominance. In contrast, the barriers to entry in the cyber domain are so low that nonstate actors and small states can play significant roles at low cost.

The Future of Power describes diffusion of power away from governments as one of the great power shifts of this century.[4] Cyberspace is a perfect example of this broader trend. The largest powers are unlikely to be able to dominate this domain as much as they have others like sea, air, or space. While they have greater resources, they also have greater vulnerabilities, and at this stage in the development of the technology, offense dominates defense in cyberspace. The United States, Russia, Britain, France, and China have greater capacity than other state and nonstate actors, but it makes little sense to speak of dominance in cyberspace. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by nonstate actors. Four decades ago, the Pentagon created the Internet, and today, by most accounts, the United States remains the leading country in both its military and societal use. At the same time, however, because of greater dependence on networked computers and communication, the United States is more vulnerable to attack than many other countries, and the cyber domain has become a major source of insecurity.[5]

The term *cyber attack* covers a wide variety of actions ranging from simple probes, to defacing websites, to denial of service, to espionage and destruction.[6] Similarly, the term *cyber war* is used very loosely for a wide range of behaviors. In this, it reflects dictionary definitions of war that range from armed conflict to any hostile contention (e.g., "war between the sexes" or "war on poverty"). At the other extreme, some use a very narrow definition of cyber war as a "bloodless war" among states that consists only of conflict in the virtual layer of cyberspace. But this avoids important issues of the interconnection of the physical and virtual layers of cyberspace discussed

above. A more useful definition of *cyber war* is, hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.

In the physical world, governments have a near monopoly on large-scale use of force, the defender has an intimate knowledge of the terrain, and attacks end because of attrition or exhaustion. Both resources and mobility are costly. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and offense is often cheap. Because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense. This might not remain the case in the long term as technology evolves, including efforts at "reengineering" some systems for greater security, but it remains the case at this stage. The larger party has limited ability to disarm or destroy the enemy, occupy territory, or effectively use counterforce strategies. Cyber war, although only incipient at this stage, is the most dramatic of the potential threats. Major states with elaborate technical and human resources could, in principle, create massive disruption as well as physical destruction through cyber attacks on military as well as civilian targets. Responses to cyber war include a form of interstate deterrence (though different from classical nuclear deterrence), offensive capabilities, and designs for network and infrastructure resilience if deterrence fails. At some point in the future, it may be possible to reinforce these steps with certain rudimentary norms, but the world is at an early stage in such a process.

If one treats hacktivism as mostly a disruptive nuisance at this stage, there remain four major categories of cyber threats to national security, each with a different time horizon and different (in principle) solutions: cyber war and economic espionage are largely associated with states, and cyber crime and cyber terrorism are mostly associated with nonstate actors. For the United States, at the present time, the highest costs come from espionage and crime, but over the next decade or so, war and terrorism may become greater threats than they are today. Moreover, as alliances and tactics evolve among different actors, the categories may increasingly overlap. In the view of ADM Mike McConnell, "Sooner or later, terror groups will achieve cyber-sophistication. It's like nuclear proliferation, only far easier."[7] We are only just beginning to see glimpses of cyber war—for instance, as an adjunct in some conventional attacks, in the denial-of-service attacks that accompanied the conventional war in Georgia in 2008, or the recent sabotage of Iranian centrifuges by the Stuxnet worm. Deputy Defense Secretary William Lynn has described the evolution of cyber

attacks from exploitation, to disruption of networks, to destruction of physical facilities. He argues that while states have the greatest capabilities, nonstate actors are more likely to initiate a catastrophic attack.[8] A "cyber 9/11" may be more likely than the often mentioned "cyber Pearl Harbor."

Nuclear Lessons for Cyber Security?

Can the nuclear revolution in military affairs seven decades ago teach us anything about the current cyber transformation? At first glance, the answer seems to be no. The differences between the technologies are just too great. The National Research Council cites differences in the threshold for action and attribution—nuclear explosions are unambiguous, while cyber intrusions that plant logic bombs in the infrastructure may go unnoticed for long periods before being used and, even then, can be difficult to trace.[9] Even more dramatic is the sheer destructiveness of nuclear technology. Unlike nuclear, cyber does not pose an existential threat. As Martin Libicki points out, destruction or disconnection of cyber systems could return us to the economy of the 1990s—a huge loss of GDP—but a major nuclear war could return us to the Stone Age.[10] In that and other dimensions, comparisons of cyber with biological and chemical weaponry might be more apt.

Moreover, cyber destruction can be disaggregated, and small doses of destruction can be administered over time. While there are many degrees of nuclear destruction, all are above a dramatic threshold or firebreak. In addition, while there is an overlap of civilian and military nuclear technology, nuclear originated in war, and the differences in its use are clearer than in cyber where the Web has burgeoned in the civilian sector. For example, the "dot mil" domain name is only a small part of the Internet, and 90 percent of military telephone and Internet communications travel over civilian networks. Finally, because of the commercial predominance and low costs, the barriers to entry to cyber are much lower for nonstate actors. While nuclear terrorism is a serious concern, the barriers for nonstate actors gaining access to nuclear materials remain steep; renting a botnet to wreak destruction on the Internet is both easy and cheap.

It would be a mistake, however, to neglect the past, so long as we remember that metaphors and analogies are always imperfect.[11] In words often attributed to Mark Twain, "History never repeats itself, but sometimes it rhymes." There are some important nuclear-cyber strategic

rhymes, such as the superiority of offense over defense, the potential use of weapons for both tactical and strategic purposes, the possibility of first- and second-use scenarios, the possibility of creating automated responses when time is short, the likelihood of unintended consequences and cascading effects when a technology is new and poorly understood, and the belief that new weapons are "equalizers" that allow smaller actors to compete directly but asymmetrically with a larger state.[12]

Even more important than these technical and political similarities is the learning experience as governments and private actors try to understand a transformative technology—and adopt strategies to cope with it. While government reports warning about computer and Internet vulnerability date back to 1991 and the Pentagon recently released a new strategy, few observers would argue that the country has developed an adequate national strategy for cyber security. It is worth examining the uneven and halting history of nuclear learning to alert us to some of the pitfalls and opportunities ahead in the cyber domain. Ernest May once described US defense policy and the development of nuclear strategy in the first half-decade following World War II as "chaotic."[13] He would likely apply the same term to the situation in cyberspace today.

Some General Lessons

Expect continuing technological change to complicate early efforts at strategy. At the beginning, both fissile materials and atomic bombs were assumed to be scarce, and it was considered wasteful to use atomic bombs against any but countervalue targets—that is, cities. Bernard Brodie and others concluded in the important 1946 book *The Absolute Weapon* that superiority in numbers would not guarantee strategic superiority, deterrence of war was the only rational military policy, and ensuring survival of the retaliatory arsenal was crucial.[14] These postulates of "finite" or "existential" deterrence persisted throughout the Cold War and serve as the basis for the nuclear strategies of countries such as France and China to this day. In the bipolar competition of the Cold War, however, the strategy of finite deterrence was challenged by the development of the hydrogen bomb in the early 1950s. Destructive power was no longer scarce but now unlimited. While hydrogen bombs could lead to explosions counted in the tens of megatons, their real revolutionary effect was to permit miniaturization, which allowed multiple weapons to pack huge destructive power into the nose cones of another technological surprise—intercontinental ballistic

missiles—which shortened response times to less than an hour. This burgeoning explosive power produced great concern about the vulnerability of limited arsenals, an enormous increase in the number of weapons, diminished prospects for active defenses, and the development of elaborate counterforce war-fighting strategies.

Both superpowers had to confront the "usability paradox." If the weapons could not be used, they could not deter. The United States and the USSR were locked in a positive-sum game that involved avoiding nuclear war, but simultaneously they were locked in a zero-sum game of political competition. In the game of political chicken, perceptions of credibility became crucial. Some prospect of usability had to be introduced into doctrine, and for decades strategists wrestled with issues of counterforce targeting, exploring strategic defense technology, and the issues of perception that disparities in large numbers might create for extended deterrence. Elaborate war-fighting schemes and escalation ladders were invented by a nuclear priesthood of experts who specialized in arcane and abstract formulas. In 1976, Paul Nitze and the Committee on the Present Danger expressed alarm about American weakness when the United States possessed tens of thousands of weapons, and in 1979, even Henry Kissinger predicted that because of American nuclear weakness, Soviet risk-taking "must exponentially increase."[15] In fact, the opposite proved to be the case. While politicians and strategists assailed the idea of mutual assured destruction as an immoral and dangerous strategy, MAD turned out to be a fact, not a policy. As McGeorge Bundy noted in his final work, when it came to the Cuban missile crisis, existential deterrence worked, and a few Soviet bombs created deterrence despite an overwhelming American superiority in numbers.[16]

Looking at today's cyber domain, interdependence and vulnerability are twin facts that are likely to persist, but we should expect further technological change to complicate early strategies. ARPANET was created in 1969, and the domain name system and the first viruses date back to 1983; however, as noted above, the mass use and commercial development of cyberspace date only from the invention of the Worldwide Web in 1989 and widely available browsers in the mid-1990s.[17] As one expert put it, "As recently as the mid-1990s, the Internet was still essentially a research tool and the plaything of a few."[18] In other words, the massive vulnerabilities that have created the security problems we face today are less than two decades old and are likely to increase. While some experts talk about

reducing vulnerability by reengineering the Internet to make attribution of attack easier, this will take time. Even more important, it will not close all vectors of attack.

Early strategies focused on the network: improving code, computer hygiene, addressing issues of attribution, and maintaining air gaps for the most sensitive systems. These steps remain important components of a strategy, but they are far from sufficient. In some ways, the invention and explosion in the usage of the Web is analogous to the hydrogen revolution in the nuclear era. By leading society and the economy to a vast dependence on networked communications, it created enormous vulnerabilities that could be exploited not only through the Internet but also through supply chains, devices to bridge air gaps, human agents, and manipulation of social networks.[19] With the development of mobility, cloud computing, and the importance of a limited number of large providers, the issues of vulnerability may change again. Given such technological volatility, a cyber security strategy will have to be multifaceted and capable of continual adaptation. It should increase the ratio of work that an attacker must do compared to that of a defender and include redundancy and resilience to allow graceful degradation of complex systems so that inevitable failures are not catastrophic.[20] Strategists need to be alert to the fact that today's solutions may not suffice tomorrow.

Strategy for a new technology will lack adequate empirical content. Since Nagasaki, no one has seen a nuclear weapon used in war. As Alain Enthoven, one of Robert McNamara's "whiz kids" of the early 1960s, retorted during a Pentagon argument about war plans, "General, I have fought just as many nuclear wars as you have."[21] With little empirical grounding, it was difficult to set limits or test strategic formulations. Elaborate constructs and prevailing political fashion led to expensive conclusions based on abstract formulas and relatively little evidence. Fred Kaplan described the environment thusly:

> The method of mathematical calculation, driven mainly from the theory of economics that they had all studied, gave the strategists of the new age a handle on the colossally destructive power of the weapons they found in their midst. But over the years the method became a catechism. . . . The precise calculations and the cool, comfortable vocabulary were coming all too commonly to be grasped not merely as tools of desperation but as genuine reflections of the nature of nuclear war.[22]

In the absence of empirical evidence, these nuclear theologians were able to spend vast resources on their hypothetical scenarios.

Cyber has the advantage that with widespread attacks by hackers, criminals, and spies, there is more cumulative evidence of a variety of attack mechanisms and of the strengths and weaknesses of various responses to such attacks. It helps that cyber destruction can be disaggregated in a way that nuclear cannot. But at the same time, no one has yet seen a cyber war, in the strict sense of the word, as defined above. Denial-of-service attacks in Estonia and Georgia and industrial sabotage such as Stuxnet in Iran give some inklings of the auxiliary use of cyber attacks, but they do not test the full set of actions and reactions in a cyber war between states. The US government has conducted a number of war games and simulations and is developing a cyber test range, but the problems of unintended consequences and cascading effects have not been experienced. The problems of escalation as well as the implications for the important doctrines of discrimination and proportionality under the Law of Armed Conflict remain unknown.

New technologies raise new issues in civil-military relations. Different parts of complex institutions like governments learn different lessons at different paces, and new technologies set off competition among bureaucracies. At the beginning of the nuclear era, political leaders developed institutions to maintain civilian control over the new technology, creating an Atomic Energy Agency separate from the military as a means of ensuring civilian control. Congress established a Joint Atomic Energy Committee. But gaps still developed in the relationship between civilians and the military. Operational control of deployed nuclear weapons came under the Strategic Air Command, which had its own traditions, standard operating procedures, and a strong leader, Curtis LeMay. In 1957, LeMay told Robert Sprague, the deputy director of the civilian Gaither Committee that was investigating the vulnerability of American nuclear forces, that he was not too concerned because "if I see that the Russians are amassing their planes for an attack, I'm going to knock the s**t out of them before they take off the ground." Sprague was thunderstruck and replied, "But General LeMay, that is not national policy," to which LeMay replied, "I don't care. It's my policy. That's what I'm going to do."[23] In 1960, when President Eisenhower ordered the development of a single integrated operational plan (SIOP-62), SAC produced a plan for a massive strike with 2,164 megatons that targeted China as well as the Soviet Union because of

the "Sino-Soviet Bloc."[24] The limited nuclear options that civilian strategists theorized about as part of a bargaining process would not have looked very limited from the point of view of the Soviet bargaining partner—not to mention China.

While Cyber Command is still new and has very different leadership from the old Strategic Air Command, cyber security does present some similar problems of relating civilian control to military operations. Time is even shorter. Rather than the 30 minutes of nuclear warning and possible launch under attack, today there would be 300 milliseconds between a computer detecting that it was about to be attacked by hostile malware and a preemptive response to disarm the attack. This requires not only advanced knowledge of malware being developed in potentially hostile systems but also an automated response. What happens to the human factor in the decision loop? Obviously, there is no time to go up the chain of command, much less convene a deputies' meeting at the White House. For active defense to be effective, authority will have to be delegated under carefully thought-out rules of engagement developed in advance. Moreover, there are important questions about when active defense shades into retaliation or offense. As the head of Cyber Command has testified, such legal authorities and rules still remain to be fully resolved.[25]

Civilian uses will complicate effective national security strategies. Nuclear energy was first harnessed for military purposes, but it was quickly seen as having important civilian uses as well. In the early days of the development of nuclear energy, it was claimed that electricity would become "too cheap to meter" and cars would be fueled for a year by an atomic pellet the size of a vitamin pill.[26] The engineers' optimism about their new technology was reinforced by a political desire to promote the civilian uses of nuclear energy. Fearful that antiwar and antinuclear movements would delegitimize nuclear weapons and thus reduce their deterrent value, the Eisenhower administration promoted an Atoms for Peace program that offered to assist in the promotion of nuclear energy worldwide. Other countries joined in. The net effect was to create a powerful domestic and transnational lobby for promotion of nuclear energy that helped provide India with the materials needed for its nuclear explosion in 1974 and justified the French sale of a reprocessing plant to Pakistan and a German sale of enrichment technology to Brazil in the mid-1970s.

The Atomic Energy Commission and the Joint Atomic Energy Committee had been created to assure civilian control of nuclear technology,

but over time both institutions became examples of regulatory capture by powerful commercial interests—more interested in promotion than regulation and security. Late in the Ford administration, both institutions were disbanded. However, after the oil crisis of 1974, it became an article of faith that nuclear would be the energy of the future; that uranium would be scarce, and thus widespread use of plutonium and breeder reactors would be necessary. When the Carter administration, following the recommendations of the nongovernmental Ford-Mitre Report,[27] tried to slow the development of this plutonium economy in 1977, it ran into a buzz saw of reaction not only overseas but also from the nuclear industry and its congressional allies at home.

As mentioned earlier, the civilian sector plays an even larger role in the cyber domain, and this enormously complicates the problem of developing a national security strategy. The Internet has become a much more significant contributor to GDP than nuclear energy ever was. The private sector is more than a constraint on policy; it is at the heart of the activity that policy is designed to protect. Risk is inevitable, and redundancy and resilience after attack must be built into a strategy. Most of the Internet and its infrastructure belong to the private sector, and the government has only modest levers to use. Proposals to create a central agency in the executive branch and a joint committee on cyber security in Congress might be useful, but one should be alert to the dangers of regulatory capture and the development of a cyber "iron triangle" of executive branch, congressional, and industry partners.

From a security perspective, there is a misalignment of economic incentives in the cyber domain.[28] Firms have an incentive to provide for their own security up to a point, but competitive pricing of products limits that point. Moreover, firms have a financial incentive not to disclose intrusions that could undercut public confidence in their products and stock prices. A McAfee white paper notes, "The public (and very often the industry) understanding of this significant national security threat is largely minimal due to the very limited number of voluntary disclosures by victims of intrusion activity."[29] The result is a paucity of reliable data and an underinvestment in security from the national perspective. Moreover, laws designed to ensure competition restrict cooperation among private firms, and the difficulty of ascertaining liability in complex software limits the role of the insurance market. Public-private partnerships are limited by different perspectives and mistrust. As one participant at a recent cyber

security conference concluded, something bad will have to happen before markets begin to reprice security.[30]

International Cooperation Lessons

Learning can lead to concurrence in beliefs without cooperation. Governments act in accordance with their national interests, but they can change how they define their interests, both through adjusting their behavior to changes in the structure of a situation as well as through transnational and international contacts and cooperation. In the nuclear domain, the initial learning led to concurrence of beliefs before it led to contacts and cooperation. The first effort at arms control, the Baruch Plan of 1946, was rejected out of hand by the Soviet Union as a ploy to preserve the American monopoly, and the early learning was unilateral on both sides.

As we have seen, much of what passed for nuclear knowledge in the early days was abstraction based on assumptions about rational actors, which made it difficult for new information to alter prior beliefs. Yet gradually, both sides became increasingly aware of the unprecedented destructive power of nuclear weapons through weapons tests and modeling, particularly after the invention of the hydrogen bomb. As Winston Churchill put it in 1955, "The atomic bomb, with all its terrors, did not carry us outside the scope of human control," but with the H-bomb, "the entire foundation of human affairs was revolutionized."[31] In his memorable phrase, "Safety will be the sturdy child of terror." On the other side of the Iron Curtain, Nikita Khrushchev recalled: "When I was appointed First Secretary of the Central Committee and learned all the facts about nuclear power I couldn't sleep for several days. Then I became convinced that we could never possibly use these weapons, and I was able to sleep again. But all the same we must be prepared."[32] These parallel lessons were learned independently. It was not until 1985 that Ronald Reagan and Mikhail Gorbachev finally declared jointly that "a nuclear war cannot be won and must never be fought." That crucial nuclear taboo has existed for nearly seven decades and was well ensconced before it was jointly pronounced.

A second area where concurrence in beliefs developed was in the command and control of weapons and the dangers of escalation as the two governments accumulated experience of false alarms and accidents. A third area related to the spread of nuclear weapons. Both the United States and the Soviet Union gradually realized that sharing nuclear technology and expecting that exports could remain purely peaceful was implausible.

A fourth area of common knowledge concerned the volatility of the arms race and the expenses and risks that it entailed. These views developed independently and in parallel, and it was more than two decades before they led to formal cooperation. Perfect concurrence of beliefs would lead to harmony, which is very rare in world politics. Cooperation in the nuclear area responded to both some concurrence of beliefs as well as actual and anticipated discord.[33]

By its very nature, the interconnected cyber domain requires a degree of cooperation and governments becoming aware of this situation. Some analysts see cyberspace as analogous to the ungoverned Wild West, but unlike the early days of the nuclear domain, cyberspace has a number of areas of private and public governance. Certain technical standards related to Internet protocol are set (or not) by consensus among engineers involved in the nongovernmental Internet Engineering Task Force (IETF), and the domain name system is managed by the Internet Corporation for Assigned Names and Numbers (ICANN). The United Nations and the International Telecommunications Union (ITU) have tried to promulgate some general norms, though with limited success. National governments control copyright and intellectual property laws and try to manage problems of security, espionage, and crime within national policies. Though some cooperative frameworks exist, such as the European Convention on Cyber Crime, they remain weak, and states still focus on the zero-sum rather than positive-sum aspect of these games. At the same time, a degree of independent learning may be occurring on some of these issues. For example, Russia and China have refused to sign the Convention on Cyber Crime and have hidden behind plausible deniability as they have encouraged intrusions by "patriotic hackers." Their attitudes may change, however, if costs exceed benefits. For example, "Russian cyber-criminals no longer follow hands-off rules when it comes to motherland targets, and Russian authorities are beginning to drop the laissez-faire policy."[34] And China is independently experiencing increased costs from cyber crime. As in the nuclear domain, independent learning may pave the way for active cooperation later.

Learning is often lumpy and discontinuous. Large groups and organizations often learn by crises and major events that serve as metaphors for organizing and dramatizing diverse sets of experiences. The Berlin crises and particularly the Cuban missile crisis of the early 1960s played such a role. Having come close to the precipice of war, both Kennedy and

Khrushchev drew lessons about cooperation. It was shortly after the Cuban missile crisis that Kennedy gave his American University speech that laid the basis for the atmospheric test ban discussions.

Of course crises are not the only way to learn. The experience of playing iterated games of prisoner's dilemma in situations with a long shadow of the future may lead players to learn the value of cooperation in maximizing their payoffs over time.[35] Early steps in cooperation in the nuclear domain encouraged later steps, without requiring a change in the competitive nature of the overall relationship. These governmental steps were reinforced by informal "Track Two" dialogues such as the Pugwash Conferences.

Thus far there have been no major crises in the cyber domain, though the denial-of-service attacks on Estonia and Georgia and the Stuxnet attack on Iran give hints of what might come. As mentioned earlier, some experts think that markets will not price security properly in the private sector until there is some form of visible crisis. But other forms of learning can occur. For example in the area of industrial espionage, China has had few incentives to restrict its behavior because the benefits far exceed the costs. Spying is as old as human history and does not violate any explicit provisions of international law. Nevertheless, at times governments have established rules of the road for limiting espionage and engaged in patterns of tit-for-tat retaliation to create an incentive for cooperation. While it is difficult to envisage enforceable treaties in which governments agree not to engage in espionage, it is plausible to imagine a process of iterations (tit for tat) which develops rules of the road that could limit damage in practical terms. To avoid "defection lock-in," which leads to unwanted escalation, it helps to engage in discussions that can develop common perceptions about redlines, if not fully agreed norms, as gradually developed in the nuclear domain after the Cuban missile crisis.[36] Discussion helps to provide a broader context (a "shadow of the future") for specific differences, and it is interesting to note that China and the United States have begun to discuss cyber issues in the context of their broad annual Strategic and Economic Dialogue, as well as in informal Track Two settings.

Learning occurs at different rates in different issues of a new domain. While the US-Soviet political and ideological competition limited their cooperation in some areas, awareness of nuclear destructiveness led them to avoid war with each other and to develop what Zbigniew Brzezinski called "a code of conduct of reciprocal behavior guiding the competition, lessening the danger that it could become lethal."[37] These basic rules of

prudence included no direct fighting, no nuclear use, and communication during crisis. More specifically, it meant the division of Germany and respect for spheres of influence in Europe in the 1950s and early 1960s and a compromise on Cuba. On the issue of command and control, concerns about crisis management and accidents led to the hotline, as well as the Accidents Measures and Incidents at Sea meetings of the early 1970s. Similarly, on the issue of nonproliferation the two sides discovered a common interest and began to cooperate in the mid-1960s, well before the bilateral arms control agreements about issues of arms race stability in the 1970s. Unlike the view that says nothing is settled in a deal until everything is settled, nuclear learning and agreements proceeded at different rates in different areas.

The cyber domain is likely to be analogous. As we have seen, there are already some agreements and institutions that relate to the basic functioning of the Internet, such as technical standards as well as names and addresses, and there is the beginning of a normative framework for cyber crime. But it is likely to take longer before there are agreements on contentious issues such as cyber intrusions for purposes like espionage and preparing the battlefield. Nevertheless, the inability to envisage an overall agreement need not prevent progress on sub-issues. Indeed, the best prospects for success may involve disaggregating the term *attacks* into specific actions that could be addressed separately.

Involve the military in international contacts. As mentioned above, the military can be under civilian control but still have an independent operational culture of its own. By its nature and function, it is charged with entertaining worst-case assumptions. It does not necessarily learn the same lessons at the same rate as its civilian counterparts. Early in the SALT talks, Soviet military leaders complained about the American habit of discussing sensitive military information in front of civilian members of the Soviet delegation. The practice had the effect of broadening communication within the Soviet side. At the same time, Soviet military leaders had little understanding of American institutions or the role of Congress and how that would affect nuclear issues. Their involvement in arms talks helped to produce a more sophisticated generation of younger leaders. As Foreign Minister Andrei Gromyko put it, "It's hard to discuss the subject with the military, but the more contact they have with the Americans, the easier it will be to turn our soldiers into something more than just martinets."[38]

In the cyber domain, the Chinese People's Liberation Army plays a major role in recruitment, training, and operations. China today provides more opportunities for PLA generals to have international contacts than was true for Soviet officers during the Cold War, but those contacts are still limited. Moreover, while political control over the Chinese military is strong, operational control is weak, as shown by a number of recent incidents. Indeed, seven of the nine members of the Standing Military Commission wear uniforms, and there is no National Security Council or equivalent to coordinate operational details across the government. The lessons from the nuclear era would suggest the importance of involving PLA officers in discussions of cyber cooperation.

Deterrence is complex and involves more than just retaliation. Early views of deterrence in the nuclear era were relatively simple and relied on massive retaliation to a nuclear attack. Retaliation remained at the core of deterrence throughout the Cold War, but as strategists confronted the usability dilemma and the problems of extended deterrence, their theories of deterrence became more complex. While a second-strike capability and mutual assured destruction may have been enough to prevent attacks on the homeland, they were never credible for issues at the low end of the spectrum of interests. Somewhere between these extremes lay extended deterrence of attacks against allies and defense of vulnerable positions such as Berlin. Nuclear deterrence was supplemented by other measures, such as forward basing of conventional forces, declaratory policy, changes of alert levels, and force movements.

Many analysts argue that deterrence does not work in cyberspace because of the problem of attribution, but that is also too simple. Interstate deterrence through entanglement and denial still exists even when there is inadequate attribution. Even when the source of an attack can be successfully disguised under a "false flag," other governments may find themselves sufficiently entangled in symmetrically interdependent relationships that a major attack would be counterproductive—witness the reluctance of the Chinese government to dump dollars to punish the United States after it sold arms to Taiwan in 2010.[39] Unlike the single strand of military interdependence that linked the United States and the Soviet Union during the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and vice versa.

In addition, an unknown attacker may be deterred by denial. If firewalls are strong or the prospect of a self-enforcing response ("an electric fence") seems possible, attack becomes less attractive. Offensive capabilities for immediate response can create an active defense that can serve as a deterrent even when the identity of the attacker is not fully known. Futility can also help deter an unknown attacker. If the target is well protected or redundancy and resilience allow quick recovery, the risk-to-benefit ratio in attack is diminished.[40] Moreover, attribution does not have to be perfect, and to the extent that false flags are imperfect and rumors of the source of an attack are widely deemed credible (though not probative in a court of law), reputational damage to an attacker's soft power may contribute to deterrence. Finally, a reputation for offensive capability and a declaratory policy that keeps open the means of retaliation can help to reinforce deterrence. Of course, nonstate actors are harder to deter, and improved defenses such as preemption and human intelligence become important in such cases. But among states, nuclear deterrence was more complex than it first looked, and that is doubly true of deterrence in the cyber domain.

Begin arms control with positive-sum games related to third parties. Although the United States and the Soviet Union developed some tacit rules of the road about prudent behavior early on, direct negotiation and agreements concerning arms race stability or force structure did not occur until the third decade of the nuclear era. Early efforts at comprehensive arms control like the Baruch Plan were total nonstarters. And even the eventual SALT agreements were of limited value in controlling numbers of weapons and involved elaborate verification procedures which themselves sometimes became issues of contention. The first formal agreement was the Limited Test Ban Treaty, where detection of atmospheric tests was easily verifiable and it could be considered largely an environmental treaty. The second major agreement was the Non-Proliferation Treaty of 1968, which was aimed at limiting the spread of nuclear weapons to third parties. Both these agreements involved positive-sum games.

In the cyber domain, the global nature of the Internet requires international cooperation. Some people call for cyber arms control negotiations and formal treaties, but differences in cultural norms and the impossibility of verification make such treaties difficult to negotiate or implement. Such efforts could actually reduce national security if asymmetrical implementation put legalistic cultures like the United States at a disadvantage compared to societies with a higher degree of government corruption. At the

same time, it is not too early to explore international talks and cooperation. The most promising early areas for international cooperation are not bilateral conflicts, but problems posed by third parties such as criminals and terrorists.

For more than a decade, Russia has sought a treaty for broad international oversight of the Internet and "information security" banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued that arms control measures banning offense can damage defense against current attacks and would be impossible to verify or enforce. And declaratory statements of "no first use" might have restraining effects on legalistic cultures like the United States while having less effect on states with closed societies. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the Internet. Cultural differences present a difficulty in reaching any broad agreements on regulating content on the Internet. The United States has called for the creation of "norms of behavior among states" that "encourage respect for the global networked commons," but as Jack Goldsmith has argued, "Even if we could stop all cyber attacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense."[41] From the American point of view, Twitter and YouTube are matters of personal freedom; seen from Beijing or Tehran, they are instruments of attack. Trying to limit all intrusions would be impossible, but on the spectrum of attacks ranging from soft hacktivism to hard implanting of logic bombs in SCADA (supervisory control and data acquisition) systems, one could start with cyber crime and cyber terrorism involving nonstate third parties where major states would have an interest in limiting damage by agreeing to cooperate on forensics and controls. States might start with acceptance of responsibility for attacks that traverse their territory and a duty to cooperate on forensics, information, and remedial measures.[42] At some later points, it is possible that such cooperation could spread to state activities at the hard end of the spectrum, as it did in the nuclear domain.

Conclusion

Historical analogies are always dangerous if taken too literally, and the differences between nuclear and cyber technologies are great. The cyber

domain is new and dynamic, but so was nuclear technology at its inception. It may help to put the problems of designing a strategy for cyber security into perspective, particularly the aspect of cooperation among states, if we realize how long and difficult it was to develop a nuclear strategy, much less international nuclear cooperation. Nuclear learning was slow, halting, and incomplete. The intensity of the ideological and political competition in the US-Soviet relationship was much greater than that between the United States and Russia or the United States and China today. There were far fewer positive strands of interdependence in the relationship. Yet the intensity of the zero-sum game did not prevent the development of rules of the road and cooperative agreements that helped to preserve the concurrent positive-sum game.

That is the good news. The bad news is that cyber technology gives much more power to nonstate actors than does nuclear technology, and the threats such actors pose are likely to increase. The transnational, multiactor games of the cyber domain pose a new set of questions about the meaning of national security. Some of the most important security responses must be national and unilateral, focused on hygiene, redundancy, and resilience. It is likely, however, that major governments will gradually discover that cooperation against the insecurity created by nonstate actors will require greater priority in attention. The world is a long distance from such a response at this stage in the development of cyber technology. But such responses did not occur until we approached the third decade of the nuclear era. With the World Wide Web only two decades old, may we be approaching an analogous point in the political trajectory of cyber security? SSQ

Notes

1. Oddly, Max Boot does not list the nuclear revolution. See his *War Made New: Technology, Warfare and the Course of History, 1500 to Today* (New York: Gotham Books, 2006).
2. Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 3.
3. A pioneering work on this question is Lloyd Etheredge, *Can Governments Learn*? (Elmsford, NY: Pergamon Press, 1985).
4. Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs Press, 2011), chap. 5.
5. This point is emphasized by Richard A. Clarke and Robert Knake in *Cyberwar* (New York: HarperCollins, 2009).
6. For skeptical views that cyberwar is overhyped, see Michael Hirsh, "Here There Be Dragons," *National Journal* 23 (July 2011): 32–37.
7. McConnell quoted in Nathan Gardels, "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly* 27, no. 2 (Spring 2010): 16.

8. Deputy Secretary of Defense William Lynn, remarks at 28th Annual International Workshop on Global Security, Paris, France, 16 June 2011, http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1586.

9. William Owens, Kenneth Dam, and Herbert Lin, eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: National Academies Press, 2009), 294.

10. Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no.1 (Spring 2011): 136. See also Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 136.

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

12. Owens et al., *Technology, Policy, Law and Ethics*, 295–96.

13. Ernest May, "Cold War and Defense," in *The Cold War and Defense*, eds. Keith Neilson and Ronald G. Haycock (New York: Praeger, 1990), 54. I am indebted to Phillip Zelikow for bringing this to my attention.

14. Fred Kaplan, *The Wizards of Armageddon* (New York: Simon and Schuster, 1983), 30.

15. Kissinger quoted in Robert Jervis, *The Meaning of the Nuclear Revolution* (Ithaca, NY: Cornell University Press, 1989), 102.

16. McGeorge Bundy, *Danger and Survival: Choices about the Bomb in the First 50 Years* (New York: Vintage, 1990).

17. Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, eds. Franklin Kramer, Starr, and Larry Wentz (Washington: NDU Press, 2009), 82–86.

18. Joel Brenner, *America the Vulnerable* (New York: Penguin Press, 2011), 15.

19. On supply chain vulnerability, see Scott Charney and Eric Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," Microsoft Corp., 25 July 2011, http://www.microsoft.com/download/en/details.aspx?id=26826.

20. I am indebted to John Mallery of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) for his work on these points.

21. Kaplan, *Wizards of Armageddon*, 254.

22. Ibid., 391.

23. Ibid., 134.

24. Ibid., 269.

25. Gen Keith Alexander, quoted in "US Lacks People, Authorities to Face Cyber Attack," *Associated Press*, 16 March 2011.

26. Brian Balogh, *Chain Reaction: Expert Debate and Public Participation in American Commercial Nuclear Power, 1945–1975* (Cambridge, UK: Cambridge University Press, 1991), 31.

27. The Nuclear Energy Policy Study Group, *Nuclear Power: Issues and Choices* (Ford-Mitre Report) (Cambridge, MA: Ballinger, 1977).

28. See Brenner, *America the Vulnerable*.

29. Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee white paper, 2011, 3, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

30. Jason Pontin, remarks at plenary panel, EastWest Institute Cybersecurity Summit, London, 2 June 2011.

31. Churchill quoted in Michael Mandelbaum, *The Nuclear Revolution* (Cambridge, UK: Cambridge University Press, 1981), 3.

32. Khrushchev quoted in Jervis, *Meaning of the Nuclear Revolution*, 20.

33. I am indebted to Robert O. Keohane for this point.

34. Joseph Menn, "Moscow gets Tough on Cybercrime," *Financial Times*, 22 March 2010.

35. See Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).

36. For a description of the gradual evolution of such learning in the nuclear area, see Joseph S. Nye Jr., "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization* 41, no. 3 (Summer 1987). See also Graham Allison, "Primitive Rules of Prudence: Foundations of Peaceful Competition" in *Windows of Opportunity: From Cold War to Peaceful Competition in U.S.-Soviet Relations*, eds. Allison, William Ury, and Bruce Allyn (Cambridge, MA: Ballinger, 1989).

37. Zbigniew Brzezinski, *Game Plan* (Boston: Atheneum, 1986), 244.

38. Arkady Shevchenko, *Breaking With Moscow* (New York: Ballantine, 1985), 270–71. See also Raymond Garthoff, "Negotiating SALT," *Wilson Quarterly* (Autumn 1977): 79.

39. For details, see Nye, *Future of Power*, chap. 3.

40. I am indebted to the unpublished writings of Jeff Cooper on these points.

41. Jack Goldsmith, "Can We Stop the Global Cyber Arms Race," *Washington Post*, 1 February 2010.

42. See, for example, Eneken Tikk, "Ten Rules for Cyber Security," *Survival* 53, no. 3 (June–July 2011): 119–32.