GEORGETOWN UNIVERSITY PRESS

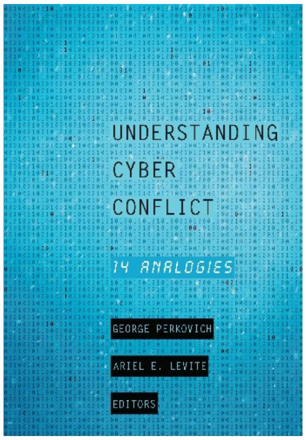
Cyber Threats, Nuclear Analogies? Divergent Trajectories in Adapting to New Dual-Use Technologies

Steven E. Miller

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



UNDERSTANDING CYBER CONFLICT

14 ANALOGIES

GEORGE PERKOVICH

ARIEL E. LEVITE

EDITORS

10 Cyber Threats, Nuclear Analogies?

DIVERGENT TRAJECTORIES IN ADAPTING TO NEW DUAL-USE TECHNOLOGIES

STEVEN E. MILLER

Alarm is mounting over large security vulnerabilities produced by the pervasive spread of cyber capabilities into vast realms of socioeconomic activity. To be sure, most cyber threats fall into the category of mischief or normal crime, but some potential cyber attacks—on nuclear power plants or other critical infrastructure or on the financial system, for example—could do enormous harm. There is a need, therefore, to seek remedies and adapt to the challenges posed by this ubiquitous dual-use technology.[1]

Other dual-use technologies have raised similar challenges of adaptation. It is natural to examine these other, possibly analogous experiences to see if there are lessons that might apply in the cyber realm. This chapter looks at the emergence of nuclear technology, examines the challenges it posed and the reactions to those challenges, explores the evolution of early thinking about the risks and benefits of nuclear technology, and considers whether the trajectories and time lines of the adaptation to nuclear technology have any resonance with the cyber issue. Is there a nuclear analogy? What elements of the response to nuclear technology, if any, have relevance for the cyber era?[2]

I attempt to answer these questions by offering a brief account of three dimensions of the nuclear experience: First, how did the nuclear age arrive and what was the response to it? Second, how did the peaceful benefits of nuclear technology fit into the picture? And, third, what answers were found to the national security threats raised by the nuclear revolution? These discussions reveal that the nuclear story is very different from the more recent experience with cyber technology in a number of fundamental respects.

One basic difference is that the nuclear tale is first and foremost about weapons with possible civilian applications rather than the other way around. The weaponized form of the technology was from the beginning, and has remained, the center of the nuclear question. In the nuclear case, civilian applications struggled to be born and in many respects were less impactful than expected. The time lines and trajectories associated with cyber and nuclear are quite different, and their areas of primary impact fall in different domains: nuclear technology is above all a geopolitical consideration, whereas cyber technology has become an enormous factor in many areas of social and economic life. Nevertheless, there are parallels as both technologies have raised the question of how to protect against an intractable threat. Some of the answers considered in the nuclear realm may find application if adapted to the cyber context.

The Nuclear Age Arrives

The nuclear age arrived with stunning suddenness. To all but the minuscule fraction of humanity that had been privy to the Manhattan Project, the unprecedented weapons employed in the bombings of Hiroshima and Nagasaki in August 1945 were completely unexpected and shockingly devastating. The world was made aware of this new development when President Harry S. Truman issued an unassuming but muscular three-page typewritten press statement on August 6, 1945.[3] "Sixteen hours ago," the statement began in almost understated plain language, "an American airplane dropped one bomb on [Hiroshima] and destroyed its usefulness to the enemy."[4]

It was necessary, of course, to explain what this meant to an unknowing world: "With this bomb we have now added a new and revolutionary increase in destruction to supplement the growing power of our armed forces. In their present form, these bombs are now in production and even more powerful forms are under development. It is an atomic bomb. It is the harnessing of the basic power of the universe. The force from which the sun draws its power has been loosed against those who brought war to the Far East."[5]

The president also spelled out in unflinching terms what this new weapon meant for Japan in the ongoing war in the Pacific: "We are now prepared to obliterate more rapidly and completely every productive enterprise the Japanese have above ground in any city. We shall destroy their docks, their factories, and their communications. Let there be no mistake: we shall completely destroy Japan's power to make war."

This language, blunt though it is, betrayed an incomplete comprehension of the destructive effects of the atomic bomb. It destroyed not docks and factories but cities, as soon became apparent when images of Hiroshima and Nagasaki were revealed to the world. But the implications for Japan's leaders were conveyed in vivid terms that left no doubt about the destructive potential of this new technology. Hoping "to spare the Japanese people from utter destruction," the president's statement called on Japan's leaders to accept the ultimatum that had been issued at the Potsdam Conference in July 1945. In perhaps his most famous passage of the statement, he continued, "If they do not now accept our terms they may expect a rain of ruin from the air the likes of which has never been seen on this earth."[6]

The extraordinary character of the atomic bomb was recognized almost instantly. In her widely read syndicated newspaper column, "My Day," for example, Eleanor Roosevelt wrote on August 8, 1945—even before Nagasaki—about the implications of the atomic bomb: "This discovery may be of great commercial value someday. If wisely used, it may serve the purposes of peace. But for the moment we are chiefly concerned with its destructive power. That power can be multiplied indefinitely, so that not only whole cities but large areas may be destroyed at one fell swoop. . . . You soon face the unpleasant fact that in the next war whole peoples may be destroyed. . . . This discovery must spell the end of war."[7]

Similarly, immediately upon hearing of the bombing of Hiroshima, Bertrand Russell wrote a small essay, published ten days later, on August 18, 1945, under the title "The Bomb and Civilization." He lamented that a historic scientific accomplishment had produced such terrible results and commented in a stunned and frightened fashion about what this development could mean for the future: "It is impossible to imagine a more dramatic and horrifying combination of scientific triumph with political and moral failure than has been shown to the world in the destruction of Hiroshima. . . . In an instant, by means of one small bomb, every vestige of life throughout four square miles of a populous city has been exterminated. . . . The prospect for the human race is somber beyond precedent."[8]

The August 20, 1945, edition of *Life* magazine, seen by millions of Americans, was devoted to the atomic bomb and included photos of Hiroshima and Nagasaki. It also contained an essay by *New York Times* military correspondent Hanson Baldwin on the implications of the atomic bomb for military power. Possibly for the first time, Baldwin raised the question of whether traditional military forces were now obsolete, thus opening a fierce debate that would haunt and damage the US military in the coming years.[9] Immediately after the bombing of Hiroshima and Nagasaki, clearly a new era had arrived that required serious rethinking of international politics and security. Above all, the sense of shock was almost universal at the scale of the destructive potential associated with this new weapon. As Paul Boyer noted in his own detailed account of reactions to the atomic revolution, "The whole world gasped."[10]

Thus was nuclear technology introduced to most of the world. The transition to the nuclear age was abrupt. From the first moments of this new era, the new technology existed as a weapon. This was not a case in which an important *civilian* technology had the potential also for malign use with wide consequences. Indeed, nuclear arrived in exactly the opposite circumstance—as a weapons technology that, it was hoped, could have civilian applications. At the birth of the nuclear age, however, no civilian uses of the new technology existed.

Nuclear technology emerged from a top-secret military program. It was in the hands of only one power that explicitly intended to keep its secret as long as possible. Further, the damage that nuclear technology could wreak was not linked to speculative scenarios or hypothetical worst cases. Two incinerated cities lay in ruins, demonstrating the gruesome destructiveness of this new technology. And in many quarters, there was immediate recognition that this new era had profound implications for international politics and security.

In its origins, the nuclear story is very different from that of cyber. No overnight passage led into a dramatically new cyber world; rather, the cyber world was built progressively across multiple decades. Though cyber history is contested, the origins of the Internet are generally traced to a relatively obscure military project in the late 1960s, the Advanced Research Projects Agency Network (ARPANET). The world did not gasp at the birth of ARPANET. It was not until the 1980s that this creation began to emerge as a public phenomenon and not until the 1990s that it began, in an accelerating fashion, to dominate communications and to penetrate wide swaths of socioeconomic life. Though it has military applications, cyber is pervasive in civilian activities and has become part of the basic infrastructure of civilian life in large portions of the world. Indeed, it is precisely the dependence of much economic and social activity on cyberspace that creates the large vulnerabilities about which we now worry. Thus, the way these two technological eras emerged and the framework of issues they raise are very different.

Developing the Peaceful Atom

The nuclear age arose out of wartime exigencies, and its initial technological manifestations were the result of a crash military program, although it was understood early on that nuclear technology might have an array of civilian applications. Even after the end of World War II, however, peaceful uses of the atom remained a subsidiary concern, especially as the Cold War rapidly emerged and an ensuing nuclear rivalry with Russia came to dominate security concerns. As Richard Hewlett and Francis Duncan observe in their still indispensable account of the early years of US nuclear policy, the postwar period was marked by "a shift from the idealistic, hopeful anticipation of the peaceful atom to the grim realization that for reasons of national security atomic energy would have to continue to bear the image of war."[11] The priorities of national policy remained fundamentally important because for more than a decade the US government retained a monopoly on the nuclear information, technology, and activity. Only after the passage of the Atomic Energy Act of 1954 was the private sector legally authorized to undertake commercial activities in the nuclear realm (and, even then, only under strict government regulation). Many of the possible peaceful uses of nuclear power experienced a protracted struggle to be realized for several reasons: Fissile material was (for a time) relatively scarce; the demand for nuclear weapons grew steadily; the weapons program retained highest priority; secrecy was highly valued; the technologies in question were expensive, challenging, and difficult to commercialize; and the number of nuclear experts was limited.[12]

Nevertheless, the apocalyptic fears of nuclear destruction were accompanied by extravagant visions of extraordinary, widespread nuclear benefits. In the initial wave of enthusiasm about the promise of the nuclear revolution, popular discussions covered everything from atomic energy vitamin tablets to atomic-propelled vehicles of all varieties (including automobiles) to breathtaking medical breakthroughs (cancer cured) to abundant and inexpensive electricity (too cheap to meter, as it was sometimes predicted). There was serious consideration of the problems that would flow from this vast nuclearization of civilian life. For example, what about the thirty million automobiles that would be rendered obsolete by the arrival of the nuclear-powered car? In the early phase of the nuclear age, the air was filled with what Boyer described as "fantasies of a techno-atomic utopia."[13] Some of this forecasting did indeed belong in the realm of science fiction, but the optimistic exploration of possible peaceful applications of nuclear technology was far from completely disconnected from policy. In 1946, for example, the Atomic Energy Commission established the Nuclear Energy for the Propulsion of Aircraft program.[14]

By the time President Dwight Eisenhower took office, however, the nuclear arms race clearly was roaring ahead, galvanized by the Soviet acquisition of nuclear weapons starting in 1949, and the peaceful atom was lagging. Moreover, Eisenhower assumed the presidency as the US nuclear arsenal was making the transition to the hydrogen bomb (H-bomb), which is vastly more powerful than the weapons employed in August 1945. Eisenhower had been briefed about the H-bomb during the presidential transition and had been "struggling with the staggering implications of a weapon that could destroy not only an entire city but perhaps civilization itself."[15] He understood the portentous implications of the H-bomb revolution and even alluded to this issue (albeit indirectly) in his inaugural address: "Science seems ready to confer upon us, as a final gift, the power to erase life from this planet."[16]

Eisenhower also had to contend with aftereffects of the nuclear testing program. By this time they raised public fears of fallout and radiation, causing international outcry and producing growing concerns about nuclear technology. After the famous Lucky Dragon incident in 1954, in which a Japanese fishing trawler was accidently showered with fallout from a US thermonuclear test, there were efforts to condemn the United States at the United Nations and there was what was described as a "worldwide expression of fear."[17] In both the private and public considerations of nuclear policy, the nuclear dangers figured prominently.

With a zeal that surprised his advisers (not least, those on the Atomic Energy Commission), Eisenhower responded to these pressures by seeking to promote the peaceful uses of nuclear power. There was "a sense of moral compulsion that drove the President to seek some redeeming value in a new technology that threatened the future of humanity."[18] Eisenhower was especially keen to see the emergence of nuclear power (that is, the generation of electricity using nuclear reactors) and was frustrated by the slow progress toward developing and commercializing that technology. His administration explored one peaceful nuclear idea after another, including the construction of nuclear-powered merchant ships (discussed in the National Security Council in 1955) and the creation of small nuclear reactors suitable for distribution as part of an "Atomic Marshall Plan."

President Eisenhower's nuclear instincts found historic expression in his remarkable "Atoms for Peace" speech, which he delivered before the UN General Assembly on December 8, 1953. In powerful and sometimes poetic language, he spoke starkly about the dangers of the nuclear arms race, noting that it was not possible to escape "the awful arithmetic of the atomic bomb." Atomic warfare, he said, would lead to “annihilation” and “desolation.” He emphasized that the United States sought to avoid this destructive result: “My country’s purpose is to help move out of this dark chamber of horrors into the light.” He therefore proposed that the world’s three nuclear powers—the United States, the Soviet Union, and the United Kingdom—divert some portion of their nuclear efforts, including fissile material, to peaceful purposes; that an international atomic energy agency be created to, among other things, control donated fissile material; and that, in general, nuclear development be pushed onto a more peaceful path. “The United States pledges before you,” he concluded, “and therefore before the world, its determination to solve the fearful atomic dilemma—to devote its entire heart and mind to find the way by which the miraculous inventiveness of man shall not be dedicated to his death but consecrated to his life.”[19] Eisenhower wanted to tilt the balance toward the peaceful uses of technology, hoping to achieve benefits on the same scale as the revolution wrought by nuclear weapons.

In his assessment of the Atoms for Peace program, Peter Lavoy writes that it “fundamentally altered the way the world treated nuclear energy.”[20] In the United States, the promotion of nuclear power helped fuel what the Atomic Energy Commission feared was a “grandiose public vision of the nuclear age,” one with an “almost unbridled enthusiasm over the potential uses of atomic power.”[21] Under pressure from Eisenhower, the commission pushed the nuclear power program, and the first reactor was completed in 1957. But the program’s impact internationally was even greater. The Eisenhower administration was eager to push peaceful nuclear technology out into the world and created a nuclear assistance program that shared research reactors and other nuclear technology with many other countries, contributing significantly to the spread of nuclear capability around the world. In retrospect, the administration seems to have both underestimated how it might boost the aspirations of some states for nuclear weapons and overestimated its ability to control the nuclear behavior of others. In 1955 and again in 1957, the United Nations sponsored the International Conference on the Peaceful Uses of Nuclear Energy. President Eisenhower’s suggestion that an international nuclear agency be established resulted several years later in the creation of the International Atomic Energy Agency, and the inspection requirements associated with the Atoms for Peace program’s assistance contained the seeds of the agency’s eventual safeguards system.

With a serious push from the highest levels of the US government, the civilian applications of nuclear technology were elevated in priority, and by the late 1950s—more than a decade into the nuclear age—tangible progress was made on a number of fronts, notably in establishing a civil nuclear power industry. Moreover, in certain sectors, such as nuclear medicine and food irradiation, civil applications over the years became important, well established, and widely used. However, many nuclear dreams never came true. The atomic energy vitamin never materialized. With one exception, the nuclear propulsion programs failed. While the US Navy first succeeded in using nuclear reactors to power many of its vessels, no nuclear automobiles, aircraft, or rockets were ever achieved.[22] Perhaps most significantly, nuclear power never lived up to the expectation of providing abundant, cheap energy. A nuclear power industry was created, of course, but nuclear power proved to be costlier, riskier, less competitive, more difficult, and more unpopular than expected. As a result, it played a much more limited role in overall energy production than the optimists had foreseen. For long periods in subsequent decades, nuclear power was simply not commercially competitive compared with alternative sources of energy, and years passed without any new reactors. Time and experience revealed the costs and limits of civilian applications of nuclear technology. It seems fair to conclude that as of 2017, compared to the enthusiasms of the late 1940s and the grandiose visions of the Eisenhower years, the peaceful nuclear revolution has had disappointing results.

In the United States, the peaceful uses of nuclear technology emerged sluggishly out of a government monopoly, in part because of a top-down process. Though Eisenhower was keen to see the peaceful atom exploited, at no point was this aim the highest priority. The civilian applications were subordinate to and probably impeded by the weapons program. Indeed, the Eisenhower administration presided over a prodigious expansion in the US nuclear arsenal (some twenty thousand weapons existed by the end of Eisenhower's term); thus, the weapons program had first claim on labs, personnel, budgets, and nuclear materials. During the 1950s, a sustained effort moved civilian nuclear activities into the private sector with some success, but extreme secrecy, strict regulation, and the scarcity of nuclear expertise in the commercial world constrained progress. The unfettered market was not a powerful factor in the early civilian exploitation of the atom, and when the market did come into play, it effectively limited the expansion of nuclear power. More generally, in areas that had been expected to yield large, possibly revolutionary gains, such as power and propulsion, programs were either discouraging or unsuccessful. The "techno-atomic utopia" never arrived.

Apart from cyber's distant origins as a military program, little in the peaceful nuclear story maps well into the cyber era. Cyber did not burst on the scene as a revolutionary weapon but made itself felt as an extremely useful civilian technology that took hold gradually, then spread rapidly far and wide. The development of civilian cyberspace did not encounter disappointing limits that truncated its reach; instead, it accelerated into the computerization of everything from watches to automobiles and to the creation of vast networks of communications and commercial activity. It is doubtful that the early users of email envisioned websites supplanting retail stores, but it did happen.

The extent and diversity of cyberspace reflect not a government monopoly and policy edicts from on high but a lively, decentralized, fast-moving private sector acting in a heavily populated, highly competitive marketplace. The rise of the Internet, according to one recent account, is explained by "innovation from the edge"—that is, "multiple perspectives originating from multiple places in an industry with almost no concentrated decision-making."[23] While cybersecurity is certainly now on the agenda of governments and attracting serious attention from defense ministries, no cyber weapon overshadows and circumscribes the civilian cyberspace. In numerous fundamental ways, the nuclear experience and the cyber context are completely different.

Seeking Security in the Nuclear Age

How could security be achieved in the nuclear age, in the presence of weapons so devastating? What strategies, policies, and postures would protect state interests without provoking catastrophic war? At the beginning of the nuclear age, these questions were raised not simply in response to the emergence of a dangerous new weapon but also in the context of a growing global rivalry with the Soviet Union, a powerful adversary that was itself nuclear armed after 1949. These concerns became core issues in the foreign and defense policies of the nuclear antagonists.

In the struggle to find answers, some offered radical solutions. Given the revolutionary existence of nuclear weapons, some believed that what was required was a new world order marked by global governance or by the banishment of war or some other visionary scheme. The famous Russell-Einstein Manifesto of July 1955 warned of the perils of nuclear weapons, for example, and stated plainly that the continued existence of the human species was "in doubt." This declaration raised what Bertrand Russell and Albert Einstein called "the stark and dreadful and inescapable" problem of the nuclear age: "Shall we put an end to the human race; or shall mankind renounce war?"[24] Others believed that the only genuine answer was disarmament—the elimination of nuclear weapons—or the placing of nuclear weapons under international control. In 1946 reflecting in part the extravagant hopes for the United Nations and the large fears of nuclear technology, the United States put forward an unsuccessful plan for the international control of nuclear energy.[25] However, visions of a peaceful future in which the nuclear danger had been tamed were overwhelmed by the intractable realities of international politics. The decades after World War II were marked not by effective international government, disarmament, and the banishment of war but by ceaseless confrontation, the massive accumulation of nuclear weapons, and the division of the world into hostile blocs.

Though visions of escaping nuclear danger by reinventing international politics failed, efforts to find solutions to the problem of security in the nuclear age persisted. The first quarter century of the nuclear age was marked by intensive deliberation and debate on how to address the threat posed by nuclear weapons. By 1970 a considerable literature on nuclear strategy and policy existed, and a broad framework of concepts for minimizing or constraining the nuclear threat was in place.[26] Four large ideas shaped the evolution of the nuclear order: deterrence, damage limitation, arms control, and nonproliferation. How did these ideas work in the nuclear context, and how relevant are they to the world of cyber?

Deterrence

The central concept that emerged for managing nuclear weapons and constraining the risks of nuclear rivalry was deterrence. The core idea was to prevent nuclear attack by the threat of severe nuclear retaliation. Given the enormous destructiveness of nuclear weapons, no attack would be worth the price of absorbing a nuclear counterstrike. Retaliatory strikes, of course, required that some nuclear forces would survive a nuclear first strike. Thus, preserving a second-strike capability became the essential precondition for achieving an effective deterrent posture. To achieve this stabilizing capability, the Soviet Union and the United States deployed large numbers of forces on diverse platforms, with some protected by hardened silos, some hidden in the sea, and some held on high levels of alert.

Over the course of the Cold War, nuclear experts engaged in arcane debates about potential vulnerabilities of the nuclear forces, the required size and character of the retaliatory force, and the type and number of targets that must be threatened to achieve deterrence. But the key insight of deterrence theory was this: If each side understood that the other was capable of nuclear retaliation, then neither side would have an incentive to strike first; and if both sides are vulnerable to devastating nuclear attacks, then each will have an incentive to avoid conflict. This condition of mutual vulnerability, in which the civilian societies on both sides are regarded as hostages, was thought to provide a kind of stability. If each side heeded the dictates of deterrence theory, then a condition of mutual assured destruction (or MAD, as it was known) would prevail and prevent the use of nuclear weapons.

Is deterrence relevant to the world of cyber threats? In principle, the same concept could apply—that is, preventing attacks by threatening retaliation. And in some contexts—notably when states launch intentional cyber attacks, probably in the connection with a wider international conflict—perhaps the concept of deterrence can be adapted to the cyber world. However, several considerations circumscribe the utility of deterrence in addressing cyber threats. First, the concept of deterrence arose in a bipolar context and was aimed above all at influencing the behavior of a single coherent state, the Soviet Union. But there is no such clarity in the cyber world. The threat could emanate from anywhere. Far from being bilateral, the threat is omnidirectional. Because the barriers to entry are low and the vulnerabilities are many, just about any state could be the source of a cyber attack (as indicated by the fact that one notable case involves North Korea). However, cyber capabilities are widely distributed not just among states but among organizations and individuals as well. The attacker could be a terrorist group or a criminal gang or a crazed individual. Can a deterrence posture be effective against a diverse and multitudinous set of potential threats?

The cyber deterrence challenge is compounded by a second consideration, the problem of attribution. US intelligence would have had no doubt who was attacking if the Soviet Union had launched a nuclear strike against the United States, but identifying the source of a cyber strike may not be easy. The number of potential attackers is vast, and clever attackers have ways of hiding or camouflaging their identities. Deterrence can be undermined if it is not clear against whom retaliation should be directed. If the attribution problem becomes more tractable, then this concern will weaken. But to the extent that attribution remains a challenge, retaliatory threats lose value.

A third consideration is that the protagonists in a cyber fight may not be symmetrically vulnerable. It was clear during the Cold War that the cities, the economic infrastructures, and the militaries of both the Soviet Union and the United States were vulnerable to nuclear attack. But in the cyber context, one party may be much more dependent on cyber assets than another. The United States is vastly more dependent on the cyber world, for example, than is North Korea. Is it likely that North Korea will be deterred by the threat of cyber retaliation? The problem may be even more difficult if the attacker is a non-state actor. How does one threaten terrorist groups or criminal organizations, much less individuals, with cyber retaliation? In short, asymmetries in cyber infrastructure and reliance on cyber assets may complicate fashioning effective retaliatory threats.

Finally, nuclear deterrence rests on assured destruction of enormous magnitude, posing an unmistakable threat of unacceptable damage. Cyber attacks are more uncertain in effect. Some imaginable attacks, such as those on critical infrastructure or military command and control, could have large consequences. But their effects may be unpredictable, temporary, or even short term; they may be thwarted by a clever defender; or the disruptions may be minimized by redundancies or resilience built into the defender's systems. No doubt some attacks could be quite damaging, but it is not certain that they would result in unacceptable damage; indeed, it is not even clear what unacceptable damage *is* in the cyber context. Any use of nuclear weapons will have devastating consequences. The same is not true of cyber. As a result, mobilizing credible and effective deterrent threats in the cyber context is more complex.

Despite these difficulties, it may still be possible, at least in some contexts, to persuade adversaries that the costs of a cyber attack exceed the benefits. Joseph Nye has suggested, for example, that modern economies are so interconnected that a cyber attack by one country on another—say, by China on the United States—can be self-harming if the resulting economic damage hurts the attacker's economy. Nye's term for this is "deterrence by entanglement."[27] But the difficulties and uncertainties associated with a doctrine of cyber retaliation have led to consideration of other sorts of retaliatory measures. When a cyber attack amounts to an act of war, retaliation using conventional military forces is seen as legitimate and can be considered.[28] This logic undoubtedly applies only to a small subset of cyber attacks, many of which are too minor or too ineffective to warrant a state of war. But perhaps cyber deterrence can take the form of credible threats of retaliatory attacks by conventional forces. Further, to deter severe, large-scale cyber attacks, perhaps nuclear retaliatory threats will come into play. In its discussion of "maintaining deterrence in the cyber era," for example, the Defense Science Board has stated that "the top of that escalation ladder is the present US nuclear deterrent."[29]

Most likely, we are still in the early stages of thinking through the relationship between cyber threats and deterrence. In the nuclear realm, the basic idea of deterrence arose soon after World War II, but some of the classics of nuclear strategy—including such notable works as Bernard Brodie's *Strategy in the Missile Age* or Thomas Schelling's *Arms and Influence*—did not appear until fifteen or twenty years after the detonations at Hiroshima and Nagasaki. Moreover, the debate over the requirements for and the reliability of nuclear deterrence raged throughout the Cold War. If the nuclear experience is any indication, then we can expect that years of wrestling with the idea of cyber deterrence lie ahead. What does seem clear, however, is that it will not be simple or straightforward to adapt the core nuclear concept of deterrence to the cyber world. Cyber deterrence may prove useful in some contexts, but it will be at best a partial solution to the problem of cyber threats. Complexities abound, and as a result deterrence is not likely to play the overwhelmingly central role that it does in the nuclear context. As one prominent analysis of cybersecurity concluded, "The force that prevented nuclear war, deterrence, does not work well in cyber war."[30]

Damage Limitation

Theorists and arms controllers promoted mutual deterrence as a policy, championed it as a desirable state of affairs, and loved the stable nuclear environment that was thought to result from this approach. To the military organizations charged with managing the nuclear arsenals, and to many of the civilian authorities to whom the militaries were answerable, there existed what was generally seen as an inescapable responsibility to be prepared to fight a nuclear war if necessary. And if nuclear war came, then it seemed obvious and compelling that one of the overriding goals would be to limit the damage to one's society as much as possible. In this framework, mutual assured destruction was a condition to be resisted rather than an objective to be sought. As Robert Jervis has observed, resistance to mutual deterrence "led to a number of attempts to escape from vulnerability."[31] In terms of military doctrine and operational preparations, the notion of damage limitation has occupied a central place in thinking about nuclear weapons and the threat they pose.

In the nuclear realm, damage limitation has had both offensive and defensive components. The offensive dimension entailed the contemplation of various first-strike options. The optimal damage-limiting scenario involves a disarming first strike on an opponent's nuclear forces, but the goal of mutual deterrence, of course, with its enormous emphasis on survivable forces, was to eliminate such preventive war temptations. The argument still remained that if escalation to nuclear war seemed likely, then it was better to strike first, degrade the opponent's forces as much as possible, and deal with the "ragged retaliation" by the other side's residual forces rather than contend with a comprehensive and coherent attack by the full, undamaged arsenal of the attacker. Such preemptive incentives exist even if disarming strikes are not possible. During the Cold War, both the Soviet Union and the United States made extensive preparations for the first use of nuclear weapons despite the mutual deterrence relationship that was thought to exist between them.

There is no question that offensive cyber attacks are possible and indeed have been happening.[32] But is offensive damage limitation a useful concept in the cyber context? Preventive attacks aimed at eliminating or degrading an opponent's cyber capabilities are rendered difficult by the decentralized and widely distributed global nature of cyber infrastructure and by the ubiquity of access to the Internet. A cyber attacker need not rely on its own infrastructure, and cyber attacks need not originate from the attacker's territory. Non-state attackers, of course, will in most cases have neither cyber infrastructure nor territory. In addition, whether or how much an opponent's capability is degraded, and for how long, will be very difficult to assess. With respect to preemptive cyber attack—that is, striking first in response to an opponent's preparations to strike—the options are limited by the opaqueness of the cyber world. Lacking any visible mobilization prior to a cyber attack, and hence having no warning of attack, makes a preemptive strike impossible.

States will have multiple reasons for conducting offensive cyber operations: to seek information, to punish adversaries, to undermine WMD programs, and to support conventional military operations. No doubt offensive damage limitation will be among them. But as with deterrence, the notion of damage limitation fits imperfectly with some realities of the cyber threat. Nevertheless, the goal of disrupting an opponent's capabilities as much as possible is likely to remain enticing. And whereas nuclear weapons came to be regarded as unusable in all but the most extreme circumstances, cyber attacks are a routine occurrence.

Nuclear damage limitation also has a defensive dimension. The vast destructiveness of nuclear weapons, the huge numbers of weapons that the Cold War superpowers amassed in their arsenals, the fact that deploying offensive rather than defensive capabilities is easier and cheaper, and the impossibility of developing perfect missile and air defenses make it difficult to envision achieving meaningful levels of defense. Indeed, concerns that an offense-defense arms race would provoke ever higher offensive deployments without providing significant protection led to the 1972 Antiballistic Missile Treaty, which placed severe limits on the deployment of missile defenses by the Soviet Union and the United States. Nevertheless, interest in defenses persisted, substantial investments in research and development on defenses were sustained, and the wisdom of remaining defenseless while relying on deterrence was recurrently challenged. Most memorably, President Ronald Reagan in his famous 1983 "Star Wars" speech announced a program aimed at achieving high levels of defense. And in the early 2000s, the United States exercised its legal right to withdraw from the Antiballistic Missile Treaty and began to deploy missile defenses. This move was prompted in part by the emergence of smaller nuclear threats, such as North Korea, against whom some level of defense is more feasible. The instinct to defend is a powerful one even in the nuclear context, where costs are high, progress is slow, and benefits are circumscribed.

This same instinct is evident in the cyber domain. Here, damage limitation is at the heart of much of the discussion concerning how to use defensive measures to respond effectively to cyber threats. A central concern is to protect critical infrastructure—such as electricity grids, nuclear power plants, the financial system, and key industrial facilities—from cyber attack. Similarly, today's most powerful states place major priority on preventing opponents from disrupting or degrading the military cyber capabilities on which these states rely. Because cyber is central to a wide array of economic, social, and military activity, a huge range of disruptive or destructive attacks is possible, and the cyber terrain to be defended is quite extensive. Many of what might be called damage-limitation measures figure in thinking about cyber defense. For example, critical infrastructure can be insulated as much as possible from the cyber world. Cyber assets can be "hardened"—that is, made more difficult to penetrate. Key cyber functions can be hidden or shifted frequently around the cyber infrastructure. Relying on redundancy can complicate an attack and possibly prevent an attacker from achieving his or her objectives. Similarly, investment in rapid recovery capabilities may allow a defender to ride out an attack and still function afterward. Much can be done to limit and neutralize the threat of cyber attack.

However, cyber shares with nuclear one fundamentally important attribute: effective defense is very hard to achieve because vulnerabilities are endemic to the technology. In its 2013 report, for example, the Defense Science Board observes that US cyber networks are based on "inherently insecure architecture" and concludes that "with present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber attacks ."[33] Thus, as in the nuclear case, defenses in the cyber world are desirable but difficult. While they will surely be pursued, for the foreseeable future there will be limits to what can be achieved. The nuclear revolution has meant living with an inescapable level of vulnerability despite our best efforts; the cyber revolution may mean the same.

Arms Control

Another approach to taming the danger of nuclear weapons began to emerge around 1960. In the Soviet-American context, the key insight was that nuclear war posed a massive, existential threat to both antagonists; hence, both had a profound interest in avoiding it. The idea of arms control was to mitigate nuclear danger by constructing a managed competition via negotiated constraints. Though the rivalry remained intense, the two antagonists could nevertheless collaborate in the joint pursuit of their shared interest in preventing a nuclear catastrophe. Beginning around 1970, nuclear arms control became a regular and central, if occasionally interrupted, feature of Soviet-American relations. It has remained so for nearly fifty years, even after the demise of the Soviet Union.

Arms control generally falls into one of three categories:

- *Limits on forces and force postures.* Many of the major strategic arms control agreements focused on placing limits on the size, character, and modernization of nuclear forces.
- *Crisis management measures.* Some arms control arrangements put in place institutions and procedures for containing the danger of crises, principally through communication and consultation.

- *Confidence-building measures*. These steps are aimed at dampening the intensity of the competition and preventing misunderstandings through such measures as information-sharing, prenotification of military exercises or missile tests, and regular consultations.

Over a period of decades, the Cold War protagonists built up an extensive web of treaties and arrangements (not all of them nuclear) that shaped their relationship and governed their nuclear competition.

Could negotiated arms control help manage the cyber environment? The answer is mixed. Some aspects of the Cold War's arms control experience do not translate into the cyber world. Strategic arms control treaties, for example, were preoccupied with observable objects and activities and were centered on things that could be counted. The parties generally believed that it was only possible to limit what could be verified. It was, however, possible to verify nuclear arms control agreements, including by remote surveillance using what were labeled national technical means.

The cyber world does not have a discrete force posture that can be constrained by numerical limits. Further, it is hard to see how sufficient levels of transparency and verifiability can be attained; hence, cyber arms control would be limited in scope. Moreover, cyber arms control will need to encompass a huge universe of actors if it is to fully address the potential sources of threat. Multilateral arms control is possible, of course, and some significant multilateral nuclear treaties, signed by large numbers of states, do exist. But in the cyber arena, states are not the only actors and, in the eyes of some, are not even the most important actors. As P. W. Singer and Allan Friedman comment in their study of cybersecurity, "There is a notion that the Internet is a place without boundaries, where governments do not matter and therefore do not belong."[34] It will not be easy to fashion multilateral cyber arms control in an environment in which states are not necessarily the dominant players and in which serious threats can emerge from an infinite mélange of individuals, corporations, criminal organizations, and terrorist groups, as well as from states.

For these reasons, neither traditional nuclear arms control as practiced between the United States and the Soviet Union nor multilateral nuclear arms control as it has existed in the past seem a promising model for cyber. There are too many relevant actors, too few countable objects, and too little verifiability for these approaches to be effective shapers of the cyber environment. However, there may still be room for other types of arms control measures—that is, crisis management and confidence-building measures. Given the opacity of the cyber realm, the potential difficulty in identifying potential attackers, and the lack of time for assessment, deliberation, and decision-making (because cyber attacks will happen in an instant), there is great potential for confusion, uncertainty, misperception, mistaken judgments, and misdirected retaliations. Hence, some states are interested in measures that facilitate consultation, rapid and reliable communication, and cooperation in addressing shared threats (such as criminal or terrorist exploitation of cyber vulnerabilities or attacks that disrupt the cyber architecture on which all depend). Some such measures already exist and many others have been proposed.[35]

Moreover, while constructing a comprehensive global regime for cyber management may not be possible, cyber governance measures can be established in important bilateral relationships or in significant groupings of states. In May 2015, for example, Russia and China signed a cybersecurity agreement. During President Xi Jinping's September 2015 visit to Washington, the United States and China issued a joint statement that addressed an array of cyber issues. Various groupings of states have agreed to measures aimed at addressing one piece or another of the cyber problem: The G20 has tackled cyber theft, the Shanghai Cooperation Organization has condemned information war, and a group of forty-seven states has accepted the Budapest Convention on Cybercrime.[36] Thus, though some forms of arms control as practiced in the nuclear realm seem unsuitable in the cyber context, negotiated rules, procedures, and constraints evidently will influence the emerging cyber order.

Nonproliferation

In the unconstrained early years of the nuclear age, the expectation was that the number of states possessing nuclear weapons would grow steadily in the future as more states developed the technical capacity to build them. This expectation was accompanied by a fear that the dangers associated with nuclear weapons would multiply as they spread into more hands. As Albert Wohlstetter suggested in an influential study, "life in a nuclear armed crowd" seemed perilous and extremely unattractive. Accordingly, efforts to prevent the spread of nuclear weapons have been one of the main hallmarks of the nuclear order and have figured prominently in the foreign policies of the major powers. Francis Gavin argues, for example, that nuclear nonproliferation has been a core imperative of US grand strategy since the end of World War II.[37]

The legal foundation of the nonproliferation regime is the 1968 Nuclear Nonproliferation Treaty (NPT), which now encompasses nearly every state in the international system. All NPT signatories without nuclear weapons have agreed not to acquire nuclear weapons. But the nonproliferation regime does not rely on this legal instrument alone. In the nuclear realm, technological choke points impede the path to acquiring nuclear weapons. Without enriched uranium or plutonium, for instance, it is impossible to manufacture them. These materials and the technologies to produce them are in relatively few hands, and access to them is limited. In effect, an elaborate system of technology denial is in place that consists of national export control regulations and increasingly harmonized international guidelines for restricting the sale of sensitive, weapons-related dual-use items. The major suppliers of nuclear technology have also institutionalized their collaboration in the Nuclear Suppliers Group.[38] Worrisome recipients can be and are denied access to dual-use items, and all exports of some sensitive technologies (such as plutonium reprocessing) are universally discouraged. In addition, the NPT system is monitored. Any peaceful civilian facility that handles nuclear materials is subject to inspection by the International Atomic Energy

Agency (IAEA). States can circumvent the nonproliferation regime by developing indigenous technology, by acquiring dual-use items illicitly on the international black market, or by misusing existing permitted facilities (though in this latter case, inspections might detect the cheating). But on the whole, with the notable exception of North Korea, the nonproliferation system of a legal regime, combined with technology denial and inspection, has been remarkably effective at preventing the spread of nuclear weapons and the technologies to make them.

In the cyber context, nonproliferation is a nonstarter. This area is where the divergence between nuclear and cyber is clearest and most stark. For one thing, cyber technology has already spread. Globally, billions of devices are connected to the Web. Individuals commonly possess multiple devices that give them access to the Internet. The only barrier to the spread of cyber technology appears to be poverty; in the wealthier parts of the world it is ubiquitous. Second, where the nonproliferation regime is built substantially on technological choke points, no such choke points exist in the cyber arena. Rather, cyber is a market of many suppliers, rapid innovation, and widespread adoption with little leverage for restraining the spread of this technology. Finally, the nonproliferation regime is a monitored system. IAEA safeguards are applied to all facilities that handle nuclear material. No equivalent system exists for cyber, and it is hard to imagine what international inspection scheme could offer assurance against the hostile use of cyber technology. The nuclear nonproliferation experience holds little relevance for cyber.

Conclusion

Nuclear and cyber technology both raise the challenge of coping with threats of enormous potential consequence. Any use of nuclear weapons, of course, would be devastating. The same is not true of most cyber attacks, but in their most dangerous incarnation, they can cause what the Defense Science Board described as "existential" levels of damage.[39] The scale of the most threatening cyber attacks invites invocation of the nuclear analogy. The board put it plainly: "The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War. . . . The Task Force believes that the integrated impact of a cyber attack has the potential of existential consequence. While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same."[40] There is a certain symmetry here: two technological revolutions, two large and potentially existential threats, two difficult but unavoidable challenges to security policy.

The analogy, however, is imperfect. The trajectories and time lines of these two technologies have been quite different. With nuclear technology, the weapons side has been preeminent while the civilian side has been government dominated, sluggish, and less extensive than expected. For cyber, market-driven civilian applications have spread like wildfire, and concerns about security vulnerabilities have followed in the wake of its penetration into most walks of economic and social life. With nuclear, the number of relevant actors is few, the sensitive technologies are relatively inaccessible, and the weapons are generally regarded as unusable. With cyber, the number of relevant actors is enormous, the technology is widely distributed and widely accessible, and attacks are frequent (though generally low impact). Though serious worries about nuclear terrorism exist, nuclear technology is still overwhelmingly the province of states, and nuclear weapons are in the hands of only a small number of states. In striking contrast, the pace and direction of the cyber world are driven by the private sector, innovation flows from companies and individuals, the state struggles to be relevant, and cyber weapons are potentially in the hands of anyone with a laptop.

Given these differences in the ecosystems of the two technologies, it is not surprising the conceptual framework that developed to cope with the nuclear threat applies only imperfectly to the cyber world. A mix of deterrence, preparations for damage limitation, arms control, and nonproliferation has managed to keep the nuclear peace for more than seven decades. As we have seen, some of these concepts will be adaptable to the cyber world, but the nuclear framework is not directly transferrable to the cyber context. The distinctive character of the cyber threat will require a distinctive set of answers.

Notes

1. For a particularly thoughtful analysis of the cyber challenge, see, for example, Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 30, no. 2 (Fall 2013): 7–40.

2. On this theme, see also Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38.

3. Because of time zone differences, this was August 7 in Japan.

4. The identity of the location is blanked out in the original document. Truman seems to have been under the impression that Hiroshima was a purely military target, which may account for the rather elliptical language. See Alex Wellerstein, "The Kyoto Misconception," *Restricted Data*, August 8, 2014, http://blog.nuclearsecrecy.com/2014/08/08/kyoto-misconception/.

5. Harry S. Truman, "Statement by the President of the United States," White House, August 6, 1945. The document is available in Ayers Papers, subject file Army US, the Harry S. Truman Library & Museum Archives, Independence, MO, http://www.trumanlibrary.org/whistlestop/study_collections/bomb/large/documents/index.php?pagenumber=1&documentdate=1945–08–06&documentid=59&studycollectionid=abomb.

6. Ibid.

7. Eleanor Roosevelt, "My Day," August 8, 1945, Eleanor Roosevelt Papers Project, digital edition, 2008, George Washington University, https://www.gwu.edu/~erpapers/myday/displaydoc.cfm?_y=1945&_f=md000097.

8. Bertrand Russell, written just as news of Nagasaki arrived, probably on August 9, 1945, originally under the title "The Atomic Bomb." Available in Russell's collected papers at Russell Editorial Project, vol. 24 of the Collected Papers of Bertrand Russell, McMaster University, Ontario, http://www.humanities.mcmaster.ca/%7Erussell/brbomb.htm.

9. Hanson W. Baldwin, "The Atomic Bomb and Future War," *Life*, August 20, 1945, 17–20.

10. Paul Boyer, *By the Bomb's Early Light: American Thought and Culture at the Dawn of the Atomic Age* (Chapel Hill: University of North Carolina Press, 1994), 3.

11. Richard G. Hewlett and Francis Duncan, *Atomic Shield: A History of the United States Atomic Energy Commission*, vol. 2, *1947–1952* (University Park: Pennsylvania State University Press, 1969), xiv.

12. This is one of the themes, in fact, of the Hewlett and Duncan histories of the Atomic Energy Commission, especially with respect to nuclear power.

13. Boyer, *By the Bomb's Early Light*, 107. Boyer's chapter covering popular visions of the atomic future provides an arresting picture of these nuclear enthusiasms.

14. Hewlett and Duncan, *Atomic Shield*, 72.

15. Richard G. Hewlett and Jack M. Holl, *Atoms for Peace and War, 1953–1961: Eisenhower and the Atomic Energy Commission* (Berkeley: University of California Press, 1989), 41.

16. Quoted in ibid., 34.

17. Ibid., 275.

18. Ibid., 239.

19. All quotes in this paragraph are from "Text of the Address Delivered by the President of the United States before the General Assembly of the United Nations in New York City, Tuesday Afternoon, December 8, 1953," Dwight D. Eisenhower Library, Abilene, KS, http://www.eisenhower.archives.gov/research/online_documents/atoms_for_peace/Binder13.pdf.

20. Peter Lavoy, "The Enduring Effects of Atoms for Peace," *Arms Control Today*, December 2003, https://www.armscontrol.org/act/2003_12/Lavoy.

21. Hewlett and Holl, *Atoms for Peace and War*, 208, 239.

22. The success of the nuclear navy is an interesting story and important more broadly because the navy program contributed significantly to the development of power reactors. The history is detailed in Richard G. Hewlett and Francis Duncan, *Nuclear Navy, 1946–1952* (Chicago: University of Chicago Press, 1974).

23. David Warsh, "Will 'Innovation from the Edge' Help with Global Warming?," *Economic Principals*, November 29, 2015, http://www.economicprincipals.com/issues/2015.11.29/1833.html. The quote is from Warsh, from his review of Shane Greenstein, *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network* (Princeton: Princeton University Press, 2015). The concept of "innovation from the edge" is Greenstein's.

24. "The Russell-Einstein Manifesto, July 9, 1955," First Pugwash Conference on Science and World Affairs, Pugwash, Nova Scotia, https://pugwash.org/1955/07/09/statement-manifesto/.

25. See, for example, Barton Bernstein, "The Quest for Security: American Foreign Policy and the International Control of Atomic Energy, 1942–1946," *Journal of American History* 60, no. 4 (March 1974).

26. A vast literature is related to the nuclear debate. For an excellent overview, see Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989).

27. Joseph S. Nye, "Can Cyber Warfare Be Deterred?," Project Syndicate, December 10, 2015, https://www.project-syndicate.org/commentary/cyber-warfare-deterrence-by-joseph-s—nye-2015–12. Nye has developed these ideas in his essay, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 58–60.

28. For a detailed discussion of the relationship between cyber attack and the laws of war, see Oona Hathaway and Rebecca Crootof, "The Law of Cyber Attack," *California Law*

Review 100 (2012): 817–85. They point out that the law of war applies only to a small percentage of cyber attacks.

29. Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, US Department of Defense, January 2013), 40.

30. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), introduction.

31. Jervis, *Meaning of the Nuclear Revolution*, 50.

32. Numerous illustrations can be found in Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016).

33. Defense Science Board, *Resilient Military Systems*, 1.

34. P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 181.

35. For a thorough and very useful survey of existing and proposed crisis management and confidence-building measures in the cyber context, see Herbert Lin, "Governance of Information Technology and Cyber Weapons," in *Governance of Dual-Use Technologies: Theory and Practice*, ed. Elisa D. Harris (Cambridge, MA: American Academy of Arts and Sciences, 2016), 141–48.

36. Ibid., 129–32, surveys some of these developments.

37. Francis Gavin, "Strategies of Inhibition: US Grand Strategy, the Nuclear Revolution, and Nonproliferation," *International Security* 40, no. 1 (Summer 2015).

38. For a full discussion of these national and international constraints, see James M. Acton, "On the Regulation of Dual-Use Nuclear Technology," in Harris, *Governance of Dual-Use Technologies*, 8–59.

39. "*Existential Cyber Attack* is defined as an attack that is capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc." See Defense Science Board, *Resilient Military Systems*, 2. Emphasis in original.

40. Ibid., 1, 5.