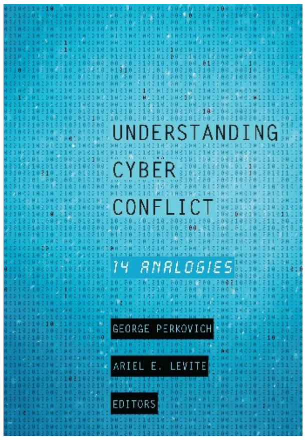
“When the Urgency of Time and Circumstances Clearly Does Not Permit . . .”: Pre-delegation in Nuclear and Cyber Scenarios

Peter Feaver and Kenneth Geers

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



13 “When the Urgency of Time and Circumstances Clearly Does Not Permit . . .”

PRE-DELEGATION IN NUCLEAR AND CYBER SCENARIOS

PETER FEAVER AND KENNETH GEERS

In a formerly top-secret document titled “Instructions for the Expenditure of Nuclear Weapons in Accordance with the Presidential Authorization Dated May 22, 1957,” the US military was notified that “when the urgency of time and circumstances clearly does not permit a specific decision by the President, or other person empowered to act in his stead, the Armed Forces of the United States are authorized by the President to expend nuclear weapons in the following circumstances in conformity with these instructions.”[1]

The significance of this directive was underlined by the fact that President Dwight Eisenhower informed Secretary of Defense Thomas Gates that the president himself had written parts of it. Furthermore, Eisenhower told Gates, “I cannot overemphasize the need for the utmost discretion and understanding in exercising the authority set forth in these documents. Accordingly, I would like you to find some way to brief the various Authorizing Commanders on this subject to ensure that all are of one mind as to the letter and the spirit of these instructions.”[2]

Eisenhower’s memo shows US national command authority wrestling with the thorniest of national security concerns—how to preserve political control when evolving technology and threats are pushing for a faster and faster response. Today the national command authority is facing similar issues in the cyber domain, and policymakers can learn from the efforts of earlier generations to adapt to the nuclear age. Cyber conflict does not constitute the same kind of civilization-ending threat that global thermonuclear war poses, but it may demand changes to the way American leaders manage national security affairs that will rival the changes wrought by the advent of nuclear weapons in the 1940s. Nuclear weapons, for example, imposed unusually dramatic constraints on traditional command-and-control (C2) arrangements; for its part, cyber conflict appears certain to strain these arrangements in new and unpredictable ways.

In this chapter, the authors examine one specific parallel, pre-delegation policy, which grants lower-level commanders the authority to use special weapons under carefully prescribed conditions. Three features of nuclear war drove policymakers to consider and, in some cases, to adopt pre-delegation: the speed with which a nuclear attack could occur, the surprise that could be achieved, and the specialized nature of the technology (that meant only certain cadres could receive sufficient training to be battle competent).

Each of these features has an obvious cyber analogue. In both the nuclear and cyber domains, defenders are under a great deal of pressure to act quickly, they may be faced with conflict scenarios no one could have imagined, and they require a high level of training and technical expertise. As a result, and in both the nuclear and cyber war cases, defenders may need some level of pre-delegated authority to act quickly and capably in defense of the nation.

Thus, the "letter and spirit" of Eisenhower's memorandum is also the topic of this chapter as it addresses the possibility that certain national security threat scenarios may oblige the national command authority to do something it would much prefer not to do—that is, to authorize military action in advance, without knowing exactly when and how it will be used.

Nuclear Pre-delegation

Early in the nuclear age, policymakers recognized a trilemma inherent in the nuclear revolution.[3] The first two horns of the trilemma constituted the "always-never dilemma": political authorities demanded that nuclear weapons always be available for use, even under the most extreme conditions (e.g., after a surprise attack), while at the same time stipulating that they would never be used accidentally or without proper authorization. Many measures designed to assure the "always" side of the dilemma posed risks for the "never" side, and vice versa. The third horn of the trilemma was that nuclear weapons should have the highest level of civilian control, far in excess of what was required for conventional military weapons and operations. Here, some measures designed to ensure strict civilian control tended to exacerbate the always-never dilemma. What happened in practice? In fact, the evolution of the US nuclear C2 system reflected an ongoing set of compromises that balanced myriad risks against these three desiderata.

As the Soviet nuclear arsenal grew in size and lethality, the challenges of this trilemma became more acute. What if a sudden illness, a natural disaster, or a surprise military attack killed or incapacitated the president, and perhaps other senior leadership figures, before he or she could even begin to manage a war? What if tactical commanders received warning of an attack or actually came under attack but political authorities delayed in responding? For certain weapons, this could create a "use them or lose them" scenario. What should US nuclear commanders do in these dire scenarios, and how could we ensure that they would not violate the principles of always, never, and civilian control?

One controversial measure designed to address these concerns was the pre-delegation of use authority (hereafter, pre-delegation), in which the president spelled out carefully delineated procedures in advance that would authorize when and how nuclear weapons could be used by tactical commanders. Of course, some form of pre-delegation is as old as warfare itself. As Martin van Creveld observed, even Stone Age chieftains wrestled with the challenges of command in war, and part of their solution likely involved explaining to the other warriors what they should do under certain anticipatable circumstances.[4] For centuries, and before technological advances solved the problem of communicating at great distances, ground and especially naval commanders departed on their missions with orders that spelled out in greater or lesser detail what political authorities expected the commanders to do while out of communication range. Indeed, some form of pre-delegation is inherent in the president's function as chief executive officer; unless the president can delegate certain of his or her powers and duties, little in the country would ever get done.[5] In 2014 Lt. Gen. Dave Deptula, USAF (Ret.), responded to a question on micromanagement in this way: "It's absolutely easy . . . trust your tactical level commanders . . . delegate engagement authority to the lowest possible level . . . give engagement authority to the people who are closest to the problem and who can observe what's going on."[6] In 2015 a paper from the Naval War College argued that the dynamic and rapidly evolving nature of the cyber domain demands that US Cyber Command (CYBERCOM) adopt the decentralized C2 doctrine of maneuver warfare to maximize the effectiveness of military cyberspace operations.[7]

Faced with the trilemma of always, never, and civilian control, US national command authorities updated the familiar tool of pre-delegation to the unfamiliar constraints of the nuclear age. It has long been known that between the Eisenhower and Gerald Ford administrations, up to seven unified and specified commanders, at the three- and four-star levels, possessed the authority to launch nuclear weapons.[8] In 1950 Commander in Chief of Strategic Air Command (CINCSAC) Gen. Curtis LeMay argued that senior officers must be able to act in the event Washington were destroyed by a surprise Soviet attack. Later he believed that he had gained this de facto authority.[9] In 1957 LeMay informed a presidential commission: "If I see that the Russians are amassing their planes for an attack, I'm going to knock the shit out of them before they take off the ground."[10] His successor, CINCSAC Gen. Thomas Power, informed Congress that he possessed "conditional authority" to use nuclear weapons. During the 1962 Cuban Missile Crisis, Supreme Allied Commander Europe Gen. Lauris Norstad was given prior authority to use nuclear weapons if Russia attacked Western Europe.[11]

The nature and scope of nuclear pre-delegation have been highly classified information in the US nuclear establishment, so the public record is murky and filled with holes. However, since 1998, a number of documents were declassified that have filled in some gaps.[12] The most dramatic revelation was the declassification of new information on "Project Furtherance," a plan that, under certain circumstances, provided for "a full nuclear response against both the Soviet Union and China," specifically "in the event the President has been killed or cannot be found."[13] In the memo dated October 14, 1968, President Lyndon Johnson's advisers recommended changes to the existing authorities: to allow the response to be tailored either to the Soviet Union or to China, to limit the response to a conventional attack at the nonnuclear level, and to outline these instructions in two documents rather than one. These revelations indicate that pre-delegation extended well beyond the use of nuclear weapons in a defensive role.

In 1976 the United States reportedly planned to revoke some, if not all, of the provisions for nuclear pre-delegation that it had established in the 1950s.[14] Currently, it is not publicly known whether any pre-delegation of authority to launch nuclear weapons continues to exist and, if so, under what constraints. However, based on recently declassified documents, into the 1980s American war planners clearly still were addressing the threat of decapitation and the difficulty of maintaining connectivity with national command authorities during a nuclear war, and pre-delegation was at least one of the options under debate.[15]

The Pros: Why Nuclear Pre-delegation

The primary benefit of pre-delegation is that it reliably circumvents the threat that an enemy could interdict communications between national command authorities and nuclear operators, decapitate the nuclear arsenal, and render it impotent. Moreover, pre-delegation accomplishes this while simultaneously reinforcing the legal chain of command. The pre-delegated instructions take the place of the orders that the national command authority presumably would have given in the scenario if it had been possible to do so; thus, pre-delegation makes the actions legal.

Pre-delegation is preferable to presidential succession, which transfers all presidential authority to subordinate officials. The Constitution and the Presidential Succession Act of 1947 prescribe a cumbersome process of succession from the president to the vice president, to the Speaker of the House, to the president pro tempore of the Senate, and finally to the cabinet officers (in the order of when the department was established). But a nuclear war could kill many if not all of these civilians suddenly or at least render them incommunicado. Given the secrecy and complexity of nuclear war planning, it is doubtful that more than a handful of these officials would be ready to manage a war, especially a nuclear war. In short, national security planners have good reason to fear that the constitutional line of succession would move too slowly during an extreme national security crisis.

A crisis-oriented alternative to succession is the "devolution" of military command, in which the president as commander in chief is replaced by the secretary of defense, who would be immediately followed by the next highest-ranking military officer, and so on. However, it is highly likely that any practicable system of de facto devolution of command would quickly diverge from the de jure line of succession. Furthermore, devolution as a national plan would seem to rest on shaky political and legal ground. It is doubtful that US civilian leadership would ever agree to cede so much power to the US military automatically, and the Supreme Court may not uphold it as constitutional. Finally, devolution of command creates the problem of "multiple presidents" if communications links with one or more of the officials in the chain of command are reconstituted and then lost again as a crisis evolved.

Pre-delegation is on much stronger legal ground and is thus preferable to devolution of command. Pre-delegation gives conditional, de facto authority to certain trusted commanders while keeping de jure authority with elected civilian leadership. Moreover, pre-delegation allows for fine-tuned civilian control since the pre-delegated authority can be as restrictive or permissive as desired. Thus, pre-delegation appears to reinforce civilian control of nuclear weapons. Last, pre-delegation allows the president to reassert command and control if communications are restored.

It is not enough, however, to have policies and doctrine aimed at mitigating the trilemma. Political authorities must also understand doctrine and actively support the policies. Military doctrine without political buy-in cannot be sustained indefinitely. Over time, gaps will emerge between what political leaders think military doctrine is and what military officers understand it to be. During a crisis, this lack of mutual understanding could lead to response failures or other breakdowns in command and control, proving disastrous for the nation.

In sum, compared with the alternatives, and provided that political authorities fully comprehend what they are doing, pre-delegation is simple and easy to implement. Building hardened command, control, and communications (C3) networks to withstand every possible worst-case scenario would be prohibitively expensive, even if it were technologically feasible in the first place. Pre-delegation offers a ready stopgap for unforeseen circumstances that could defeat C3 networks in the United States and is, by comparison, essentially free.

The Cons: Why Not Nuclear Pre-delegation

The pre-delegation of nuclear authority has an age-old Achilles' heel, human nature. For the system to work in the extreme scenarios when it would be needed, it couldn't be stymied by technical measures that physically block its use (such as a permissive action link or other coded systems that separate possession from usability[16]). Pre-delegation was intended as the solution for cases in which all communication with political authority would be broken. Therefore, a military commander possessing pre-delegation authority must also have everything that he or she would need to give a legitimate launch order. Logically, a commander with pre-delegated authority must be able to make an unauthorized use look authorized to anyone downstream in the chain of command. Thus, pre-delegation favors the "always" side of the trilemma at the expense of the "never" and the "civilian control" sides. These risks are tolerable provided that commanders honor the terms of their pre-delegated authority—that is, they must operate with complete integrity. Of course, the nuclear establishment invests extensive resources to ensure such integrity, but this risk is not inconsequential.

Pre-delegation seems to imply that de jure political control would give way very quickly to de facto military control and that there would be some level of automaticity to nuclear retaliation akin to the interlocking mobilizations of World War I or to the Soviet Union's "Dead Hand" system.[17] In short, pre-delegation poses a strain on civil-military relations. As personified by General LeMay and parodied in *Dr. Strangelove*, in war as in peacetime, civilian and military leaders may have different tendencies. On the one hand, military officers may want to use nuclear weapons in preemptive or retaliatory action to protect assets, forces, or territory, even if the bombs explode over domestic or allied territory. They may feel a certain pressure to "use them or lose them." On the other hand, civilians might prefer to absorb tactical military losses for other perceived strategic gains, such as to prevent an escalation of the conflict.

As a concept, pre-delegation is simple, but in practice it must be a highly complex mechanism. For example, how far down the chain of command should nuclear authority go? How wide should the latitude be and how specific the instructions? It is hard to anticipate in advance what would be the preferred course of action under scenarios that can only dimly be imagined. In practice, for pre-delegation to be effective, prescribed conditionality would have to be balanced with implied flexibility, yet having too much interpretive latitude with nuclear weapons is undesirable. And how public should pre-delegation policy be? Revealing some information helps deterrence, but revealing too much gives the enemy opportunities to figure out how to defeat the system.[18] It is worth noting that presidential delegations of authority should be published in the *Federal Register*, but this never happened with nuclear authorities.[19] Finally, how should nuclear authority revert to civilian control? In theory, it should happen as soon as reliable communication with the president or his or her successor is restored, but in practice it would be difficult to accomplish during a rapidly unfolding crisis.

Theoretically, pre-delegation could apply to both offensive and defensive weapons. However, the case for nuclear pre-delegation is much stronger for defensive weapons, such as air defense missiles tipped with nuclear warheads. Defensive weapons have a very short operational window to be effective, and the consequences of an unauthorized defensive use may be less severe than for an unauthorized offensive use. Defensive nuclear weapons would explode primarily over US and Canadian airspace. By contrast, offensive weapons would detonate on enemy territory, greatly increasing pressure to escalate the crisis.

However, even defensive pre-delegation scenarios threatened the territory of other states, and this proved to be one of the most sensitive and difficult aspects of the policy. The declassified record shows that President Eisenhower reluctantly acquiesced to pre-delegation policy; however, he became personally involved in the acute political challenge of pre-delegating nuclear activity that directly threatened our closest allies. In the declassified notes from a top-secret meeting held on June 27, 1958, "The President stressed the weakness of coalitions as bearing on this matter [referring to the pre-delegation of authority to fire nuclear air defense weapons]. He recalled that this was largely the secret of Napoleon's success, which was not seen until Clausewitz wrote about it. He recalled that Clausewitz had stressed that war is a political act—we must expect the civil authorities to seek control."[20]

Cyber Pre-delegation

While the nuclear revolution began with a massive explosion in the New Mexico desert, the cyber revolution has quietly sneaked up on us. The Internet has provided innumerable benefits to civilization, but a looming downside is that we may have grown too dependent on a range of networking technologies that are quite vulnerable to attack. Although we are still at the dawn of the Internet era, almost every kind of network-connected critical infrastructure has been targeted by hackers: air traffic control, financial sector, elections, water, and electricity.[21] Over time, this problem may only get worse, as formerly closed, custom information technology systems are replaced with less expensive commercial technologies that are both easier to use and easier to hack.[22] National security thinkers rightly worry that militaries, intelligence agencies, terrorists, insiders, and even lone hackers will target such systems in the future.

Cyber weapons do not pose an immediate, apocalyptic threat on the scale of nuclear weapons. For the foreseeable future, the always-never dilemma will not apply in the cyber domain quite like it applies in the nuclear domain. Indeed, in the nuclear era, apart from the bombs dropped on Hiroshima and Nagasaki, the US military always prepared for nuclear war but never fought it. By contrast, the US national security establishment (as well as the private sector) is almost always under some form of cyber attack even though many victims (and other key stakeholders) have scarcely begun to prepare for it. The United States may have a low tolerance for the kind of catastrophic cyber attack envisioned in worst-case scenarios, but it manifestly has a high tolerance for the low-level cyber attacks that its citizens endure every day.

Still, as the infamous Morris worm of 1988 and the more recent Stuxnet computer worm illustrate, there are reasons to worry about the intended and unintended effects of authorized and unauthorized use of cyber weapons.[23] And we do not know how damaging a cyber attack could be. In mid-February 2016, the *New York Times* reported that Operation Olympic Games (the alleged cyber attack on Iran's nuclear program) may actually have been dwarfed by Nitro Zeus, a proposed cyber attack that would have disabled Iran's air defenses, communications systems, and crucial parts of its power grid.[24] Moreover, cyber has a novel dimension that naturally generates concern about political control: the line between the military-intelligence and civilian-commercial domains is unclear, and activities in one domain will almost certainly seep over into the other, raising sensitive privacy and civil liberty concerns. As a result, on the notional spectrum from bayonets to ballistic missiles, cyber weapons are often considered to be closer to the ballistic missile end and, thus, much like nuclear weapons, require extraordinary C2 arrangements. After all, even conventional weapons have rules of engagement. In the cyber domain, we can expect politicians to act more conservatively not least because of uncertainty over impacts on civilian systems and challenges of attribution.

The cyber battlefield is new and evolving quickly. Iran may have waited two years to retaliate for Stuxnet, eventually hitting targets in three countries: Saudi Aramco, Qatari RasGas, and multiple US banks.[25] North Korea conducted a preemptive cyber attack against Sony Pictures Entertainment in a vain attempt to prevent the release of a satirical Hollywood movie about a Central Intelligence Agency (CIA) plot to assassinate North Korean leader Kim Jong-un.[26] In such cases, the nature and timing of a national response will usually be a complex and time-consuming process. In the former case, the Federal Bureau of Investigation (FBI) recently indicted seven Iranians; in the latter, President Obama announced that the United States would "respond proportionally . . . in a place and time and manner that we choose."[27]

There are three important analogues between nuclear attacks and cyber attacks: malicious code can travel across computer networks at lightning speed, successful cyber attacks are often based on novel ideas (the archetype here is the zero-day vulnerability plus exploit, which only the attacker knows about), and computer security is a complex, highly technical discipline that many decision makers do not understand. These three characteristics—speed, surprise, and specialization—may force national civilian leadership to give tactical military commanders a pre-delegated authority to operate in cyberspace so that they are able to competently and successfully defend US computer networks.

Yet the cyber challenge differs from the nuclear one in two key aspects—attribution and impact. Together, they point to the need for caution in adopting the nuclear era "fix" of pre-delegation. In cyberspace, it is often difficult to know with certainty who is attacking you, at least until a full-scope investigation is complete. This poses a significant obstacle to quick retaliation. There are analogous concerns in the area of nuclear terrorism, but for most of the Cold War, the attribution concern from state-based attacks was a secondary consideration. Ballistic missiles have a return address. In addition, if cyber attacks do not pose an existential threat to American society, they also do not pose the always-never dilemma. Therefore, it is politically fraught to assume the risks inherent in pre-delegation because the benefits and requirements are more open to debate. Pre-delegation was controversial during the nuclear era, when the C2 exigencies made it seem necessary. By contrast, cyber commanders should have more difficulty than their nuclear predecessors did in convincing political leaders on the wisdom of pre-delegation.

The Pros: Why Cyber Pre-delegation

First, planning a cyber attack may take months or even years, but once an attacker pulls the trigger, electrons move far more quickly than ballistic missiles—at close to the speed of light. In fact, even layered cyber attacks may unfold at such a high rate that pre-delegation alone is insufficient. For nuclear war, pre-delegation was deemed necessary to eliminate cumbersome interactions between national command authorities and tactical commanders; however, under most scenarios, tactical commanders would likely have enough warning to make their own deliberative response. With cyber attacks, the damage is often done before tactical commanders have a chance to collect evidence, evaluate data, and prepare a response. The cyber analogue therefore might not be the pre-delegated authority to respond but the automated authority to respond. One of the primary fears of nuclear pre-delegation was that there would be an automatic response, but with cyber attacks, the minuscule time windows involved will make some level of automation inevitable, especially to defend networks, and has led to increased discussions regarding the importance of developing autonomous systems.[28] This should be easy to pre-delegate, as long as the actions are defensive in nature. By contrast, an aggressive counterattack may not need pre-delegation because the technical challenges would require significant human intervention and deliberative planning.

Second, nuclear pre-delegation hedged against surprise attacks and unforeseen scenarios. Cyber attacks are also characterized by a high level of surprise. Information technology and cyber attacks are evolving at a blinding rate; thus, it is impossible to be familiar with every hacker tool and technique. Antivirus companies routinely gather over 100,000 unique samples of malicious code in a day, and still many cyber attacks pass undetected.[29] The most advanced attacks, which exploit so-called zero-day vulnerabilities, epitomize this challenge; such attacks are almost impossible to defend because they use a novel attack method for which there is no signature. Thus, security experts today are forced to defend against broad categories of cyber attacks instead of focusing on individual threats because it is hard to say exactly what the next cyber attack will look like.[30] The wide variety of possible attack vectors means that a cyber C2 system that restricted use authority narrowly to the topmost national command authority would likely be impotent, for by the time policymakers had figured out what was happening, and how they wished to respond, the damage would be done. Indeed, the attack may have migrated to new and unanticipated forms, always leaving policymakers several steps behind. Of course, the near-inevitability of surprise could mean that policymakers will be hard pressed to develop the carefully prescribed pre-delegation conditions of the nuclear era. Therefore, pre-delegation in the cyber domain may need to be more permissive and flexible than what was likely adopted for nuclear C2 purposes.

Third, like nuclear war, cyber war involves highly technical considerations that even dedicated policymakers are unlikely to master. The cyber sophistication of political leaders can improve with their participation in cyber exercises and their deeper familiarization with the cyber C2 system. But the rapid evolution of information technology makes it challenging even for technical professionals to keep pace, so there will likely always be a gulf in understanding between the operators and policymakers. Whereas an inability to understand the finer points of aerodynamics may not limit the quality of political guidance regarding air strikes, confusion over the nature of computer hacking could materially degrade decision-making on cyber responses. In a 2010 Black Hat conference keynote address, former CIA director Michael Hayden stated that conventional operations such as air strikes are discrete events that can be easier than cyber attacks for decision makers to manage. The president, he argued, could choose to bomb a factory at any time, but sophisticated cyber attacks take months, if not years, of painstaking, multifaceted technical subversion. Cyber pre-delegation, which would allow policymakers to develop guidance focused on desired outcomes in a deliberate manner and well before a crisis, may be the best way for political authorities to get what they want and not merely what they ask for.

Above and beyond these factors, national security decision makers around the world cannot ignore the official statements of other governments. The US military claims to employ "integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries."[31] The Israeli military claims it uses cyber attacks "relentlessly" to thwart the enemy "at all fronts and in every kind of conflict," and in peacetime it uses them to maintain Israel's qualitative military advantage over its enemies, including by influencing "public opinion."[32] The French Ministry of Defense has written that all modern military operations have a "cyber component" similar to "earth, sea, air, and space," and that the "strategic" nature of cyberspace means that operations there fall under the "highest level" of decision-making in Paris.[33] In Russia Vladimir Putin stated that "information attacks" are being used to achieve political and military goals and that their impact can be "higher" than that of conventional weapons. Anatoly Tsyganok, the director of the Center for Military Forecasting and a lecturer at Moscow State University's Global Policy Department, opined that cyber attacks are now "second in importance only to nuclear arms."[34] Given the prevalence of such high-level rhetoric, skeptics may have a point when they say the threat of cyber war is sometimes overstated, but they are living in denial if they say the threat simply does not exist.

The Cons: Why Not Cyber Pre-delegation

Cyber pre-delegation involves many of the same risks that policymakers wrestled with in the nuclear era. Pre-delegation would require trusting the cyber operators with decisions that political leaders might prefer to retain for themselves. With cyber weapons, the level to which authority would need to be delegated should be even lower in the chain of command than was needed for nuclear pre-delegation. The complexity and uncertainty of cyber mean that pre-delegation procedures could be especially fraught; specifying in advance the conditions under which certain actions would be taken might be very cumbersome. Moreover, the cyber-nuclear analogy breaks down in two ways that cut against the desirability of pre-delegation.

First, the attribution problem is much more acute in the cyber domain than in the Cold War nuclear domain. The most vexing challenge for cyber defense today is that of the anonymous hacker. Attackers hide within the international, maze-like architecture of the Internet, leaving a tenuous trail of evidence that often runs through countries with which a victim's government has poor diplomatic relations or no law enforcement cooperation. Most cyber investigations end at a hacked, abandoned computer, after which the trail goes cold. Moonlight Maze, a multiyear investigation to find a hacker group that had successfully stolen US technical research, encryption techniques, and war-planning data, discovered "disturbingly few clues" about its true origin.[35]

Vint Cerf, one of the Internet's inventors, has acknowledged that security was not an important consideration in the Internet's original design. If given the chance to start over, he maintains, "I would have put a much stronger focus on authenticity or authentication."[36] From a technical perspective, solving the attribution problem is theoretically possible. For example, the language of computer networks is now shifting from Internet Protocol version 4 (IPv4) to IPv6, which will raise the number of computer addresses from 4 billion to—for all practical purposes—infinity. Everyone and everything on planet Earth could be tagged and traced with a permanently associated number. IPv6 also supports (but does not require) Internet Protocol Security, which can be used to authenticate Internet traffic. For example, in 2006, this future capability allowed the Internet Society of China chairwoman Hu Qiheng to announce that "there is now anonymity for criminals on the Internet in China. . . . With the China Next Generation Internet project, we will give everyone a unique identity on the Internet."[37]

However, the future of cyber attribution, even in a next-generation network environment, is far from certain. Technologies such as IPv6 may be used to mitigate the threat of anonymous cyber attacks, but human rights groups fear that governments will use this new capability to quash political dissent by reducing online privacy. In 2012 the South Korean Constitutional Court overturned a five-year-old law that required citizens to use their real names while surfing the Web. Stating that the rule amounted to "prior censorship," which violated privacy, it also found the rule was technically difficult to enforce and generally ineffective.[38] Although it is possible to redress some of the Internet's current technical shortcomings, connectivity will likely continue to outdistance security for many years to come. Progress in attribution will be incremental and involve a slow harmonization of national cybercrime laws, improved cyber defense methods, and a greater political will to share evidence and intelligence.

For the time being, however, the attribution problem would often limit cyber pre-delegation to a defensive role. In the absence of reliable intelligence regarding a hacker's true identity, deterring, prosecuting, or retaliating against anyone is difficult. For example, in 2008 the US military experienced its "most serious" cyber attack ever when malicious code was discovered on US Central Command's unclassified, classified, and C2 systems.[39] The attack was presumed to be directed by a foreign intelligence agency, perhaps in Russia, but the true culprit could not be determined with precision.[40] However, the Pentagon was forced to undertake a large-scale response to the attack, code-named Operation Buckshot Yankee. Because the initial attack vector had been the insertion of a removable USB flash drive into a US military laptop in the Middle East, the Pentagon decided to issue a blanket prohibition on the use of flash drives throughout the world.[41]

The second way in which the nuclear analogy breaks down concerns impact. Nuclear pre-delegation involved extreme scenarios that were unlikely—and, indeed, never came to pass—and yet whose consequences were so daunting that political leaders saw pre-delegation as an acceptable hedge. Cyber attacks, in the extreme, could reach catastrophic levels but likely not levels contemplated at the middle range, let alone the extreme range, that were envisioned in global thermonuclear war. Some real-world examples have been alarming, but many credible national security thinkers are still skeptical of the risk posed by cyber warfare.[42] The effects of cyber attacks are often transient and may even sometimes be quickly reversed. Cyber operations typically do not move (like electrons) at light speed but at human speed, with numerous steps in a cyber "kill chain" that can be spotted and countered by defenders at numerous points in its life cycle. These aspects of cyber attacks should give victims more flexibility in decision-making relative to mitigation and response. Cyber would involve scenarios that are comparatively more likely—indeed, may already have happened—yet their consequences are not (yet) seen as so daunting that we should run the risks of pre-delegation.

Furthermore, some of the consequences of cyber pre-delegation might be readily felt, or at least perceived, in the civilian and political worlds through a loss of privacy and the politically sensitive blurring of civilian-military divides. Properly circumscribing any pre-delegated cyber authority would require common agreement on the likely threats, but cyber risk analysis and damage assessments are notoriously difficult and time-consuming endeavors. One 2013 think tank report concluded: "At present, neither the procedures nor the tools are sufficiently robust to merit a delegation of offensive cyber authorities beyond the very limited ways in which they have been utilized thus far. But a reasonable determination of whether the potential operational benefits outweigh the real and legitimate potential costs . . . necessitates further capability development, albeit in a very controlled context."[43]

At this stage in the evolution of cyber warfare, there are many more questions than answers, including national perceptions of what constitutes cyber attack, defense, and escalation. Cyber espionage and cyber attack, for example, have an odd relationship; the former is required to achieve the latter, but in fact, the latter may never actually take place. The victim, however, must take cyber espionage, especially if it occurs at a sensitive military location, as a precursor to cyber war. Many organizations today do not even have a good map of their own network infrastructure, let alone confidence in their network security. To date, still no legislation is in place that requires US commercial enterprises to employ best practices in cyber defense. Moreover, in stark contrast to a nuclear explosion, some major cyber attacks go absolutely unnoticed by the public and with only the direct participants being witting.[44] For example, according to the reporters who broke the story, the public was never supposed to know about Stuxnet, and it could be that a simple misconfiguration in some of the attack code betrayed the existence of Operation Olympic Games.[45]

If and when a real cyber war takes place, the attacker's identity should be clear because there will be other, circumstantial evidence.[46] However, the often intangible nature of most cyber attacks is likely to make cyber pre-delegation difficult for national security decision makers to approve. And if the odds of a catastrophic cyber attack are low, the consequences perceived to be manageable, and the national command authority assumed to be available to manage a cyber crisis, then the political stars may simply not align for cyber pre-delegation.

The Cyber Pre-delegation Sweet Spot?

No analogy works in all respects, but nuclear pre-delegation holds at least one clear lesson for cyber conflict: if cyber commanders do receive pre-delegation authority, it will likely be for defensive rather than offensive operations. In fact, defensive pre-delegation may be all that is needed and may even be more than is necessary to confront many cyber threats.

In stark contrast to a nuclear attack, most cyber attacks can be stopped—at least in a tactical sense—with purely defensive measures. There is no immediate need to know who the perpetrators are, where they are located, or what their true intention is. The urgency stems from a need to locate, isolate, and neutralize the malicious code as quickly as possible. Furthermore, blocking malicious data is far easier than shooting down a ballistic missile. In this light, cyber pre-delegation may not even be necessary because system administrators already have the authority and capability to protect their networks from what has become an incessant barrage of malware.

Some cyber threats, such as botnets, pose more complicated challenges and may require cyber defenders to go "outside the wire." Botnet mitigation can even entail the shutdown or hostile takeover of the botnet C2 server(s). But this type of intricate cyber operation, which normally involves the collection of evidence and acquisition of court orders, is unlikely to occur in real time. To some degree, this seems to obviate the need for cyber pre-delegation. For example, the celebrated Coreflood takedown in 2011 required both Department of Justice user notification and FBI user authorization before the federal government could remove malware from any infected computer.[47]

Still, there may be scenarios in which cyber commanders desire offensive or counterstrike options and in which there is simply no time to consult with a traditional chain of command. One could imagine that a fleeting window of opportunity would close during which crucial cyber evidence and intelligence could be gained. Here, cyber pre-delegation might be useful, but its parameters must be governed by the existing laws of war. For example, just as US forces in Afghanistan are authorized to return fire and even to pursue adversaries outside the boundaries of a military base, logically cyber pre-delegation should reflect these same principles. One limitation could be that, in hot pursuit, the counterstrike (or perhaps even a preemptive attack) could not deny, disrupt, degrade, or destroy adversary data or computer resources except when there is no other way to stop a grievous cyber attack on the United States.

Tactical cyber commanders are likely to have rules of engagement that are much more liberal than those given to nuclear commanders, because cyber attacks are simply not as dangerous as nuclear attacks. If malicious code is found already installed on a compromised US government computer, defensive actions may be straightforward, as in Operation Buckshot Yankee. If a cyber attack emanates from the US private sector, the FBI and Department of Homeland Security could take the lead with technical support from the National Security Agency and CYBERCOM if necessary.[48] When a cyber attack on the United States emanates from a foreign network, it is preferable to contact that nation's law enforcement and system administration personnel to help stop it. However, there will be occasions when foreign cooperation is not forthcoming or when there is no time for consultation before irreparable harm would be done to the United States. In this case, pre-delegation might authorize a preemptive strike or a counterattack against the offending computer or computers.

Due to the attribution problem, this pre-delegation policy should recognize that US computer networks must be protected even when the assailant is unknown. Positive cyber attribution should be required for significant retaliation, but simple, defensive blocking actions against an ongoing cyber attack should be permissible. As noted, ballistic missiles have a return address, but we may never know the true source of some cyber attacks, as we may be successfully deceived by a false flag operation. However, even without knowing the true identity of an attacker, CYBERCOM may still be able to target the proximate source of the attack according to the laws of war (e.g., with discretion, proportionality, and so on).[49] For some forms of cyber attack, such as a denial of service, the easiest and most passive form of defense is to use black holes, or silently discard the malicious traffic somewhere on the Internet, before it reaches its target.[50] For the most serious forms of cyber attack, such as a malicious manipulation of US critical infrastructure, CYBERCOM may be able to conduct a pinpoint cyber strike to terminate the malicious process(es) active on the attacking computer while leaving the other processes intact (if they are presumed to be legitimate).

If neither of these options is possible, the attacking computer may be completely shut down via cyber attack or, in extreme cases, a kinetic attack. This alternative is not ideal, because the attacking computer may have other legitimate processes or functions that could be associated with the national critical infrastructure of another country. Just as soldiers sometimes fire from within hospitals and operate against the laws of war, cyber attackers can also launch attacks from Internet servers that are related to public health and safety. Here, CYBERCOM would have to calculate risk versus reward and still minimize any collateral damage to the extent possible. Any pre-delegated cyber response should be conducted in legitimate self-defense and supported by as much public transparency as security and intelligence constraints allow. During the operation, CYBERCOM could notify the targeted computer's system administrator and national law enforcement of its actions and the rationale. In 2013 the United

States and Russia created a White House–Kremlin direct communications line between the US cybersecurity coordinator and the Russian deputy secretary of the Security Council to help manage potential crises stemming from future cyber attacks.[51]

Conclusion

The history of nuclear pre-delegation offers helpful insight into whether and how nation-states should grant pre-delegation in the cyber domain. In the United States, nuclear pre-delegation was an easy-to-implement work-around that seemed to avoid the potential pitfalls of presidential succession and command devolution. In a similar fashion, cyber pre-delegation may help national cyber commands defend critical infrastructure in the new and fast-evolving domain of cyberspace, which, like the nuclear domain, presents vexing challenges to reliable command and control.

Nuclear attacks and cyber attacks have several similarities, including speed, surprise, and specialization. Together, these characteristics could make some level of cyber pre-delegation inevitable. However, important differences between nuclear and cyber include impact and attribution, both of which national security leadership must consider before granting any level of cyber pre-delegation.

Unlike a nuclear holocaust, cyber attacks do not pose an apocalyptic threat to the United States, at least not yet. Therefore, they neither pose the always-never dilemma nor demand pre-delegation. Although attackers have a considerable tactical advantage on the cyber battlefield, it is not clear that they possess a strategic advantage. One recent study on the war in Ukraine suggested that while every facet of the crisis has been affected by cyber attacks, the cyber dimension of the conflict has nonetheless not played a critical role in the war.[52] When the element of surprise is gone, and especially if positive attribution is made, traditional political, military, and diplomatic might should determine the victor in a real-world conflict, a fact that already provides some degree of cyber attack deterrence.

The tactical advantages that hackers enjoy, however, must be addressed, and a national dialogue on cyber pre-delegation could be the right opportunity. The Internet is worth protecting as it offers a higher level of efficiency, transparency, accountability, and responsibility in government, civil society, and the marketplace. Therefore, the public should support a national effort to give cyber defenders clear rules of engagement that, in turn, would notify malicious actors (and cyber defenders) of red lines they may not cross. Finally, if some level of cyber pre-delegation already exists, it should be possible to make this policy more transparent while at the same time boosting deterrence.[53]

As with nuclear pre-delegation, a stronger case can be made for using defensive cyber weapons, especially if their impact is limited to domestic networks. However, we now know that pre-delegation during the Cold War extended beyond the use of nuclear weapons in a defensive role. It is even more likely that this would happen with cyber weapons, given their less destructive nature.

In the United States, civilian leaders demanded that they retain positive control over nuclear weapons. In the cyber domain, this will also likely be the case, as the public now spends the majority of its time connected to the World Wide Web. President Eisenhower understood that any nuclear war might take place over allied territory, and he personally took measures to address that risk. The cyber analogy is that future military conflicts will be fought on the same terrain that we use for banking, email, games, and news, all of which may come under enemy or friendly fire.

Some aspects of nuclear pre-delegation and cyber pre-delegation are similar—how far down the chain of command to go, how much latitude to give commanders for interpretation, and so on—but some characteristics of cyber conflict are unique. Information technology convergence now sends practically all communications through the same wires, so unintended damage may be difficult to avoid.[54] If any cyber attack, even in self-defense, leads to the disruption of Internet sites related to public health and safety, war crimes charges could follow. Finally, information technology is evolving so rapidly that rules for cyber pre-delegation granted today may not be valid tomorrow. That said, some aspects of modern communications could mitigate the need for pre-delegation altogether. For example, President Obama was able to sit and watch in real time the raid on Osama bin Laden's hideout in Abbottabad, Pakistan. While no real-time orders were given from the White House (so far as we know), there would have been no technological barrier to such activity. Future national decision makers will likely want to monitor operations at a similar level of intrusiveness and may choose to be more involved than the president was.

In summary, political leaders may be forced to authorize some level of pre-delegation to the military to defend national sovereignty in cyberspace, but they are also likely to be every bit as skittish about its risks. At a minimum, they will want to preserve most of the form and substance of political control.

The US experience wrestling through nuclear pre-delegation questions and scenarios during the Cold War can inform its policymakers today. Given the rapid proliferation of interest in cyber war, those same lessons learned in the United States may shed light on how other states' leaders are confronting the same challenges and opportunities. A priority for future research is to compare and contrast the US experience and interpretation of that experience with those of other relevant international actors.

Notes

Approved for public release; distribution is unlimited. The views expressed in this document are those of the authors and do not reflect the official policy or position of the Department of Defense or the US government. An earlier version of this chapter appeared in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014).

[1] "Document 3: Instructions for the Expenditure of Nuclear Weapons in Accordance with the Presidential Authorization Dated May 22, 1957," declassified on April 4, 2001,

and available at the National Security Archive, Gelman Library, George Washington University, Washington, DC (hereafter National Security Archive), http://nsarchive.gwu.edu/NSAEBB/NSAEBB45/doc3.pdf.

2. Letter from President Dwight Eisenhower to Deputy Secretary of Defense Thomas Gates, November 2, 1959, declassified on January 18, 2000, National Security Archive, http://nsarchive.gwu.edu/NSAEBB/NSAEBB45/doc2.pdf.

3. Peter Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca: Cornell University Press, 1992).

4. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985).

5. This authority is spelled out in 3 U.S.C. § 301.

6. Lt. Gen. Russell Handy et al., "C2 Battle Management," Panel at AFA—Air & Space Conference and Technology Exposition, Washington, DC, September 15, 2014.

7. Maj. Wilson McGraw, USMC, *Beyond Mission Command: Maneuver Warfare for Cyber Command and Control* (Newport, RI: Naval War College Press, 2015).

8. Paul Bracken, *The Command and Control of Nuclear Forces* (New Haven, CT: Yale University Press, 1983). See also Scott Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton: Princeton University Press, 1989); and Bruce Blair, *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, DC: Brookings Institution Press, 1985).

9. Feaver, *Guarding the Guardians.*

10. Fred Kaplan, *The Wizards of Armageddon* (New York: Simon & Schuster, 1983).

11. Feaver, *Guarding the Guardians.*

12. The first tranche of sixteen documents was declassified and published in 1998 and summarized here: "First Documented Evidence that U.S. Presidents Predelegated Nuclear Weapons Release Authority to the Military," March 20, 1998, National Security Archive, http://www.gwu.edu/~nsarchiv/news/19980319.htm. The original declassified documents are available here: "Documents on Predelegation of Authority for Nuclear Weapons Use," National Security Archive, http://www.gwu.edu/~nsarchiv/news/predelegation/predel.htm. See also Christopher Bright, "Cold War Air Defense Relied on Widespread Dispersal of Nuclear Weapons, Documents Show," November 16, 2010, National Security Archive, http://www.gwu.edu/~nsarchiv/nukevault/ebb332/index.htm. For a good summary of more recently declassified documents, see William Burr, ed., "U.S. Had Plans for 'Full Nuclear Response' in Event President Killed or Disappeared in an Attack on the United States," December 12, 2012, National Security Archive, http://www.gwu.edu/~nsarchiv/nukevault/ebb406/. See also Marc Trachtenberg, David Rosenberg, and Stephen Van Evera, "An Interview with Carl Kaysen," MIT Security Studies Program, 1986, http://web.mit.edu/SSP/publications/working_papers/Kaysen%20working%20paper.pdf.

13. "Notes of the President's Meeting," October 14, 1968, declassified, and available at the National Security Archive, http://www.gwu.edu/~nsarchiv/nukevault/ebb406/docs/Doc%205A%20Furtherance%20document%20Oct%201968.pdf.

14. Feaver, *Guarding the Guardians.*

15. As a 1978 Defense Science Board study put it, if the attack came while the president was in Washington, DC, then "it would be possible . . . for the President either to command the forces until the attack hit Washington and he was killed or to try to escape and survive, but not both." Quoted in Joint Secretariat, "A Historical Study of Strategic Connectivity, 1950–1981," Joint Chiefs of Staff (Historical Division), July 1982, declassified September 21, 2012, and available at the National Security Archive, http://www.gwu.edu/~nsarchiv/nukevault/ebb403/docs/Doc%201%20-%20connectivity%20study%201982.pdf.

16. A permissive action link is a security device for nuclear weapons, whose purpose is to prevent unauthorized arming or detonation of the nuclear weapon.

17. Keir Lieber argues that the new historiography on World War I casts doubt on the "automaticity" of the mobilization plans. On the Soviet's Dead Hand system, which provided for a nuclear response if the system detected physical signs of a nuclear strike, see Keir Lieber, "The New History of World War I and What It Means for International Relations Theory," *International Security* 32, no. 2 (Fall 2007); and David Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (New York: Random House, 2014).

18. The British resolved this public-private question with a "Letter of Last Resort," a handwritten note from the prime minister to a submarine commander that was normally kept locked in a safe and presumably never read (and then destroyed upon completion of a tour). It provided instructions for what to do in the event of a nuclear war. *See* Ron Rosenbaum, "The Letter of Last Resort," *Slate*, January 9, 2009.

19. Feaver, *Guarding the Guardians*.

20. Gen. Andrew J. Goodpaster, "Memorandum of Conference with the President, June 27, 1958—11:05 AM," June 30, 1958, declassified on April 4, 2001, available at the National Security Archive, http://nsarchive.gwu.edu/NSAEBB/NSAEBB45/doc1.pdf.

21. See Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers," *Wall Street Journal*, May 7, 2009. Regarding the financial sector, after the Dow Jones surprisingly plunged almost a thousand points, White House adviser John Brennan stated that officials had considered but found no evidence of a malicious cyber attack. For issues with elections, see Daniel Wagner, "White House Sees No Cyber Attack on Wall Street," Associated Press, May 9, 2010. In 2007 California held a hearing on the security of its touch-screen voting machines, in which a Red Team leader testified that the voting system was vulnerable to attack. See R. Orr, "Computer Voting Machines on Trial," *Knight Ridder Tribune Business News*, August 2, 2007. In 2006 the Sandia National Laboratories' Red Team conducted a network vulnerability assessment of US water distribution plants. See Chris Preimesberger, "Plugging Holes," *eWeek* 23, no. 35 (2006): 22. Regarding electricity, Department of Homeland Security officials briefed CNN that Idaho National Laboratory researchers had hacked into a replica of a power plant's control system and changed the operating cycle of a generator, causing it to self-destruct. See Evan Perez, "US Official Blames Russia for Power Grid Attack in Ukraine," CNN, February 11, 2016.

22. Preimesberger, "Plugging Holes."

23. William Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

24. David Sanger and Mark Mazzetti, "US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times*, February 16, 2016.

25. Nicole Perlroth, "In Cyberattack on Saudi Firm, US Sees Iran Firing Back," *New York Times*, October 23, 2012.

26. David Sanger and Martin Facklerjan, "NSA Breached North Korean Networks before Sony Attack, Officials Say," *New York Times*, January 18, 2015.

27. FBI, "International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector," FBI.gov, March 24, 2016, https://www.fbi.gov/news/stories/2016/march/iranians-charged-with-hacking-us-financial-sector; and Steve Holland and Matt Spetalnick, "Obama Vows US Response to North Korea over Sony Cyber Attack," Reuters, December 19, 2014.

28. Office of the Chief Scientist, "Autonomous Horizons: System Autonomy in the Air Force—a Path to the Future," vol. 1, "Human-Autonomy Teaming," AF/ST TR 15-01 (Washington, DC: US Air Force, June 2015).

29. Author interview with Mikko Hyppönen, chief research officer for F-Secure, November 11, 2011.

30. For example, there are myriad types of SQL injection, which can be impossible to predict individually and are best defended conceptually.

31. US Army Cyber Command, "Our Mission," April 26, 2016, http://arcyber.army.mil/.

32. Rotem Pesso, "IDF in Cyber Space: Intelligence Gathering and Clandestine Operations," Israel Defense Forces, June 3, 2012, http://www.idf.il/1283-16122-en/Dover.aspx.

33. Ministère de la Défense de France, "La cyberdéfense," January 19, 2015, http://www.defense.gov.fr/portail-defense/enjeux2/cyberdefense/la-cyberdefense.

34. Anastasia Petrova, "Russia to Get Cyber Troops," *Vzglyad*, July 16, 2013.

35. James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May/June 2001).

36. Joseph Menn, "Founding Father Wants Secure 'Internet 2,'" *Financial Times*, October 11, 2011, http://www.ft.com/cms/s/2/9b28f1ec-eaa9-11e0-aeca-00144feab49a.html#axzz42YZ8qj2L.

37. Thomas Crampton, "Innovation May Lower Net Users' Privacy," *New York Times*, March 19, 2006.

38. Evan Ramstad, "South Korea Court Knocks Down Online Real-Name Rule," *Wall Street Journal*, August 24, 2012.

39. William Lynn, "Defending a New Domain: The Pentagon's New Cyberstrategy," *Foreign Affairs* 89, no. 5 (Fall 2010).

40. Noah Shachtman, "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)," *Wired*, August 25, 2010.

41. Ellen Nakashima, "Defense Official Discloses Cyberattack," *Washington Post*, August 25, 2010.

42. Persuasive skeptics include Cambridge University professor Ross Anderson, former hacker Kevin Poulsen, author Evgeny Morozov, cryptographer Bruce Schneier, Professor Thomas Rid, and even the man who wrote "Cyber War Is Coming" in 1993, Naval Postgraduate School professor John Arquilla.

43. Maren Leed, *Offensive Cyber Capabilities at the Operational Level: The Way Ahead* (Washington, DC: Center for Strategic and International Studies and Georgia Tech Research Institute, 2013).

44. Martin Libicki, *Sub Rosa Cyber War* (Amsterdam: IOS Press, 2009).

45. David Sanger and Mark Mazzetti, "US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times*, February 16, 2016.

46. This was the case in Estonia in 2007, for example, when even chocolate shipments to Russia were canceled.

47. Greg Keizer, "Feds to Remotely Uninstall Coreflood Bot from Some PCs," *Computer World*, April 27, 2011.

48. The private sector organization may not be ultimately responsible for the attack; rather, a hacker may be using a compromised computer in the organization's network from which to launch the operation.

49. Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

50. Denial of service is an attempt to make a computer or network resource unavailable to its intended users, usually by sending it so much bogus traffic that it cannot respond to legitimate requests. For many networks, setting up a black hole can be done easily enough with a configuration change at an organization's external router, disposing of the unwanted network traffic.

51. Office of the Press Secretary, "Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security," White House, June 17, 2013.

52. Nation-state cyber espionage may be an exception to this rule. By 1999 the US Energy Department had determined that cyber attacks from abroad, particularly from China, posed an "acute" intelligence threat to US nuclear weapons laboratories. See Jeff Gerth and James Risen, "1998 Report Told of Lab Breaches and China Threat," *New York Times*, May 2, 1999. As stated earlier, all things nuclear may have a strategic character. See also Kenneth Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015).

53. Here is one existing US patent that specifically references pre-delegation: Craig Cassidy and Christopher Coriale, "Pre-Delegation of Defined User Roles for Guiding User in Incident Response," US Patent 20150242625 A1, filed February 24, 2015, issued August 27, 2015.

54. Ross Dawson, "The Flow Economy: Opportunities and Risks in the New Convergence," in *Living Networks: Leading Your Company, Customers, and Partners in the Hyper-Connected Economy* (Upper Saddle River, NJ: Financial Times/Prentice Hall, 2003).