

Detering Strategic Cyberattack

Deterrence by denial might provide an effective model for protection against future cyberattacks. However, this approach presents several challenges.



DAVID ELLIOTT
Stanford
University

The concept of deterring adversaries by possessing demonstrated means to inflict unacceptable damage in retaliation for an attack has existed throughout history, as has the concept of an impenetrable defense to discourage or frustrate attacks (“deterrence by denial”). Deterrence in practice has varied over time and depended on an era’s technology.

Most recently, nations (particularly the US) have applied these concepts in much greater detail to nuclear forces. Debate over the US nuclear forces’ adequacy, the survivability of its retaliatory capacity, and the practicality of successful defense occupied the nation. A distinct literature arose around the specifics of retaliatory targeting to maximize its deterrent effects. In addition, normative deterrence through international legal restraints evolved, extended deterrence (in which the US provides a nuclear umbrella to its allies) arose, and a form of self-deterrence owing to collateral consequences emerged.

The growing prospect of cyberattacks directed at military and civilian targets (particularly a nation’s cyber-dependent infrastructure) as an important adjunct to war, or even as a separate act of coercion or punishment, has kindled interest in deterrence’s role in constraining such attacks. (See, for example, Initiative 10 of US President Barack Obama’s “Comprehensive National Cybersecurity Initiative.”¹) Does the deterrence regime that’s the most highly developed—the nuclear one—provide guidance for the deterrence of cyberattacks?

The (often necessary) lack of access to details of

nations’ specific techniques, procedures, and policies regarding cyberattacks and defense limits full public examination of these matters. But this doesn’t rule out useful study. (For example, see the US National Research Council’s open reports.^{2,3}) Furthermore, though the potential targets of cyberattack are diverse, I focus here on strategic deterrence to protect the essentially civilian national infrastructure. (Broader examinations of cyber deterrence issues appear elsewhere.^{3–5})

A Compelling Demonstration

The destruction of Hiroshima and Nagasaki made a permanent impression on the world, and the atmospheric tests of the H-bomb convincingly demonstrated the scale of ruin that could result from nuclear war. To the extent that nuclear deterrence is psychological at the elemental level, these events are central factors.

Regarding cyberattacks, no attack or demonstration has provided images and dread comparable to that of Hiroshima and Nagasaki. Notable attacks—involving Estonia and Georgia, for example—have been more disruptive than damaging. The recent introduction of the Stuxnet worm, directed at Iranian centrifuge controllers, had a specific target and wasn’t intended to have broad national effect. And, the purported Israeli spoofing of Syria’s air defenses by cyber means before the attack on the reactor site near Tal al-Abiad was more tactical than strategic.⁶ Deterrent lessons haven’t emerged in any of these instances. In-

stead, they might have motivated others to undertake the development of cyberattack capability.

A large emulation might make cyberretaliation's consequences more tangible, but that would be costly, expose sensitive techniques, and likely seem contrived and unconvincing. (Considerations such as these presumably were factors in the US's decision not to conduct a noncombat demonstration of the first atomic bomb as the Franck Committee had proposed.⁷)

Political leaders in any country will learn about the risk posed by an in-kind retaliatory response from those responsible in their governments for the development and conduct of cyberattack capacity, those in charge of national cyberdefense, and those who estimate other countries' retaliatory capabilities. This story will be highly qualified and will unlikely have a great deterrent effect, particularly for countries less reliant on cybernetworks than the US. So, barring an often-mentioned but perhaps fanciful electronic Pearl Harbor of the future,⁶ visceral deterrence won't likely be a strong inhibiting factor.

Identifying the Attacker

Credible retaliation depends on being able to unambiguously identify the attack's source. US nuclear strategy presumes that any large nuclear attack against the US homeland will be delivered by means traceable to its perpetrator. A small number of nuclear weapons could be secreted in the US or its ports and triggered remotely. However, such scenarios have been discounted, for various reasons, as a significant threat from most nuclear-armed states.

The situation is quite the contrary regarding cyberattacks: uncertainty in the attribution of the attack's origin will probably be a major limiting factor. However, states with strategic cyberattack ambitions will have to pre-position the tools of attack in the targeted states. They'll also need the means to maintain, update, and synchronously trigger those tools to carry out a comprehensive, disabling attack. It's during this preparatory phase that defenders have the best chance of intercepting an attacker's preparations and learning the attacker's identity. Failing such interception, postattack forensics and traceback are demanding and would likely be a lengthy process requiring considerable international cooperation. An attacked nation might only be able to infer the attacker's identity from the global-security situation at the time, which is a weak position from which to retaliate.

Assured Response

Nuclear retaliation relies on two key factors:

- the nuclear forces' clear ability to survive an initial attack in adequate numbers, and

- the surviving forces' ability to continue under national control and to promptly inflict damage on any attacking country at a level that is unacceptable to the attacker.

No one today doubts that the US has this capacity. In addition, US conventional forces could execute a major attack against the homeland of any enemy, if the US decided not to retaliate in kind—that is, to de-escalate its response.

The US's capacity to respond in some form to a strategic cyberattack is evident, but the circumstances would determine the response's nature and speed. The US's ability to retaliate in kind is secret and will depend particularly on how successful the nation has been in developing detailed knowledge of the target's networks and infiltrating those cybersystems in advance. However, even with the ability to attack in place, ambivalence would exist about use because of the exposure of a fragile capability and the uncertainty of collateral effects. (Purportedly, former US President George W. Bush decided against a cyberattack on Iraqi banks as a prelude to US invasion in 2003 because of fear the damage would be widespread, given the financial system's global connectivity.⁸) Retaliation isn't limited to in-kind response, of course; it could take other forms, including an escalatory strike by conventional military forces directed at an attacker's homeland. Nor must retaliation be *ex post facto*. However, preemption has been more discussed than planned for in nuclear strategy, and the same constraints might operate in the cyber case.

Declaratory Policy and Targeting

The US considers it important—and to have deterrent value—to describe, broadly, the circumstances in which it might employ nuclear forces. These statements are nuanced, containing special cases and exceptions, with a helping of ambiguity. Whether a potential adversary would pay great attention to these declarations in making offensive decisions and whether the US itself would scrupulously observe its stated restraints in times of conflict are open questions.

To be able to implement the nuclear-use policy, defense officials prepare detailed plans for allocating targets and weapons at various response levels. These plans are closely guarded; a potential attacker would know of them only indirectly, if at all. This secrecy might seem a contradiction because the targets are chosen to maximize their deterrent effect, but exposure carries the risk of an adversary knowing where to concentrate its defenses.

In the years since former US President Bill Clinton recognized cyberattack as a potential strategic issue, there has been no national statement outlining

the US response to cyberattacks against military or civilian targets. Such a statement would presumably be conditional, threatening a range of responses from economic reprisal to retaliation in kind to conven-

[A nation under strategic cyberattack] might only be able to infer the attacker's identity from the global-security situation at the time, which is a weak position from which to retaliate.

tional military action. (Stephen Lukasik has described an array of possible declaratory policy statements and their underlying purpose.⁹) Such a statement's utility is uncertain; in any event, there's no sign that the current administration is considering making one. This might change, however, as the newly established US Cyber Command defines and implements its agenda. President Obama, speaking in May 2009 about the cyberthreat, said only, "We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage"¹⁰—nothing comparable to the US's nuclear posture statements.

One feature of the nuclear declarations that might be useful to the cyber case relates to proxy attack. That is, the US could make clear that if a state obtained the means of attack from another state or employed an attack facilitated by another state, both would be held responsible and subject to retaliation.

Although planners consider retaliatory cyberattack targets, the capacity to conduct an orchestrated attack with predictable and controllable results is thought to be more an option under development than a current capability. Furthermore, it will be even more important than in the nuclear case to keep such information secret to avoid premature exposure and disablement. So, specific targeting choices will be unlikely to play a part in deterrence beyond the general existential one.

Deterrence by Denial: The Role of Defense

Defense against a major nuclear attack has never achieved a level that provides a significant deterrent. The offense has had the advantage both in cost and technology. Even a reasonably effective defense has been considered inadequate given the catastrophic power of just a few weapons that elude defenses. During the Cold War, the two sides agreed to erect only a modest local defense to avoid a costly, ineffective race.

Cyberattack represents the flip side. Defense is difficult, but possible. The US's current primary strategy is to pursue a strong defense as the main answer to the

threat. Although costly, the price will certainly be less than the figures estimated for comprehensive missile and air defenses. Furthermore, although the factors haven't been specifically analyzed, the effectiveness of a partial but growing cyberdefense will scale with that growth. From an attacker's perspective, the likelihood of success will decline, the risk of discovery of preparatory actions will increase, and the cost in dollars and intelligence resources to keep up with the defense might become discouragingly high.

Deterrence by denial is, in principle, an answer to cyberattack. Reaching that goal, however, will be difficult. Short of a major reversal in US government policy and a major increase in government financial commitment, the goal might remain perpetually out of reach. Since 1996, when the Commission on Critical Infrastructure Protection made its report to President Clinton,¹¹ it has been apparent that the steps necessary to achieve strategic cyberdefenses would require a large, focused commitment by the government to secure the systems and networks under its control. And, it would also require the full cooperation of the private owners of much of the nation's infrastructure. Such cooperation would be costly in several dimensions, including the use of advanced security practices and adoption of trusted hardware and software components.¹² It would certainly be beyond the scope of normal business activity. No paradigm exists for private enterprise to undertake and budget for measures to combat threats to national security. Compounding the challenge, much of the infrastructure and many of the services involved will, for good reasons, be increasing their cyber dependence and connectivity, which brings the accompanying difficulty of securing them. (The commitment to the smart grid is a case in point.)

President Obama's 2009 assessment of the progress in securing cyberspace was bleak.¹³ In response, he established a cyber coordinator in the White House and committed his administration to

- develop a comprehensive strategy to secure America's networks,
- invest in necessary R&D,
- collaborate with the industry in finding solutions, and
- strengthen the public-private partnership critical to securing the nation's infrastructure.

These were essentially the same statements President Clinton made 10 years previously¹⁴—with the important difference that President Clinton didn't rule out having to impose security standards on private companies, whereas President Obama did. That position will most likely have to be reconsidered over time.

It will require several years to judge the adequacy

of the progress being made in defending the potential targets of strategic cyberattack, and there might be calls for basic changes in the defense model. In the meantime, without major technical advances and significant new policies, the prospect of deterrence by denial will remain uncertain.

Normative Deterrence and International Agreements

Several international agreements establish norms for and limits on weapons and their use. For nuclear weapons, all but nine countries in the world have foresworn development and possession of them. Furthermore, agreements prohibit nuclear states from helping nonnuclear states obtain such weapons, restrict the regions of the weapons' deployment, limit how they are tested, and (between the US and Russia) bound the number of delivery systems and strategic warheads. However, no specific agreements limit nuclear weapons' use other than the general restriction of proportionality in the Laws of Armed Conflict.

An important feature of arms control agreements is their verifiability. In most instances, the parties feel they can adequately verify compliance by national and international intelligence means. In a few cases, agreements contain detailed cooperative verification procedures. Several non-first-use agreements exist. These, however, don't lend themselves to verification because they don't restrict possession or preparation for retaliatory use of the weapons (which is essentially indistinguishable from preparation for first use). Non-first-use agreements' effectiveness depends on the parties' good intentions to observe their commitments and on the fear of retaliation. Perhaps surprisingly, few violations have occurred.

Given this background, would it serve the US's interest to seek an agreement that would constrain parties, perhaps as a first step, from carrying out cyberattacks on another party's critical, nonmilitary infrastructure and from transferring underlying technology and know-how to other parties? (I explored this issue in greater length elsewhere.¹⁵) The reason for restricting the prohibition to nonmilitary targets is that key states (including the US) have shown little interest in a more comprehensive prohibition. Such an agreement wouldn't be verifiable and would rely on states finding it advantageous to observe the prohibitions. Over the years, the US has been reluctant to consider establishing such strategic cyber norms, but as it finds its other primary option of robust defense to be elusive, it might revisit the question.

Escalation Control

In contrasting nuclear and cyber deterrence, the role of secondary deterrence following an attack (escalation

control) is also important to consider. The concept of nuclear deterrence relies heavily on containing escalation in instances of first use at the tactical (or non-homeland) level. Much has been written on its likely or unlikely success, but thankfully it remains untested.

The same question applies to cyber deterrence. However, since the damage from cyber escalation would be much less than that of nuclear escalation, and the targets more diverse, secondary deterrence might not provide an obvious stopping point.

Nuclear deterrence's main tenets don't transfer to the prevention or limitation of cyberconflict. The best solution in the cyber case is effective defense—deterrence by denial, an approach that was notably unavailable in nuclear deterrence. However, cyber-defense of civil infrastructure involves major hurdles, and progress to date hasn't been encouraging. President Obama has promised action, but it will be several years before we can judge these actions' effectiveness. Normative deterrence through international agreement is an additional option, but it lacks convincing means of verifying compliance. However, the history of observance of non-first-use norms might provide some positive expectations. □

References

1. "Comprehensive National Cybersecurity Initiative," White House, 2 Mar. 2010; www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.
2. US Nat'l Research Council, *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, W.A. Owens, K.W. Dam, and H.S. Lin, eds., Nat'l Academies Press, 2009.
3. "Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy," Nat'l Academies Press, Oct. 2010.
4. M.C. Libicki, *Cyberdeterrence and Cyberwar*, RAND, 2009.
5. R.L. Kugler, *Cyberpower and National Security*, Potomac Books, 2009, ch. 13.
6. R.A. Clarke and R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, HarperCollins, 2010.
7. *Report of the Committee on Political and Social Problems* (Franck Report), Univ. of Chicago, 11 June 1945; www.nuclearfiles.org/menu/key-issues/ethics/issues/scientific/franck-report.htm.
8. J. Markoff and T. Shanker, "Halted '03 Iraq Plan Illustrated US Fear of Cyberwar Risk," *The New York Times*, 2 Aug. 2009.
9. S.J. Lukasik, "A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policy for These Domains," *Proc. Workshop*

Detering CyberAttacks: Informing Strategies and Developing Options for US Policy, Nat'l Academies Press, 2010, pp. 99–122.

10. "Remarks by the President on Securing Our Nation's Cyber Infrastructure," White House, 29 May 2009; www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.
11. "Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection," White House, 11 Oct. 1997; www.fas.org/sgp/library/pccip.pdf.
12. W.K. Clark and P.L. Levin, "Securing the Information Highway," *Foreign Affairs*, Nov./Dec. 2009, pp. 2–10.
13. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," White House, 29 May 2009; www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

14. "Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0," White House, 7 Jan. 2000; www.fas.org/irp/offdocs/pdd/CIP-plan.pdf.

15. D. Elliott, "Weighing the Case for a Convention to Limit Cyberwarfare," *Arms Control Today*, Nov. 2009; www.armscontrol.org/act/2009_11/Elliott.

David Elliott is an affiliate at Stanford University's Center for International Security and Cooperation and contributes to policy research in strategic nuclear and cyber fields. He has been the US National Security Council's Director for Science and Technology, vice president of SRI International, and senior vice president of SAIC. Elliott has a PhD in high-energy nuclear physics from Caltech. Contact him at ddelliott3@aol.com.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.



Take the CS Library wherever you go!

 All 2011 issues of IEEE Computer Society magazines and Transactions are now available to subscribers in the portable ePub format.

Just download the articles from the Computer Society Digital Library, and you can read them on any device that supports ePub. For more information, including a list of compatible devices, visit

www.computer.org/csdl/epub_info.html

 **IEEE**  **IEEE computer society**