Cyber Deterrence

Tougher in Theory than in Practice?

Will Goodman

> *In theory, there's no difference between theory and practice. In practice, there is.*
>
> —Yogi Berra

How difficult is cyber deterrence? Some theorists argue that it is quite difficult.[1] These skeptics make valid points; the domain of cyberspace does pose unique challenges for an effective deterrence strategy. But treating cyber deterrence only theoretically—that is, ignoring the geopolitical context in which cyber attacks occur—unintentionally exaggerates its difficulty. Cyber deterrence proves easier in practice than it seems to be in theory because cyber attacks are ultimately inseparable from the physical domain, where deterrence has a long-demonstrated record of success.

Why Yet Another Article (Chapter, Book) on Cyber Deterrence?

Security scholars have recently given more attention to cyberspace because it has evolved into an important domain of interstate conflict. In 2007 Estonia experienced a campaign of cyber attacks that temporarily damaged its economy. Georgia experienced a similar cyber attack campaign in 2008 as an element of its war with Russia. In 2009 the United States and South Korea endured a series of cyber attacks that some suspect originated in North Korea (or Florida, or perhaps elsewhere).[2] Some

The author thanks Alex T. J. Lennon, Diego Chojkier, Lit Kilpatrick, Sergiy Chemezov, Derek Grossman, Rishi Kapoor, and Stephen Abott for their thorough review and helpful comments on earlier drafts of this article. Thanks also to Rain Ottis and Kenneth Geers of the Cooperative Cyber Defense Centre of Excellence for their assistance with research materials.

Will Goodman presently serves as an adviser on defense and veterans issues to Senator Patrick Leahy. As the assistant for plans to the assistant secretary of defense for homeland defense and America's security affairs, he oversaw operational and contingency plans, participated in national-level exercises, and managed several counterterrorism portfolios. Mr. Goodman is a graduate of Georgetown University and the University of Florida.

major powers, such as China, have adapted their military strategies to the characteristics of the cyber environment.[3] Real cases of "cyber war" and overt strategizing by government and military analysts around the world have attracted more scholars to the subject of conflict in cyberspace.

As theorists have questioned how to prevent or defend against cyber attacks in the future, they have included deterrence as a possible approach. Deterrence strategy goes back at least to Thucydides and the Peloponnesian War,[4] and the subject had a major renaissance during the Cold War as the United States and the Soviet Union sought to avoid a nuclear exchange. Since that conceptual high-water mark,[5] analysts have applied deterrence concepts to contemporary security problems, like terrorism, with at least some success.[6] Authors have asked if deterrence could prove useful in cyberspace, too.

In addition to its potential effectiveness, deterrence is cheaper than its alternative, continuous conflict. Cyber warfare like the 2007 attack on Estonia can inflict substantial economic costs on the victim.[7] When states combine cyber attacks with conventional operations, cyber attacks can cost lives.[8] Although cyber deterrence requires expenditures on new capabilities, these costs seem minor compared to an even temporary loss of networked marketplaces or vital financial information. Conflict imposes human and material costs, and deterrence, as conflict avoidance, offers a way to escape those costs. The possibility of securing cyberspace without the costs of conflict keeps scholars interested in cyber deterrence.[9]

These three factors—a future potentially filled with cyber wars, the past efficacy of deterrence in other domains, and its relatively low cost—have made cyber deterrence a popular subject for articles, chapters, and books. When Prof. James Der Derian coined the term *cyber deterrence* in a 1994 issue of *Wired Magazine*, he considered the deterrent effect that network technologies might have on the physical battlefield.[10] Scholar Richard Harknett focused the subject on conflict taking place in cyberspace itself in a 1996 article.[11] Since Harknett, at least 20 other authors have made varying contributions to the study of cyber deterrence. All this work has laid a solid theoretical foundation.

Despite the theoretical scholarship, a critical lack of case studies has created debate over the efficacy of cyber deterrence. Articles on the subject offer theories but nothing to test those theories. Theorists agree that cyberspace poses new challenges for deterrence not found in other domains, but they do not agree on whether those challenges can be overcome.[12] With

the literature consisting of nothing but theories, scholars can offer only educated opinions.

This study aims to augment the existing literature by evaluating the generally agreed-upon challenges of cyber deterrence using cases where cyber deterrence failed. The cases will demonstrate whether in fact those difficulties played an actual role in several cases of cyber conflict. Although different analysts may draw different conclusions from the evidence, using cases as the grounds for debate should give theorists more to discuss than pure theory.

Method and Findings

The analysis begins with the basics of deterrence theory, advances a brief specific theory of cyber deterrence, describes several cases of cyber conflict to illuminate and evaluate the problems of cyber deterrence, and concludes with the implications of its findings for future cyber deterrence strategies. The cases each address deterrence failures because a deterrence failure results in conflict, a phenomenon which can be studied. On the other hand, deterrence success results in the absence of conflict—in other words, the absence of an identifiable political phenomenon—so it cannot be conclusively studied. Unfortunately, evaluating why some conflicts occur cannot fully or satisfyingly explain why conflict does not occur in other cases. This method does get the conversation started, however, and analysts may presume that future cyber deterrence strategies must address at least those factors which led to cyber conflict in the cases addressed here.

Each case highlights a different aspect of cyber conflict. The 2007 Estonia case exemplifies a "pure" cyber war, where conflict took place only in cyberspace. It provides the best opportunity to evaluate the "contestability" of cyber deterrence and the potential for assigned responsibility. The 2008 Georgia case exemplifies cyber attack as one of several combined arms in an ongoing war and offers an example of the adverse effects of scalability and temporality in cyberspace as well as the potentially positive effects of futility as an element of cyber deterrence. Cases OP 1, OP 2, and OP 3[13] exemplify why cyber espionage deserves a distinct category in cyber deterrence strategies. Although these supposed cases of cyber espionage against the United States evoked anger in Americans and a desire to retaliate,[14] the refusal of the United States to reassure its potential adversaries that it will also forgo spying in cyberspace kept the government from hitting back aggressively. Among these cases, OP 3 in particular reinforces the

need for thorough investigation to avoid convicting innocent parties in cyber attacks.

This study evaluates only cases of suspected state-instigated cyber attack because states are the preeminent actors in cyberspace. States are the most capable and highly funded potential adversaries, so deterring state-based attacks will yield the greatest benefit to overall security. Moreover, if malicious state-based cyber activity decreases, states can focus their resources on defending against and prosecuting malicious nonstate and criminal activities in cyberspace. Finally, a clear articulation of what is acceptable behavior for states in cyberspace should help create norms for everyone.

The cases have major implications for future cyber deterrence strategies. The Estonia and Georgia cases reveal that attribution is not the insurmountable challenge that theoretical models suggest. While an unambiguous *strategic* cyber threat has yet to materialize, some of today's attacks may be harbingers of much worse attacks to come. While futility, interdependence, and counterproductivity are potent in the cyber domain, they have yet to prove themselves as potent as retaliation. The cyber espionage (OP 1–3) and the Estonia cases demonstrate that while reassurance cannot enforce deterrence, its absence certainly can detract from an otherwise effective deterrence posture. The Estonia and Georgia cases also prove that escalation dominance is a key component of cyber deterrence. Finally, the cases imply that the United States and other countries must be clearer about how they will respond to certain types of cyber attacks. While deterrence in cyberspace does pose challenges, the cases evaluated in this study prove that deterrence in cyberspace remains inextricably linked to the geopolitics of the physical world. As a consequence, cyber deterrence turns out to be simpler in real life than it appears to be in many theoretical models.

Deterrence Basics

While "no single theory of deterrence exists,"[15] authors offer mostly similar lists of deterrence components. For the purposes of this study, deterrence has eight elements: an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost-benefit calculation.

A state employs a deterrence strategy to protect an interest.[16] To keep adversaries from attacking the interest, a state makes a deterrent declaration,[17] "Do not do *this*, or else *that* will happen." *This* is any adversary action that would threaten the interest. *That* includes either denial

measures,[18] penalty measures,[19] or both. For other states to take a deterrent declaration seriously, the declaration must be credible and reassuring. Credibility means that the deterrent declaration is believable,[20] and reassurance means that if a state does not attack the interest, it can rest assured that it will not face penalties.[21] Fear also plays a role.[22] If a potential adversary fears the denial or penalty measures, that actor is less likely to take an undesirable action. These elements all factor into an adversary cost-benefit calculation: what are the benefits and costs of action versus the benefits and costs of restraint?[23] While these basic definitions may suffice, denial, penalty, credibility, and reassurance each deserve some further explanation.

Denial is the defensive aspect of deterrence and consists of prevention and futility. Deterrence by prevention means that if an attack is launched, defensive measures will disrupt the attack to keep it from succeeding. Deterrence by futility means that even if an attack breaches defenses, it will not have its desired effect on the target.[24] Effective prevention and futility both signify that attacks will inevitably fail and thus serve to deter even the attempt to attack.

Penalty is the offensive aspect of deterrence and consists of retaliation, interdependency, and counterproductivity. Retaliation is a familiar concept: during or after an attack, the defender launches a counterstrike that imposes costs on the attacker that outweigh the benefits gained from the initial attack. Interdependency and counterproductivity are less familiar. Interdependency means both the attacker and the defender hold the interest in common.[25] The more both parties agree on the commonality of the interest, the more costly an attack becomes for the attacker and defender alike. Counterproductivity relates an attacker's tactical goals to its strategic goals. If a defender can convince potential attackers that a tactically successful attack will frustrate larger strategic or normative goals, that may keep the attackers at bay. For example, if the United States punished the families of suicide bombers, terrorists might be deterred from suicide bombing; however, such an approach would be morally repugnant to the United States (normatively counterproductive) and would have adverse effects on broader US goals (strategically counterproductive). Retaliation, interdependency, and counterproductivity together comprise deterrence by penalty.

Credibility is the attacker's calculation of the defender's capability and intent to carry out the deterrent declaration[26] and whether the deterrent measures can be contested. Capabilities are a defender's tools of denial or

penalty: can those tools be used as described by the deterrent declaration? For example, no one would find a threat of nuclear retaliation credible if it came from a state that has only conventional capabilities. To be credible, a defender must also have the intent to use the capabilities to carry out the deterrent declaration. An attacker would not question whether the United States has nuclear weapons, for example, but an attacker might question whether or not the United States would use them to retaliate against a conventional attack. The concept of contestability is more complex. To be incontestable, deterrent measures (either denial or penalty) must be certain, severe, and immediate.[27] The less certain, severe, or immediate a deterrent measure, the less credible potential adversaries will find deterrence declarations, and the more potential adversaries will seek to test them. Capability, intent, and incontestability together define the credibility of a deterrent declaration.

Last, reassurance means giving a potential adversary a reason not to attack the interest. Reassurance most often comes in the form of reciprocal security guarantees—one state promises to forgo an activity if others do so as well. In some cases, however, it may mean other linked benefits such as foreign aid or a special trading status. While deterrence increases the potential costs and lowers the potential benefits of acting against an interest, reassurance lowers the costs and increases the benefits of inaction.

All of these components (an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost-benefit calculation) together form a strong and effective deterrence strategy.

A Theory of Cyber Deterrence

Cyber deterrence, like all other deterrence, succeeds when an adversary decides not to act aggressively. This decision follows two separate assessments: whether the costs of cyber aggression outweigh its benefits and whether the benefits of restraint in cyberspace outweigh its costs. These assessments are made partly rationally, partly irrationally. To be completely rational, a decision maker would need both perfect information about the scenario of potential conflict and the willingness to make a decision only on the basis of its strategic implications. In real life, decision makers have incomplete information, which is rife with inaccuracies, and consider many factors (personal emotions and interests, domestic politics, etc.) when making decisions. Therefore, continual dialogue, in the form of a regular exchange of deterrent messages, is the first necessary condi-

tion to deter cyber aggression. During the Cold War, the United States and the Soviet Union famously created channels for crisis and noncrisis communications (for example, "the Hotline") to engender this exchange of deterrent messages. If states currently exchange cyber deterrence messages, they do so quietly and with little fanfare—likely contributing to the prevalence of cyber attacks.

Both denial and penalty measures feed into an adversary's calculation of whether or not the costs of cyber aggression outweigh the benefits. By taking cyber attack targets offline, by making them impenetrably secure, or by making attacks impossibly futile, denial measures diminish the benefits of a possible cyber attack. Denial, however, is not in itself sufficient to deter aggression in cyberspace. Adversaries must also face some threat of penalty—which raises the costs of cyber attack—for deterrent messages to take effect. If adversaries do not face penalties, they will continue to mount unsuccessful cyber attacks until they find an effective approach. While denial admittedly cannot stand alone, strong denial measures coupled with a reasonable expectation of penalty will go a long way toward deterring cyber aggression.

In addition to strong denial measures, classical deterrence theory demands that penalty measures be certain, severe, and immediate; however, cyber deterrence emphasizes certainty more so than severity or immediacy. Because of the dire consequences involved, nuclear deterrence necessitated that mutually deterring states be able to quickly and overwhelmingly counterattack. But cyber attacks typically involve less-serious consequences, less-identifiable attackers, and a wider variety of tools for counterattack. With less-serious consequences, counterattacks do not need to involve overwhelmingly severe (and disproportionate) retaliation. Neither does the counterattack need to come immediately, for unlike a surprise nuclear first strike, few, if any, cyber attacks can render a victim state completely impotent to respond. For these reasons, neither severity nor immediacy is ultimately necessary for cyber deterrence penalty measures—only certainty.

For a cyber counterattack to be certain, the deterring state must first know who to counterattack. Gathering this information in the cyber domain is trickier than in the physical domain. It takes thorough investigation enabled by international cooperation. States that will not assist in cyber investigations can prevent the identification of the culprits behind cyber attacks. However, in such instances, victim states can, based on mutual legal aid agreements or the inherent right to self-defense, assign

responsibility for the attack to the non-cooperating state. In such cases, assigned responsibility obviates the need for further investigation and incentivizes future cooperation.

Besides knowing who to counterattack, states must also have the means and the will to counterattack to deter cyber aggression. Because cyber attacks can disable networks used to command and control military technologies, and because more and more military technologies are enabled by linkages to cyberspace, states must either inure their weapon systems to cyber attack or remove them from the grid entirely. Otherwise, in some extreme cases, a victim state may find much of its counterattack weaponry preemptively disabled. A victim state must also have the will to counterattack to convincingly threaten retaliation. In this area, cyber deterrence greatly resembles conventional deterrence. A victim state must count the cost before retaliating—if it cannot match its adversary in an escalating series of retaliations, then it should forgo retaliation in the first place. The state with escalation dominance, the coup de grâce, will eventually win. So to have an effective cyber deterrent, a state must have at least geopolitical symmetry with its adversary, if not a favorable asymmetry, to protect itself as the conflict in cyberspace escalates and spills over into the physical domain.

Last, while reassurance does not necessarily bolster cyber deterrence, its absence certainly encourages conflict. States should consider reassurance the "velvet glove" of cyber deterrence—without an iron fist of interlocking denial and penalty measures giving force to reassurance, promises to give up certain types of cyber attacks are an invitation to be victimized. Yet without some reassurances overlaying denial and penalty measures, states will never cease to probe for and exploit minor weaknesses in each others' cyber networks.

Combined, these conditions and variables add up to cyber deterrence. States must continually communicate on matters of cyber conflict to ensure that deterrent messages are projected, received, and understood. States must maintain effective denial measures and threaten credible penalties. If attacked, victim states must be able to correctly identify the responsible state or states to counterattack, either through effective investigation or assigned responsibility. States must ensure that at least some of their counterattack capabilities cannot be disabled by an overwhelming cyber first strike. Most importantly, the deterring state must have geopolitical symmetry, if not a favorable asymmetry, with potential adversaries to deter

them from cyber aggression. Last, the absence of reassuring promises can hinder states wishing to reach a stable cyber deterrence relationship. In each of the cases that follow, the absence of one or more of these variables led to a breakdown in mutual cyber deterrence.

Cyber Deterrence Failure Cases

Estonia, 2007

The cyber attacks began shortly after a decision by the Estonian government to move a WWII–era statue that memorializes the sacrifice of Soviet troops who fought against the Nazis. Since 1947, the Bronze Soldier stood at a busy intersection in central Tallinn, the capital of Estonia, but the government decision relocated it to a nearby military cemetery. Although such a change might seem minor to outsiders, moving the statue heightened tension between ethnic Estonians, ethnic Russians living in Estonia, and the governments of Russia and Estonia. According to at least one commentator, the statue symbolized that Estonia remained in the Russian sphere of influence.

This cyber barrage on Estonian government, banking, and media websites began on 27 April 2007 and lasted for 22 days. The attacks mostly consisted of huge numbers of privately owned computers jamming Estonian government and business websites with meaningless or malicious information. These "distributed denial of service" (DDOS) attacks flooded their targets with data to prevent the processing of legitimate Internet traffic.[28] Hackers also defaced websites, but these attacks seemed minor in comparison to the DDOS attacks that froze web servers, e-mail servers, and the Estonian network infrastructure. The DDOS attacks used "bot nets," or networks of infected "zombie" computers owned by potentially unwitting and innocent bystanders. The mass attacks lasted until 18 May, although isolated and easily mitigated attacks continued thereafter.[29] While police were able to quickly quell a real-world riot over the Bronze Soldier, the cyber attacks on Estonia continued for weeks.[30]

Because Estonia depends heavily on its cyber infrastructure, the attacks could have been devastating. Commentators call Estonia "a primitive cyber society" because of how integral the Internet has become for commercial, government, and interpersonal transactions. For example, Estonians vote online, 98 percent of all bank transactions occur online, doctors store

medical records online, and Estonian police and courts use an online case management system.[31]

Estonia's response to the attacks proved effective. It initially closed off parts of its network to some international traffic. States with numerous clients but few attackers were slowly permitted back onto Estonian networks. While the attacks targeted sectors of Estonian cyber society that were especially critical, the attacks did not cause serious damage because of the highly capable members of Estonia's computer emergency response team.[32]

Analysts debated and continue to debate whether or not the Russian government ordered the attacks. Only one person, an Estonian of Russian descent, was actually charged and convicted; however, Estonian officials claimed to have also identified responsible individuals in Russia.[33] Russian-language forums and websites posted instructions on when and how to execute the DDOS attacks. Some evidence has implicated Russian criminal networks as "bot net herders," or those responsible for controlling personal computers infected with bot net viruses.[34] Estonian officials claim that Internet protocol (IP) addresses belonging to members of Putin's cabinet were used in the attacks.[35] Although Russia and Estonia have a mutual legal assistance treaty which Estonia invoked after the attacks, Russia refused to assist Estonian investigation efforts. That refusal made in-depth investigation of the attacks impossible and cast a shadow of Russian culpability, or at least complicity, over the attacks.[36] During the period of the computer attacks, the Russian government also banned heavy commercial traffic with Estonia across the border bridge at Narva, seeming to provide an official sanction for anti-Estonian behavior.[37] However, none of this circumstantial evidence constitutes a conclusive "smoking gun" that proves the Russian government authorized the attack.

Disadvantages of Cyber Deterrence: Contestability. The 2007 cyber attacks on Estonia showcase a major problem for cyber deterrence strategies, contestability. Cyber deterrence messages seem contestable because of three mutually reinforcing factors: anonymity, asymmetry, and superempowerment.

Without a doubt, anonymity poses great difficulty for cyber deterrence. Because Internet protocols were not developed with identity authentication in mind, investigators must battle the anonymity inherent to the Internet every time they look for clues about who executed a cyber attack.[38] Although it may appear that a cyber attack originated in a certain computer system, that system may have served only as a transit point. In fact,

some actors may use transit points to stage "false flag operations" with the objective of fomenting strife between two other parties (e.g., Russia and Estonia).[39] Even if an investigator can verify an attacker's identity, the investigator cannot know the attacker's motive—did the attacker freelance, act on orders, or attack by accident?[40] A thorough investigation may take quite some time; some so long that the counterattack seems more like aggression than retaliation.[41] Combined, these factors lessen the likelihood that the defending state will retaliate, or if it does, that it will correctly target the responsible entities. The anonymity of cyberspace causes big problems for cyber deterrence.

The 2007 Estonia case also exemplifies the asymmetry of cyberspace. Even if investigators could attribute the attack to an actor (say, Russia), that actor may not offer Estonia any target in cyberspace worthy of retaliation. Estonia depends much more on the Internet than Russia—any Estonian counterattack on Russian networks would not have nearly the impact of a Russian attack on Estonian networks. On the other hand, states face a challenge trying to create proportional effects in the physical world. If one state has more to lose in cyberspace than another, the defending state must find other interests to hold hostage.[42] But can states really "kill people who kill bits?"[43] At the very least, cyberspace asymmetry will cause defenders to think twice before retaliating asymmetrically or disproportionately, which weakens deterrence.

Finally, the 2007 cyber attacks on Estonia illustrate how the Internet creates super-empowered actors. Although Estonia insists that others were involved, only one individual has faced criminal charges for the attacks. If an individual using a personal computer can execute an attack on major national or international targets, then individuals become the equals of states in cyberspace.[44] This poses obvious problems as states attempt to develop an effective cyber deterrence strategy. The deterring of states poses enough of a challenge; deterring super-empowered individuals seems almost impossible.

Advantages of Cyber Deterrence: Assigned Responsibility. The 2007 Estonia case does not offer only bad news. While contestability does pose challenges for cyber deterrence, cyberspace also allows for assigned responsibility. Although cyberspace may be a stateless domain, the individuals that manipulate information in cyberspace do so sitting in the real world—where states are supreme. International law and domestic criminal laws could be updated and improved to hold states responsible, make them

liable, or at least encourage mutual assistance in fighting cyber attacks that originate in their territory (like the treaty shared by Estonia and Russia that Russia failed to honor).[45] Moreover, information travels the World Wide Web along technology owned by a handful of private network infrastructure firms.[46] Although states would not retaliate against businesses for third-party traffic on their networks, states could establish agreements under which these companies would provide key information to investigators seeking to attribute malicious activity in cyberspace.[47] Cyber attacks offer the possibility of assigning responsibility to states or infrastructure providers if they refuse to help attribute cyber attacks to the guilty parties.

Why Did Cyber Deterrence Fail? Although many attackers clearly got away with participating in the 2007 attack, Estonia had the opportunity to assign responsibility to Russia—an opportunity it could not exploit because of the geopolitical imbalance between the two states. Anonymity and super-empowerment did play a role. Investigators still disagree among themselves over whether or not the evidence proves Russian culpability. They cannot conclude that Russia officially ordered the attacks, partly because super-empowered individuals could have hijacked the network addresses of Russian officials and others to make the attacks appear state sponsored. Attackers probably considered these advantages before deciding to attack.

On the other hand, Estonia could have assigned responsibility for the attacks to Russia. International law provides a basis for assigning the culpability of the attacks to Russia even if Russia did not officially direct them.[48] Setting matters of attribution aside,[49] Russia reneged on a standing mutual legal aid agreement with Estonia that required its investigation assistance. Russia's refusal to honor its international agreements meant that the perpetrators escaped justice. Attribution poses no challenge at all in the 2007 cyber attack on Estonia because Russia accepted responsibility for the attack on behalf of the guilty parties.

As a counterargument to assigning responsibility to Russia, some might question whether Russia had a legitimate reason to refuse to support Estonia's investigation—but most reasons seem strained. According to Estonian cyber investigator Rain Ottis, Estonia made "a formal investigation assistance request" to Russia that Russia refused despite "the fact that this type of cooperation is specifically 'enumerated in the Mutual Legal Assistance Treaty' between Estonia and Russia."[50] If Russia considered such investigation assistance unwise in principle, its leaders probably would not have agreed to the mutual legal aid treaty in the first place. Moreover, Russia

should have no fear of Estonian investigators exploiting its networks, since Russian investigators could observe, manage, and control the investigation assistance they provided. The facts of the case do not seem to offer Russia a good reason to refuse legal assistance to Estonia other than that further investigation might have revealed official Russian involvement.

Asymmetry also played a role in the attack on Estonia, but physical asymmetry more so than cyber asymmetry. Russia—or groups sympathetic to Russia—had cyber-bullied tiny Estonia. Certainly, Russia did not offer to Estonia the broad selection of cyberspace targets that Estonia offered to Russia. More importantly, Estonia could not have retaliated in any manner without risking further unwanted Russian escalations. Had the two states shared a more reasonable geopolitical balance, Estonia might have looked to the effects of Russia's attack—on Estonia's economy, business transactions, media, and the like—to determine a course of retaliatory action that might yield similar effects (whether the counterattacks targeted Russian cyberspace or not).[51] Instead, Russia's substantial power compared to its relatively powerless neighbor deterred Estonian retaliation. Physical asymmetry between Estonia and Russia, more so than cyber asymmetry, facilitated the 2007 cyber attack.

Estonia's cyber deterrence posture did prove as contestable as theorists have predicted but not to the degree that they have predicted. Although attribution efforts proved inconclusive, this was a consequence of Russia's refusal to honor its standing legal agreements with Estonia. That refusal gave Estonia the option of assigning responsibility for the attack to Russia. However, even if Estonia had assigned responsibility to Russia, the geopolitical asymmetry between the two states would have left it with few retaliatory options. Instead, Estonia sought to rebalance its relationship with Russia by appealing to its NATO allies to add cyber defense to the NATO charter.[52] By seeking NATO involvement in combined cyber defense, Estonia passed over retaliation in favor of improving its geopolitical parity with Russia and increasing its chances at deterring future cyber attacks through the threat of combined NATO response.

Georgia, 2008

In the summer of 2008, many days prior to Russia's military invasion of Georgia, cyber attacks began on its websites and network infrastructure.[53] These attacks effectively disabled Georgia's web-based communication with the outside world and made it very difficult to offer the global

media its perspective on the conflict. According to reports, attacks were "well-coordinated with what Russian troops were doing on the ground"[54] and lasted through the duration of the 2008 Russian-Georgian conflict.[55]

The attacks share remarkable similarities with the cyber attacks on Estonia the previous year.[56] Government, bank, business, and media websites suffered worst. To raise international awareness about the attack, Georgia had to work around its Internet blackout to plead for international support and assistance.[57] The attacks mostly consisted of DDOS, again with some limited attempts at network intrusions. Attackers even targeted Russian media outlets that provided a more balanced, occasionally pro-Georgian take on the war. Based on subsequent network activities, analysts now speculate that some intruders left malware "time-bombs" to create havoc even after the shooting war concluded.[58]

Unlike the Estonian attacks, the cyber attacks on Georgia had "a strategic economic impact." In addition to sowing general confusion, combined physical and cyber attacks diverted business from Georgian fuel pipelines over to Russian infrastructure offering a similar service at twice the expense. The attacks reinforced Russian military operations by limiting access to secondary sources of power after physical attacks disabled Georgian electrical power grids. To execute such coordinated assaults, attackers used social networking services like Twitter and Facebook.[59] According to at least one Russian media source, Georgian hackers mounted an ineffective counterattack.[60]

Georgia was less prepared than Estonia to confront the cyber assault, but its international partners and private industry jumped to assist. Estonia, Lithuania, and Poland offered to host some Georgian government websites on their better-defended systems.[61] Google also provided assistance to some of Georgia's private business websites, hosting them on higher-bandwidth Blogspot accounts.[62] Russia prevailed over Georgia in cyberspace, although at the time Georgia probably feared Russia's physical attack more than its cyber attack.[63]

Although the strategic context strongly indicates official Russian involvement, like the 2007 attacks on Estonia, investigations have not revealed a smoking gun. The Russian government may have directed the attacks, but some other organization, like the Russian Business Network (RBN), probably coordinated them. The RBN is a "cyber mafia" that traffics in child pornography, identity theft, and other web-based crime and rents its expertise, including DDOS attacks, out to the highest bidder.[64]

Computers belonging to Russian, Ukrainian, and Latvian civilians with no connections to the Russian government or military actually carried out the attacks.[65]

Disadvantages of Cyber Deterrence: Scalability and Temporality. The 2008 Russian operation against Georgia highlights a couple of additional cyber deterrence problems: scalability and temporality. Scalability refers to the wide variety of effects that a single capability can achieve in cyberspace. In the physical world, capabilities have a limited set of purposes, and "both the modalities for attack and the severity of outcomes generally scale predictably."[66] A tank, a nuclear weapon, and a balled fist all have certain predictable effects. In cyberspace, a single tool can achieve a wide spectrum of effects, making it much harder to predict the scale of an attack from attack indications and warnings. For example, during the attack on Georgia, hackers defaced government websites, causing some mild inconvenience but no long-term disruption. They also left hidden, time-sensitive viruses on government systems that unpredictably wreaked havoc on Georgian networks after the intrusions had concluded. Since the same platform and similar techniques were used for both immediate and long-term attacks, defenders were challenged to define beforehand how they would respond to certain adversary actions.

Scalability thus creates problems for establishing deterrence thresholds.[67] Because a single capability can produce a variety of outcomes, deterrence messages must address effects, not actions. A formerly simple message, "You cannot do *this*," becomes much more complicated, "You cannot do *anything* that has *these effects*." This "effects-based" approach must also account for potential effects—such as those caused by time-delayed malware. Not knowing the scale or purpose of a potential adversary's cyber activities makes it difficult to craft an effective and incontestable deterrent declaration.

Temporality refers to the instantaneous nature of cyber attacks.[68] The physical world, hampered as it is by friction, gives defenders early warning of attacks: aircraft or missile radar signatures, satellite photographs of launch preparations, massed tanks on the border. Some activities in cyberspace, like bot net viruses, "packet sniffing," and network reconnaissance,[69] indicate some kind of future malice. But these digital signals do not signify when, how, against whom, and for what purpose network intrusions or other cyber attacks might occur, whereas physical signals provide most or all of that information. Cyberspace provides no unambiguous attack signatures like those offered by the physical world.

Advantages of Cyber Deterrence: Futility. On the other hand, futility offers defenders some major deterrence advantages in cyberspace. Digital information can be replicated endlessly.[70] Redundancy and recovery—very expensive in the physical domain—cost almost nothing in cyberspace.[71] As the Georgia case proved, even if a defender has not taken precautions against cyber attack, outside assistance (like that offered by Georgia's neighbors and Google) can still quickly create redundant systems to help in recovery. Although attackers may corrupt or destroy data saved in one location, that data can have numerous copies elsewhere, rendering many cyber attacks futile and eliminating the motive to execute them.

Defenders can also render cyber attacks futile by disconnecting systems from public networks or removing known vulnerabilities. As analyst Martin Libicki points out, there is "no forced entry in cyberspace."[72] Attackers can only attack where a vulnerability in the network already exists. Removing vulnerability or taking equipment offline means any attempt to attack that equipment through cyberspace will be futile. For example, Georgian advanced air defense systems proved resilient in the face of Russian attack and shot down several highly capable Russian aircraft. Some suggest that Georgian air defenses proved less vulnerable to Russian blackout because the Georgians had not networked them.[73] Taking some critical systems off of the network may at times prove a better option than attempting to secure critical systems from cyber attack.

Why Did Cyber Deterrence Fail? The cyber attack on Georgia occurred in the context of an ongoing war with Russia in another case where geopolitical factors trumped the theoretical difficulties of cyber deterrence. Although anonymity and super-empowerment did play a role in the 2008 cyber conflict, most observers assume a connection between the Russian military attacks on Georgia and concurrent "anonymous" cyber attacks. Super-empowered private citizens did appear to play a role in the cyber attacks,[74] but Russia led the overall war effort.

Scalability also played a role rendered moot by the two countries' conventional asymmetry. As noted earlier, hackers placed malware time bombs in Georgian network systems. Deterring less-obvious cyber attack tactics like this one will prove challenging in the future. Georgia probably had more concerns about the physical bombs falling on its territory than any digital "bombs" hidden in its networks.

Cyber asymmetry, temporality, assigned responsibility, and futility also pale in importance to the geopolitical asymmetry between Russia and

Georgia. How, if it could not deter Russia's full-scale kinetic attack, could Georgia possibly hope to deter its cyber attack? Although temporality, under other circumstances, might have made it more difficult to deter a Russian cyber attack, Georgia might have also had the opportunity to invoke assigned responsibility if Russia proved unwilling to help in Georgia's investigation (creating circumstances similar to those in Estonia in 2007). However, even under those circumstances, Georgia would have had few options. To what end would it assign responsibility to Russia? It could not strike back against its behemoth neighbor. In every aspect, the geopolitical relationship between Russia and Georgia trumped the advantages and disadvantages of cyber deterrence identified by theorists.

In the case of the 2008 Russo-Georgian war, cyber deterrence did prove very difficult but not for the reasons identified by the theorists. With cyber attacks used as one of several combined arms, cyber deterrence became a lesser included subset of conventional deterrence. Between more balanced states (such as the United States and Russia), factors like mutual legal aid or, alternatively, assigned responsibility probably would have kept cyber attacks from commencing. In seeming recognition of this point, Georgia has long pushed to gain membership in NATO. While analysts interpret this desire in different ways, at least some suggest that Georgia seeks parity with Russia through combined defense.[75] As in the case of Estonian cyber conflict, geopolitics played a greater role than the challenges of cyber deterrence.

Cyber Espionage

OP 1

The US government purportedly first discovered OP 1 in March 1998, and the attacks continued through at least 2001. No apparent international crises or behaviors precipitated this series of intrusions; they consisted purely of attempts to collect information through cyber espionage. OP 1 intrusions targeted government and military cyber networks, with attackers penetrating systems by "tunneling" through routine programs and scripts, making it difficult for security analysts to detect the intrusions. According to an FBI source, OP 1 intrusions stole "unclassified but still sensitive information" about technical research, contracts, encryption, and war planning.[76]

Although investigators have not publicly identified a culprit, the OP 1 attacks appear to have come from Russian Internet addresses.[77] Some analysts outside the government conjecture that the sophistication of OP 1 suggests Russian state direction. Others consider "direction" an overstatement, but even some of these believe the attacks must be, at a minimum, "state allowed."[78] "The hackers have built 'back doors' through which they can re-enter the infiltrated systems at will and steal further data; they have also left behind tools that reroute specific network traffic through Russia."[79] While confusion about authorship lingers, circumstantial evidence again points to Russia.

The United States has pursued a few response options. First, the US government lodged a formal diplomatic complaint with Russia. Media reports state that although "hack-backs" (intruding on the systems used to launch attacks on US networks) would provide better information about the source of the attacks, investigators have relied on passive detection due to concerns about legality and the risk of creating an international incident.[80] Although OP 1 led to "the largest cyber-intelligence investigation" ever conducted by the US intelligence community prior to 2001, that investigation yielded "disturbingly few clues" about the perpetrators.[81]

OP 2

Like OP 1, OP 2 consists of attempts to collect US secrets through cyber espionage. In OP 2, hackers exploited NASA, the Sandia National Labs, and other government and military networks that contained unclassified but sensitive and proprietary information.[82] The attacks had a broad scope and collected a substantial volume of information. Regardless, officials report that OP 2 is "not the biggest thing going on out there" in the world of cyber espionage.[83]

The OP 2 attackers' methods exhibited a high level of professionalism. The attacks extracted sensitive information quickly and deliberately wiped away evidence of transiting the networks in an attempt to keep the attacks clandestine. Outside observers note that only highly skilled and experienced hackers tend to use such tactics.[84] The attackers targeted export-controlled information with substantial value to foreign governments and businesses. The OP 2 attacks pose the latent threat that hackers could shut down Pentagon or other government networks should they choose to do so.[85]

According to *Time*, the FBI and other law enforcement agencies were not up to the challenge posed by OP 2. Instead, American cyber vigilantes

got involved. One of them, supposedly with US government knowledge, hacked into Chinese routers to detect and characterize the OP 2 intrusions, gain information as to their origins, and provide a detailed report of stolen information.[86] Subsequently, the Defense Department's Joint Task Force—Global Network Operations also investigated OP 2.[87]

The US government has not openly identified suspects in OP 2. In response to media questions, Chinese government officials call claims that China backs the intrusions "totally groundless, irresponsible, and unworthy of refute." However, China has refused to cooperate with FBI investigation.[88] The *Washington Post* reports one US official as stating, "Is this an orchestrated campaign by [China] or just a bunch of disconnected hackers? We just can't say at this point."[89]

OP 3

In February 1998, Israeli hacker Ehud Tenenbaum and two California teens intruded on unclassified DoD networks.[90] According to media reports, the teens hacked the systems just for fun.[91] Their attacks followed a predictable process. First, the intruders would reconnoiter network systems to determine if a vulnerability existed. Then, if they found one, they would exploit it to gain unauthorized access to the network. Once they had network access, they would emplace a packet sniffer to gather data then return later to download the sniffer-collected data.[92]

Officials initially suspected that the attacks originated in Iraq.[93] Coming during a period of heightened tension in the Persian Gulf and as "the most organized and systematic attack to date" on Pentagon networks, according to then–deputy secretary of defense John Hamre, observers jumped to the conclusion of Iraqi responsibility based on the circumstantial evidence. A team of investigators led by the FBI eventually used technical means to track the attacks, not to Iraq but back to the three teenagers.[94]

Disadvantages of Cyber Deterrence: Lack of Reassurance. Cyber espionage highlights one more problem plaguing cyber deterrence: the lack of reassurance. Presently, few international laws or norms define acceptable and unacceptable behavior in cyberspace,[95] meaning that states cannot rest assured that they will not be targeted by cyber attacks if they refrain from targeting others. The United States may have only recently begun to consider legal restrictions on its cyberspace freedom of action,[96] but laws will help all state actors, including the United States, be assured that certain types of egregious cyber attacks will not occur.[97] The difficulty

in attributing cyber attacks to certain actors may explain why some states choose not to agree to legal restrictions on their Internet behavior. If a state considers it likely that it might be framed in a "false flag" operation, that state has little incentive to forgo attacks (since it will be blamed anyway). The absence of reassurance incentivizes hitting first in cyberspace so states can victimize others before they become victims themselves.

Advantages of Cyber Deterrence: Information Quantity and Interdependence. Cyber spies also face some difficulties. The huge amount of low-quality information in cyberspace bolsters deterrence by denial. Because individuals can generate information with so little expense, "noise" can overcome "signal."[98] To mount effective cyber espionage, spies must know the cyber terrain well. What information is worthwhile, and what is junk? Understanding, reconnoitering, and mapping networks take time; while some reconnaissance can be automated, targeted reconnaissance to steal, corrupt, or destroy the *right* information often takes human reasoning. The quantity of worthless information makes cyber espionage more difficult.

In addition to the volume of information in cyberspace, interdependency might help to deter states from cyber espionage. The nature of cyberspace is connection, and interconnectedness enforces deterrence by interdependency.[99] Part creator, part beneficiary of globalization, cyberspace allows states to "embrace" each other through electronic connections.[100] This interdependency increases the value of accurate information to all actors and increases the harm caused by inaccurate information.[101] As states connect further, the incentives of attack will gradually decrease, and disincentives will increase. This theory resembles those offered by advocates of economic interdependence.[102] Although interdependence will not lead states to ignore their vital interests in favor of economic or information benefits, they will forgo lesser interests if they see the loss of those interests as less valuable than interconnection. The more states pursue the "friendly conquest" of interconnectedness in cyberspace,[103] the more interdependency will deter cyber attacks.

Why Did Cyber Deterrence Fail? Observers cannot really know to what extent attribution difficulties played a role in cyber deterrence breaking down in these cases. Understandably, the US government is very circumspect about how much or how little it knows about cases of cyber espionage, but media reports suggest some very strong leads. In the instance of OP 3, the United States identified its attackers and brought them to justice, demonstrating that thorough and effective investigations are possible in at

least some cases of cyber espionage. Without more evidence, the innuendo surrounding the cases makes attribution seem possible.

Asymmetry did not pose that much of a challenge. In the absence of evidence, one can assume that while states like China and Russia may have less confidential information stored on networked systems than the United States, they probably do generate and store at least some confidential information on networked computer systems. If true, that symmetry makes proportional retaliation possible. For the criminals discovered in the OP 3 case, the Israeli and US governments pursued legal action. Asymmetry thus did not cause the breakdown in cyber deterrence.

More so than anonymity and asymmetry, a lack of reassurance caused deterrence to fail in the OP 1 and OP 2 cyber espionage cases. Although news reports do not mention the possibility, presumably the United States also uses cyberspace to spy. If not, it is high time to start. Although commentators and analysts alike express outrage and frustration when others penetrate sensitive US networks, the US government may be sinning as much as sinned against in cyberspace.

That lack of reassurance keeps the United States from retaliating against cyber spies. Although some columnists seem to suggest that retaliation could keep adversaries from stealing military technology secrets,[104] most retaliatory measures would seem disproportionate to espionage. If the United States demands that other states allow the FBI to investigate intrusions into US cyber networks, it must grant the law enforcement agencies of those states similar access to its own intelligence community.

The scalability of cyber attacks creates further incentives for cyber espionage and might have caused deterrence to break down. The theft of information from confidential networks may be a harbinger of much worse things to come. As the Georgians found out after the 2008 war, hackers may leave hidden code in computer systems that network administrators do not detect until after that code has done its damage. Intrusions onto US networks suggest that hackers could harm or even disable those networks if they were able to retain access to them. Such attacks would lie dormant while states are at peace but could cripple military, intelligence, and command and control networks if activated during times of war. If intrusions involve nuclear command and control networks, cyber espionage becomes an existential threat. "Precisely because [cyber attacks are] counter [command and control] warfare par excellence, the resort to [cyber attacks] almost compels a WMD-armed opponent to strike first and pre-

emptively."[105] Cyber espionage poses a much more serious *potential* threat because hackers could graduate from stealing information to harming the network itself. To deter these types of scalable attacks, states must maintain at least some retaliatory capabilities that are impervious to cyber attack.

The sheer volume of information in cyberspace has the potential to bolster cyber deterrence in the future, but it does not appear to have mattered much in these cases. Certainly, adversaries will face a diminishing return on their cyber espionage investments if the United States can hide its "signal" in the midst of an overwhelming supply of "noise." The United States could, for example, load existing networks with meaningless files and disinformation. Or, the United States could create huge numbers of fake networks with automated, human-simulated packet traffic to deceive cyber spies into wasting time with decoys. Although these strategies seem plausible, states would never reveal whether or not they employ them to avoid compromising their defenses.

Likewise, interdependence seems promising but does not appear to have strengthened deterrence in these cases of cyber espionage. If the United States could convince Russia, China, and other states that they depend equally on the confidentiality of US classified information, interdependence might diminish anticipated gains from spying. Prof. Peter Feaver makes a very strong case for the deterrent effect of information interdependence. Because intelligence operations are often compartmented, Russia, China, and other states risk confusing their own intelligence communities if they alter or corrupt secret information on US networks.[106] OP 1, OP 2, and OP 3 involve only stolen information, so interdependence has had no effect.

Although states should include cyber espionage in their cyber deterrence strategies, cyber espionage deserves distinction from other types of cyber attack. Information security consists of confidentiality, integrity, and availability.[107] Cyber espionage involving only intelligence collection harms confidentiality, but not integrity or availability. And, as scholar and professor Martin Libicki notes, "The law of war rarely recognizes [information collection] as a *casus belli*, and a good case for changing this has yet to be made."[108] So states probably could not justifiably retaliate against other states for cyber attacks involving only the collection of confidential information; however, DDOS attacks or varieties of cyber espionage, such as deception operations that harm the integrity or availability of information, could involve retaliatory measures (depending on their effects). In sum, while cyber deterrence strategies should address cyber espionage,

most forms of cyber espionage deserve separate treatment from more aggressive and harmful types of cyber attack.

The lack of mutually reassuring treaties also keeps states from retaliating against each other. In its simplest form, deterrence is reciprocity: if you do something to me, I will do it back to you, and if you forgo doing something to me, then I will forgo doing that thing back to you. If the United States does cyber spy, it will have a very tough time justifiably retaliating against other states for following its lead.

With retaliation off the table, decision makers may want to seriously consider deterrence strategies for cyber espionage based on futility, interdependence, and counterproductivity. In addition to the futility strategies discussed earlier, the United States might be able to link economic or trade benefits to restraint in cyberspace. As information gains further value, the interconnectedness of the World Wide Web might itself become a benefit the United States could use to its advantage by threatening to take it away. The United States may also have an opportunity to make successful cyber spying strategically counterproductive for other states. The legitimacy of the Chinese government, for example, largely depends on China's economic growth.[109] If cyber spying causes US businesses to purchase fewer Chinese goods or in some other way harms that growth, those effects might deter China from using cyberspace to spy.

Last, OP 3 proves that states need more than context clues to attribute cyber attacks to specific actors. Some theorists argue that investigations need not find a smoking gun because circumstantial evidence is sufficient.[110] OP 3 proves conclusively that this argument does not hold water. Had the United States proceeded with only the available context clues, it would have targeted Iraq without cause. Moreover, OP 3 demonstrates that investigators can positively attribute cyber attacks, at least in some cases, further lessening the rationale for states to shoot first and ask questions afterwards. The United States should investigate all cyber attacks to the fullest extent possible before declaring any suspect guilty.

Implications for a US Cyber Deterrence Strategy

How Difficult is Attribution?

Attribution surely poses difficulties, but the evidence suggests that it is possible in many cases. Under some circumstances, attribution may not even be necessary for deterrence.

OP 3 demonstrates that attribution is not always the impossible challenge that some commentators make it out to be. The United States clearly has the ability to link at least some cyber attacks to their perpetrators. As more and more actors recognize the need to further secure cyberspace, and as identity authentication in cyberspace improves,[111] attribution should gradually become easier.

The 2007 cyber war in Estonia also shows that definite attribution may not be necessary in every case. In some circumstances, third parties may, by shielding the guilty from investigation, make themselves a legitimate target of retaliation. If victim states do begin to assign responsibility to obstructionist third parties, those states or infrastructure providers may be deterred from protecting the culprits. Those culprits, once exposed to investigation and judicial punishment, may themselves be deterred from conducting cyber attacks in the first place.

In instances of cyber attack as a combined arm, attribution may be reasonably inferred regardless of whether private citizens or states conduct attacks. Since these attacks occur in the midst of a physical war, attribution does not pose its typical challenges.

How Much of a Problem is Scalability?

Experts bombard the public with warnings about the "strategic" cyber threat. They describe threats to US digital banking and financial information and networked critical infrastructure. The Department of Homeland Security (DHS) has even run tests to demonstrate how power generators could be remotely damaged by a cyber attack.[112] But do these threats exist outside of our collective imagination?

The attack on Estonia did not represent a strategic cyber threat. The attack did not even force Estonia to return the Bronze Soldier to its original location. Estonia responded effectively and seemed to recover quickly.

The attack on Georgia is somewhat different. Coming as it did alongside a Russian invasion of Georgian territory, this cyber attack did have strategic implications. However, if one disaggregates the effects of the cyber attacks from the physical invasion, that clarity dissipates. Would a cyber attack alone have accomplished Russia's strategic goals without the tanks and soldiers? Probably not.

The thorniest of the cases for cyber deterrence strategists are undoubtedly OP 1, OP 2, and OP 3. Although these instances of cyber espionage have not yet had a strategic effect on our national security, they might in the

future. Foreign states could, for example, penetrate critical US networks during times of peace and then lay dormant, retaining access without drawing the attention of network administrators. Then, if the foreign state and the United States ever entered into conflict, the foreign state could scale those attacks drastically upward to cripple military command and control systems at a decisive moment. Such scalable cyber attacks, coupled with physical attacks, could lead to strategic defeat for the United States. The US government must tailor its cyber deterrence messages—and its retaliatory capabilities—to prevent such a scenario from ever occurring.

Is Defense More Compelling than Retaliation?

The cases do not offer a conclusive answer to this question. Defense, especially futility, seems to have great potential in cyber deterrence strategies, but only time will tell if the defensive strategies that states employ live up to their potential.

Estonia's defensive measures offer reason for hope. At least one subsequent DDOS attack on Estonia since the 2007 case has not yielded any significant success for the attacker.[113] This kind of successful defense deters attackers from similar attacks in the future and leads them to search for new vulnerabilities. The more that defending states prove they can capably handle many varieties of cyber attack, the less attractive the cyber domain will seem as an avenue of attack.

Are Interdependence and Counterproductivety More Compelling than Retaliation?

Perhaps so, but again, the evidence lags behind the theory. In none of the cases did interdependence have a major deterrent effect. Closing the bridge at Narva to commercial traffic demonstrates that Russia does not depend on trade exchanges with Estonia, and its military domination of Georgia suggests a similar imbalance between those two states. Presumably interdependence with the United States has not kept Russia and China from cyber spying, or vice versa.

Interdependence in the cyber world seems to follow rules similar to economic interdependence, a topic addressed more completely by other studies.[114] Suffice it to say, interdependence between great powers and near-peer neighbors may have positive implications for cyber deterrence in the future, but they have not yet played a discernable role in cases of cyber attack.

The same goes for counterproductivity. Concerns that aggressive actions in cyberspace would prove politically counterproductive did not keep Russia from its role in the cyber attacks on Estonia and Georgia (whatever that role may have been). Political "fair play" does not prepossess states like Russia or China in the way that it concerns the United States and our European allies. However, because Russia and China rely on economic strength for domestic political legitimacy, the United States and other countries might find counterproductivity strategies targeting economic growth more effective than strategies focused on international political legitimacy.

Whither Reassurance?

The cases demonstrate that while reassurance might not help, its absence will certainly harm otherwise effective cyber deterrence. A lack of reassurance certainly did not prompt the attack on Estonia, since Western democratic states that strongly value the rule of law (like Estonia) are not likely to execute surreptitious DDOS attacks on other states. Likewise in the Georgia case, reassurance was not at issue. However, the cyber espionage cases show that an otherwise effective cyber deterrence posture requires reassurance. States face an uphill battle trying to deter activities in which they themselves indulge. In view of this, the United States and other countries should seek to reassure others by limiting their own aggressive behaviors in cyberspace. Without reassurance based on international and domestic law, cyber deterrence cannot reliably succeed.

How Important is Escalation Dominance?

The cases show escalation dominance comprises a critical component of cyber deterrence. Without it, Estonia and Georgia could not respond to Russia. If the United States deters strategic cyber attacks in the future, it must maintain strategic escalation dominance. If, in OP 1, OP 2, or other cyber intrusions, the United States fears command and control attacks on its nuclear weapons or other military capabilities, it should clearly indicate how it will respond to and escalate conflict in the instance that its survival appears to be at stake. Without escalation dominance, the United States will be left with no recourse in the aftermath of an attack.

Clearer and More Prevalent Deterrent Messages

US cyber deterrence languishes because other states do not understand what interests are off limits from attack and the consequences they face

for attacking those interests. If the United States considers certain types of intrusions on command and control systems harbingers of strategic attack, the government should indicate how it will overwhelmingly and justifiably respond to such attacks. Because cyber attacks have a broad spectrum of severity, the United States need not open itself up to salami tactics[115] by providing a menu-style list of punishments for various crimes. However, higher-level strategic attacks and threats should have specific and clearly delineated consequences. Last, the United States should create new channels of communication for cyber deterrence messages. While cyber deterrence may not require the level or extent of messaging necessitated by nuclear deterrence in the Cold War, senior leaders are mistaken if they believe a casual statement from time to time to domestic media outlets will suffice to deter foreign states.

Conclusion

While cyberspace does pose unique challenges for deterrence strategists, real-world cases demonstrate that those challenges can be overcome.

The 2007 Estonia case demonstrates that attribution and asymmetry in cyberspace may not be as challenging as many authors argue. Instead, assigned responsibility can alleviate the need for attribution, and asymmetry in the physical domains proves more consequential than cyber asymmetry.

The 2008 Georgia case reinforces the conclusions of the Estonia case. Although Russia might deny a role in the cyber attacks, attribution becomes a moot issue as Russian tanks roll across the Georgian border. Again, geopolitics trumped the difficulties unique to cyber deterrence.

The cases of cyber espionage demonstrate several more key points. First, without reassuring potential adversaries of reciprocal restraint, the United States will continue being the victim of cyber espionage (just as it may victimize other states). Moreover, without offering reassurance, the United States cannot legitimately retaliate against cyber spies—it must instead seek to deter these attacks through strategies of futility, interdependence, and counterproductivity. Although these areas have theoretical promise, the cases show they have not lived up to their potential.

Together, these cases have implications for cyber deterrence strategies. Attribution may be difficult, but it is not impossible. Strategic cyber attacks may not have materialized yet, but cyber deterrence strategies must account for the scalability of surreptitious cyber attacks. While futility,

interdependence, and counterproductivity have promise, they have not yet yielded the desired results. Reassurance is an important and as yet unaccounted for component of a reliable cyber deterrence strategy. Escalation dominance remains a key component of effective deterrence, including cyber deterrence. Even if the United States remains ambiguous about less-dangerous cyber threats, it must be painstakingly clear about what activities it will not tolerate in cyberspace and the consequences of those activities.

The cases and their implications demonstrate that cyber deterrence is challenging, but with a measured and realistic strategy, cyber deterrence can accomplish most of its desired effects. Yogi Berra was right. Despite theorists' predictions, cyber deterrence remains connected to the physical and political worlds and seems tougher in theory than it will turn out to be in practice. SSQ

Notes

1. Although much of the literature conveys this message, some good examples include Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica, CA: RAND, 2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf; Richard Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (Autumn 1996); and Stephen Blank, "Can Information Warfare be Deterred?" in *Information Age Anthology, Volume III: The Information Age Military*, eds. David S. Alberts and Daniel S. Papp (Washington: Command and Control Research Program, 2001), 125–57, http://www.dodccrp.org/files/Alberts_Anthology_III.pdf.

2. "US Eyes N. Korea for 'Massive' Cyber Attacks," *MSNBC.com*, 9 July 2009, http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security; and Jack Goldsmith, "The New Vulnerability," *New Republic* 241, no. 4885 (24 June 2010): 23.

3. Chris Wu, "An Overview of the Research and Development of Information Warfare in China," in *Cyberwar, Netwar, and the Revolution in Military Affairs*, eds. Edward Halpin et al. (New York: Palgrave MacMillan, 2006), 192–93.

4. Austin Long, *Deterrence: From Cold War to Long War* (Santa Monica: RAND, 2008), 5, http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf.

5. Although Cold War–era studies on deterrence are too numerous to count, Thomas Schelling offers a paramount example in *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

6. For example, Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on al-Qaeda* (Santa Monica: RAND, 2002), http://www.rand.org/pubs/monograph_reports/MR1619/MR1619.pdf.

7. In Mark Landler and John Markoff, "Digital Fears Emerge after Data Siege in Estonia," *New York Times*, 29 May 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html, the authors report that many of the attacks on Estonia targeted its banks. In Peeter Lorents, Rain Ottis, and Raul Rikk, "Cyber Society and Cooperative Cyber Defence," a paper presented at the 3rd International Conference on Internationalization, Design, and Global Development, San

Diego, CA (2009), 184, the authors reiterate that cyber attacks on the banking infrastructure of a highly networked society like Estonia's can cause serious economic losses.

8. Shane Harris, "The Cyberwar Plan: It's Not Just a Defense Game; Cyber-Security Includes Attack Plans Too, and the U.S. Has Already Used Some of Them Successfully," *National Journal*, 14 November 2009, http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php.

9. Long, *Deterrence*, 17–22, 59–61, explains this phenomenon at length, as does Libicki, *Cyberdeterrence and Cyberwarfare*, 32–35.

10. James Der Derian, "Cyber-Deterrence," *Wired Magazine* 2.09, September 1994, http://www.wired.com/wired/archive/2.09/cyber.deter_pr.html.

11. Harknett, "Information Warfare and Deterrence."

12. For examples, see Richard Kugler's optimistic chapter, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington: NDU Press, 2009); and Michael Tanji's pessimistic blog, "Deterring a Cyber Attack? Dream On . . . ," *Wired.com Danger Room*, http://www.wired.com/dangerroom/2009/02/deterring-a-cyb/.

13. OP 1, OP 2, and OP 3 are supposed cases of cyber espionage by foreign states against the United States. At the direction of security review authorities of the DoD, the author can neither confirm nor deny the existence of such or similar cases. However, the deputy secretary of defense and other US government officials have openly acknowledged and discussed, in public speeches, articles, and testimony to Congress, cases highly similar to those described by the author. The author has freely drawn from media accounts of similar supposed cases and will address their details as though they did occur. This analysis should not be misinterpreted to lend credence to any unofficial account of a case of cyber espionage against the United States.

14. See, for example, Thomas Skypek, "A Pearl Harbor by Keystroke?" *Washington Times*, 7 May 2009, Op-ed section, http://www.washingtontimes.com/news/2009/may/07/a-pearl-harbor-by-keystroke/; and Skypek, "New Cyber Attacks Showcase Need for Cyber Deterrence Policy," *Hope Is Not a Foreign Policy,* http://www.hopeisnotaforeignpolicy.org/2009/07/08/new-cyber-attacks-showcase-need-for-cyber-deterrence-policy/.

15. K. A. Taipale, "Cyber-deterrence," in *Law, Policy, and Technology: Cyberterrorism, Information Warfare, Digital and Internet Immobilization* (Hershey, PA: IGI Global, forthcoming 2010), 12, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045 #368665.

16. Andrew J. Goodpaster, C. Richard Nelson, and Seymour J. Deitchman, "Deterrence: An Overview," in *Post–Cold War Conflict Deterrence*, ed. Naval Studies Board and National Research Council (Washington: National Academies Press, 1997), 13; Kugler, "Deterrence of Cyber Attacks," 330; and Long, *Deterrence*, 8.

17. Goodpaster et al., "Deterrence," 22–23; Schelling, *Arms and Influence*, 264–74; Kugler, "Deterrence of Cyber Attacks," 326, 332; Long, *Deterrence*, 8; DoD, *Deterrence Operations Joint Operating Concept Version 2.0* (Washington: Defense Technical Information Center, 2006), 42–44, http://www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc; and Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington: NDU Press, 1996), 4, http://permanent.access.gpo.gov/websites/nduedu/www.ndu.edu/inss/books/Books%20-%201996/Information%20Warfare%20 and%20Deterence%20-%20Feb%2096/.

18. Kugler, "Deterrence of Cyber Attacks," 320, 334–35; Long, *Deterrence*, 10; DoD, *Deterrence Operations*, 26; and Taipale, "Cyber-deterrence," 13.

19. Kugler, "Deterrence of Cyber Attacks," 320, 334–35; Long, *Deterrence*, 10; DoD, *Deterrence Operations*, 26; Taipale, "Cyber-deterrence," 13; and Wheatley and Hayes, *Information Warfare and Deterrence*, 4.

20. Goodpaster et al., "Deterrence," 22; Schelling, *Arms and Influence*, 36; Long, *Deterrence*, 11; and Taipale, "Cyber-deterrence," 17–18.

21. Goodpaster et al., "Deterrence," 14; Kugler, "Deterrence of Cyber Attacks," 328; Long, *Deterrence*, 10; and DoD, *Deterrence Operations*, 27–28.

22. Schelling, *Arms and Influence*, 36–43; and Long, *Deterrence*, 7–8.

23. Long, *Deterrence*, 7; and DoD, *Deterrence Operations*, 20–23.

24. Kugler, "Deterrence of Cyber Attacks," 327; and Taipale, "Cyber-deterrence," 36–39.

25. Taipale, "Cyber-deterrence," 39–40; and Peter D. Feaver, "Blowback," *Security Studies* 7, no. 4 (June 1998): 98–111.

26. Wheatley and Hayes, *Information Warfare and Deterrence*, 4.

27. Ibid.; Taipale, "Cyber-deterrence"; and Schelling, *Arms and Influence*, 227–32.

28. For a lengthier and much more detailed and technical discussion of denial of service attacks, see Carnegie Mellon Software Engineering Institute (CERT), "Denial of Service Attacks," http://www.cert.org/tech_tips/denial_of_service.html.

29. Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs* 9, no. 1 (Winter/Spring 2008): 122–23; Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," paper presented at the 8th European Conference on Information Warfare and Security, Lisbon, Portugal, 2009, 178–79; and Landler and Markoff, "Digital Fears Emerge after Data Siege in Estonia."

30. Ottis, "Analysis of the 2007 Cyber Attacks," 177–78; Lorents et al., "Cyber Society and Cooperative Cyber Defense," 183–84; and Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, no. 3 (May/June 2008): 227.

31. Lorents et al., "Cyber Society and Cooperative Cyber Defense," 183.

32. Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, 19 May 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

33. Ibid.

34. Ottis, "Analysis of the 2007 Cyber Attacks,"178; and Libicki, *Cyberdeterrence and Cyberwarfare*, 2–3.

35. Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic."

36. Ottis, "Analysis of the 2007 Cyber Attacks,"179–80.

37. Ibid., 178.

38. Executive Office of the President, *Cyberspace Policy Review* (Washington: GPO, 2009), 33–34, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May–June 2001): 109; Jason Miller, "Administration to Set New Vision for ID Management," *1500 AM Federal News Radio*, 22 September 2009, http://www.federalnewsradio.com/index.php?nid=11-&sid=1768455; Kugler, "Deterrence of Cyber Attacks," 309–10, 317, 337–38; Blank, "Can Information Warfare Be Deterred?" 149; and Roger Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review* (Spring 1998), http://www.iwar.org.uk/iwar/resources/nwc-review/io-spring-1998.htm.

39. Taipale, "Cyber-deterrence," 21–24.

40. Libicki, *Cyberdeterrence and Cyberwarfare*, 75–90.

41. Ibid., 52.

42. Adams, "Virtual Defense," 110; Barnett, "Information Operations, Deterrence, and the Use of Force"; Blank, "Can Information Warfare Be Deterred?" 145; Taipale, "Cyber-deterrence"; and Libicki, *Cyberdeterrence and Cyberwarfare*, 25–26.

43. Taipale, "Cyber-deterrence," 18.

44. Harknett, "Information Warfare and Deterrence"; Timothy Thomas, "Deterring Information Warfare," *Parameters* 26, no. 4 (Winter 1996–1997), http://www.carlisle.army.mil/usawc/Parameters/96winter/thomas.htm; Kugler, "Deterrence of Cyber Attacks," 315; Taipale, "Cyber-deterrence," 7–8, 25; and Kevin R. Beeker, "Strategic Deterrence in Cyberspace: Practical Application" (MSc thesis, Air Force Institute of Technology, June 2009), 10–11, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502250&Location=U2&doc=GetTRDoc.pdf.

45. Thomas, "Deterring Information Warfare"; Taipale, "Cyber-deterrence," 33–36; and Eneken Tikk, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm, and Liis Vihul, *Cyber Attacks against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008), 29–31, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

46. Bryce Meyer, "Defending the New Silk Road," *Armed Forces Journal* 146, no. 2 (September 2009): 12–16, 34–35.

47. The "cyber Silk Road" model of shared responsibility does not envision punishing Internet infrastructure providers for attacks they neither authorized nor participated in. Instead, the model envisions offering infrastructure providers incentives to cooperate with cyber attack investigations to criminally prosecute or otherwise carry out punitive measures against cyber attack perpetrators. However, if infrastructure providers refuse to provide investigative assistance, they put themselves at risk of obstructing justice and suffering legal consequences.

48. Tikk et al., *Cyber Attacks against Georgia*, 22.

49. For those interested, in "Web War I," Stephen Blank offers a passionate argument that Russia bears the guilt, and Martin Libicki offers a counterargument in *Cyberdeterrence and Cyberwarfare*, 2–3. Kugler, "Deterrence of Cyber Attacks," 318–20, makes an argument for convicting states with only circumstantial evidence, but that policy would increase the incentive for third parties to mount "false flag" operations.

50. Ottis, "Analysis of the 2007 Cyber Attacks," 179.

51. Economic sanctions provide one example. An even more severe course of action might involve physically destroying Russian profit-yielding infrastructures (e.g., oil and natural gas pipelines) in ways that would not threaten Russian lives. Of course, the latter reaction raises the peril of further retaliatory escalation by Russia, potentially even to full-scale war.

52. Jim Michaels, "NATO to Study Defense against Cyberattacks," *USA Today*, 15 June 2007, http://www.usatodayeducate.com/wordpress/?dl_id=9.

53. Travis Wentworth, "You've Got Malice: Russian Nationalists Waged a Cyber War against Georgia. Fighting Back Is Virtually Impossible," *Newsweek*, 23 August 2008, http://www.newsweek.com/id/154965.

54. David Fulghum, "Cyberwar is Official," *Aviation Week & Space Technology* 171, no. 10 (14 September 2009).

55. George Donovan, "Russian Operational Art in the Russo-Georgian War of 2008," (MSc thesis, US Army War College, March 2009), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500627&Location=U2&doc=GetTRDoc.pdf.

56. Wentworth, "You've Got Malice."

57. STRATFOR, "Georgia, Russia: The Cyberwarfare Angle," *STRATFOR.com*, 12 August 2008.

58. Fulghum, "Cyberwar is Official."

59. Ibid.

60. Sergey Samoylov and Yekaterina Yeliseyeva, "War: Hackers Attacked Our Media," *Moskovskiy Komsomolets* (Moscow), 12 August 2008.

61. Wentworth, "You've Got Malice."

62. STRATFOR, "Georgia, Russia."

63. Libicki, *Cyberdeterrence and Cyberwarfare*, 2, fn. 5.

64. Wentworth, "You've Got Malice."

65. Fulghum, "Cyberwar is Official."

66. Taipale, "Cyber-deterrence," 19.

67. Kugler, "Deterrence of Cyber Attacks," 338; Blank, "Can Information Warfare Be Deterred?" 139; John P. Callaghan and Rudi Kauffman, "Building Cyber-Security," paper presented at the 66th Annual Meeting of the Midwest Political Science Association, April 2008, 9–11, http://ubiwar.files.wordpress.com/2009/09/2008_callaghan_kauffman_building_cybersecurity_prospects_for_deterrence1.pdf; and Libicki, *Cyberdeterrence and Cyberwarfare*, 65–68.

68. Blank, "Can Information Warfare Be Deterred?" 143; Taipale, "Cyber-deterrence," 20–21; and Beeker, "Strategic Deterrence in Cyberspace," 12.

69. A "bot net" is a network of computers surreptitiously controlled by another central computer, or "bot net master." A computer that is part of a bot net can be exploited for access to the user's personal information or as a platform for attacking other computers or networks. "Packet sniffing" is observing the traffic of data packets across a network to find and exploit packets that contain valuable data. Network reconnaissance can involve a wide variety of activities such as scanning ports on a router, identifying network IP addresses, or collecting network usage information.

70. Taipale, "Cyber-deterrence," 24.

71. Barnett, "Information Operations, Deterrence, and the Use of Force"; Wheatley and Hayes, *Information Warfare and Deterrence*, 13; Taipale, "Cyber-deterrence," 36–38; Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 84–85; and Dorothy Denning, *Information Warfare and Security* (Boston: Addison Wesley, 1999), 384–85.

72. Libicki, *Cyberdeterrence and Cyberwarfare*, 16–18; and Libicki, *Conquest in Cyberspace*, 31–37.

73. Fulghum, "Air Defense Mystery in Georgia," *Ares: A Defense Technology Blog*, http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogscript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3A54d4 da21-e359-4da4-b03b-44a98562a8af.

74. Fulghum, "Cyberwar is Official."

75. Robert Farley, "But What Does It Mean for NATO?" *American Prospect*, 15 August 2008, http://www.prospect.org/cs/articles?article=but_what_does _it_mean_for_nato.

76 Vernon Loeb, "NSA Adviser Says Cyber-Assaults On Pentagon Persist with Few Clues," *Washington Post*, 7 May 2001; and Adams, "Virtual Defense," 99.

77. Adams, "Virtual Defense," 100.

78. Loeb, "NSA Adviser Says Cyber-Assaults on Pentagon Persist with Few Clues."

79. Adams, "Virtual Defense," 100.

80. Loeb, "NSA Adviser Says Cyber-Assaults on Pentagon Persist with Few Clues."

81. Adams, "Virtual Defense," 99–100.

82. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *Time Magazine*, 29 August 2005, http://www.time. com/time/magazine/article/0,9171,1098961,00.html.

83. Bradley Graham, "Hackers Attack via Chinese Websites: US Agencies' Networks are among Targets," *Washington Post*, 25 August 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

84. Thornburgh, "The Invasion of the Chinese Cyberspies."

85. Ibid.

86. Ibid.

87. Graham, "Hackers Attack via Chinese Websites."

88. Ibid.

89. Ibid.

90. "[REDACTED]," *GlobalSecurity.org*, http://www.globalsecurity.org/military/ops/[REDACTED].htm.

91. Kevin Poulsen, "Video: [REDACTED], the Best FBI-Produced Hacker Flick Ever," *Wired Online Threat Level*, 23 September 2008, http://www.wired.com/threatlevel/2008/09/video-[REDACTED]/.

92. "[REDACTED]."

93. Poulsen, "Video."

94. Kevin Poulsen, "[REDACTED] Hacker 'Analyzer' Escapes Jail, Community Service for Terrifying US Army," *SecurityFocus.com*, 15 June 2001, http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_ analyzer_escapes/.

95. Adams, "Virtual Defense," 103–4; Thomas, "Deterring Information Warfare"; and Beeker, "Strategic Deterrence in Cyberspace," 11.

96. Siobhan Gorman, "US Backs Talks on Cyber Warfare," *Wall Street Journal*, 4 June 2010, http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html?mod=WSJ_Tech_LEFTTopNews.

97. Scott W. Beidleman, "Defining and Deterring Cyber War" (MSc thesis, US Army War College, June 2009), 19–20, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500795&Location=U2&doc=GetTRDoc.pdf.

98. Libicki, *Conquest in Cyberspace*, 50–71.

99. Harknett, "Information Warfare and Deterrence"; and Thomas, "Deterring Information Warfare."

100. Executive Office of the President, *Cyberspace Policy Review*, 34; and Wheatley and Hayes, *Information Warfare and Deterrence*, 13.

101. Blank, "Can Information Warfare Be Deterred?" 136; Feaver, "Blowback," 98–111; and Taipale, "Cyber-deterrence," 39–40.

102. See, for example, Dale C. Copeland, "Economic Interdependence and War: A Theory of Trade Expectations," *International Security* 20, no. 4 (Spring 1996): 5–41; and Susan M. McMillan, "Interdependence and Conflict," *Mershon International Studies Review* 41, no. 1 (May 1997): 33–58.

103. Libicki, *Conquest in Cyberspace*, 126, 220–22.

104. Skypek, "A Pearl Harbor by Keystroke?"

105. Blank, "Can Information Warfare Be Deterred?" 142.

106. Feaver, "Blowback."

107. Denning, *Information Warfare and Security*, 41.

108. Libicki, *Cyberdeterrence and Cyberwarfare*, 23–24.

109. Minxin Pei, "Will the Chinese Communist Party Survive the Crisis?" *Foreign Affairs*, 12 March 2009, http://www.foreignaffairs.com/articles/64862/ minxin-pei/will-the-chinese-communist-party-survive-the-crisis?page=show.

110. See, for example, Kugler, "Deterrence of Cyber Attacks," 318–20.

111. Ben Bain, "Authentication Said Key to Cybersecurity," *Federal Computer Week*, 22 September 2009, http://www.fcw.com/articles/2009/09/22/web-mcconnell-cybersecurity.aspx.

112. Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN*, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

113. Robert McMillan, "Another Estonia Cyberattack," *PC World*, 16 January 2008, http://www.pcworld.com/article/141438/another_estonia_cyberattack.html.

114. Blank, "Can Information Warfare Be Deterred?" 136; Feaver, "Blowback," 98–111; and Taipale, "Cyber-deterrence," 39–40.

115. Schelling, Arms and Influence, 66–68. Schelling describes "salami tactics" as follows:

> Tell a child not to go in the water and he'll sit on the bank and submerge his bare feet; he is not yet 'in' the water. Acquiesce, and he'll stand up; no more of him is in the water than before. Think it over, and he'll start wading, not going any deeper; take a moment to decide whether this is different and he'll go a little deeper . . . pretty soon we are calling to him not to swim out of sight, wondering whatever happened to all our discipline . . . this [is] the low-level incident or probe, and tactics of erosion. One tests the seriousness of a commitment by probing it in a noncommittal way, pretending the trespass was inadvertent or unauthorized if one meets resistance, both to forestall the reaction and to avoid backing down." The enemy slices the "salami" of a deterrence declaration, "if there is no sharp qualitative division between a minor transgression and a major affront, but a continuous gradation of activity, one can begin his intrusion on a scale too small to provoke a reaction, and increase it by imperceptible degrees, never quite presenting a sudden, dramatic challenge that would invoke the committed response.