Journal of Military and Strategic Studies

VOLUME 14, ISSUE 2, 2012

Shattered Boundaries: Whither the Cyber Future

Harvey Rishikof[1] and Bernard Horowitz

Under strain exerted by the internet boom of the early 2000's, the legal framework of boundaries applied to commerce, communications, law enforcement and even some aspects of armed conflict began to groan and fracture. Obsolescence was temporarily postponed by buttressing; one key reform of the USA PATRIOT Act was that it characterized internet service companies as communications providers. Police access to voicemail was directed through wiretap warrants rather than physical searches. Old communications-related statutes were adapted and "duct-taped." Over the past couple of years, however, these fractures have grown to such magnitude that the old framework may no longer be adjusted to keep pace; it finally may be shattering

For example, in any new or unusual war paradigm, first impulses direct us to rely on what has worked in the past, to transpose core ideas (e.g., deterrence and containment) and systems (e.g., the Laws of Armed Conflict, the National Security Act

[1] Harvey Rishikof, ABA Chair, Standing Committee on Law and National Security, is former legal counsel to the Deputy Director of the FBI, former Administrative Assistant to the Chief Justice of the United States, and former Dean of Roger Williams University School of Law. The opinions and views expressed in this article are his own and do not reflect the opinions or views of any entity of the United States government.

ISSN : 1488-559X

of 1947). Cybersecurity presents an entirely different challenge. It is possible that the traditional fundamentals can no longer be adapted and re-applied. We need not be afraid – it is only natural that technological progress results in the need for new approaches.

One might suggest we look to the example of the Cold War for deterring cyber attacks. In the RAND Corporation's *Cyberdeterrence and Cyberwar,* Martin Libicki effectively challenges this approach:

- Attribution wasn't a problem – it wasn't that hard to pin actions to actors
- The prospect of damage was clear – actors could anticipate results accurately
- The one thousandth bomb was as powerful as the first – cyber-weapons are situational, and they also lose effectiveness if applied repeatedly.
- Counterforce was possible
- No third parties were involved
- Private firms were not expected to defend themselves
- There was a clear threshold for what constituted an "unacceptable" activity
- No higher levels of war than a nuclear exchange – the prospects for cyber-attacks are hazy. How does one judge one attack relative to another?
- Both sides always had a lot to lose[2]

Deterrence theory may not hold the answer to cybersecurity; our discussion therefore will address the vulnerabilities of cyberspace, difficulties in characterizing cyber-events and the variant motivations of hackers, followed by a review of various solutions and approaches for addressing major hurdles in cybersecurity.

[2] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (The Rand Corporation: 2009), p. xvi http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

The Vulnerabilities of Cyberspace

An analysis of threats posed via cyberspace must commence with a fundamental explication of how the cyber-realm differs from the kinetic one, both in principle and function. Cyberspace yields a new type of volatility, chiefly resulting from (1) divestment of control from human actors, (2) inability to anticipate tactical vulnerabilities and (3) societal overlap – cybercrime, cyber-espionage and cyberwar all use a common internet backbone, and are this interwoven with internet social interactions and commerce.

The first and most unprecedented development is the subtraction of human input. In the world of cruise missiles and tanks, operations and maneuvers could be adjusted or canceled by operators. Cyberoperations are conducted on three levels: (A) human policymakers devising systems, (B) humans interacting with hardware and software, but, due to the speed with which computer operations must be conducted, (C) computer algorithms, not humans, are the main line of defense and reaction. Even if humans could respond to malicious code with inordinate accuracy, the volume of attacks would eclipse what could be realistically handled by even the best-trained staff of experts (the Department of Defense's networks are attacked 250,000 times per day[3]).

A second hallmark of cyberspace volatility involves the unpredictability of cyber attacks in both location and form. During the Cold War, studying potential Soviet attacks on the U.S. mainland may have been hair-raising, but was at least straightforward: the targets would be major cities and critical infrastructure and the method of delivery would be nuclear missiles, whose heat signatures could be observed from satellites. Nuclear war with the Soviets would have been apocalyptic, but still predictable (in form and targeting) and visible. These attributes are inapplicable to cyberspace; a more accurate threat analogy to cyberattacks reckons from a far earlier period: when the Conquistadores attacked the Aztecs at Tenochtitlan -- the Aztecs had never encountered horses. Aztec accounts of the invasion put a face on the level of confusion when utterly alien forces are unleashed – Cortes's horses and riders were thought to constitute single living entities and the Aztecs had no idea how to fight

[3] American Bar Association FISA Task Force Report, January 6, 2012, p.11.

them.[4] To complete the analogy, imagine if the Spanish had also been invisible until they appeared inside the city. The creative range of electronic coding is such that cyberattacks could conceivably fall into the same category – analysts discuss the serious potential of a "Zero-Day" attack, a type of cyber-force which has never been seen before, and for which defenses cannot see and for which they are unprepared.

The third major volatile new trait afforded by cyberspace is its natural proclivity to affect neutral parties. The Laws of Armed Conflict seek in part to direct violence away from civilians to minimize collateral damage and suffering. However, avoiding non-combatants becomes exceedingly difficult in cyberspace: in the first place, correctly identifying a target is difficult. And, when somebody does "shoot" on the internet, they may hit their intended target, but malware can spread unpredictably.

This "collateral" problem is compounded by the increasing accessibility of hacking software and coding; anybody can buy a "gun." Noah Schachtman compares the internet to "The South Bronx, circa 1989 – a place where crooks hold such sway that honest people find it hard to work or live there."[5] And the neighborhood is getting easier to visit; while cloud-computing facilitates a central cyber-work space it also necessitates hundreds more entry points (wherein penetration at any of them moves past security measures). And of course shooters are often anonymous; packet switching and P2P data transfers make it extremely difficult to pin identities or even locations on data, and malicious actors easily use innocents as proxies to disguise themselves.

How Do We Characterize Events in Cyberspace?

Governments working to develop legal frameworks for cyberspace are faced with a critical dilemma: basic characterizations of cyber-events dictate whether law enforcement (or other) responses are triggered. Hence, such frameworks are structured to limit scope so that the number of cyber-events which qualify under the banner of

[4] See Stewart B. Schwartz: *Victors and Vanquished: Spanish and Nahua Views of the Conquest of Mexico* (Bedford/St. Martin's Press: 2000).

[5] Noah Schachtman, "A Crime Wave in Cyberspace," *The Washington Post,* July 22, 2011. http://www.washingtonpost.com/opinions/a-crime-wave-incyberspace/2011/07/21/gIQAYfbIUI_story.html

malicious activity is manageable. Many analysts draw a distinction between Computer Network Exploitations (CNE's) and acts of "Cyberwar," suggesting that (almost) exclusively, events of the latter category ought to trigger responses. Even the term "CNE" raises complications because it may imply hostility.

As typically defined, acts of "Cyberwar" reflect initiatives seeking to damage targeted systems while CNE's feature information access (i.e. theft), but not damage. In RAND's report on Cyber-deterrence, Martin Libicki explains the rationale behind the Cyberwar vs. CNE breakdown:

> … CNE (spying) is not an attack (as disruption and corruption are)… CNE deserves to be distinguished from cyberattack. First, CNE does not deprive the user of the full use of the machine. The user suffers no consequential harm other than having secrets stolen. Second, because CNE is so difficult to detect, a deterrence policy could only be activated by exception. Harsh punishments for crimes that are rarely detected tend to lose credibility as law enforcement mechanisms, and this is even more true if such methods are used to try to govern the activities of other states. Third, the law of war rarely recognizes espionage as a *casus belli*, and a good case for changing this has yet to be made, even though the means of espionage have changed. Fourth, everyone does it.
>
> Those who try to establish deterrence policies to prevent others from doing what they do themselves perforce reveal themselves to be fools or hypocrites—unless they are so powerful that they can get away with it. It is doubtful whether even the United States qualifies as being that powerful. A deterrence posture against CNE would be viewed as hypocritical and probably not credible—indeed, as incredible. That stated, CNE is often called an "attack"…. True, a great deal of state-sponsored CNE is going on. The PLA stands accused of having broken into thousands of civilian and unclassified military systems, in the United States and elsewhere (e.g., Germany), to steal large quantities of information. The Chinese are also said to have dropped implants into such systems in ways that make it difficult to clean up individual machines without allowing them to become reinfected. Germany's chancellor,

> Andrea Merkel, felt confident enough in this attribution to complain to China's premier in person. China has steadfastly denied all responsibility.[6]

However, applying the CNE vs. Cyberwar framework raises major conceptual problems beyond the *casus belli* implications of the term "CNE": while "cyberwar" attacks would be calamitous, CNE's arguably result in by far the most damage, especially for the private sector. It is clear from NCIX's 2011 *Report to Congress on Foreign Economic Collection and Industrial Espionage* that stolen information rather than "cyberwar" has been the area where the United States has suffered the most damage in cyberspace:

> Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods.[7]

While it is hard to argue with Libicki about the problematic nature of responses to malicious cyber-events falling short of "cyberwar," this approach may sidestep most of the adverse cyber-events. One usefully illustrative analogy comes from soccer: the team with the ball penetrates deeply into the opposing zone but correspondingly increases its own defensive vulnerabilities. Moreover, what appears to be a mere "exploitation" may in a split second become much more damaging than a CNE.

Perhaps hesitancy to tabulate our cybersecurity calculus to include CNE-type events is partly due to discomfort with the paradigm shift to cyberspace. CNE's can yield information thefts on a scale unimaginable to previous generations – also, the parties being exploited are in the private sector, not the government.

---

[6] Libicki, p.25.

[7] Office of the National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011: Foreign Spies Stealing US Economic Secrets in Cyberspace* (October 2011), p.i http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

One way to begin tackling the question of how to respond to malicious behavior short of "cyberwar" is to examine the motivations of the attackers.

Motivations Matter: The Goals of Hackers

Due to the hazy nature and unpredictability of cyberspace and coding, even if one traces the attribution of malicious activity, it is rarely discernible whether the malicious behavior manifested was fully anticipated by the initiator. For this reason, "characterization" of cyber-events is even more crucial; if one has a benchmark system or policy for responding to cyber-events, less guesswork regarding intentions and motivations is necessary. But, intentions must be discussed nonetheless.

Motivations for malicious cyber-behavior can be roughly grouped into three categories: (1) ideological "hacktivism," (2) hacking for profit, and (3) hacking for the purposes of espionage.

Ideological "hacktivism" is animated either by intra-national disputes or other issues. The *Ghostnet* bot attacks targeted the office of the Dalai Lama after China-Tibet friction. Estonia was subject to a wave of attacks after it moved a politically-sensitive statute (commemorating Russian soldiers who had liberated the city of Talinn in 1944) from its original site to a military cemetery. But hacktivism is not always animated by nationalism; the simultaneous US government shutdown of "Megaupload" and promulgation of the Stop Online Piracy Act (SOPA) resulted in aggressive behavior claimed by the hacking group known as "Anonymous," which proceeded to (allegedly) retaliate for the purposes of its opposition to internet regulation. The websites of the FBI, DoJ, White House, Warner Music, Universal Music, Recording Industry Association of America (RIAA), New Zealand Police Department were each targeted and taken offline by Distributed Denial of Service (DDOS) attacks.[8] The motivations are ideological.

[8] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks," *The Internet Protocol Journal* 7, No.4.
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

The second main type of hacking (for profit, not ideology) is a function of information theft and sale – such activities are now routine. In *America the Vulnerable*, Joel Brenner cites the example of Heartland Payment Systems:

> Heartland [Payment Systems] processes bank card payments for merchants… These businesses are an essential cog in the credit and debit card clearing process, and Heartland is one of the biggest, processing one hundred million transactions per month for more than 250,000 merchants. The company maintains millions of credit and debit card numbers on its network…. [the attackers] stole about 130 million credit and debit card numbers from Heartland. The company didn't figure this out for about a year. On January 20, 2009, Heartland publicly disclosed the theft, and immediately its stock began to tank. From over $15 per share on January 19, it fell to $3.78 by March 9. A year later it had still not fully recovered…. Heartland has reserved about $100 million to deal with this intrusion, and the figure could go much higher.[9]

Other examples might include the seventy-seven million Sony Playstation Three network account entries stolen in April 2011. In 2010, Verizon "reported that over nine-hundred million sensitive data records had been stolen from Americans in the previous six years."[10]

Brenner notes that the theft of credit card and identity data is now prevalent to the point that it has effectively self-regulated: so much data has been stolen that black market prices for stolen credit card records have been driven down near zero: "from between $10 and $16 per record in mid-2007 to less than $.50 per record" by late 2008."[11]

Customers and subscribers will continue to suffer periodic abuses of credit card fraud and identity theft, but at least the incentives for stealing such data have dropped. However, hacking for the purposes of stealing valuable secrets is a separate, far more nettlesome problem.

The 2011 NCIX *Report to Congress on Foreign Economic Collection and Industrial Espionage* observes:

---

[9] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare* (New York: The Penguin Press, 2011), pp.40-41.
[10] Brenner, pp. 24-25.
[11] Brenner, p.27.

> Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security.[12]

The Report recounts how China, Russia, and other states are heavily engaged in the theft of military and civilian technology, business plans, another other valuable information.

The quantity of information storable on a thumb drive has inflated the amount of information which can be easily transmitted exponentially. Hence, the prospective value of these heists – either to private or public-sector entities – is astronomical. However, while the motivations are clear, exfiltration of sensitive information – unlike "hacktivism" – often leaves no trace. In the next decade, with the introduction of the "cloud," data-protection technology will migrate towards the implementation of "dumb terminals," so that the identities of those who access sensitive data are carefully tracked. Unfortunately, dumb terminals (tagging data) are a limited solution since there will still be carbon units (human beings) and master network programmers with access to entire systems.

FISA, CALEA and Cybersecurity: Old Statutes Don't Mix with New Technology

The aforementioned vulnerabilities are only intensified as technological evolution vigorously challenges our communications statutes. In several key rulings concerning internet regulation, the FCC has principally relied upon the Communications Act of 1934.[13] This framework for communications technology is now frequently inapplicable to modern innovations, as exemplified by the Foreign

[12] Office of the National Counterintelligence Executive, p.i. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[13] See, e.g., *First Report and Order and Further Notice of Proposed Rulemaking*, (First RO) in ET Docket No. 04-295, FCC 05-153, Sep 23, 2005 at 13.

Intelligence Surveillance Act (FISA) and the Communications Assistant to Law Enforcement Act (CALEA).

A critical feature of the original FISA statute (1978) was its "location" requirement: the statute stipulated that warrants identify the "facilities to be monitored" and certify their affiliation with a "foreign power." FISA originates from an era where "agents of foreign powers" in the United States stole information and propagated it abroad. Today, many such "agents" can gain access to sensitive information without leaving a desk in their home country – which is beside the point because no matter where an internet user is located, accessible technology makes it simple to mask location. Hence, "location" as a concept is becoming increasingly obsolete:

> Computers do not leave distinct physical evidence behind. The world contains billions of nearly identical machines capable of sending nearly identical packets. Attacks can come from anywhere. State sponsored hackers could operate from a cybercafé, a public library with Wi-Fi access, or a cutout. Finding rogue packets that can be traced back to the network (IP) address of a government bureaucracy reveals a bureaucracy that is stupid, is arrogant, runs so many hackers that it cannot be anything less than obvious, or operates a network that has been hijacked by others. Packets can be bounced through multiple machines on their way to the target. They can be routed through a bot that only needs to erase the packet's originating address and substitute its own to mask the true origin. Attacks can be implanted beforehand in any machine that has been compromised.[14]

In *Intelligence: Secrets to Policy*, Mark Lowenthal estimates that 80% of intelligence information during the Cold War was classified and only 20% was obtained through Open-Source Intelligence (OSINT).[15] He then estimates that in the cyber-age, this ratio has now at least inverted. Limitless caches of information are available through the internet without the need to invoke legal authority. Since major cyberattacks and CNE's are conducted by entities disguising themselves by using proxies anywhere else in the world, the concept of "location" is not only difficult to establish, but misleading – one

[14] Libicki, pp.43-44

[15] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (4th ed.) (Washington, D.C.: CQ Press, 2009), p.104

need only examine *The SecDev Group*'s "Tracking Ghostnet: Investigating a Cyber Espionage Network" to see that skilled operators executing botnet attacks can easily infect and also control servers and individual computers on any continent (including North America).

A conventional view of the FISA statute is that while it may not be ideal, it is functional and worth retaining. FISA has been adapted several times to accommodate technological advances. The advent of cell-phones antiquated the "facilities to be monitored" language. This was addressed in the USAPA in 2001. More reform of FISA followed the public discussion of the "President's Surveillance Program" (PSP). Some asserted FISA was designed to be the *exclusive* national security wiretapping authority (while the administration had relied on the Authorization of Military Force for the PSP). The subsequent debate resulted in the passage of the FISA Amendments Act of 2008 (FAA), which systematized the monitoring of activity which cannot be linked to a specific person or location: if surveillance of unattributed activity leads to the discovery that the targeted party is located in the United States (or a U.S. person located abroad), the surveillance is transferred under the authority FISA.[16]

However, even with the FAA, FISA is crumbling under the cyber-revolution, and falls into the category of "shattered boundaries." So much information is available through OSINT that FISA (once the most-sought legal authority by federal prosecutors heading investigations[17]) has become unnecessary in cases where it was once a critical tool. The ABA's Task Force on FISA noted:

> [The] Central power exercised by the IC is no longer the warrant, but the application of algorithms to data. ([A] participant added that in the cyber-age, with the legal framework for information gathering in cyberspace so porous, information gathering is no longer the issue – for example, most of the info on [Nidal] Hasan was OSINT.)

[16] See: Elizabeth B. Bazan, "The Foreign Intelligence Surveillance Act: An Overview of Selected Issues," *Congressional Research Service*, July 7, 2008 (http://www.fas.org/sgp/crs/intel/RL34279.pdf).
[17] United States Department of Justice, *Attorney General's Review Team on the Handling of the Los Alamos Laboratory Investigation*, a.k.a. "The Bellows Report," p. 729.

> In the old world, we were protected by ineffectiveness of tech[nology] – targeting was where to put the rules because it [successfully and evenly] applied [to acquisition]. Now, the running of… algorithm[s] to collate… data (which is ever-accessible) is the issue. [18]

Passed in October 1994, CALEA arose among concerns that new communications technology would hamper the ability of law enforcement to lawfully conduct wiretapping. CALEA requires telecommunications carriers to modify their equipment, facilities, and services, wherever reasonably achievable, to ensure that they can comply with authorized electronic surveillance.

In the early 2000's, the rise of packet switching facilitated increased use of Voice-over-Internet-Protocol (VoIP) -- online phone conversations without use of a traditional telephone. Law enforcement agencies requested that the FCC clarify which technologies, services and providers were subject to CALEA. In August 2005, the FCC ruled that CALEA applied to private Internet access providers.[19] The FCC conferred guidelines for which of these companies faced CALEA's regulations based on whether or not the providers tied their customers' communications into the Public Switched Telephone Network (PSTN). Providers who did not provide "fully switched" service to the PSTN were exempted because they were rural and small-scale, unable to afford to modify their equipment.

Shifts in communications technology in the late 2000's resulted in a decline of dependence on the PSTN – customers did not care whether they used regular phones or not, they just wanted cheap service. Now that communications programs can be created by any skilled software designer, communications services can easily be designed to fall outside the reach of CALEA. For example, Skype offers separate services for outgoing and incoming calls -- because the services are separate, the company does not qualify as "fully switched," and is not subject to CALEA.[20]

---

[18] American Bar Association FISA Task Force Report, January 6, 2012. p. 4.

[19] *See First Report and Order and Further Notice of Proposed Rulemaking*, (First RO) in ET Docket No. 04-295, FCC 05-153, Sep 23, 2005 at 13.

[20] Harvey Rishikof, Stewart Baker and Bernard Horowitz (ed.), *Patriots Debate: Contemporary Issues in Naitonal Security Law* (Chicago: ABA Publishing, 2012), pp. 135-138.

Like FISA, CALEA falls distinctly into the category of major communications-related statutes rendered dissonant by technology; one may agree or disagree with its advisability – some analysts (and many industry advocates) have expressed concern that government regulation of communications technology raises civil liberties issues and also might constrain innovation and business. However the fact remains that CALEA was designed to apply to all major communications providers, yet is increasingly inapplicable to communications technology due to the "fully-switched" PSTN loophole.

FISA and CALEA just scratch the surface; many other communications statutes (e.g., the Electronic Communications Privacy Act of 1986) constitute pieces of the "shattered" old legal framework.

The Future of Cybersecurity: Possible Models and Approaches

The combination of antiquated communications laws and information sharing difficulties has yielded an environment where government-private sector collaboration as been and remains difficult:

> DoD's partnership with cleared defense contractors (CDCs) highlights difficulties in establishing an effective framework to improve the IC's understanding of foreign cyber threats and promote threat awareness in industry. The defense industrial base conducts $400 billion in business with the Pentagon each year and maintains a growing repository of government information and intellectual property on unclassified networks. CDCs are required to file reports of suspicious contacts indicative of foreign threats—including cyber—to their personnel, information, and technologies.
>
> …
>
> … Contractors do not always report theft of intellectual property unless it relates specifically to Pentagon contracts, according to outreach discussions with corporate officers. Corporate security officers also have noted that US Government reporting procedures are often cumbersome and redundant, with military services and agencies such as [Defense

> Security Service] and the FBI often seeking the same information but in different formats.[21]

The public and private sectors both confront the "attribution problem" and attempt to trace their own attackers. Private firms increasingly take to hiring contractors to fight hackers operating on their servers, resulting in rapid growth in the cyber-defense industry – corporate officers like the idea of active defense and are demonstrating substantial willingness to open their wallets to arrange long-term arrangements.[22]

Defense in cybersecurity includes major hardware, software, and insider threat components which must be addressed holistically. Bureaucratically, this requires merging IT and security departments with general counsel's offices, which is particularly difficult because of the cultural differences between the IT culture (geeks), security culture, (policy wonks/law enforcement) and lawyers (privacy advocates).

Cybersecurity contractors are involved in a struggle to protect networks and interests. Currently, the contractors work by building profiles of individual actors and counteracting them on a case-by-case basis.[23] Unfortunately, as sophisticated malicious code from operations such as Stuxnet and Flame becomes public, high-level hacking code is being rapidly proliferated, which will inevitably lead to an increase in the number of actors capable of highly-advanced hacking operations. As the volume of hacking increases (commensurately with the spread of hacking software and knowledge), a feedback system between the government and the private sector for reporting and addressing breaches would be helpful in the future.

Governmental cybersecurity assistance for the private sector is a multi-layered and large-scale task since the firms are bent on competition with one another; the United States is testing pilot programs which direct Cleared Defense Contractors (CDC's) to submit feedback. Unfortunately, only 10% of the CDC's have followed even some reporting requirements, usually electing to report cyber incidents only if the breach

[21] Office of the National Counterintelligence Executive, p. 13.
[18] Tom Gjelten, "Cybersecurity Firms Ditch Defense, Learn to 'Hunt,'" *National Public Radio* (May 10, 2012) http://minnesota.publicradio.org/features/npr.php?id=152374358
[19] Ibid.

corresponded directly to United States government contracts.[24] The two-way process of sharing critical information between the private sector and public sector has proven elusive despite years of effort. Some believe antitrust laws are barriers, while others contend that there exist legitimate fears of compromising sources or methods, or that the ability to create trusted relations between international corporations where "product" is sovereign has undermined special relations. The US does not have "national champions" who are protected agents of the state. In any case, failure to find a solution to private-public cybersecurity information sharing is increasingly compromising US interests.

Whether the government will mandate cyber-incident reporting in cases where publicly-traded companies have been subject to theft or attack remains an open question and is currently under review in legislation pending before Congress.[25] Some analysts suggest that not disclosing theft of company data may potentially result in shareholder lawsuits. Recently, the SEC has formulated guidelines for reporting cybersecurity breaches. These guidelines for reporting are not mandatory, but some analysts speculate this may change soon,[26] depending on the nature of future attacks.

In the face of many recent reports indicating lax security precautions and under-estimation of the exfiltration and malicious cyber threats in the private sector, how to incentivize and stimulate cybersecurity has become a popular question. Indeed, some cybersecurity analysts who ordinarily favor some regulation make an exception for the enforcement of cybersecurity standards. In his essay *Law and Cyberwar: The Lessons of History*, Stewart Baker suggests that lawyers be almost entirely excluded from the

[20] Office of the National Counterintelligence Executive, p. 13.
[21] See, e.g., "Cybersecurity Act of 2012," S. 2105
http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf
[22] Peter J. Toren, "Disclosing Cyber Security Incidents: The SEC Weighs In," *Forbes* (June 4, 2012)
http://www.forbes.com/sites/ciocentral/2012/06/04/disclosing-cyber-security-incidents-the-sec-weighs-in/

conduct of cyberwar.[27] However, at the same time, Baker feels that in the case of enforcing standards for cybersecurity in the private sector, government action is exigent.[28]

According a study conducted by the North American Energy Reliability Corporation (NERC), 73% of respondents claimed no critical assets (including cyber assets) whatsoever, indicating that they did not understand what a critical cyber asset entailed.[29] Joel Brenner quotes Mike Assante of NERC describing the dearth of security practices at energy facilities:

> "It's a sad state of affairs. The analytic tools are so bad," [Assante] said, speaking about those in use at some of the companies, "that you couldn't even do the analysis. They couldn't see the communication flow on their own networks. They weren't grabbing that traffic, so they weren't analyzing it… When you asked the engineers those questions it was like speaking Greek. They had no idea why you'd want those things." And because they couldn't see the cybertraffic in their own systems, they had no idea who had penetrated them. Then, when he went to the owners and operators with his concerns, Assante said, "they'd insist there was a lack of evidence [that] they were penetrated."[30]

Numerous other recent studies reinforce Assante's depiction of cybersecurity practices throughout private sector.[31]

Aside from penalization, three potential strategies which might help to incentivize private sector cooperation with government standards for cybersecurity are indemnification, tax breaks, and insurance premiums. Companies victimized by malicious behavior but adhering to a government-approved security regimen could be

---

[23] *Patriots Debate: Contemporary Issues in National Security Law*, pp. 181-188.
Also see: Stewart A. Baker and Charles J. Dunlap, Jr., "What is the Role of Lawyers in Cyberwarfare," *ABA Journal* (May 2012). Available at:
http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/
[24] Tom Gjelten, "Bill Would Have Businesses Foot Cost of Cyberwar," *National Public Radio* (May 8, 2012)
http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war
[25] Brenner, p. 101.
[26] Brenner, pp. 106-107.
[31] See, e.g., Jody R. Wesby, "Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks," *Carnegie Mellon University CyLab*, 2012
http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf

compensated for their losses in certain cases (indemnified), afforded tax credits, or compensated with friendlier insurance premiums based on compliance. While all three strategies are heavily contingent on the effectiveness of the prescribed cybersecurity standards, if such a regimen could be created, it would arguably make for a significant increase in private sector cybersecurity and more appropriate sharing between the private and public sector.

Cybersecurity analysts envision a wide variety of other tactics which they feel might be critical in securing the internet moving forward. For example, in "State of the Art: Attackers and Targets in Cyberspace," John B. Shelton emphasizes that one important area of focus should be the allocation of resources in accordance to the severity of threats. He suggests that paying too much attention to hacktivist groups such as "Anonymous" hampers ability to confront threats posing great danger, diverting critical cybersecurity resources that do not warrant such attention.[32]

In "Wild, Unsubstantiated Predictions: The Future of Computer and Network Security," John Aycock predicts that the future of cybersecurity lies not in the development of new technology, but in the social and political responses to existing technology over the next five-to-ten years. He further envisions a security regimen entailing the fragmentation of the internet via the "extension of physical borders into cyberspace" – the creation of border and treaty-based choke points so that internet traffic can be monitored and filtered as it enters.[33]

Not all internet security strategies for the future involve substantial increases in regulation (which Aycock and others seem to view as inevitable). In "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Ron Deibert warns that the internet and cyberspace have reached a "watershed moment." He strongly emphasizes his conviction that the internet best serves the public good as an open, disturbed network, and warms that "major social forces are converging that threaten to subvert cyberspace's core characteristics as an

[27] John B. Sheldon, "State of the Art: Attackers and Targets in Cyberspace," *Journal of Military and Strategic Studies* 14, no. 2 (2012).
[28] John Aycock, "Wild, Unsubstantiated Predictions: The Future of Computer and Network Security," *Journal of Military and Strategic Studies* 14, no. 2 (2012).

open distributed network, including growing assertions of state power, interstate competition, espionage, crime and warfare," also noting that "there is a large market for technologies, products, and services that facilitate censorship, surveillance and information warfare."[34]

Diplomacy, Multilateralism and Unilateralism

By the count of John Sheldon, there are at least 18 separate international definitions of cyberspace and also numerous disparate definitions of cyberpower.[35] Considering the fluidity of cyberspace and the ability of internet users to access sites anywhere on the globe, one overriding area for reform is international cyberspace diplomacy – one is not hard-pressed to recognize the need for international norms for regulating cyberspace. Granted, hopes for consensus may be naïve; a 2007 study found that 26 of 40 countries examined engaged in internet censorship, and at least 14 specifically barred access to certain political, social, or international conflict-related content.[36]

Even though some diplomatic barriers are unlikely to abate, without international standards for regulation cyberspace will remain judicially impracticable, and will incur unilateralist policy strategies and operations. While domestic models for cybersecurity can be helpful for addressing problems in cyberspace, true progress – the molding of new boundaries – must also be an international enterprise. Only time will tell whether the international community will rise to the challenge of creating the new cyber boundaries, marrying security with convenience.

[29] Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," *Journal of Military and Strategic Studies* 14, no. 2 (2012).
[30] Sheldon, "State of the Art: Attackers and Targets in Cyberspace".
[31] *The Handbook of Internet Politics* (ed. Andrew Chadwick and Philip N. Howard), Ronald J. Deibert, "The Geopolitics of Internet Control: Censorship, Sovereignty and Cyberspace" (Routledge: 2008), p. 327. (http://www.handbook-of-internet-politics.com/pdfs/chapter_23.pdf)