Information Security Journal: A Global Perspective, 18:1–7, 2009

The Cyber Threat to National Critical Infrastructures: Beyond Theory

Kenneth Geers
Naval Criminal Investigative Service (NCIS)
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

ABSTRACT

Adversary threats to critical infrastructures have always existed during times of conflict, but threat scenarios now include peacetime attacks from anonymous computer hackers. Current events, including examples from Israel and Estonia, prove that a certain level of real-world disorder can be achieved from hostile data packets alone. The astonishing achievements of cyber crime and cyber espionage – to which law enforcement and counterintelligence have found little answer – hint that more serious cyber attacks on critical infrastructures are only a matter of time. Still, national security planners should address all threats with method and objectivity. As dependence on IT and the Internet grow, governments should make proportional investments in network security, incident response, technical training, and international collaboration.

NATIONAL SECURITY IN THE INTERNET ERA

In 1948, international relations theorist, Hans Morgenthau (1904–1980) theorized that national security depends on the integrity of a nation's borders and its institutions.[1] In 2009, the most certain way to threaten the security of a nation-state remains via physical, military invasion, or terrorist attack. However, as more critical national infrastructures are computerized and connected to the Internet, the fear is growing of national security threats that emanate solely from computer network attacks.

The mission of the U.S. Federal Bureau of Investigation (FBI) is to "protect and defend the United States." Currently, the FBI's three top priorities are preventing terrorist attacks, foreign intelligence operations, and high-technology crimes including cyber attacks.[2] The urgency with which the FBI views the threat from cyberspace should no longer be

[1] Morgenthau, H. J. (1960). *Politics among nations: The struggle for power and peace*, 3rd Edition. New York: Alfred A. Knopf.
[2] FBI website. About us – quick facts. http://www.fbi.gov/quickfacts.htm

surprising: information systems, including client and server computers, databases and the networks that connect them are now used to facilitate the management of myriad government and civilian infrastructures. Many of these, such as water, electricity, and telecommunications, provide the basic services necessary for the functioning of a modern society. The need to maintain their integrity is clear.

In the year 2000, former U.S. Special Advisor to the President Richard Clarke introduced much of the world to the idea of a "Digital Pearl Harbor." Since then, computer security analysts have argued whether such a scenario is possible, even in theory. A decade later, the astonishing achievements of cyber crime and cyber espionage – to which law enforcement and counterintelligence personnel have found little answer – hint that more serious cyber attacks on national critical infrastructures are only a matter of time.

At a minimum, national security planners should attempt to answer the following questions:

1. How dependent is the nation's critical infrastructure on IT?
2. To what degree is that IT connected to (and dependent upon) the Internet?
3. In theory, what would the most successful cyber attack against this infrastructure look like, and would it rise to the level of a national security threat?

THE MAGIC OF CYBER ATTACKS

All political and military conflicts now have a cyber dimension, whose size and impact are difficult to predict. National security experts must now acknowledge that real political and military objectives can be won or lost in cyberspace, even if only on the propaganda front. Globalization and the Internet have aided foreign intelligence services and terrorists as much as any other part of society. Communications, fund-raising, public relations, and information gathering are all greatly aided by networking technologies, and the pure amplifying power of the Internet means that the battles fought there can be just as important as events taking place on the ground.

Terrorists and spies can now use Open Source Intelligence (OSINT) via the Web for much of their information-collection needs, but offensive computer network operations, using hacking techniques to obtain information not publicly available, appear to be commonplace. Government leaders around the world now complain publicly of cyber espionage.[3] The high level of interest stems from the extraordinarily high return on investment that computer spies seek: free research and development data, access to sensitive communications, and much more. The elegance of computer hacking is that it can be attempted for a fraction of the cost and risk of other illicit information collection strategies.

[3] See, for example, "Espionage report: Merkel's China visit marred by hacking allegations." *Spiegel Online*, August 27, 2007, followed by Cody, E. "Chinese official accuses nations of hacking." *Washington Post*, September 13, 2007.

Cyber attacks which aim to manipulate critical infrastructures take more time, effort, and expertise than mere data theft, for reasons discussed below. However, computer network defenders should understand that time, effort, and expertise are resources that foreign intelligence services have in abundance. Breaking the Purple and Enigma ciphers during World War II, for example, demonstrated not only the immense undertaking required to achieve such feats but also its invaluable service to national security affairs. On the defensive side, the Allies spared no effort (including technical deception) to convince the German military leadership that the D-Day invasion would take place at Pas-de-Calais instead of Normandy.

Currently, the balance of power in cyberspace appears to favor the attackers. Although the Internet has a modular design that has proven remarkably resilient, in terms of security it is imperfect. Hackers persistently find ways to secretly read, delete, and/or modify information stored on or traveling between computers. Beyond simple but effective social engineering attacks, there are dozens of additions to the Common Vulnerabilities and Exposures (CVE) database every month.[4] Armed with constantly emerging new malicious code, hackers likely have more paths into your network than your system administrators can protect.

One of the most revolutionary aspects of cyber warfare is that the physical distance between attacker and victim can be irrelevant. The essence of connectivity, encompassing all nodes in between any two points on the Internet, can boil down to available bandwidth and the latency of the communications medium. In short, hardware and software determine the landscape of the battlefield, not mountains, valleys, or waterways. The most formidable obstacles, and the best offensive and defensive tactics, are usually not the most physically imposing, but the most logical and innovative.

In spite of all this, it is important to remember that cyber attacks are constrained by the limited terrain of cyberspace. While the ultimate goal of a cyber attack is to effect change in the physical world, the immediate battles take place in an artificial world of computers, databases, and networks, often in the form of prosaic vulnerabilities and exploits. As with the advent of chariots and artillery in the past, the strategies and tactics of cyber warfare are revolutionary, but limited in scope. Moreover, cyber terrain changes dynamically, often with no warning. Attackers and defenders are both challenged by computers and networks that undergo frequent updates and reconfiguration, where insurmountable obstacles can appear and disappear as if by magic. Often, hackers do not know if a planned attack will succeed until they launch it. Exploits one expects to succeed may fail, and vice versa.[5] Attacks that work in one instance may never work again.[6]

---

[4] CVE list main page, http://cve.mitre.org/cve/index.html.

[5] Parks, R. C. and Duggan, D. P. (2001). Principles of Cyber-warfare. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy*, West Point, NY, June 5–6.

[6] Lewis, J. A. (2002, December). "Assessing the risks of cyber terrorism, cyber war and other cyber threats." Center for Strategic and International Studies.

To finish this section, a word on computer network defense. Remember in the Monte Python skit, when King Arthur was told that he was not riding a horse, but walking and banging together two empty halves of a coconut? Things may not be that bad, but it is true that law enforcement and counterintelligence are often woefully behind their competition. Traditional skills are inadequate, and it is difficult to retain employees with highly marketable technical knowledge. The international, maze-like architecture of the Internet offers smart attackers a high degree of anonymity, and the plausible deniability gained from proxy-hopping and cyber spoofing serves to slow investigations to a crawl. Globalization and the Internet continue to increase the impact of a wide range of nonstate actors (e.g., the media); in the case of state sponsored operations, law enforcement cooperation will always be nonexistent.

HACKING CRITICAL INFRASTRUCTURE

Attacking a nation's critical infrastructure is an old idea. Militaries seek to win not just individual battles, but wars. Toward that end, they must reduce an adversary's long-term ability to fight. Advice from the *Art of War* demonstrates this point clearly:

> Sun Tzu said: There are five ways of attacking with fire. The first is to burn soldiers in their camp; the second is to burn stores; the third is to burn baggage trains; the fourth is to burn arsenals and magazines; the fifth is to hurl dropping fire amongst the enemy.[7]

The goals of cyber warfare – inflicting painful, asymmetric damage on an adversary from a distance – are similar to those of aerial bombardment, submarine warfare, special operations forces, and assassins.[8]

Following World War II, the United States published a Strategic Bombing Survey (USSBS) that may hold lessons for cyber war planners. The USSBS concluded that no indispensable industry was ever permanently destroyed during the war, and that "persistent re-attack" was always necessary. Still, the authors of the Survey left no doubt about their overall opinion of air power:

> Allied air power was decisive in the war in Western Europe. Hindsight inevitably suggests that it might have been employed differently or better in some respects. Nevertheless, it was decisive. In the air, its victory was complete. At sea, its contribution, combined with naval power, brought an

---

[7] Giles, L. (1994). *Sun Tzu on the art of war*. Project Gutenberg eBook. (First Published in 1910). www.gutenberg.org/etext/132

[8] Parks, R. C. and Duggan, D. P. (2001). Principles of cyber-warfare. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy*, West Point, NY, June 5–6.

> end to the enemy's greatest naval threat -- the U-boat; on land, it helped turn the tide overwhelmingly in favor of Allied ground forces.[9]

Today, national critical infrastructures are, like everything else, increasingly connected to the Internet. The first reason for this is that it is more cost-effective to manage large systems remotely with the aid of easy-to-understand software and well known network protocols than to send a human technician to a physical site with pen and paper. But this convenience comes at a price. The infrastructure's hardware may have insufficient computing resources to allow for robust security practices (e.g., firewalls). Furthermore, instant or automatic response may be required, and it is unrealistic to expect that a human would be available to concur with every command the infrastructure is given.

Complicating matters is the fact that most critical infrastructures are in private hands. Internet Service Providers (ISP), for example, typically lease communication lines to government as well as to commercial entities. It is not uncommon for satellite management corporations to offer bandwidth to multiple countries at the same time.

Military leaders should expect to receive Denial of Service (DoS) attacks during operations. These can range from common network flooding techniques to data modification, physical destruction of hardware, and the use of electromagnetic interference. During the war over Kosovo in 1999, likely nonstate actors attempted to disrupt NATO military operations through hacking, and were able to claim minor victories.[10] Today, black market botnets provide anyone with massive Distributed DoS (DDoS) resources and a high level of anonymity. Given the challenges facing cyber defenders, it should be possible simply to tie up adversary IT resources with diversionary attacks while the critical maneuvers take place elsewhere. It should be noted here that some cyber investigations have continued for years with little progress on attribution and no hope of prosecution.

The examination of seized computer hard drives proves that terrorist organizations now study computer hacking.[11] The question for national security thinkers concerns how much real damage can be done via the Internet, and the answer is still highly theoretical. Governments may want to begin by evaluating the security of their electrical grids. Electricity has no substitute, and all other infrastructures depend on it.[12] In April 2001, the FBI investigated a Honker Union of China (HUC) hack of a California electric power grid test network.[13] The case was widely dismissed as media hype at the time, but the CIA informed

---

[9] United States Strategic Bombing Survey: Summary Report (European War), Washington, DC, September 30, 1945. http://ftp.metalab.unc.edu/hyperwar/AAF/USSBS/ETO-Summary.html.
[10] Verton, D. (1999). "Serbs launch cyber attack on NATO." *Federal Computer Week,* April 4; "Yugoslavia: Serb hackers reportedly disrupt U.S. military computer." Bosnian Serb News Agency SRNA, March 28, 1999 (BBC Monitoring Service, March 30, 1999).
[11] "Terrorists brandish tech sword, too." *Federal Computer Week*, August 28, 2006.
[12] Divis, D. A. (2005). Protection not in place for electric WMD. UPI, March 9.
[13] Weisman, R. (2001). "California power grid hack underscores threat to U.S." June 13.

industry leaders in 2007 that not only is a tangible hacker threat to such critical infrastructure possible, it in fact has already happened.[14]

THE SKY IS FALLING, BUT VERY SLOWLY

Alarmists have been accused of equating computer vulnerabilities with vulnerabilities in whole critical infrastructures. Closer to the truth is that modern infrastructures – like the governments which created them – are powerful beasts. They were designed to survive human failings and even natural disasters. To attackers, they represent diverse and distributed targets, comprising not one system, technology, or procedure, but many. Their failsafe mechanisms include personnel who vary considerably in their abilities but may well navigate novel challenges with poise and acumen.

Despite the USSBS citation above, cyber attacks alone should never have the lethality of strategic bombers, especially in the era of nuclear weapons and precision-guided munitions. Even in the case of a successful cyber attack, incident responders will take corrective action, and it is hard to imagine life not going on much as before.

It remains important to imagine scenarios in which creative and well-timed cyber attacks could cause real pain to a government or society. The extent to which we have grown dependent on electronic banking, the Global Positioning System (GPS), and more may only become apparent if and when these systems suffer prolonged downtime.

Devastating cyber attacks on critical infrastructure lie well within the realm of possibility. They represent a particular danger in the context of a traditional kinetic attack. In 2007, it was reported that a cyber attack on Syrian air defense systems preceded the Israeli air force's destruction of an alleged nuclear reactor.[15] If true, that event demonstrates the clear power of cyber attacks to inflict damage on critical infrastructure and could even be called a mini-Digital Pearl Harbor.

Nonetheless, a multitude of challenges stands in the way of cyber attackers and the kind of event that changes the course of history. For example, the convergence of many of our communications media has increased an attacker's theoretical "attack surface." However, the cyber defender is also a direct beneficiary of the proliferation in communications technologies. Today, sensitive sites may well have wired, wireless, and satellite communications that provide an inexpensive level of redundancy and survivability unimagined in the past.[16]

---

[14] Nakashima, E. and Mufson, S. (2008). "Hackers have attacked foreign utilities, CIA analyst says," *Washington Post*, January 19.

[15] Fulghum, D. A., Wall, R., and Butler, A. (2007, November 26). "Cyber-combat's first shot." *Aviation Week & Space Technology*, 167(21), 28.

[16] Lewis, J. A. (2002, December). "Assessing the risks of cyber terrorism, cyber war and other cyber threats." Center for Strategic and International Studies.

Finally, is it possible to undermine our economic well-being through cyber attacks? Could hackers destroy the world's financial markets? At the nation-state level, governments are unlikely to try because the world economy is now intimately interconnected, and they would only be harming themselves in the process. Nonstate actors such as al-Qaeda probably do not possess the time or means to attempt such an attack, although law enforcement must anticipate the attempted physical destruction of high-value computers by terrorists. The high costs in money, time, and effort that are expended by cyber defenders should never be downplayed, but financial institutions are already under constant cyber assault. Hopefully, they are learning valuable lessons in this era of rampant cyber crime that will benefit us all in the future.

PROOFS OF CONCEPT

Current events suggest that cyber attacks on national critical infrastructures are already commonplace around the world. This paper highlights two examples: Israel and Estonia.

During the Cold War, the Middle East often served as a proving ground for military weapons and tactics. In the Internet era, it has done the same for cyber warfare.

In October 2000, following the abduction of three Israeli soldiers in Lebanon, blue and white flags and a sound file playing the Israeli national anthem were planted on a hacked *Hizballah* Website. Subsequent pro-Israeli attacks targeted the official Websites of military and political organizations perceived hostile to Israel, including the Palestinian National Authority, *Hamas*, and Iran.[17]

Retaliation from Pro-Palestinian hackers was quick, and much more diverse in scope. Israeli political, military, telecommunications, media, and universities were all hit. The attackers specifically targeted sites of pure economic value, including the Bank of Israel, e-commerce, and the Tel Aviv Stock Exchange. At the time, Israel was more wired to the Internet than all of its neighbors combined, so there was no shortage of targets. The ".il" country domain provided a well-defined list that pro-Palestinian hackers worked through methodically.

Wars often showcase new tools and tactics. During this conflict, the "Defend" DoS program was used to great effect by both sides, demonstrating in part that software can be copied more quickly than a tank or a rifle. Defend's innovation was to continually revise the date and time of its mock Web requests; this served to defeat the Web-caching security mechanisms at the time.[18]

---

[17] For example, the Zone-H Website lists 67 such defacements from pro-Israeli hacker m0sad during this time period.

[18] Geers, K. (2004). "Cyber Jihad and the globalization of warfare." Black Hat. http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-geers.pdf

The Middle East cyber war demonstrated that Internet- era political conflicts can quickly become internationalized. For example, the Pakistan Hackerz Club penetrated the U.S.-based pro-Israel lobby AIPAC, and published sensitive emails, credit card numbers, and contact information for some of its members.[19] The telecommunications firm AT&T – clearly an international critical infrastructure service provider to all sectors of the world economy – was targeted for providing technical support to the Israeli government during the crisis.[20]

Since 2000, the Middle East cyber war has generally followed the conflict on the ground. In 2006, as tensions rose on the border between Israel and Gaza, pro- Palestinian hackers shut down around 700 Israeli Internet domains, including those of Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel, and McDonalds Israel.[21]

Fast-forward seven years, and spin the globe 3,000 km due north. On April 26, 2007, the Estonian government moved a Soviet World War II memorial from the center of its capital to a military cemetery. The move inflamed public opinion both in Russia and among Estonia's Russian minority population. Beginning on April 27, Estonian government, law enforcement, banking, media, and Internet infrastructure endured three weeks of cyber attacks, whose impact still generates immense interest from governments around the world.

Estonians conduct more than 98% of their banking via electronic means. Therefore, the impact of multiple Distributed Denial-of-Service (DDoS) attacks that severed all communications to the Web presence of the country's two largest banks for up to two hours and rendered international services partially unavailable for days at a time, is obvious.

Less widely discussed but likely of greater consequence – both to national security planners and to computer network defense personnel – were the Internet infrastructure (router) attacks on one of the Estonian government's ISPs, which disrupted government communications for a "short" period of time.[22] On the propaganda front, a hacker defaced the Estonian Prime Minister's political party Website, changing the homepage text to a fabricated government apology for having moved the statue, along with a promise to move it back to its original location.

Diplomatic interest in the Estonia case was high in part due to the possible reinterpretation of NATO's Article 5, which states that "an armed attack against one [Alliance member] . . . shall be considered an attack against them all."[23] Article 5 has been invoked only once, following the terrorist attacks of September 11, 2001. Potentially, it could one day be interpreted to encompass cyber attacks as well.

---

[19] "Israel lobby group hacked." (2002). *BBC News*, November 3.
[20] Page, B. (2000). "Pro-Palestinian hackers threaten AT&T." *TechWeb News*, November 11.
[21] Stoil, R. A. and Goldstein, J. (2006). "One if by land, two if by modem." *The Jerusalem Post*, June 28.
[22] This case-study relies on some data available exclusively to CCDCOE.
[23] *The North Atlantic Treaty*, Washington DC, April 4, 1949.

THE FUTURE

The Internet is changing most of life as we know it, to include the nature and conduct of warfare. While threats to critical infrastructure have always existed during wartime, threats now include attacks even during peacetime, from computer hackers who may be able to remain entirely anonymous.

Current events demonstrate that it is no longer a question of whether computer hackers will take national security planners by surprise, but when and under what circumstances. The cases of Israel and Estonia prove that a certain level of real-world disorder can be achieved from data packets alone: banks were knocked offline, media went silent, e-commerce was down, and government connectivity with its own citizens was threatened. Furthermore, the examples we have seen so far may be pure proof of concept; serious, capable adversaries likely hold some aces high up their sleeves, saving them for the advent of war.

To some extent, all national critical infrastructures are vulnerable, but their true vulnerability – especially to cyber attack – is theoretical by nature. In due course, as the real and virtual worlds continue to interact with each other on a more intimate basis, future attacks will bring theory and reality closer together.

While nations robust in IT have numerous advantages over their less wired peers, the Internet is a prodigious medium through which a weaker party can attack a stronger conventional foe. Currently, because cyber attackers appear to have the advantage, many governments and even nonstate actors have likely concluded that the best cyber defense is a good offense. Tactical victories, even of a purely digital nature, can affect strategic-level decision making, especially if they threaten the critical infrastructures (or "institutions," as Morgenthau put it) of an adversary. It is therefore critical that defense against hostile computer network operations – from espionage to propaganda to attacks on critical infrastructures – should now play a role in all national security planning.

Still, national security planners should remain levelheaded and address cyber threats with method and objectivity. First, they should evaluate the level of their infrastructure's dependence on IT, and, second, its level of connectivity to the Internet. Finally, they should vividly imagine worst-case scenarios: if a hostile actor had complete control of a critical system, how much damage could be done? In part, cyber attacks are scary because they involve esoteric tools and tactics. But it is worth considering that, just as attempting a cyber attack can be easier and cheaper than mounting a physical attack, the level and length of disruption cyber attacks cause may be proportionately less.[24] For the foreseeable future, to inflict lasting damage on critical infrastructures via cyber attack alone is probably closer to *Don Quixote* than *War Games*.

---

[24] Lewis, J. A. (2002, December). "Assessing the risks of cyber terrorism, cyber war and other cyber threats," Center for Strategic and International Studies.

Critical infrastructures are designed to fail gracefully, and to be rebooted. Therefore, the goal should not be perfection, but good crisis management. Over time, as the control of critical infrastructures shifts from dedicated networks to the open Internet, and employs common network protocols over proprietary ones, there will be increased opportunities for hackers to invade once-closed systems. As our dependence on IT and Internet connectivity grows, governments should make proportional investments in network security, incident response, and technical training for law enforcement. Finally, they should begin to invest in international collaborative initiatives that are specifically designed to counter the transnational nature of cyber attacks.[25]

Alexander Eisen, University of Advancing Technology, Tempe, Arizona USA, served as technical editor for this article.

[25] Ibid.