Cyberspace and the Changing Nature of Warfare

Kenneth Geers
U.S. Representative
Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

kenneth.geers@mil.ee

ABSTRACT

Practically everything that happens in the real world is mirrored in cyberspace. For national security planners, this includes propaganda, espionage, reconnaissance, targeting, and – to an unknown extent – warfare itself.

Strategists must be aware that part of every political and military conflict will take place on the Internet, whose ubiquitous and unpredictable characteristics mean that the battles fought there can be just as important, if not more so, than events taking place on the ground.

This paper offers five strategic reasons why cyber warfare is on the rise:

- *The Internet is vulnerable to attack*
- *A high return on investment*
- *The inadequacy of current cyber defenses*
- *Plausible deniability*
- *The increased participation of non-state actors*

The author describes five common tactics used in cyber warfare:

- *Espionage*
- *Propaganda*
- *Denial-of-Service (DoS)*
- *Data modification*
- *Infrastructure manipulation*

Finally, this paper summarizes lessons learned from five case studies:

- *1994: Russia and Chechnya*
- *1999: NATO and the war over Kosovo*
- *2000: Middle East cyber war*
- *2001: American and Chinese "patriotic" hackers*
- *2007: Cyber war in Estonia*

Aggressive cyber warfare strategies and tactics offer many advantages to their prospective employers, and current events demonstrate that cyber conflict is already commonplace around the world. As a consequence, national security leadership must dramatically improve its understanding of the technology,

law, and ethics of cyber attack and defense, so that it can competently factor cyber warfare into all stages of national security planning.

1.0 CYBER WARFARE: STRATEGY

1.1 The Internet is Vulnerable

The Internet's imperfect design allows hackers to surreptitiously read, delete, and/or modify information stored on or traveling between computers. There are about 100 additions to the Common Vulnerabilities and Exposures (CVE) database each month.[i] Attackers, armed with constantly evolving malicious code, likely have more paths into your network and the secrets it contains than your system administrators can protect.

1.2 High Return on Investment

The objectives of cyber warfare practitioners speak for themselves: the theft of research and development data, eavesdropping on sensitive communications, and the delivery of powerful propaganda deep behind enemy lines (to name a few). The elegance of computer hacking lies in the fact that it may be attempted for a fraction of the cost – and risk – of any other information collection or manipulation strategy.

1.3 The Inadequacy of Cyber Defense

Cyber defense is still an immature discipline. Traditional law enforcement skills are inadequate, and it is difficult to retain personnel with highly marketable skills. Challenging computer investigations are further complicated by the international nature of the Internet. Finally, in the case of state-sponsored computer network operations, law enforcement cooperation will be either Potemkin or non-existent.

1.4 Plausible Deniability

The maze-like architecture of the Internet offers cyber attackers a high degree of anonymity. Smart hackers can route attacks through countries with which the victim's government has poor diplomatic relations and no law enforcement cooperation. Even successful investigations often lead only to another hacked computer. Governments today face the prospect of losing a cyber conflict without ever knowing the identity of their adversary.

1.5 Participation of Non-State Actors

Nation-states endeavor to retain as much control as they can over international conflict. However, globalization and the Internet have considerably strengthened the ability of anyone to follow current events, as well as the power to shape them. Transnational subcultures now spontaneously coalesce online, and influence myriad political agendas, without reporting to any chain-of-command. A challenge for national security leadership is whether such activity could spin delicate diplomacy out of control.

2.0 CYBER WARFARE: TACTICS

2.1 Espionage

Increasingly, governments around the world complain publicly of cyber espionage.[ii] On a daily basis, anonymous computer hackers secretly and illegally copy vast quantities of computer data and network communications. Theoretically, it is possible to conduct devastating intelligence-gathering operations, even on highly sensitive political and military communications, remotely from anywhere in the world.

2.2 Propaganda

Cheap and effective, propaganda is often both the easiest and the most powerful cyber attack. Digital information, in text or image format – and regardless of whether it is true – can be instantly copied and sent anywhere in the world, even deep behind enemy lines. And provocative information that is removed from the Web may appear on another website in seconds.

2.3 Denial-of-Service (DoS)

The simple strategy behind a DoS attack is to deny the use of a computer resource to legitimate users. The most common tactic is to flood the target with so much superfluous data that it cannot respond to real requests for services or information. Other DoS attacks include physical destruction of computer hardware and the use of electromagnetic interference, designed to destroy unshielded electronics via current or voltage surges.[iii]

2.4 Data Modification

Data modification is extremely dangerous, because a successful attack can mean that legitimate users (human or machine) will make an important decision(s) based on maliciously altered information. Such attacks range from website defacement (often referred to as “electronic graffiti”, but which can still carry propaganda or disinformation) to database attacks intended to corrupt weapons or Command and Control (C2) systems.

2.5 Infrastructure Manipulation

National critical infrastructures are, like everything else, increasingly connected to the Internet. However, because instant response is often required, and because associated hardware may have insufficient computing resources, security may not be robust. The management of electricity may be especially important for national security planners to evaluate, because electricity has no substitute, and all other infrastructures depend on it.[iv] Finally, it is important to note that almost all critical infrastructures are in private hands.

3.0 CHECHNYA 1994: PROPAGANDA

In the Internet era, unedited news from a war front can arrive in real-time. Internet users worldwide play an important role in international conflicts simply by posting information, in either text or image format,

to a website.

Since the earliest days of the World Wide Web, pro-Chechen and pro-Russian forces have waged a virtual war on the Internet, simultaneous to their conflict on the ground. The Chechen separatist movement in particular is considered a pioneer in the use of the Web as a tool for delivering powerful public relations messages. The skillful placement of propaganda and other information, such as the number to a war funds bank account in Sacramento, California, helped to unite the Chechen diaspora.[v]

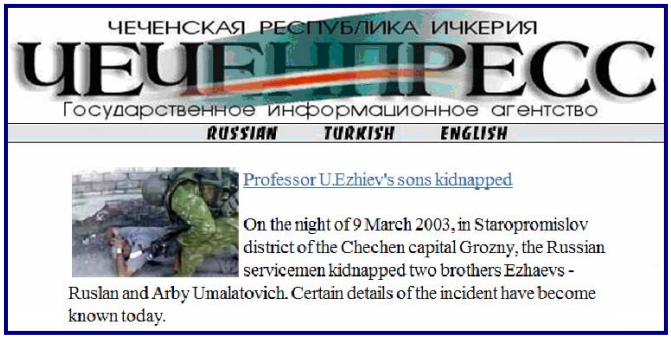


Figure 1: *Chechen Press* on Russian military activities

The most effective information, however, was not pro-Chechen, but anti-Russian. Digital images of bloody corpses served to turn public opinion against perceived Russian military excesses. In 1999, just as Kremlin officials were denying an incident in which a Chechen bus was attacked and many passengers killed, images of the incident appeared on the Web.[vi] As technology progressed, Internet surfers watched streaming videos of favorable Chechen military activity, such as ambushes on Russian military convoys.[vii]

The Russian government admitted the need to improve its tactics in cyberspace. In 1999, Vladimir Putin, then Russia's Prime Minister, stated that "we surrendered this terrain some time ago ... but now we are entering the game again." Moscow sought the help of the West in shutting down the important pro-Chechen kavkaz.org website, and "the introduction of centralized military censorship regarding the war in the North Caucasus" was announced.[viii]

During the second Chechen war (1999-2000), Russian officials were accused of escalating the cyber conflict, by hacking into Chechen websites. The timing and sophistication of at least some of the attacks suggested nation-state involvement. For example, kavkaz.org (hosted in the U.S.) was reportedly knocked offline simultaneous to the storming by Russian special forces of a Moscow theater under siege by Chechen terrorists.[ix]

4.0 KOSOVO 1999: HACKING THE MILITARY

In globalized, Internet-era conflicts, anyone with a computer and a connection to the Internet is a potential combatant. NATO's first major military engagement followed the explosive growth of the Web during the 1990's. Just as Vietnam was the world's first TV war, Kosovo was its first broad-scale Internet war.

As NATO planes began to bomb Serbia, numerous pro-Serbian (or anti-Western) hacker groups, such as the "Black Hand", began to attack NATO Internet infrastructure. It is unknown whether any of the hackers worked directly for the Yugoslav military; regardless, their stated goal was to disrupt NATO's military operations.[x]

Figure 2: the Black Hand, version 1.0

The Black Hand, which borrowed its name from the Pan-Slavic secret society that helped to start World War I, claimed it could enumerate NATO's "most important" computers, and that through hacking it would attempt to "delete all the data" on them. The group claimed success on at least one U.S. Navy computer, and stated that it was subsequently taken off-line.[xi]

NATO, U.S., and UK computers were all attacked during the war, via Denial-of-Service and virus-infected email (twenty-five different strains of viruses were detected).[xii] In the U.S., the White House website was defaced, and a Secret Service investigation ensued. While the U.S. claimed to have suffered "no impact" on the overall war effort, the UK admitted to having lost at least some database information.[xiii]

At NATO Headquarters in Belgium, the attacks became a propaganda victory for the hackers. The NATO public affairs website for the war in Kosovo, where the organization sought to portray its side of the conflict via briefings and news updates, was "virtually inoperable for several days." NATO spokesman Jamie Shea blamed "line saturation" on "hackers in Belgrade." A simultaneous flood of e-mail successfully choked NATO's e-mail server. As the organization endeavored to upgrade nearly all of its computer servers, the network attacks, which initially started in Belgrade, began to emanate from all over the world.[xiv]

5.0 MIDDLE EAST 2000: TARGETING THE ECONOMY

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.

Figure 3: vandalized *Hizballah* website

In October 2000, following the abduction of three Israeli soldiers, 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.[xv]

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 also targeted sites of pure economic value, including the Bank of Israel, e-commerce sites, 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 of the time.[xvi]

Figure 4: pro-Palestinian hacker portal

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,[xvii] and the telecommunications firm AT&T was targeted for providing technical support to the Israeli government during the crisis.[xviii]

Since 2000, the Middle East cyber war has generally followed the conflict on the ground. In 2006, as tensions rose 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.[xix]

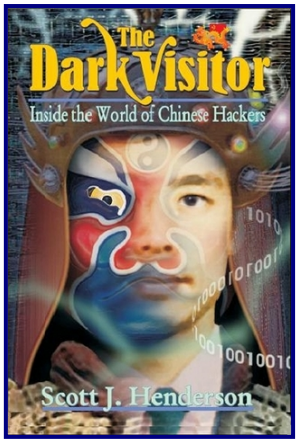
6.0 U.S. & CHINA 2001: PATRIOTIC HACKING

On April 26, 2001, the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) released advisory 01-009:

"Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems … Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC…"[xx]

Figure 5: the downed EP-3 on Hainan Island

Tensions had risen sharply between the two countries following the U.S. bombing of the Chinese embassy in Belgrade in 1999, and after the mid-air collision of a U.S. Navy plane with a Chinese fighter jet over the South China Sea in 2001, followed by the prolonged detainment of the American crew in the PRC.



Hackers on both sides of the Pacific, such as China Eagle Alliance and PoizonB0x, began wide-scale website defacement, and built hacker portals with titles such as "USA Kill" and "China Killer". When the cyber skirmishes were over, both sides claimed defacements and DoSs in the thousands.[xxi]

The FBI investigated a Honker Union of China (HUC), 17-day hack of a California electric power grid test network that began on April 25th.[xxii] The case was widely dismissed as media hype at the time, but the CIA informed industry leaders in 2007 that not only is a tangible hacker threat to such critical infrastructure possible, it in fact has already happened.[xxiii]

Figure 6: Interest remains high

On the anniversary of this cyber war, as businesses were bracing for another round of hacking, the Chinese government is said to have successfully called for a stand-down at the last minute, suggesting that Chinese hackers may share a greater degree of coordination than their American counterparts.[xxiv]

7.0 ESTONIA 2007: TARGETING A NATION-STATE

On April 26, 2007, the Estonian government moved a Soviet World War II memorial out of the center of its capital, Tallinn, in a move that inflamed public opinion both in Russia and among Estonia's Russian minority population.

Figure 7: Physical destruction in Tallinn

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.

Because Estonians conduct over 98% of their banking online, the impact of multiple distributed denial-of-service (DDoS) attacks, that severed all communications to 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 are said to have disrupted government communications for at least a "short" period of time.

On the propaganda front, a hacker defaced the Estonian Prime Minister's political party website on April 27, 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.[xxv]

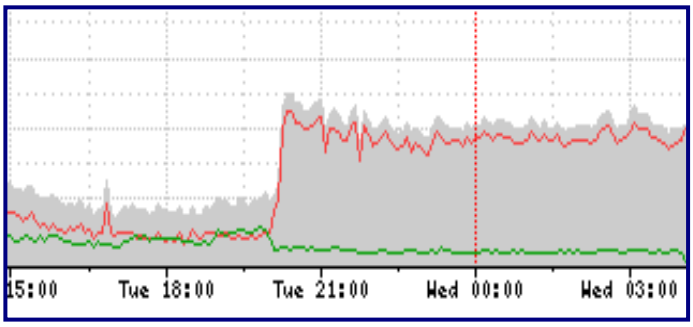


Figure 8: How the attack appeared in cyberspace

Diplomatic interest in this cyber attack 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".[xxvi] 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.

8.0 SUMMARY

All political and military conflicts now have a cyber dimension, whose size and impact are difficult to predict. Attackers have at their disposal a wide variety of effective cyber warfare strategies and tactics.

Above all, the Internet is vulnerable to attack. Further, its amplifying power means that future victories in cyberspace could translate into victories on the ground. Both state and non-state actors enjoy a high return on investment in cyber tactics, which range from the placement of carefully crafted propaganda to the manipulation of an adversary's critical infrastructure.

Five case studies suggest that it is no longer a question of whether computer hackers will take national security planners by surprise, but when and under what circumstances. To summarize the lessons learned:

- The conflict in Chechnya demonstrated the strength of the Internet to disseminate unpredictable and influential propaganda.

- During the war over Kosovo, non-state actors attempted to disrupt military operations through hacking, and were able to claim minor victories.
- The Middle East cyber war quickly became globalized, and brought targets of pure economic value into the conflict.
- In 2001, simmering tensions between two countries spilled over into a "patriotic" hacker war, with uncertain consequences for national security leadership.
- The politically-motivated cyber attacks on IT-dependent Estonia brought unprecedented attention to cyber security from governments around the world.

The Internet is changing much of life as we know it, to include the nature and conduct of warfare. At times, cyber tools and tactics will favor nations robust in information technology, but the Internet is a prodigious tool for a weaker party to attack a stronger conventional foe. As with terrorism and weapons of mass destruction, the dynamic, asymmetric, and still-evolving nature of cyber attacks makes all aspects of cyber defense – including detection, analysis, investigation, prosecution, retaliation, and more – critical questions for national security planners to answer.

---

[1] CVE List Main Page, http://cve.mitre.org/cve/index.html.

[2] See, for example, Cody, Edward. "Chinese Official Accuses Nations of Hacking", *Washington Post*, September 13, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791_pf.html#.

[3] "Electromagnetic bomb", Wikipedia, http://en.wikipedia.org/wiki/Electromagnetic_bomb.

[4] Divis, Dee Ann. "Protection not in place for electric WMD", UPI, March 9, 2005, http://www.globalsecurity.org/org/news/2005/050309-electric-wmd.htm.

[5] Thomas, Timothy L. "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?", Foreign Military Studies Office, Fort Leavenworth, 2002, and in Chapter 11 of *Russian Military Reform 1992-2002*, Frank Cass Publishers, 2003, http://leav-www.army.mil/fmso/documents/iwchechen.htm.

[6] Goble, Paul. "Russia: Analysis from Washington -- a Real Battle on the Virtual Front," Radio Free Europe / Radio Liberty, October 11, 1999, http://www.rferl.org/features/1999/10/F.RU.991011135919.asp.

[7] Thomas, see above.

[8] Goble, see above.

[9] Bullough, Oliver. "Russians Wage Cyber War on Chechen Websites", Reuters, November 15, 2002, http://seclists.org/isn/2002/Nov/0064.html.

[10] "Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer", Bosnian Serb News Agency SRNA, March 28, 1999 (BBC Monitoring Service, March 30, 1999).

[11] *Ibid.*

[12] "Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries", mi2g, April 19, 1999.

[13] Geers, Kenneth. *Hacking in a Foreign Language*, Black Hat 2005, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-geers-update.pdf.

[14] Verton, Daniel. "Serbs Launch Cyberattack on NATO", *Federal Computer Week*, April 4, 1999, http://www.fcw.com/print/5_62/news/69130-1.html.

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

[16] Geers, Kenneth. *Cyber Jihad and the Globalization of Warfare*, Black Hat, 2004, http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-geers.pdf.

[17] "Israel lobby group hacked", BBC News, November 3, 2000, http://news.bbc.co.uk/2/hi/middle_east/1005850.stm.

[18] Page, Barnaby. "Pro-Palestinian Hackers Threaten AT&T", *TechWeb News*, November 11, 2000, http://www.techweb.com/wire/story/TWB20001110S0010.

[19] Stoil, Rebecca Anna and Goldstein, James. "One if by Land, Two if by Modem", *The Jerusalem Post*, June 28, 2006, http://www.jpost.com/servlet/Satellite?cid=1150885871095&pagename=JPost%2FJPArticle%2FPrinter.

[20] IWS - The Information Warfare Site, http://www.iwar.org.uk/infocon/advisories/2001/01-009.htm.

[21] Wagstaff, Jeremy. "The Internet could be the site of the next China-U.S. standoff", *The Wall Street Journal*, April 30, 2001, http://online.wsj.com/article/SB98856633376453558.html?mod=googlewsj, and Allen, Patrick D. and Demchek, Chris C., "The Cycle of Cyber Conflict", *Military Review*, March-April 2003.

[22] Weisman, Robyn. "California Power Grid Hack Underscores Threat to U.S.", June 13, 2001, http://www.newsfactor.com/perl/story/11220.html.

[23] Nakashima, Ellen and Mufson, Steven. "Hackers Have Attacked Foreign Utilities, CIA Analyst Says", *Washington Post*, January 19, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277_pf.html.

[24] Hess, Pamela. "China prevented repeat cyber attack on US", UPI, October 29, 2002, http://www.upi.com/view.cfm?StoryID=20021029-121924-5101r.

[25] This case-study relies on some data available exclusively to the CCD-CoE.

[26] *The North Atlantic Treaty*, Washington D.C., April 4, 1949, http://www.nato.int/docu/basictxt/treaty.htm.