

Kenneth Geers
Naval Criminal Investigative Service (NCIS)
Cooperative Cyber Defence Centre of Excellence (CCD COE)
12 Filtri Street
Tallinn, Estonia 10132
kenneth.geers@ccdcoe.org

The Challenge of Cyber Attack Deterrence

Abstract

National security planners have begun to look beyond reactive, tactical cyber defense to proactive, strategic cyber defense, which may include international military deterrence. The incredible power of nuclear weapons gave birth to deterrence, a military strategy in which the purpose of armies shifted from winning wars to preventing them. Although cyber attacks per se do not compare to a nuclear explosion, they do pose a serious and increasing threat to international security. Real-world examples suggest that cyber warfare will play a lead role in future international conflicts. This article examines the two deterrence strategies available to nation-states (denial and punishment) and their three basic requirements (capability, communication, and credibility) in the light of cyber warfare. It also explores whether the two most challenging aspects of cyber attacks – attribution and asymmetry – will make cyber attack deterrence an impossible task.

Keywords

Cyber attack, deterrence, Internet, hacker, critical infrastructure, military strategy, nuclear, security, war

1. Introduction: Cyber Attacks and Deterrence Theory

The advent of nuclear weapons disrupted the historical logic of war completely. Deterrence theory emerged after the United States and the Soviet Union created enough military firepower to destroy human civilization on our planet. From that point forward, according to the American military strategist Bernard Brodie (1946), the purpose of armies shifted from winning wars to preventing them.

Nothing compares to the destructive power of a nuclear blast. But cyber attacks loom on the horizon as a threat that is best understood as an extraordinary means to a wide variety of political and military ends, many of which can have serious national security ramifications. For example, computer hacking can be used to steal offensive weapons technology (including for weapons of mass destruction) or to render an adversary's defenses inoperable during a conventional military attack (Fulghum et al., 2007). In that light, attempting proactively to deter cyber attacks may become an essential part of na-

tional military strategies. This article examines whether it is possible to apply deterrence theory to cyber attacks.

What military officers call the ‘battlespace’ grows more difficult to define – and to defend – over time. In 1965, Gordon Moore correctly predicted that the number of transistors on a computer chip would double every two years. There has been similar growth in almost all aspects of information technology (IT), including practical encryption, user-friendly hacker tools, and Web-enabled open source intelligence (OSINT). Even the basic services of a modern society such as water, electricity and telecommunications are now computerized and often connected to the Internet (Geers, 2009).

Advances in technology are normally evolutionary, but they can be revolutionary: artillery reached over the front lines of battle; rockets and airplanes crossed national boundaries; today, cyber attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity. Political and military strategists now use and abuse computers, databases, and the networks that connect them to achieve their objectives. In the early 1980s, this concept was already known in the Soviet Union as the Military Technological Revolution (MTR); after the 1991 Gulf War, the Pentagon’s Revolution in Military Affairs was almost a household term (Mishra, 2003).

However, the real-world impact of cyber conflict is still difficult to appreciate, in part because there have been no wars between modern, cyber-capable militaries. But an examination of international affairs over the past two decades suggests that cyber battles of increasing consequence are easy to find. Since the earliest days of the World Wide Web, Chechen guerilla fighters, armed not only with rifles but with digital cameras and HTML, have demonstrated the power of Internet-enabled propaganda (Goble, 1999). In 2001, tensions between the United States and China spilled over into a non-state, “patriotic” hacker war, with uncertain consequences for national security leadership.¹ In 2007, Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli air force demolished an alleged Syrian nuclear reactor (Fulghum, 2007). In 2009, the entire nation-state of Kyrgyzstan was knocked offline during a time of domestic political crisis (Keizer, 2009), and Iranian voters, in “open war” with state security forces, used peer-to-peer social-networking websites to avoid government restrictions on dialogue with the outside world (Stöcker et al., 2009). Such a quick evolution in the use of cyber tools and tactics suggests that they will play a lead role in future international conflicts.

While the Internet has on balance been hugely beneficial to society, law enforcement and counterintelligence personnel struggle to keep pace with its security implications. The ubiquity of the Internet makes cyber warfare a strategic weapon; adversaries can exchange blows at will, regardless of the physical distance between them. By contrast, cyber defense is a tedious process, and cyber attack investigations are typically inconclusive. The astonishing achievements of cyber crime and cyber espionage should hint at the potential damage of a true, nation-state-sponsored cyber attack. Intelligence offi-

¹ On April 26, 2001, the Federal Bureau of Investigation’s (FBI) National Infrastructure Protection Center (NIPC) released Advisory 01-009, Increased Internet Attacks against U.S. Web Sites and Mail Servers Possible in Early May.

cials such as former CIA director James Woolsey fear that even terrorist groups will possess cyber weapons of strategic significance in the next few years.

Military leaders have begun to look beyond reactive, tactical cyber defense² to the formulation of a proactive, strategic cyber defense policy, which may include international military deterrence.³ However, two challenging aspects of cyber attacks – attribution and asymmetry – will be difficult to overcome.

In theory, nation-states have two primary deterrence strategies:

1. denial, and
2. punishment.

Both strategies have three basic requirements:

1. capability,
2. communication, and
3. credibility.⁴

This paper will examine each concept in turn, and explore whether it is possible to deter cyber attacks at the nation-state level.

2. Cyber Attack Deterrence by Denial

Deterrence by denial is a strategy in which an adversary is physically prevented from acquiring a threatening technology. This is the preferred option in the nuclear sphere, because there is no practical defense against a nuclear explosion; its heat alone is comparable to the interior of the sun, and its blast can demolish reinforced concrete buildings three kilometers away (Sartori, 1983). The abhorrent nature of nuclear warfare makes even a theoretical victory difficult to imagine. Deterrence by denial is a philosophy embodied in the Non-Proliferation Treaty (NPT), and one reason behind current international tension with North Korea and Iran (Shultz et al., 2007).

2.1. Denial: Capability

Despite the diplomatic efforts of NPT, the well-funded inspection regime of the International Atomic Energy Agency (IAEA),⁵ and unilateral military operations such as Israel's

² E.g., how to configure a network or an intrusion detection system.

³ In May, 2009, the head of the U.S. Strategic Command, Air Force Gen. Kevin Chilton, stated that retaliation for a cyber attack would not necessarily be limited to cyberspace.

⁴ These deterrence strategies and requirements I took from a personal interview with Prof. Peter D. Feaver, Alexander F. Hehmyer Professor of Political Science and Public Policy at Duke University and Director of the Triangle Institute for Security Studies (TISS).

⁵ The IAEA is the world's nuclear inspectorate, with more than four decades of verification experience. Inspectors work to verify that safeguarded nuclear material and activities

destruction of nuclear facilities in Iraq in 1981 and in Syria in 2007, the size of the world's nuclear club is growing. In addition to the five permanent members of the United Nations Security Council,⁶ de facto members now include India, Israel, Pakistan, and North Korea (Huntley, 2009).

Cyber attack tools and techniques are not nearly as dangerous as their nuclear counterparts, but they are by comparison simple to acquire, deploy, and hide. Hacker training and conferences are abundant: over the past 17 years, almost 1,000 how-to presentations have been given at DEFCON. More sensitive hacker information can be kept secret, physically transported on a miniscule hard drive, or sent encrypted across the Internet. A nuclear weapons program is difficult to hide (Milhollin & Lincy, 2009); a cyber weapons program is not. Cyber attacks can be tested discretely in a laboratory environment⁷ or live on the Internet, anonymously. Further, it appears increasingly common to outsource the illegal business of hacking to a commercial or criminal third party.⁸

A major challenge to cyber attack tool anti-proliferation is how to define malicious code. A legitimate path for remote system administration can also be used by a masquerading hacker to steal national secrets. Even published operating system and application code is difficult for experts to understand thoroughly, as there are simply too many lines of code to analyze (Cole, 2002). The dynamic and fast-evolving nature of cyber attack technology contrasts sharply with the fundamental design of nuclear warheads, which, with the exception of the neutron bomb, has not changed much since the late 1950s.⁹ In the single month of May 2009, Kaspersky Anti-Virus Lab reported that it found 42,520 unique, suspicious programs on its clients' computers.

Finally, in nuclear warfare, one of the most important considerations is the retention of a second-strike capability. Following a surprise attack, is it still possible for the victim to fight back? In nuclear and conventional warfare, this is a constant worry among strategic planners. A unique characteristic of cyber attacks is their ability to be launched from anywhere in the world, at any time. During the cyber attacks on Estonia in 2007, most of the compromised and attacking computers were located in the United States.¹⁰ Cyber attacks can be set to launch under predetermined conditions or on a certain date in the future. Discovered attack tools can also be difficult to remove from a computer net-

are not used for military purposes. The annual budget of the IAEA is almost \$500 million USD.

⁶ China, France, Russia, the United Kingdom and the United States.

⁷ With nuclear weapons, a hard-to-conceal test is required to prove that a capability exists. If the goal were cyber attack tool anti-proliferation, it would seem difficult to know if or when success had been achieved.

⁸ In 2009, the French Interior Ministry investigated the collection of "strategic intelligence" by a former intelligence agent and a for-hire computer hacker on behalf of some of France's biggest companies (Jolly, 2009).

⁹ There have, however, been many design modifications relating to safety, security, and reliability.

¹⁰ As computer incident response teams began to block hostile network packets, the source of the attack moved to countries with less mature and/or helpful network management practices.

work completely, even by forensic experts. With cyber attack technology, it seems impossible to know for sure that all adversary attack options have been eliminated.

2.2. Denial: Communication

Cyber attacks now have the attention of the world's national security planners. In the U.S., enhancing cyber security was one of the six "mission objectives" of the 2009 Director of National Intelligence (ODNI) National Intelligence Strategy,¹¹ and counteracting the cyber threat is currently the third-highest priority of the Federal Bureau of Investigation (FBI), after preventing terrorist attacks and thwarting foreign intelligence operations.

However, cyber warfare is a new phenomenon; national and international norms have yet to be established. Different approaches are under consideration. One is to broaden international law enforcement coordination, specifically via the Council of Europe Convention on Cybercrime. Objections to this strategy include the possible infringement of national sovereignty by foreign law enforcement agencies. Another approach is to prohibit the development of cyber weapons via international treaty, such as that negotiated for chemical weapons. Articles to such a treaty might ban supply chain attacks, the disruption of non-combatant networks, and increase international management of the Internet. One objection to the second approach is that it does little to improve cyber attack attribution (Markoff & Kramer, 2009).

The Convention on Cybercrime is the first such international treaty. It describes law enforcement powers and procedures related to data interception and the search of computer networks. In 2009, forty-six nations were signatories; twenty-six had ratified the treaty.¹² Its main objective, set out in the Preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially via national legislation and international cooperation. Deterrence is specifically mentioned as a goal: "the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems."

The continued success of the Convention on Cybercrime requires addressing myriad national and international data security and privacy concerns, including the respect for national sovereignty. A non-governmental organization in Thailand, for example, has claimed that similar legislation there has been used by the government more to threaten Thai citizens than to protect them (Anonymous, 2009). A proposed international treaty banning the development and use of hacker tools would be no less challenging to sign and enforce, because many hacker tools can properly be called dual-use technology.¹³

¹¹ The other five objectives were Combat Violent Extremism, Counter WMD Proliferation, Provide Strategic Intelligence and Warning, Integrate Counterintelligence Capabilities, and Support Current Operations.

¹² The U.S. acceded to the Council of Europe Convention on Cybercrime on January 1, 2007.

¹³ System administrators often use hacker tools such as a password cracker to audit their own networks. Cyber defense studies in academia require hacker tools for laboratory purposes.

The Council of Europe's protocol on criminalizing racist and xenophobic statements on the Web may offer a partial solution. Because countries have wildly varying laws regarding what constitutes free speech, universally-accessible websites can create international legal headaches.¹⁴ This protocol recommends a nationally-tailored approach to regulation that allows for implementation at the local ISP and end-user levels. In this way, signatories are able to project their norms of free speech onto the Internet, without extending liability beyond national borders (Oberdorfer Nyberg, 2004).¹⁵

2.3. Denial: Credibility

Deterrence theory states that capability and communication alone are insufficient. The threatened party must believe that the threat of retaliation – or of a preemptive strike – is real. This third requirement of deterrence is the most difficult for national security leadership to assess, because it involves evaluating human psychology, rationality, the odds of miscalculation, and foreign political-military affairs.

At the beginning of the year 2010, it is still not likely that nation-states will sacrifice much to prevent the proliferation of cyber attack tools and techniques. Although it is indisputable that cyber attacks cause enormous financial damage, that world leaders increasingly complain of cyber espionage, and that Internet-connected critical infrastructures are now at risk, deterrence theory was created for nuclear weapons. In terms of their destructive power, nukes are in a class by themselves. Cyber attacks per se do not cause explosions, deadly heat, radiation, an electro-magnetic pulse (EMP), or human casualties.¹⁶

A future cyber attack, by causing any of the above effects, could change this perception. Worldwide technological convergence, as described by Dawson (2002), is constantly expanding what hackers call the “attack surface.” In theory, the successful conquest of an adversary's Internet space could equate to assuming command and control of the adversary's military forces, and firing their own weapons against their own cities. But for now, this scenario still lies in the realm of science fiction.

3. Cyber Attack Deterrence by Punishment

Deterrence by punishment is a strategy of last resort. It signifies that deterrence by denial was not possible or has failed, and that Country X possesses the technology it needs to threaten Country Y or its government. The goal of deterrence by punishment is to prevent aggression by threatening greater aggression, in the form of painful and perhaps fatal

¹⁴ For example, a French judge found a U.S. ISP criminally liable for hosting an auction of Nazi paraphernalia, the sale of which is illegal in France.

¹⁵ The named methods of implementing the protocol are self-regulation of content by ISPs, government regulation of specific content, government regulation of end-users, and government regulation of local ISPs.

¹⁶ Persuasive cyber war skeptics include Cambridge University Professor Ross Anderson and *Wired* “Threat Level” Editor Kevin Poulsen.

retaliation. For the strategy to work, Country X must be convinced that victory is not possible, even given the option of using its new technology.

Two key aspects of cyber attacks present challenges to national security planners who would seek to deter them by punishment:

1. attribution, and
2. asymmetry.

The first challenge undermines a state's capability to respond to a cyber attack, and the second undermines its credibility.

3.1. Punishment: Capability

All nations with robust military, law enforcement, and/or diplomatic might theoretically have the power to punish a cyber attacker in some way, either in cyberspace or in the real world. And if a known attacker is beyond the reach of physical pursuit, the victim could at least present incriminating evidence in an international forum. But in practice, for punishment to be a viable option, the victim must know for sure who the attacker is, and be able to prove it.

In cyber warfare, the attacker enjoys a formidable advantage: anonymity. Proof in cyberspace is hard to come by. Smart hackers hide within the maze-like architecture of the Internet. They route attacks through countries with which the target's government has poor diplomatic relations or no law enforcement cooperation, and exploit unwitting, third-party networks. Cyber investigations typically end at a hacked, abandoned computer, where the trail goes cold. Plausible deniability is also a concern. Because hackers obscure the true origin of an attack by hopping through a series of compromised computers to reach their target, the real attacker could always claim that her computer had merely been hacked and used in someone else's operation. This aspect of cyber attacks also makes "false flagging," or intentionally trying to pin the blame on a third party, an attractive option.

Even in the event that cyber attack attribution is positively determined, deterrence by punishment is still inherently less credible than deterrence by denial. It requires decision-makers to make more difficult choices. A proactive law enforcement strategy is easier to justify than the use of military force, which can cause physical destruction, human casualties, or other collateral damage. At the very least, there will be serious diplomatic consequences.

One important decision facing decision-makers in the aftermath of a cyber attack would be whether to retaliate in kind or to employ more conventional weapons. It may seem logical to keep the conflict within cyberspace, but a cyber-only response does not guarantee proportionality, and a cyber counterattack may lack the required precision. A misfire in cyberspace might adversely affect critical national infrastructure such as a hospital, which could result in a violation of the Geneva Convention and even bring war crimes charges against national authorities (Graham, 1999). The Law of Armed Conflict

states that the means and methods of warfare are not unlimited:¹⁷ commanders may use “only that degree and kind of force ... required in order to achieve the legitimate purpose of the conflict ... with the minimum expenditure of life and resources.”¹⁸

3.2. Punishment: Communication

Whereas deterrence by denial relies on a criminal law framework for support, the foundation of deterrence by punishment lies in military doctrine. When bombs begin to fall on adversary targets, diplomatic and law enforcement options have normally run their course. Military doctrine serves at least two important purposes: to prepare a nation’s military forces for conflict and to warn potential foes of the consequences of war.

It should not be surprising that the advent of an open and ubiquitous communications medium like the Internet demands a reassessment of military strategy, tactics, and doctrine. In 2006, a secret Israeli government report argued for a “sea change” in military thinking: the national security paradigm of army versus army was under assault by suicide bombers, Katyusha rockets and computer hackers, none of whom has to have direct ties to government or even be susceptible to political pressure (Fulghum, 2006). In China, the potential impact of computer network operations on the nature of warfare is thought to be strong enough even to have transformed 2,500 years of military wisdom; the Chinese military has almost certainly quit the defensive depth of the Chinese countryside to conquer international cyberspace (Rose, 1999). In Washington, one of the first reports that incoming President Obama found on his desk was “Securing Cyberspace for the 44th Presidency,” which argued that the U.S. must have a credible military presence in cyberspace to act as a deterrent against operations by its adversaries in that domain (Lewis, 2008).

Cyber doctrine must address how military and civilian authorities will collaborate to protect private sector critical information infrastructure. Even cyber attacks that strike purely military sites are likely to traverse civilian networks before reaching their target. In fact, the destruction of civilian infrastructure may be the cyber attacker’s only goal. A further challenge is that private sector enterprises such as banks have been reluctant to disclose successful cyber attacks against them for fear of an impact on their bottom line. This dynamic could make it difficult for national security leadership even to know that an attack on its national territory – in violation of its national sovereignty – has occurred. Thus, proactive cyber attack deterrence by government to defend civilian infrastructure will be difficult to achieve, and any national response may be too little, too late.

The dynamic nature of cyber attacks could ensure that defenders never see the same attack twice. Therefore, decision makers will need a range of diplomatic and military options to consider for a punitive response. In terms of military doctrine, one possibility might be the delineation of red lines in cyberspace. Propaganda and low-level com-

¹⁷ See Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, International Committee of the Red Cross.

¹⁸ This quote is from *The Manual of the Law of Armed Conflict*. Section 2.2 (Military Necessity). United Kingdom: Ministry of Defence. Oxford: OUP. (2004).

puter network exploitation (CNE) may trigger the first line of passive cyber defense, while the manipulation of code in an operational weapons system could be grounds for real-world retaliation. Finally, to support a deterrence strategy, cyber doctrine must be clearly written. An adversary should have no doubt what the consequences will be if the red lines are crossed.

3.3. Punishment: Credibility

As we have seen, the credibility of cyber attack deterrence by denial is low. The political will and even the capability to attempt such a denial are lacking. Therefore, a strategy of cyber attack deterrence by punishment is a more likely scenario.

The trouble with a punishment strategy, however, is that governments are always reluctant to authorize the use of military force (for good reason). Deterrence by punishment is a simple strategy but one that demands a high burden of proof: a serious crime must have been committed, and the culprit positively identified. The challenge of cyber attack attribution, described above, means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion.

But there is another characteristic of cyber attacks that undermines the credibility of deterrence by punishment even more: asymmetry. At the nation-state level, some countries are more dependent upon the Internet than others. Some governments possess sophisticated computer network attack programs while others have none at all. Non-state actors such as a lone hacker or a terrorist group may not possess any computer network or other identifiable infrastructure against which to retaliate.

The asymmetric nature of information technology and cyber warfare manifests itself in countless ways. From a technical perspective, the Smurf attack is a classic example: a hacker sitting at computer X pretends to be coming from computer Y, then requests data from hundreds of other computers at once. Myriad responses easily overwhelm computer Y, creating a denial-of-service condition.¹⁹ From a human perspective, the case of Briton Gary McKinnon is illuminating. According to McKinnon, he is a "bumbling hacker" who was merely looking for UFO data on unsecured Pentagon networks. But the U.S. prosecutor seeking his extradition describes McKinnon's exploits as "the biggest military computer hack of all time" (Lee, 2006).²⁰ In terms of financial damages, 'mafia-boy' – a 15 year-old kid from Montreal – in 2001 was able to deny Internet service to some of the world's biggest online companies, causing an estimated \$1.7 billion in damage (Verton, 2002).

4. Conclusion: Mutually Assured Disruption (MAD)

¹⁹ See CERT Advisory CA-1998-01: Smurf IP Denial-of-Service Attacks.

²⁰ The press have speculated whether one reason for prosecuting McKinnon is for the deterrent effect it could have on other cyber attackers (Glendinning, 2006).

There is a growing relationship between computer security and national security. Military leaders, fearing the potential impact of cyber warfare as well as the start of a cyber arms race, are now considering whether it is possible proactively to deter cyber attacks.

At the nation-state level, there are two possible deterrence strategies: denial and punishment. In cyberspace, both suffer from a lack of credibility. Denial is unlikely due to the ease with which cyber attack technology can be acquired, the immaturity of international legal frameworks, the absence of an inspection regime, and the perception that cyber attacks are not dangerous enough to merit deterrence in the first place. Punishment is the only real option, but this deterrence strategy lacks credibility due to the daunting challenges of cyber attack attribution and asymmetry.

At a minimum, attribution must improve before a cyber attacker may feel deterred. This will take time. In the short term, organizations must improve their ability to collect and transmit digital evidence, especially to international partners; in the long term, national security planners should try to create a Distant Early Warning Line (DEWL) for cyber war, and the capability to select from a range of rapid response tactics.

To pave the way forward, a legal foundation for cyber attack, defense, and deterrence strategies is needed as soon as possible. Because information technology changes so quickly – no one can predict what the next cyber attack will look like – it may be necessary to adopt an effects-based approach. If a cyber attack results in a level of human suffering or economic destruction equivalent to a conventional military attack, then it could be considered an act of war, and it should be subject to the existing laws of war. Therefore, national security planners have no time to waste in reevaluating, and updating if necessary, the Geneva, Hague and Human Rights conventions, Just War theory, and more.

Back to the Cold War. By the year 1968, Soviet mastery of nuclear technology had made one-sided nuclear deterrence meaningless.²¹ The U.S. and the USSR were forced into a position of mutual deterrence, or Mutually Assured Destruction (MAD). Both sides had the ultimate weapon, as well as a second-strike capability. Although cyber attacks do not possess the power of a nuclear explosion, they do pose a serious and increasing threat to international security, and anti-proliferation efforts appear futile. Welcome to the era of Mutually Assured Disruption (Pendall, 2004; Derene, 2009).

References

- Anonymous. (2009, Mar 28). "Thai cybercrime law denounced as 'threat to freedom'." *Bangkok Post* website, Bangkok, Thailand in English. *BBC Monitoring Asia Pacific* (2009, Mar 29).
- Brodie, B. (1946). *THE ABSOLUTE WEAPON: Atomic Power and World Order*. New York: Harcourt, Brace and Co.
- Cole, E. (2002). *Hackers Beware*. London: New Riders.

²¹ Specifically, it was the Soviet Union's ability to mass produce nuclear weapons, and to compete in the nuclear arms race, that changed the strategic equation in 1968.

- Dawson, R. (2003). *Living Networks: Leading Your Company, Customers, and Partners in the Hyper-Connected Economy*. Chapter 7, "The Flow Economy: Opportunities and Risks in the New Convergence." New Jersey: Prentice Hall.
- Derene, G. (2009). "Weapon of Mass Disruption." *Popular Mechanics*, 186(4), 76.
- Fulghum, D. A. & Wall, R. & Butler, A. (2007). "Cyber-Combat's First Shot." *Aviation Week & Space Technology*, 167(21), 28.
- Fulghum, D. A. (2006). "Redefining Victory." *Aviation Week & Space Technology*. 165(10), 58.
- Geers, K. (2009). "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Information Security Journal: A Global Perspective*, 18(1), 1-7.
- Glendinning, L. (2006, May 10). "Briton faces extradition for 'biggest ever military hack'." *Times Online*.
- Goble, P. (1999, Oct 9). "Russia: Analysis from Washington: a Real Battle on the Virtual Front." *Radio Free Europe/Radio Liberty*.
- Graham, B. (1999, Nov 8). "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia." *The Washington Post*. p. A.01.
- Huntley, W. L. (2009). "Abandoning Disarmament? The New Nuclear Nonproliferation Paradigms." In D. Krieger (Ed.) *The Challenge of Abolishing Nuclear Weapons*. New Jersey: Transaction Publishers.
- Jolly, D. (2009, Jul 31). "In French Inquiry, a Glimpse at Corporate Spying." *The New York Times*.
- Keizer, G. (2009, Jan 28). "Russian 'cyber militia' knocks Kyrgyzstan offline." *Computerworld*.
- Lee, M. (2006, May 10). "Who is Gary McKinnon?" *ABC News*.
- Lewis, J. A. (2008, Dec 8). "Securing Cyberspace for the 44th Presidency." *Center for Strategic and International Studies (CSIS)*.
- Markoff, J. & Kramer, A. E. (2009, Jun 27) "U.S. and Russia Differ on a Treaty for Cyberspace." *The New York Times*.
- Milhollin, G. & Lincy, V. (2009, Sep 29). "Lifting Iran's Nuclear Veil." *The New York Times*.
- Mishra, S. (2003). "Network Centric Warfare in the Context of Operation Iraqi Freedom." *Strategic Analysis*, 27(4), pp. 546-562.
- Oberdorfer Nyberg, A. (2004). "Is All Speech Local? Balancing Conflicting Free Speech Principles on the Internet." *Georgetown Law Journal*, 92(3), 663-689.
- Pendall, D. W. (2004). "Effects-Based Operations and the Exercise of National Power." *Military Review*, 84(1), pp. 20-31.
- Rose, A. (1999, Oct 25) "China studies the art of cyber-war." *National Post*. p. A 14.
- Sartori, L. (1983). "The weapons tutorial-Part five: When the bomb falls." *Bulletin of the Atomic Scientists*, 39(6), 40-47.
- Shultz, G. P., Perry, W. J., Kissinger, H. A., & Nunn, S. (2007, Jan 4). "A World Free of Nuclear Weapons." *The Wall Street Journal*.
- Stöcker, C., & Neumann, C., & Dörting, T. (2009, Jun 18). "Iran's Twitter Revolution: Ahmadinejad's Fear of the Internet." *Spiegel*.
- Verton, D. (2002). *The Hacker Diaries: Confessions of Teenage Hackers*. New York: McGraw-Hill/Osborne.