International Journal of Sustainable Development Research
2015; 1(1): 1-6
Published online September 12, 2015 (http://www.sciencepublishinggroup.com/j/ijsdr)
doi: 10.11648/j.ijsdr.20150101.11

Cyberwar-The New Frontier of International Warfare

Bello O. A.[1, *], Aderbigbe F. M.[2]

[1]Department of Computer Science, Adekunle Ajasin University, Akungba Akoko, Ondo State, Nigeria
[2]Department of Mathimatical Science, Ekiti State University, Ado-Ekiti, Ekiti State Nigeria

Email address:
boniyide@gmail.com (Bello O. A.)

To cite this article:
Bello O. A., Aderbigbe F. M.. Cyberwar-The New Frontier of International Warfare. *International Journal of Sustainable Development Research*. Vol. 1, No. 1, 2015, pp. 1-6.doi: 10.11648/j.ijsdr.20150101.11

Abstract: In cyberwar, people use technological means to launch a variety of attacks. Some of these attacks take a very conventional form. Computers can be used, for example, for propaganda, espionage, and vandalism. Denial of service attacks can be used to shut down websites, silencing the enemy and potentially disrupting their government and industry by creating a distraction. Cyberwar can also be utilized to attack equipment and infrastructure, which is a major concern for heavily industrialized nations which rely on electronic systems for many tasks. Using advanced skills, people can potentially get backdoor access to computer systems which hold sensitive data or are used for very sensitive tasks. A skilled cyberwarrior could, for example, interrupt a nation's electrical grid, scramble data about military movements, or attack government computer systems. Stealthier tactics might involve creating systems which can be used to continually gather and transmit classified information directly into the hands of the enemy or using viruses to interrupt government computer systems.

Keywords: Cyberwarfare, Cyberspace, Espionage, Virtual Attacks, Cyberattacks, Propaganda, Denial-of-Service (DoS)

1. Introduction

Cyberwarfare is a form of warfare that occurs in “cyberspace,” which is the abstract location in which Internet websites and databases exist. This is not a physical space in the sense that the servers and other hardware running websites exist in real space, but instead refers to the collective digital information that makes up the Internet. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. Cyberwarfare typically consists of activities over the Internet that represent new forms of attack, while still resembling older military or combat practices. This can include vandalism, espionage, and sabotage to gain information and access to critical computer systems.

Sometimes also referred to as cyber warfare, cyber spying, and cyber terrorism, cyberwarfare can consist of any type of aggressive or malicious action taken against a corporation, private citizen, or government agency that occurs in cyberspace. There are a number of different forms of cyber attacks that can be perpetrated against a person, business, or government and these different attacks typically build on each other toward a single goal. Espionage is a common form of cyberwarfare, often referred to as cyber espionage, and typically consists of attempting to learn secret or private information about a person, business, or government.

Information gained this way can be used in cyber sabotage in a cyberwarfare campaign. For example, a cyber terrorist or cyber soldier could gain access to data regarding pressure controls of a natural gas pipeline. This information could be further used to take over those pressure controls and even override safety systems and cause the pipeline to explode or otherwise shut down. Attacks such as these, in a large enough coordinated effort, could cause serious damage, injury, or otherwise negatively affect operations of a company or country.

While cyberwarfare is a fairly new form of warfare, it is being taken quite seriously by many corporations and countries across the world. Security concerns for governments and businesses have increasingly revolved around cyber attacks, and many nations are moving toward something of a cyber arms race to amass computer experts to defend against and launch cyber attacks. Many military officials consider cyber attacks to be of great importance, and future military campaigns will likely include cyberspace as well as land, sea, air, and space operations.

As the world becomes more networked, more crucial systems become susceptible to attacks in cyberspace. Although certain military systems remain accessible only by being present at a terminal on site, the vast majority of critical systems that control modern nations are now tied into

the Internet in some way or another. While these systems are defended by high levels of security, they are nonetheless breakable, and cyber warfare concerns itself with finding weaknesses and exploiting them. In the USA,critical infrastructure protection became a veritable watchword in local and national security policy circles, even before the 9/11 terrorist attack and the establishment of the Department of Homeland Security. The success of the 9/11 conspiracy has been attributed in part to a "failure of imagination" on the part of the U.S. defense and intelligence community. This, in turn, has spawned reactive, "worst case" predictions, along the lines that, "the attack the experts say cannot happen or that terrorists are not interested in pursuing is simply an attack that hasn't happened yet.

In February 2010, top American lawmakers warned that the "threat of a crippling attack on telecommunications and computer networks was sharply on the rise." According to The Lipman Report, numerous key sectors of the U.S. economy along with that of other nations, are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are now dependent on computers for daily operations. There are three major sectors targeted by most nations involved in cyber warfare: financial, infrastructure, and governmental. Financial attacks could disrupt the world's major markets by taking down electronically-controlled commodity exchanges, or by shutting down web-based operations of major banks or retailers. Infrastructure attacks can damage a nation by shutting down critical utility systems, such as electrical grids, or by wrecking havoc on others, such as opening dams, or interfering with the air traffic control system. Governmental attacks can shut down the ability of government officials to communicate with one another, steal secret digital communications, or release things like tax information, social security information, or other personal data to the public.

In 2009 a report was released showing that the United States electrical grid was incredibly susceptible to attacks in cyberspace which could cripple the nation by shutting off electricity to hundreds of millions of people. The report claimed that the grid had already been breached by both Russia and China, both of whom had left behind software that could be activated remotely to control the system. Although such an attack has not yet happened anywhere in the world, if combined with a conventional military attack it could prove catastrophic.

Many critical military systems are also susceptible to virtual attacks. Satellite systems, for example, although protected by extensive security, have been breached on occasion. If an enemy were to take control of spy satellites or satellites which feed GPS data to aircraft and missiles, it could be a major blow to the military.

In recent years, it has become apparent that the major military nations of the world are each devoting large amounts of energy and money to cyber warfare. China has received the most press for its programs, but reports have also surfaced about the programs of both the United States and Russia as well. Although these attacks have, for the most part, been benevolent, they are laying the groundwork for future wars which could be waged predominantly through the use of communications technology.

Seasoned observers, such as military analyst Anthony H. Cordesman writing on cyber warfare and related matters, pointed out the need for calm reflection and accurate calibration of the problem before allocating scarce tax dollars to critical infrastructure protection. With respect to cyber warfare, Cordesman observed in December 2000:

"There is a flood of uncertain and poorly defined data on the threat, much of which is highly anecdotal. Incidents tend to be exaggerated while the overall pattern in the threat may be understated or missed altogether. Cost and risk estimates are issues that are little more than guesstimates, often using ridiculous methods and data. There is a critical lack of technological net assessment of the trends in offense and defense…"

There exists the possibility that foreign nation-states—not only the U.S.—could mount and

finance a well-organized cyber warfare program. This would allow them to utilize a cyber attack

capability against an adversary. A multi-faceted cyber attack employing various techniques could

be highly disruptive if the United States and its allies were unprepared for it. A cyber attack by nation-states targeting the transportation, communications, or banking sector computer systems in the United States would, at a minimum, entail significant economic costs and its effect will go beyond the level of temporary nuisance to inflict sustained uncertainty, confusion, and even chaos across significant elements of the population. In the most extreme of cases, these disruptions could cause human casualties.

Cyber attacks occur on a frequent basis and in a near-instantaneous manner; as the world becomes more connected, more machines and more people will be affected by an attack. In the months and years to come, cyber attack techniques will evolve even further, exposing various— and possibly critical—vulnerabilities that have not yet been identified by computer security experts. Moreover, such attacks could also be coordinated to coincide with physical assaults, in order to maximize the impact of both.

2. Recent Developments

During the past five years, the world has witnessed an escalation in the number of cyber attacks involving hackers attacking and counterattacking in the context of regional or local disputes. When peacekeeping operations began in Kosovo, NATO and Serbian hackers attacked back and forth attempting to control each other's electronic resources. The same has occurred during the Palestinian-Israeli conflict, the India-Pakistan disagreement over Kashmir, and between Chinese and American hackers during the accidental bombing of the Chinese Embassy in Belgrade in 1999 and the May 2001 downed spy-plane incident. A cyber war

between Chechen and Russian hackers has also taken place during the conflict between the Russian military and Chechen fighters. These cyber wars coincided with actual physical conflicts but intrusions, in one form or another, also have taken place in isolation. In recent years, the scope and sophistication of cyber attacks have also expanded. Whereas antecedent attacks were relatively benign, more recent intrusions have compromised vital communications and critical infrastructure systems, such as public utilities connected to the Net.

The Slammer worm, for example, exploited a vulnerability in Microsoft's SQL database software that led to cascading effects in electronic infrastructure that were certainly not predicted beforehand. Airline booking systems and bank Automated Teller Machines (ATMs) were among other systems impacted by Slammer infections. The Slammer worm also significantly degraded computer systems that control monitoring capabilities at the Davis-Besse nuclear power plant in Ohio.

3. Why Cyber Warefare

Although cyberwarfare will probably not displace traditional,kinetic warfare, it will become an increasingly important weapon in the arsenals of nation-states for several reasons. First, developing the capacity to wage cyberwar costs little compared to the cost of developing and maintaining the capacity to wage twenty-first century kinetic war. The expense of cyberwarfare primarily encompasses training and paying cyberwarriors, and purchasing and maintaining the hardware and software needed to launch and counter cyberattacks, because nations will wage cyberwarfare primarily over publicly accessible networks. Second, cyberwarfare provides an appealing option for nations because of the relative conservation of human and non-human resources. While cyberattacks are likely to generate human casualties and property destruction, cyberattacks will inflict far less damage than kinetic attacks. This conservation of resources erodes has the added advantage of insulating cyberwarriors from physical injury: unlike their counterparts in traditional military organizations, cyberwarriors operate remotely and launch cyberattacks from within the territory of their own nation-state. The remoteness of cyberwarfare effectively eliminates the likelihood of injury or death in a physical encounter with forces from an opposing nation-state. Therefore, a nation-state needs only a relatively small cadre of cyberwarriors to wage cyberwarfare, and it can assume that few, if any, of those warriors will be lost in the conflict. Third, nation-states are likely to find cyberwarfare attractive because the sponsoring nation-state may be able to disguise the source of the attacks and thereby avoid responsibility. Even if Nation A suspects Nation B launched the cyberattacks that targeted its infrastructure, Nation A probably will not (and under the existing laws of war cannot lawfully) retaliate against Nation B unless and until it confirms that suspicion. For these and other reasons, nation-states will be forced to deal with the phenomenon of cyberwarfare in the years and decades to come. Cyberwarfare is a new phenomenon that differs in a number of respects from traditional warfare, and these differences raise legal, policy, and practical issues that nation-states will have to resolve,both individually and collectively.Some of these issues includes:

3.1. 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.1 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.

3.2. 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.

3.3. 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, and, in the case of state-sponsored computer network operations, law enforcement cooperation will be either Potemkin or non-existent.

3.4. 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 faces the prospect of losing a cyber conflict without ever knowing the identity of their adversary.

3.5. 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.

3.6. Low Entry Cost

For the price of a computer and connection to the Internet anyone can conduct cyber warfare operations. A variety of cyber warfare tools are openly available on a multitude of Internet sites worldwide. Consequently, the potential number of organizations capable of conducting cyber warfare is incalculable.

3.7. Blurred Traditional Boundaries

Cyber warfare creates its own fog of war. Given the infinite number of potential threat to organizations, the number of different cyber attack tools and the interconnectivity of the World Wide Web, it becomes increasingly difficult to determine between foreign and domestic sources of cyber warfare. This creates a cyber response dilemma. If you don't know who is attacking you, how do you respond to the incident? . The use of third parties by adversaries to conduct cyber warfare attacks can further complicate this issue.

3.8. Expanded Role for Perception Management

Our adversaries now have the ability to effortlessly manipulate public perception by digitally manufacturing information or altering multimedia files. The cyber world never sleeps—it is available 24 hours a day. Perception management requires an equal amount of counter-perception management. This effort consumes valuable resources. Counter-perception management may detract from the original mission or may cause the mission to be canceled outright if the efforts are not successful. For example,American participation in Somalia Operations from 1992-1994 was a case in point. The Clinton administration's efforts were doomed when it could not counteract the negative domestic perceptions caused by photos showing a dead American service member being dragged through the city streets of Mogadishu.

3.9. Lack of Strategic Intelligence

Traditional intelligence gathering methods and subsequent analytic techniques are outdated. Current intelligence and law enforcement organizations are not prepared for cyber warfare intelligence gathering. The blurring of traditional boundaries is a factor in this issue. Who, legally, collects what intelligence on whom?

3.10. Difficulty of Tactical Warning and Attack Assessment

As a result of the ease and availability of cyber warfare tools and the fact that anyone can potentially launch a cyber attack, there is little to differentiate the "thrill-seeker" attack from the nation-state attack. Consequently, a country may not know when an attack is underway, how the attack is being conducted, or by whom. The anonymous nature of cyberspace can be pierced over time but the initial cyber assault favors the attacker.

4. Types of Cyberwarfare

4.1. Espionage

Increasingly, governments around the world complain publicly of cyber espionage. 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. Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world. Specific attacks on the United States have been given codenames like Titan Rain and Moonlight Maze. General Alexander notes that the recently established Cyber Command is currently trying to determine whether such activities as commercial espionage or theft of intellectual property are criminal activities or actual "breaches of national security."

4.2. 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.

4.3. 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.

4.4. 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.

4.5. 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. Also, it is important to note that almost all critical infrastructures are in private hands.

5. Conclusion

Cyber-warfare is different from conventional, kinetic warfare. Both it and its parent, information warfare, depend upon the frailties of human beings for many characteristics. One of the fundamental differences between cyber-warfare and kinetic warfare is the nature of their environments. Kinetic warfare takes place in the physical world, governed by physical laws that we know and understand. Cyber-warfare takes place in an artificial, man-made world that is chaotic with imperfections. Cyber-warfare can use some of the principles of kinetic warfare, but there are other principles that have little or no meaning in cyberspace. For these reasons, the principles of cyber-warfare are, ultimately, different from those of kinetic warfare.

References

[1] DOD – Cyberspace. Dtic.mil. Retrieved 8 November 2011.

[2] Richard Clarke, *Cyber War* (New York: Harper-Collins, 2010), p. 6.

[3] Markoff, “A Code for Chaos”; "Cyberwar: War in the Fifth Domain" *Economist*, 1 July 2010.

[4] The Lipman Report, 15 October 2010.

[5] "Malware Hits Computerized Industrial Equipment" *New York Times*, 24 September 2010.

[6] Reuters: US concerned power grid vulnerable to cyber-attack. In.reuters.com (9 April 2009).

[7] Gorman, Siobhan. (8 April 2009) Electricity Grid in U.S. Penetrated By Spies. Online.wsj.com.

[8] "Clarke: More defense needed in cyberspace" *HometownAnnapolis.com*, 24 September 2010.

[9] Shiels, Maggie. (9 April 2009) BBC: Spies 'infiltrate US power grid'. BBC News.

[10] AFP: Stuxnet worm brings cyber warfare out of virtual world. Google.com (1 October 2010).

[11] Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon | Video on. Ted.com.

[12] "War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?". *The Economist*. 1 July 2010. http://www.economist.com/node/16478792.

[13] Tom Gjelten (23 September 2010). "Seeing The Internet As An 'Information Weapon'". *National Public Radio*. http://www.npr.org/templates/story/story.php?storyId=130052701

[14] Arquilla, John, and David Ronfield. *Networks and Netwars*. Santa Monica, CA: Rand Corporation, 2001.

[15] Bush, George W.. *The President’s Commission on Critical Infrastructure Protection, The National Strategy to Secure Cyberspace* . Washington D.C.: The White House September 2002.

[16] Cater, Ashton. *The Architecture of Government in the Face of Terrorism* . International Security, vol. 26.

[17] Cordesman, Anthony. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction* . New York, NY: Praeger Publishers Inc., 2002.

[18] Cordesman, Anthony. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection* . New NY: Praeger Publications Inc., 2002.

[19] Ford, Warwick, and Michael S. Baum. *Secure Electronic Commerce*. Upper Saddle River, NJ: Prentice-Hall Inc., 2001.

[20] Garfinkel, Simson. *Web Security, Privacy, and Commerce*. Sebastopol, CA: O’Reilly & Associates, Inc., 2002.

[21] Green, Joshua, (2002). The Myth of Cyber Terrorism. http://www.washingtonmonthly.com/features/2000/0211.green.html.

[22] Hoffman, Bruce. *Inside Terrorism* . New York, NY: Columbia University Press, 1998.

[23] Huntington, Samuel P.. *The clash of civilizations and the remaking of world order*. New York, NY: Simon & Schuster Inc., 1996.

[24] Institute for Security Technology Studies. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Darmouth College, 2001.

[25] Institute for Security Technology Studies. Combating Terrorism: *A Compendium of Recent Counterterrorism Recommendations from Authoritative Commissions and Subject Matter Experts*. Darmouth College, 2001.

[26] Kusher, Harvey. *The Future of Terrorism: Violence in the new millennium* . London, U.K.: Sage Publications Inc., 1998.

[27] Laquer, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford, U.K.,1999.

[28] Lesser, Ian, Bruce Hoffman, John Arquilla and Michelle Zanini. *Countering the New Terrorism* . Santa Monica, CA: Rand Corporation,1994.

[29] Molander, Rodger C., Andrew S. Riddile and Peter A. Wilson. *Strategic Information Warfare. A new face of war*. Santa Monica, CA: Rand Corporation, 1996.

[30] Nelson, Bill, Major, Major Rodney Choi, Major Michael Iacobucci, Major Mark Mitchell, and Captain Greg Gagnon. *Cyberterror, Prospects and Implications*.

[31] Monterey, CA: Center for the Study of Terrorism and Irregular Warfare. Naval Post Graduate School. 1999.

[32] Parks, Raymond C. and David P. Duggan. *Principles of Cyber-Warfare*. Proceedings of the 2001 IEEE workshop on Information and Security.

[33] Pillar, Paul. *Terrorism and U.S. Foreign Policy*. Washington, DC: Brookings Institution Press. 2001.

[34] Thomas, Douglas and Brian D. Loader. *Cybercrime, Law enforcement, security and surveillance in the information age*. New York, NY: Routledge Inc., 2000.

[35] Sofaear, Abraham D. and , Seymour E. Goodman. *The Transnational dimension of cyber crime and terrorism* . Stanford, CA: Hoover Institution Press. 2001.

[36] U.S. Joint Chief of Staff. *Joint Doctrine for Information Operations*. Joint Publication 3-13. Washington, D.C.: Joint Chief of Staff, 9 October 1998.

[37] Wall, David S. *Crime and the Internet*. New York, NY: Routledge Inc., 2001.

[38] ITU Toolkit for Cybercrime Legislation, p. 12, www.itu.int/cybersecurity.

[39] The United States Army's *Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010, p. 6.

[40] Cabinet Office, **"**Cyber Security Strategy of the United Kingdom" (Safety, Security and Resilience in Cyber Space), June 2009, p. 7.

[41] Federal Ministry of the Interior, "The New Cyber Security Strategy for Germany," Berlin, February 2011, p. 14.

[42] Sebastian M. Convertino II, Lou Anne De Mattei, Tammy M. Knierim, *Flying and Fighting in Cyberspace* (Alabama: Air University Press, July 2007).

[43] Amos Granit, *Cyberspace as a Military Domain – In What Sense?* Institute for Intelligence Studies at IDF Military Intelligence, March 2010.

[44] "RSA Computerization Infrastructures Breached; Risk to Customer Information Security," *The Marker*, March 19, 2011.

[45] U.S. Department of Defense, Office of the Assistant Secretary of Defense**,**"Remarks on Cyber at the RSA Conference," as delivered by William J. Lynn, III, San Francisco, California, February 15, 2011 [hereafter: Lynn, February 15,2011]. http://www.defense.gov/speeches/speech.aspx?speechid=1535.

[46] John Markoff, "A Code for Chaos," *New York Times*, October 2, 2010, based on Thomas C. Reed, a former secretary of the Air Force, in his book *At the Abyss: An Insider's History of the Cold War* (New York: Ballantine Books, 2004).

[47] Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009.

[48] Yitzhak Ben-Horin, "War on the Web: Fictitious Bloggers Serving the US," *Ynet*, March 18, 2011.

[49] Anshel Pfeffer, "Weapon against Oppression: Plane for Internet Connection," *Haaretz*, February 9, 2011.

[50] William J. Lynn, "The Pentagon Cyber Strategy," *Foreign Relations*, August 2010.

[51] Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1(February 6-13, 2012).

[52] Yaniv Leviatan, "This is how we Fought with Computers, about Computers, and through Computers in the Last Decade," *Maariv Online*, December 31, 2009.

[53] "The NATO Cyber War Agreement," *Strategy Page* (www.strategypage.com),May 1, 2010.

[54] U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign.

[55] Matan Mittelman, "Another Step in Exposing the Mystery Surrounding Stuxnet," *The Marker*, November 16, 2010.

[56] "Ahmadinejad Admits: Virus Damages Nuclear Computers," *Walla,* November 29, 2010.

[57] Yossi Hatoni, "The War for the Atom," *People and Computers* website, September 26, 2010.

[58] "Iran Accuses: Israel and the United States Created the Stuxnet Computer Worm," *Haaretz Online*, April 16, 2011.

[59] *International Strategy for Cyberspace,* The White House, May 2011. See http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[60] Allied Command Operations (ACO), "NATO's 'Cyber Coalition' Exercise a Collaboration in Cyber Defence," www.aco.nato.int, November 18, 2010.

[61] *Spacewar*, "US: NATO Networks Vulnerable to Cyber Threat," www.spacewar.com, January 25, 2011.

[62] "DOD Report Cyber Attacks Could Elicit Military Response," November 16, 2011,http://www.infosecisland.com/blogview/18218-DoD-Report-Cyber-Attacks-Could-Elicit-Military-

[63] Yossi Hatoni, "The United States: The Pentagon to Establish Headquarters for Online Warfare against Terrorism and Crime," *People and Computers* website, June 24, 2009.

[64] TEHILA website, www.tehila.gov.il.

[65] Israel Government Information Security website, www.cert.gov.il.

[66] General Security Service (Shabak) website, www.shabak.gov.il.

[67] Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," *Military and Strategic Affairs* 3, no. 1 (2011): 96, at http://www.inss.org.il/upload/(FILE)1308129638.pdf.

[68] Amir Oren, "IDF's New Fighting Arena – in Computer Networks," *Haaretz*, January 2, 2010.