© ISTOCK

Dimensions of Cyber-Attacks

Social, Political, Economic, and Cultural

ROBIN GANDHI, ANUP SHARMA, WILLIAM MAHONEY, WILLIAM SOUSAN, QIUMING ZHU, AND PHILLIP LAPLANTE

Digital Object Identifier 10.1109/MTS.2011.940293
Date of publication: 8 March 2011

Essential systems providing water, electricity, healthcare, finance, food, and transportation are now increasingly software dependent, distributed, and interconnected. The detrimental consequences of this growing dependence become apparent during times of political conflict, social instability, and other traumatic events. The Internet has made information exchange easier and more efficient, but it has also created a new space in which criminals and terrorists can operate almost undetected. No longer is modern human conflict confined to the physical world; it has spread to cyberspace.

Cyberspace is a massive socio-technical system of systems [25], with a significant component being the humans involved. Current anomaly detection models focus primarily on analyzing network traffic to prevent malicious activities [13], [24], [27], [35], but it has been shown that such approaches fail to account for human behaviors behind the anomalies. Evidence is growing that more cyber-attacks are associated with social, political, economic, and cultural (SPEC) conflicts [34], [39], [42]. It is also now known that cyber-attackers' level of socio-technological sophistication, their backgrounds, and their motivations, are essential components to predicting, preventing, and tracing cyber-attacks [28], [36]. Thus, SPEC factors have the potential to be early predictors for outbreaks of anomalous activities, hostile attacks, and other security breaches in cyberspace.

We believe analyzing potential correlations between historical/current SPEC events and cyber-attacks may provide valuable insights regarding the origin, agents, means, motives, and potential targets of future cyber-attacks. Towards this goal, we describe how several SPEC events have led to cyber-attacks, and then present a taxonomy and analysis of these attacks along the SPEC dimensions. We do not attempt to analyze why past SPEC events have triggered cyber-attacks, nor do we propose solutions to reduce or prevent them.

Categorical Record of Cases

Cyber-attacks cover a wide range of actions, including defacing a website and stealing valuable information. Howard [21] defines a cyber-attack as an "event that occurs on a computer or network that is intended to result in something that is not authorized to happen." Such attacks can affect data, processing, and programs, and the network environment [17]. We define a cyber-attack as any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation.

To thoroughly understand a cyber-attack, we study the nature of the attack and the motivation behind it. Some attacks are due to political conflict, while others are triggered by social tension. Some attacks occur because of religious belief and extremism and others are the result of revenge and anger. In the following we summarize some of the typical SPEC-related cyber-attacks in a few of these categories. The discussed events are by no means exhaustive, as it will be impossible to enumerate them all; our selection is only meant to highlight the types of attacks that can occur.

Politically Motivated Attacks

Cyber criminals involved in politically motivated attacks can be members of extremist groups who use cyberspace to spread propaganda, attack websites and networks of their political enemies, steal money to fund their activities, or plan and coordinate physical-world crime [10]. Based on the nature of an attack, politically motivated attacks can be further subdivided as: protests against political actions, protests against laws or public documents, and outrage against acts related to physical violence.

Protesting Political/ Government Actions

June 1998, India, attack on an atomic research center – Hackers from the United States, England, the Netherlands, and New Zealand (calling themselves "Milworm") attacked the website of India's Bhabha Atomic Research Center (BARC) to protest nuclear testing. The attackers posted text to the web site and destroyed data [4].

September 1998, Indonesia, attack on websites to protest against human right abuse in East Timor – Portuguese hackers modified the websites from 40 Indonesian servers to protest against human right abuses in East Timor. The hackers posted the slogan "Free East Timor" on the websites [4].

October 1998, Mexico, the website of president attacked – The website of Mexican president Ernesto Zedillo was attacked to demonstrate against colonization, genocide, and racism throughout the world [32].

June 1999, Cologne, Germany, cyber-attack to protest against the G8 summit – Hackers from Indonesia, Israel, Germany, and Canada reportedly launched 10 000 cyber-attacks over five hours on various companies protesting the G8 meeting in Cologne. The attackers intended to disrupt financial centers, banking districts, and multinational corporate power bases [4].

1999, Serbia, Kosovo war – Serbian hackers attacked U.S. and NATO sites using a "fraggle attack" (when large numbers of packets are sent to paralyze a system) [10]. The attackers disrupted services on several government computers and websites to object to NATO and Yugoslav aggression [4]. The hackers also used cyberspace to share text, images, and video clips to reach an international audience.

December 2008, Beijing, website of French Embassy attacked – The

French embassy website came under attack by Chinese hackers immediately after the meeting of French President Nicolas Sarkozy with the Dalai Lama [18].

Dissatisfaction with the Launch of a Public Document, Policy, or Law

December 1995, France, cyber-attack against French Government websites – A group called the "Strano Network" launched an hour-long Net strike attack against government web sites to protest the French Government's nuclear and social policy. Attack organizers encouraged protestors to point their browsers at the government website, which generated a high volume of web traffic and rendered it unavailable for other users [4].

1996, U.S., attack on a Department of Justice (DOJ) website – When the Communications Decency Act was passed several protestors were involved in deleting the contents from the U.S. DOJ website [10].

March 2001, South Korea/Japan, attack on Japanese Education Ministry's website – South Korean hackers attacked the Japanese Education Ministry's website to protest the publication of controversial history textbooks, which they felt did not fairly address past Japanese military aggression. All of these hackers were later identified as university students [7].

Outrage against Acts Related to Physical Violence

May 1999, Belgrade, Chinese Embassy bombing – Chinese hackers attacked U.S. government sites for accidentally bombing the Chinese embassy in Belgrade. A Chinese slogan "down with barbarians" was placed in the home page of the U.S. Embassy in Beijing, and the Department of Interior web site showed images of three journalists killed during the bombing [4].

August 1999, China/Taiwan, cyber conflict – The political conflicts between China and Taiwan led to cyber warfare. Chinese hackers took several Taiwanese and government websites under their control, placing inflammatory messages. Taiwanese hackers placed an anti-communist message on a Chinese high-tech internet site [4].

> To thoroughly understand a cyber-attack, we study the nature of the attack and the motivation behind it.

November 2000, Israel/Palestine, cyber-attack on Lucent Technology, – Lucent Technology, a company doing business with Israel, was targeted by a Palestinian group called Unity [10]. In the fall of 2000, cyber warfare between pro-Israeli and pro-Palestinian groups resulted in a server crash that caused the Israeli stock market to decline by 8% [26].

April 2001, U.S./China, spy plane crisis – Immediately following the crash of a U.S. spy plane, numerous website defacing incidents were reported in the U.S. and China. From April 28 to May 8, Chinese "hactivists" defaced almost 1000 U.S. websites and launched a distributed denial-of-service (DDoS) attack against the White House and the Central Intelligence Agency [15]. These attacks on the U.S. government's websites were highly sophisticated and bold. Three hactivist groups – the Hacker Union of China, China Eagle, and the Green Army Corps – were suspected of having launched these attacks [10], [46].

August 2001, China/Japan, Yasukuni shrine conflict – Chinese hackers routinely attacked the websites and Internet Services in Japan. An attack was also launched on the homepage of Yasukuni Shrine, which is dedicated to Japanese war dead and is a constant source of friction between these two countries [19].

April 2007, Estonia/Russia, DoS Attack – World War II monument conflict – A botnet attack was launched upon the Estonian Government and commercial websites by Russian hackers causing a DoS [10]. About one million computers worldwide were used to conduct the attack on the government and corporate websites [14]. Over three weeks these attacks shut down Estonia's cyber infrastructure. The Estonian government blamed Russian hackers for this attack; the Russian government denied involvement. Security experts speculated that the hackers were protesting the Estonian government's decision to move a popular monument [14].

Socio-Cultural Conflict Triggered Attacks

Socio-cultural conflict can be viewed as competition between individuals or groups over incompatible goals, scarce resources, or power, including the denial of control to others [5]. Cross-cultural conflict can also manifest as ethnic conflict. Cyber conflicts incited for cultural reasons include conflicts between Taiwan-China (August 1999), Russia-Estonia (2007) and Russia-Georgia (2008). Similarly, The Israel-Palestine cyber conflict, where national symbols – the Israeli flag, Hebrew text, and a recording of the Israeli national anthem – were put into Hezbollah home page [23], belongs in this category.

Land Dispute Triggered Attacks

2000, India/Pakistan, attack on Indian websites to protest conflict in Kashmir – Pakistani hackers – the Muslim online Syndicate (MOS) – attacked more than 500 websites in India to protest against the conflict in Kashmir [4].

March 2005, Indonesia/Malaysia, Ambalat conflict – Indonesia

and Malaysia dispute ownership of Ambalat and East Ambalat, leading to military posturing and attacks on government websites. Attacks escalated dramatically against Malaysian government's website during the weeks of increased tension over the Ambalat issue [46].

March 2005, Korea/Japan, 'Dokdo/Takeshima' territorial conflict – The dispute over the Dokdo and Takeshima islets, claimed by Japan but controlled by South Korea, caused an outbreak of cyber warfare. The homepage of the Japanese Foreign Ministry came under attack, making access to the site erratic. Japanese hactivists retaliated by attacking the homepage of South Korea's Ministry of Foreign Affairs and Trade. The attack prompted South Korea's government to issue a cyberterrorism warning for all its overseas diplomatic missions [9], [46].

August 2008, Russia/Georgia, conflict resulting in cyber-attacks – The outbreak of the Russia-Georgia war over land disputes spilled into cyberspace; Russian Internet forums were used for a coordinated cyber-attack against Georgia's Internet infrastructure. This incident reveals an emerging trend of cyber activity as a new dimension to conventional war [11].

December 2008, Israel/Palestine conflict – Since the start of the Gaza campaign, hacking groups from Morocco, Lebanon, Turkey and Iran have attacked Israeli websites; a Moroccan Islamic group hacked into the registration system server of "domainthenet.com" and defaced more than 300 websites including banks, weather channels, and news. While trying to access these sites, visitors were rerouted to a website featuring images of casualties from the Israeli offense against Gaza, and anti-Israeli anti-U.S. messages. Israeli students retaliated by attacking Hamas websites [3].

Specific Anniversaries or Historic Events Triggered Attacks

April 1999 CIH/Chernobyl – The CIH/Chernobyl, a timed virus, was spread over the Internet, causing great damage to business and home computer users. These specific viruses activated on a predefined date on the anniversary of Chernobyl nuclear disaster [10], and overwrote a portion of the hard drive Symantec reported that as many as one million Korean computers were affected, resulting in more than $250 million in damages [44].

April 2008, Belarus/Eastern Europe, DoS attack – Radio Free Europe/Radio Liberty in Belarus reported that their websites came under a sustained DDoS attack. These attacks coincided with the anniversary of Chernobyl disaster and the 2007 cyber-attack against Estonia [2].

April 1, 2009, April fool's day, Conficker worm – Widespread panic surrounded the discovery of the Conficker worm, also known as "Downadup", "Kido", and "Confick" [1]. The worm, a variant of "win32/d", would trigger on April 1. As of this writing no such issues have been reported.

Economically Motivated Attacks

Economic situations and personal or corporate financial greed often provide motives for cyber-attacks. Cyber mercenaries and organized cartels also operate in cyber space.

2008-2009, China, IT Professionals attracted towards cybercrime

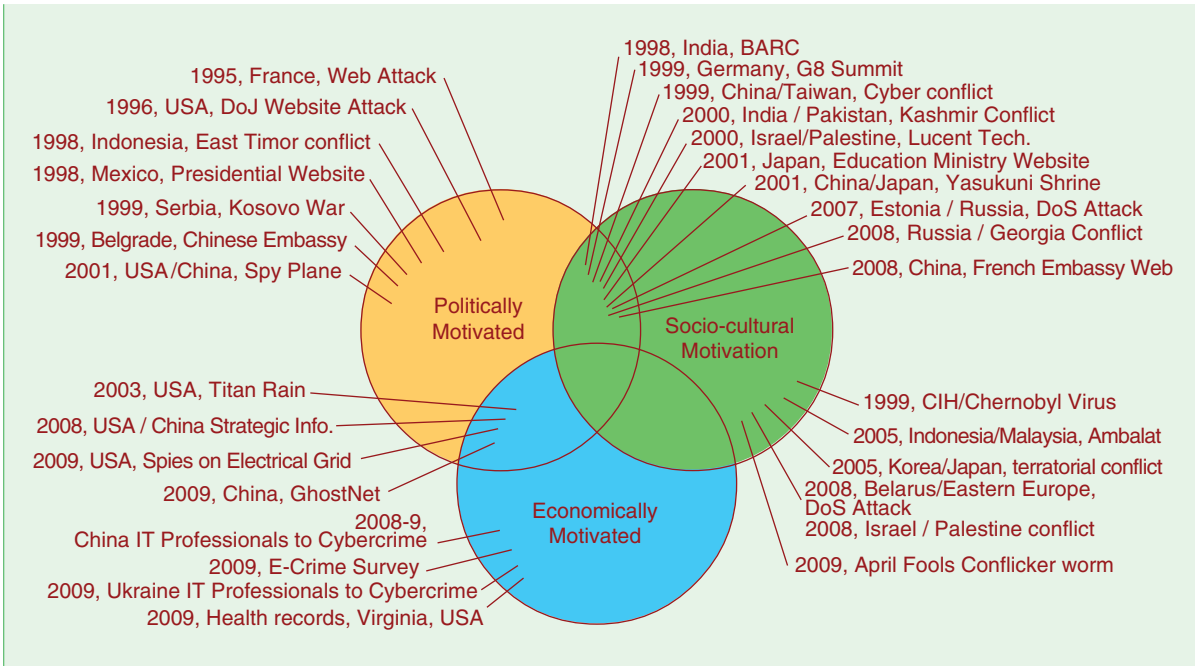


Fig. 1. The distribution of cyber-attacks across CSEP dimensions.

due to economic recessions – The Economic slowdown has affected many countries. Many IT professionals lost significant amounts of money in the stock market, particularly in China, where some IT professionals are turning to cybercrime [29].

2009, Ukraine, IT professionals in cybercrime – Some IT professionals employ cybercrime because it pays. For example, Ukrainian cyber criminals were able to steal $172,000 in goods and services over a 16-day period [31].

2009, Health records held hostage for ransom, Virginia, U.S. – Vulnerabilities in the website of the Virginia Department of Health Professions were exploited by hackers to gain access to eight million patient records. The hackers encrypted the records in the database and later deleted the plaintext copy. A ten million dollar ransom was demanded for the password to decrypt the data [22].

Espionage (Political/ Economic) Related Attacks

September 2003, U.S., Titan Rain cyber espionage issue – In an incident code-named Titan Rain, hackers penetrated NASA and other networks, and retrieved aviation specifications and flight-planning software [23], [38].

2008, U.S./China, Government trying to steal strategic information – The U.S. and Chinese governments exchanged accusations of launching hacking campaigns aimed at stealing strategic information [20].

2009, China, GhostNet – Researchers uncovered a cyber-espionage network named GhostNet, suspected of being used by the Chinese Government to extract information from the Dalai Lama's computer. The investigation led to the discovery of infected machines in Britain, U.S., Indonesia, Iran, the Philippines, and Laos [8].

2009, U.S., Spies on electricity grid – U.S. national security officials claimed that cyber spies from China and Russia penetrated the U.S. electrical grid, searching for vulnerabilities and leaving behind malware. These allegations were not confirmed [16].

Visualizing Cyber-Attacks

We organized the cases discussed above as a Venn diagram (Fig. 1). While these cases are by no means complete or representative of their subsets, our analysis demonstrates the kinds of insights that could be gained from a more comprehensive record. In Fig. 1 note the large number of cyber-attacks identified as politically and socially motivated; these types of attacks have been occurring for some time. Conversely, there is a relative dearth of attacks motivated principally by economics; such attacks seem to be a relatively recent phenomenon. Attacks classified as purely political (without socio-cultural or economic motives) in nature seem to be diminishing or are less publicized, with the most recent high-profile event reported in 2001.

Another way to gain insights into the attacks is via a world map (Fig. 2). Note the *lack* of attacks in some regions, such as Australia and South America with a relatively stable political and cultural environment. This observation seems to reinforce the notion that attacks are strongly positively correlated to political and cultural conflicts. In the case of Africa, a poor computer infrastructure could account for the lack of attacks.

Fig. 3 presents a timeline of the cyber-attacks previously described. Inspection of the figure reveals that over time the types of attacks have been changing. Early

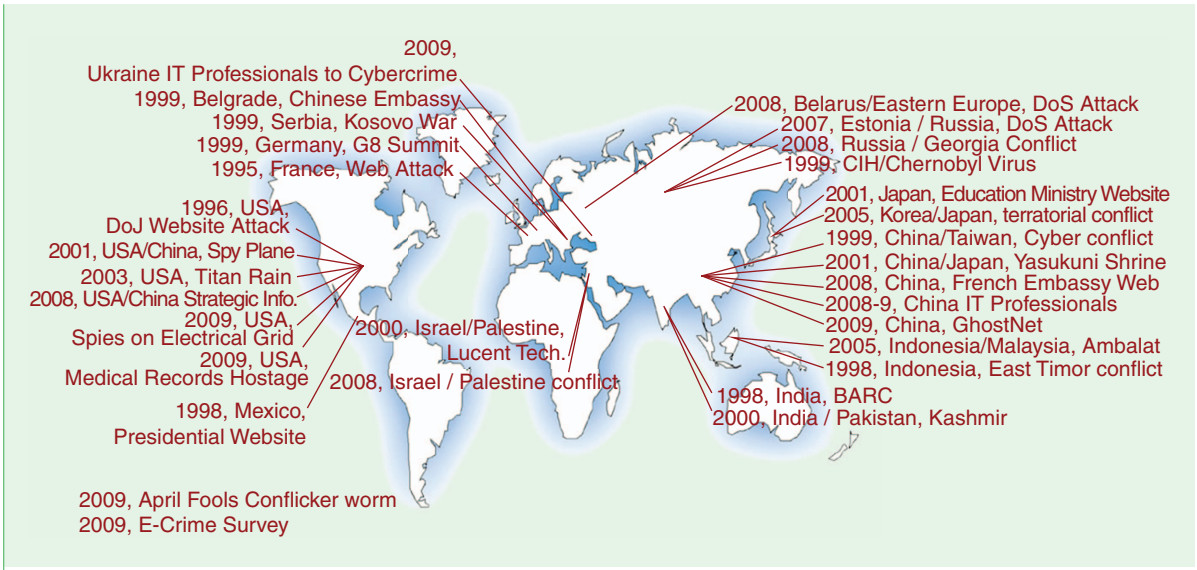


Fig. 2. Country-wise distribution of Cyber-attacks from CSEP dimensions.

cyber-attacks tended to be against web sites, such as the French government and East Timor attacks. This trend may be caused in part by the lack of security in earlier versions of web infrastructure software, providing easy targets for individuals and small groups. More recent attacks are different. These are frequently DDoS attacks, involving a sophisticated group taking over large numbers of computers ("bots") to attack political adversaries. Examples include the Russia/Georgia conflict and the Estonia DoS attack. Other recent attacks involve stealthy, targeted, and sophisticated attacks; for example the Chinese infiltration of the U.S. electrical grid.

Insights from the Record

Our record of historic cases clearly demonstrates that over time more cyber-attacks can be directly attributed to some form of SPEC events. Furthermore, the origination of active malware content has shown to vary significantly across different countries and geophysical regions, and in some instances is largely disproportionate to the number of Internet users [30].

Interesting questions for information security research arise. Can the awareness of SPEC dimensions across geographical borders facilitate early detection and prevention of attacks on cyber systems? Are SPEC factors correlated with the efficient and sustainable operations of a cyber system? Can future anomalous activities in cyberspace be predicted based on SPEC events? Which SPEC factors can serve as strong predictors of an impending cyber-attack, the means that will be used to carry it out, and the potential targets?

Answers to these questions will require organizing SPEC factors into an integrated model of trustworthy cyber system operations. Such a study reaches beyond the traditional transmission or network models of cyber security [29] and provides a more holistic perspective that also spans "human networks" across international borders and cultures.

Below we give some insights gained from analyzing the record of cases. Our analysis has helped identify and categorize several dimensions of a cyber-attack (Fig. 4). Appropriate metrics for defining and modeling cyber-attacks in the SPEC dimensions need to be developed, and we hope that our analysis will provide new insights in that direction.

Attack Dimensions

Attack Agents

While the direct participants (attackers and victims) in a cyber-attack are computer systems, behind each attack is a human agent with a motivation. The attacker type is a fundamental component in the cyber-attack dimension, as these human agents are the first transition point between events in the physical world and events in the cyber world. Understanding the existence and closely monitoring variances in the possible numbers of a particular attacker type due to SPEC events can be used as a key predictor for a cyber-attack.

> Cyber-attacks are strongly correlated to political and cultural conflicts.

The human agents that perpetrate a cyber-attack can be broadly classified into four categories: 1) script kiddies (hacking for fun, low skill); 2) mercenaries (hacking for money, organized and skilled); 3) social protestors (hacktivists, loosely organized); and 4) nation states (hacking under orders for a purpose, highly skilled and well funded). A more elaborate list of attackers and their motives has been developed [40].

Attack Coordination

Massive cyber-attacks are often linked to groups of human agents working in unison. From a collaboration dimension, cyber-attacks can be classified into two categories: 1) Non-organized /Non-coordinated; and 2) Organized/Coordinated. Non-organized attacks are not disorganized. Instead, we mean that the attacks could be implicitly, semi-, or auto-organized. The massing effect of the attack occurs once other individuals become aware of an attack taking place. Non-organized groups leverage nationalism, patriotism, and sensitive issues to motivate participation. Such groups are loosely linked using social networking tools such as chat rooms, forums, and blogs. The recruits participate in a large scale and distributed attacks that rely on several individuals performing different tasks or overwhelming the target by DDoS. A mass email attack on the Yasukuni Shrine web host in Japan [19], allegedly from China, is an example of such an attack. During the Russia and Georgia conflict [11], reports indicated that step-by-step instructions for launching a cyber-attack against the Georgia cyber infrastructure were actively distributed on web forums to voluntarily mobilize Russian loyalists.

Conversely, organized attacks involve highly coordinated activities among a close group of individuals working together covertly. These groups include crime syndicates or groups of individuals recruited by a military or government especially for the purpose of launching attacks.

Attack origin and attribution

"Attribution" is a significant challenge for cyber security. Current technology allows for only the speculative location of attackers. Decentralized peer-to-peer command and control networks ("zombies") obscure the origin of a cyber-attack. For example, many months after the Russia-Georgia conflict,

> Countries such as the U.S and China have a significant number of victimized computers or zombies that are used to launch an attack.

a possible link was discovered to a botnet services provider. Yet it may still be impossible to trace the *human* network that is ultimately responsible for planning and coordination. Unless certain groups take responsibility, it is difficult to accuse a nation or individual of launching an attack with irrefutable evidence [6]. Investigators often have to follow a breadcrumb trail in both the cyber and physical worlds to substantiate any claims with evidence.

Studies show that countries such as the U.S and China have a significant number of victimized computers or zombies that are used to launch an attack [37]. The last thing we want to see is a triggering of conflicts between nations in both the cyber and physical world based on misinformation.

Attack Motive

The compiled record suggests that many cyber-attacks are somehow motivated by deeply-rooted socio-cultural issues. Attacks can also be politically motivated or used to influence government policy [12], [14].

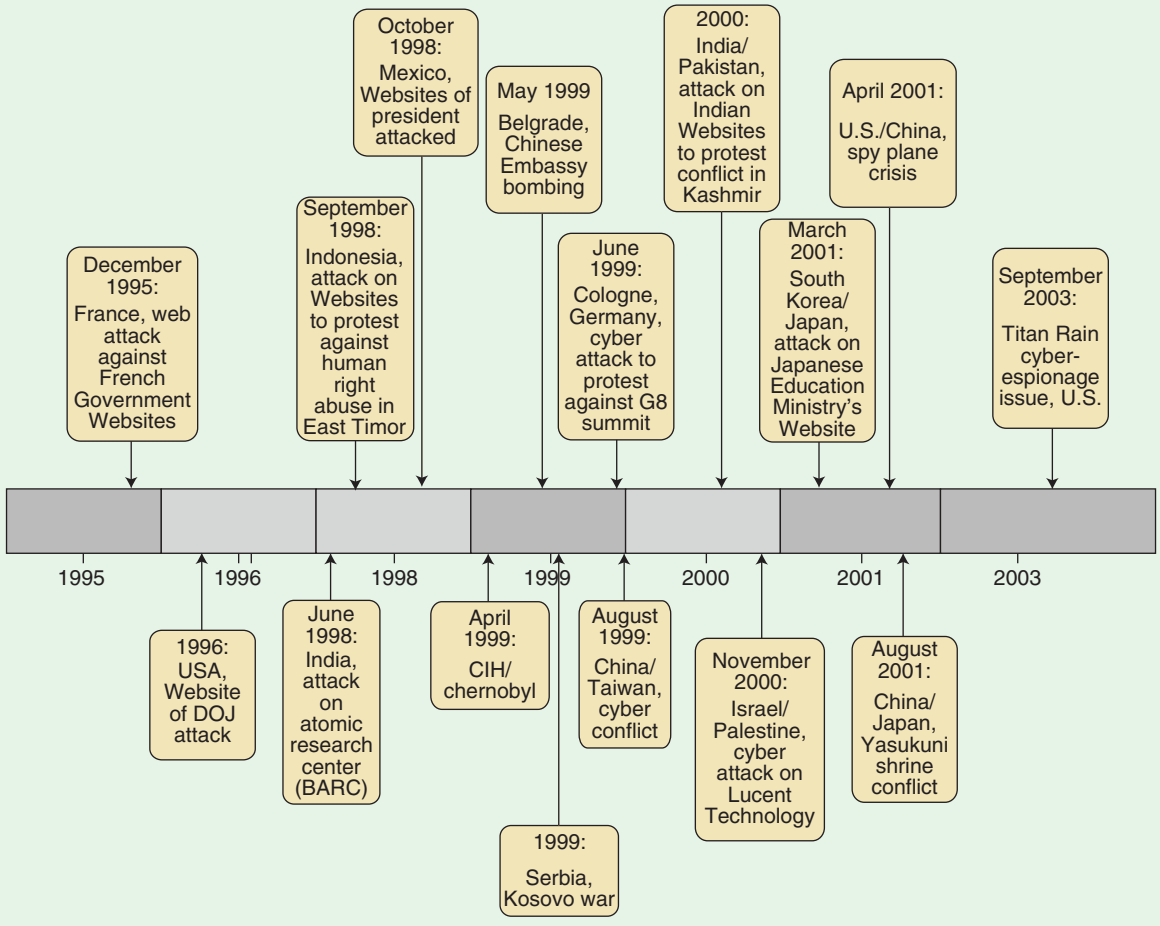


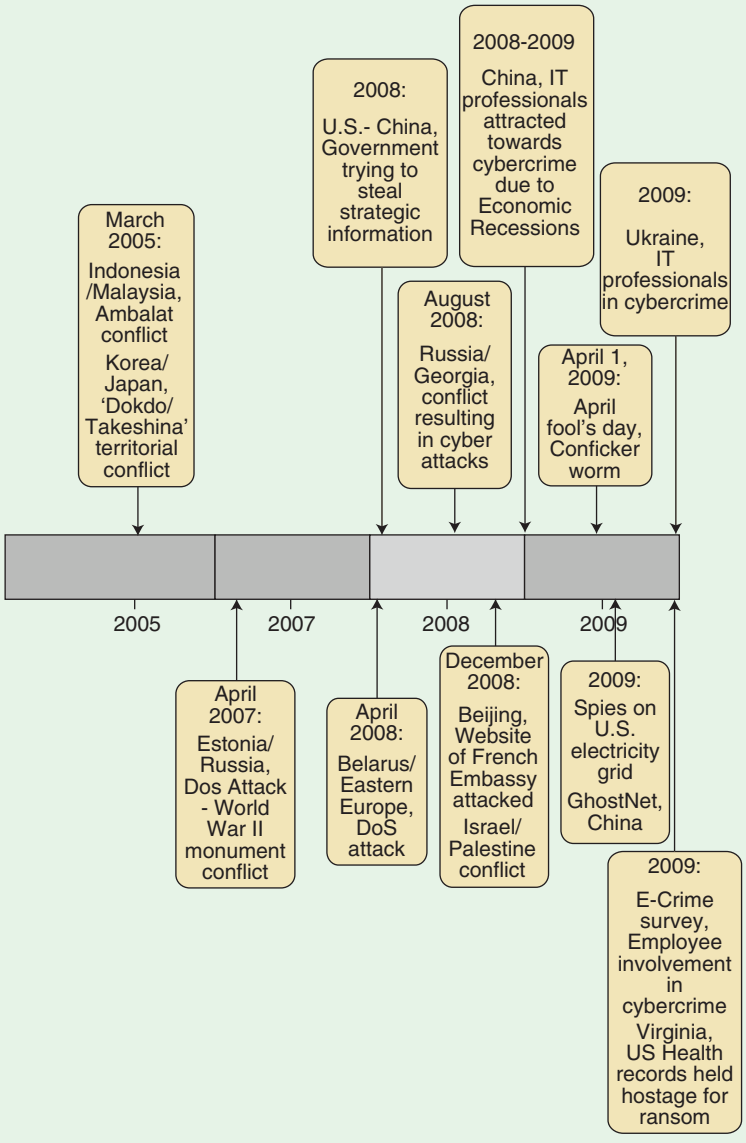
Fig. 3. A timeline of cyber-attacks from the CSEP dimensions during 1995–2009.

In some cases the motivation is ethical, i.e., a fight for social justice, and human rights. This was the case in attacks launched against the Indonesian and Mexican governments [4], [32], [46]. Financial gain is a significant motive for criminal gangs to attempt breaking into financial institutions. Cyber-attacks often involve anger and revenge. Many of the cyber-attacks we reviewed involve groups or individuals who were harmed by a government, another group, or industrial entity.

> The last thing we want to see is a conflict triggered between nations in both the cyber and physical worlds based on misinformation.

Attack Timing

When cyber-attacks are used in protest they are often launched immediately following a triggering event in the physical world. In contrast, many attacks (coordinated and uncoordinated) have been launched prior to or in sync with a military attack on a region; the movements of Russian troops in Georgia were correlated with cyber-attacks on the Georgian communications infrastructure and defacement of government websites. Cyber-attacks are also timed to express outrage, or for revenge over, specific dates or anniversaries; a Burmese Web site came under devastating cyber-attack on the anniversary of last year's failed uprising against the Burmese junta. There has also been speculation about the planting of malicious software in systems that control critical infrastructure [16]. Such malicious software is suspected to activate in a time of crisis or in coordination with aggressive military operations.



Attack Means

History shows that DoS attacks are a favored means to compromise the availability of services or to escalate a hacker's privileges in order to deface websites and steal data. Non-coordinated attacks using Internet forums, chat rooms, and blogs to recruit attackers also distribute attack code injection scripts and lists of vulnerable targets, as part of attack mobilization efforts coupled with propaganda. Malware that can amass a large bot army are forms of DDoS, which is difficult to protect against. Zero-day exploits could be potentially amassed as weapons which can be exploited in time of conflict.

Attack Outcomes

Attack Victims

Individuals are not usually the target of mass cyber-attacks [43], [44]. Infrastructure is usually the target, and the after-effects can be far

> Many cyber-attacks are motivated by deeply-rooted socio-cultural issues.

reaching. For example, it has been estimated that a mass cyber-attack could leave 70 percent of the U.S. in total darkness without electrical power for six months [45]. In times of conflict, cyber-attacks have been primarily targeted towards government or military installations. But as witnessed during the recent Russia-Georgia and Estonia conflicts, financial institutions and banks are also attractive targets [33].

In contrast to mass cyber-attacks, small scale attacks target users who are unaware of technical system vulnerabilities [13]. Such users can be naïve, disabled, disadvantaged, desperate, lonely, or emotionally weak [10]. Symantec estimates that about 93 percent of the non-organized cyber criminals target home users [43]. Data breaches at financial institutions ultimately lead to the identity compromise of individuals. Massive botnets composed of covertly victimized machines are used to prevent attribution and generate large amounts of attack traffic in order to launch a cyber-attack.

Governments and military establishments are often victimized for espionage, theft of intellectual property, or exposure of secret information. Such attacks are covert in nature and are only discovered upon vigilant monitoring and tracking of cyber activities. In most cases investigators can only speculate on the activities of the attackers

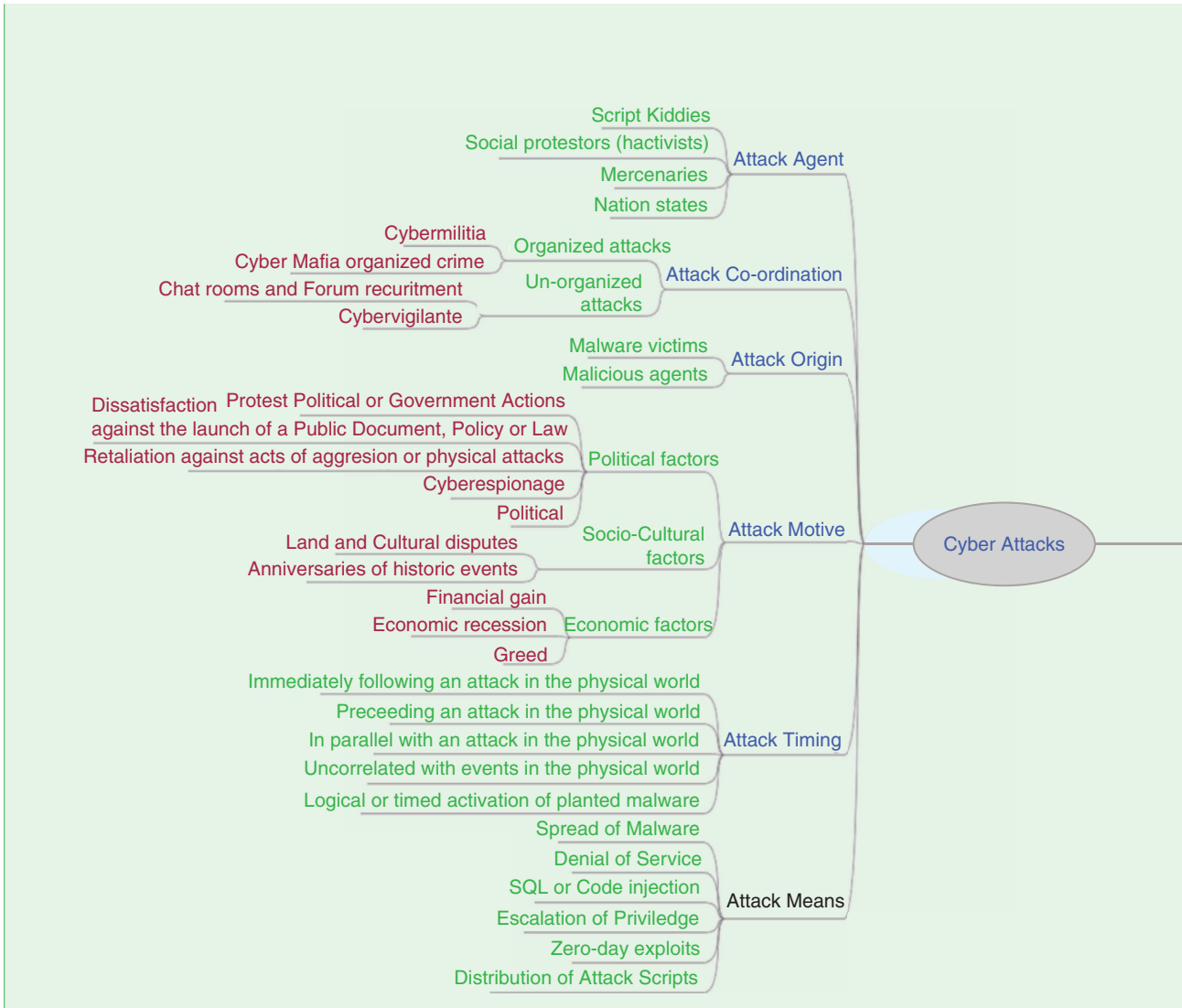


Fig. 4. Categorization of cyber-attack dimensions.

after the attacks have taken place [8], [16], [23], [38].

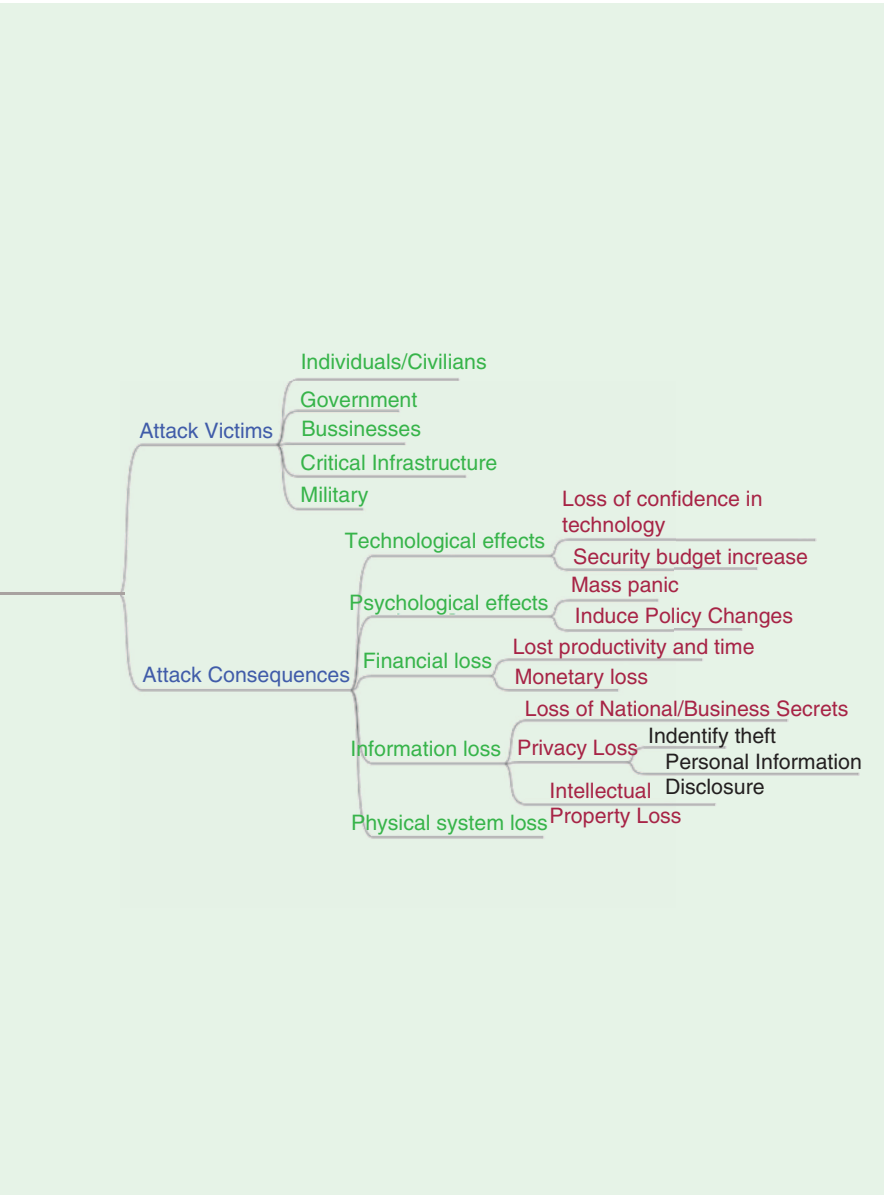
Attack Consequences

The consequences of a cyber-attack are as diverse as the SPEC dimensions. Along the technological dimensions, a cyber-attack can leave users distrustful of services such as banking, healthcare, and finance. The objective is similar in concept to spreading fear by conducting terrorist activities against a transportation infrastructure. Another consequence of a cyber-attack is increased spending on securing critical assets, which imposes additional costs on taxpayers and consumers.

> In some cases the motivation for an attack is ethical.

Psychological effects can be significant, spreading widespread fear. Consider the panic among the people of Estonia when significant parts of their cyber infrastructure were inaccessible due to DoS attacks. Such panic may also induce policy changes, as observed with the restoration of the bronze statue in Estonia, whose removal sparked the cyber-attacks.

Consequences along the dimensions of financial, information, and physical losses are the more tangible and direct outcomes of a cyber-attack. Physical loss in most instances occurs when the cyber world is tightly integrated with the physical world, as in the case of systems that control the distribution of power, gas, water, sewage, oil, and critical services.



Pathology of SPEC-Triggered Cyber-Attacks

Attacks triggered by SPEC events have pathology similar to biological pandemics [25], where each outbreak develops in stages over its life cycle [41]. Therefore it is critical to identify features that can be observed or discovered as early predictors or indicators, and monitor these factors before the actual attack takes place or propagates.

Cyber-defense is harder than cyber-offense, and technological mechanisms alone are never sufficient. To build appropriate expertise, understanding is needed in a broad range of issues related to the global cyber environment. We need to investigate a full range of factors that shape and alter the cyber security environment including social, political, economic, cultural, and technological trends.

Achieving global cyber security is a matter of strategic economic interest for all nations. Developing a global culture of cyber security also means assisting developing economies in adopting the "technology, processes, and people" of cyber security.

Author Information

Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, and Qiuming Zhu are with the

University of Nebraska at Omaha, Omaha, NE.

Phillip Laplante is with the School of Graduate Professional Studies, Penn State University, 30 East Swedesford Road, Malvern, PA 19355; email: plaplante@gv.psu.edu.

References

[1] R. Adhikari, "Security sleuths work overtime to confound Conficker," *TechNewsWorld,* Mar. 30, 2009; http://www.technewsworld.com/story/66666.html.

[2] A. Amirzai, "Belarus: A telling cyberattack," *Stratfor Global Intelligence*, 2008; http://www.stratfor.com/analysis/belarus_telling_cyberattack.

[3] M. Amona, "Cyberwar emerges amid the Israeli-Palestinian conflict in Gaza," http://cyberstrategies.wordpress.com/, Jan. 4, 2009; http://cyberstrategies.wordpress.com/2009/01/14/cyberwar-emerges-amid-the-israeli-palestinian-conflict-in-gaza/.

[4] J. Arquilla and D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand, 2001.

[5] K. Avruch, "Cross-cultural conflict" (Conflict Resolution), in *Encyclopedia of Life Support Systems (EOLSS)*. Oxford, U.K.: Eolss, 2002.

[6] M.A. Caloyannides, "Forensics is so 'yesterday'," *IEEE Security & Privacy*, vol. 7, no. 2, pp. 18-25, 2009.

[7] CNN, "Japanese textbook dispute sparks cyber-attack," *CNN.com*, Mar. 31, 2001; http://edition.cnn.com/2001/WORLD/asiapcf/east/03/31/japan.korea.website/index.html.

[8] CNN, "China analysts dismiss cyber-espionage claims," *CNN.com*, 2009, http://www.cnn.com/2009/TECH/03/30/ghostnet.cyber.espionage/.

[9] CCRC staff, "Japan declared a cyberwar against S. Korea," *Computer Crime Research Center*, Mar. 22, 2005; http://www.crime-research.org/news/22.03.2005/1067/.

[10] M. Cross, *Scene of the Cybercrime*. Syngress, 2008, pp. 443–450.

[11] D. Danchev, "Coordinated Russia vs Georgia cyber-attack in progress," *Zero Day*, Aug. 11, 2008; http://blogs.zdnet.com/security/?p=1670.

[12] D. Denning, "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy", presented at," Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, 1999; http://faculty.nps.edu/dedennin/publications/activism-hacktivism-cyberterrorism.pdf.

[13] J. Eom, Y. Han, *et al*. "Active Cyber-attack model for network system's vulnerability assessment," in *Proc. Int. Conf. Information Science and Security*, 2008, pp. 153-158.

[14] J. Germain, "The art of cyber warfare, Part 1: The digital battlefield," *TechNewsWorld*, 2008; http://www.technewsworld.com/rsstory/62779.html.

[15] G. Gilmore, "Navy aircraft not a 'spy plane,' DoD says," *American Forces Press Service*, 2001, http://www.defenselink.mil/news/newsarticle.aspx?id=45042.

[16] S. Gorman, "Electricity grid in U.S. penetrated by spies," *Wall Street J*., Apr. 8, 2009; http://online.wsj.com/article/SB123914805204099085.html.

[17] R. Hundley and R. Anderson, "Emerging challenge: Security and safety in cyberspace," *IEEE Technology & Society Mag.*, vol. 14, no. 4, pp. 19-28, 1996.

[18] M. Handelman, "French embassy in Beijing under cyber-attack," infosecurity.us, Dec. 12, 2008; http://infosecurity.us/?p=4408.

[19] S. Herman, "VOA's Steve Herman reports from Tokyo," *Globalsecurity.org,* 2005; http://www.globalsecurity.org/security/library/news/2005/01/sec-050106-3f7c3184.htm.

[20] M. Hines, "Cyber-espionage moves into B2B," *InfoWorld*, Jan. 15, 2008; http://www.infoworld.com/t/business/cyber-espionage-moves-b2b-546?page=0,0.

[21] J. Howard and T. Longstaff, "A common language for computer security incidents," *Sandia Labs,* SAND98-8667, 1998.

[22] HSdailyWire.com, "Virginia medical records hijacking;" May 8, 2009; http://homelandsecuritynewswire.com/virginia-medical-records-hijacking-update.

[23] Athina Karatzogianni, *Cyber-Conflict and Global Politics*, Routledge, 2008

[24] M.E. Kuhl, J. Kistner, *et al*. "Cyber-attack modeling and simulation for network security analysis," in *Proc. Winter Simulation Conf.,* 2007, pp. 1180 –1188.

[25] P. Laplante, B. Michael, and J. Voas, "Cyberpandemics: History, inevitability, response," *IEEE Security & Privacy*, vol. 7, no. 1, pp. 63-67, 2009.

[26] J. Laprise, "Cyber warfare seen through a mariner's spyglass," *IEEE Technology & Society Mag.*, 2005.

[27] Z. Liu, C. Wang, and S. Chen; "Correlating multi-step attack and constructing attack scenarios based on attack pattern modeling," in *Proc. Int. Conf. Information Security and Assurance*, 2008, pp. 214–219.

[28] J. Markoff, "Internet attacks seen as more potent and complex," 2008, http:/ / www.iht.com/articles /2008/11/10/ technology/10attacks.php.

[29] R. McMillan, "China becoming the world's malware factory," *Network World*, 2009, http://www.networkworld.com/news /2009/032409-china-becoming-theworlds-malware.html.

[30] "MessageLabs Intelligence: 2008 Annual Security Report," 2009; http://www.messagelabs.com/intelligence.aspx.

[31] E. Messmer"Ukrainian cybercriminals raked in $10K/day," 2009, http://www.networkworld.com/news/2009/032309-ukrainian-cybercriminals.html?page=1.

[32] M. Manion and A. Goodrum, "Terrorism or civil disobedience: Toward a hacktivist ethic," *Computers and Society*, 2000.

[33] J. Miks, "Asian countries looking to bolster cyber defenses," *World Politics Rev. Exclusive*, 2008, http://www.worldpoliticsreview.com/articlePrint.aspx?ID=2576.

[34] M. Myers and F. Tan, "Beyond models of national culture in information systems research," *Advanced Topics in Global Information Management*, ch. 1, 2003.

[35] X. Peng and H. Zhao, "A framework of attacker centric cyber-attack behavior analysis," in *Proc. IEEE Int. Conf. on Communications*, 2007, pp. 1449 –1454.

[36] G. Rasche, E. Allwein *et al*. "Model-based cyber security," in *Proc. 14th Ann. IEEE Int. Conf. and Workshops on the Engineering of Computer-Based Systems*, 2007, pp. 405–412.

[37] SecureWorks, "Compromised U.S. and Chinese Computers Launch Greatest Number of Cyber-attacks," 2008, http://www. securework s .com /media /press_releases/20080922-attacks.

[38] E. Shannon, "The invasion of the Chinese cyberspies," *Time*, 2005.

[39] J. Slay, "IS security, trust and culture: a theoretical framework for managing IS security in multicultural settings," *J. Campus-Wide Information Systems*, 2003, vol. 20, no. 3, pp. 98-104.

[40] S. Redwine, Ed., *Secure Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software*, Version 1.1, Department of Homeland Security, SEI/CMU, 2006.

[41] World Health Organization, Centers for Disease Control and Prevention, "Stages of an influenza pandemic," June 11, 2009; https://www.health.harvard.edu/flu-resource-center/stages-of-an-influenza-pandemic.htm.

[42] Strategypage.com, "Information Warfare Article Index: Cyber War as the Ultimate Weapon," Jan. 5, 2008; http://www.strategypage.com/htmw/htiw/articles/20080105.aspx.

[43] Symantec.com, "Symantec's Internet Security Threat Report," vol. XII, 2007, vol. XIII, 2008; http://www.symantec.com/business/theme.jsp?themeid=threatreport.

[44] Symantec Security Response, W95 CIH," accessed Feb. 2010; http://www.symantec.com/security_response/writeup.jsp?docid=2000-122010-2655-99.

[45] T. Reid, *Times Online*, "China's cyber army is preparing to march on America," Sept. 8, 2007; http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece.

[46] M. Zubir, "Exchange of 'cyberfire' during the Malaysia-Indonesia Ambalat Dispute: A lesson for the future," Centre for Maritime Security and Diplomacy, MIMA, 2005.