ANGELYN FLOWERS
AND SHERALI ZEADALLY

Cyberwar: The What, When, Why, and How

Cyberwar is insidious, invisible to most, and is fought out of sight. It takes place in cyberspace, a location that cannot be seen, touched, nor felt. Cyberspace has been defined as the fifth domain of war [1]. We can see the physical instruments, such as computers, routers, cables, however these instruments interact in a virtual and unseen realm. This facilitates a reach that can extend from one part of the world to attacks on public or private sector entities in another part of the world, while perpetrator remains unknown in a legally provable sense. The defining questions for life in the 21st century may be: what is cyberwar? Will we know it when we see it? If so, what do we do in response?

The lack of precision in the terminology helps to cloud the issue. Terms such as cybercrime, cyberespionage and cyberattack are often used interchangeably. We speak of hackers, cybercriminals, and cyberterrorists as if they were identical. In many cases, they may be, or at least they may be closely related. The term cyberwar has been used in a variety of different contexts. Since war itself is generally considered as a military enterprise, cyberwar has often been linked to a conceptual framework associated with traditional notions of warfare. These notions generally involve force, physical harm, and violence. In this work, we examine the challenges this definition presents in a 21st century cyber-connected and cyber-dependent world, and we propose an expanded conceptual framework for cyberwar.

Underlying factors, such as the level of activity or behavior involved in cyberwar, and how many or what type of cyberattacks it takes for it to be defined as a cyberwar, become important. In recognizing the role that cyberattacks will play in future military conflicts, two threshold requirements have been identified when nation-states assess the consequences and their potential response. First, what is the threshold for considering a cyber-event an act of war or comparable to the use of force? Second (which will not be addressed in this article), what is the threshold between tactical and strategic applications of cyberattacks [2]?

> Cyberwar is insidious and is fought out of sight, invisible to most.

This evolution of war is particularly important when addressing cyberwar, which can include both kinetic and non-kinetic activities. Kinetic activities are associated with motion. In the military arena, this typically includes armed attacks, bombs dropping, etc. Non-kinetic cyberwar actions are typically directed towards targeting any aspect of an opponent's cyber systems such as communications, logistics, or intelligence. When used in conjunction with a kinetic battle, non-kinetic cyber activities can include disruption of an opponent's logistical supply chain or diversion of essential military supplies. Other types of non-kinetic cyber activity can include the destabilization of a government's financial system, interference with a government's computer systems, or infiltrating a computer system for the purposes of espionage. The ongoing debate discusses the extent to which these non-kinetic activities should be considered as cyberwarfare when they are not associated with an actual physical battle.

How Can Cyberwar Be Defined?

Efforts have been made to address the definition of cyberwar. The recently completed *Tallinn Manual on International Law Applicable in Cyberwarfare* [3] was developed at the request of the North Atlantic Treaty Organization (NATO) and the Cooperative Cyber Defense Center of Excellence (CCD-COE). The difficulty is that nation-states and non-state actors do not always follow laws when it comes to war. More importantly, increases in asymmetrical warfare, and the exponentially evolving nature of the Internet, tend to make

Digital Object Identifier 10.1109/MTS.2014.2345196
Date of publication: 17 September 2014

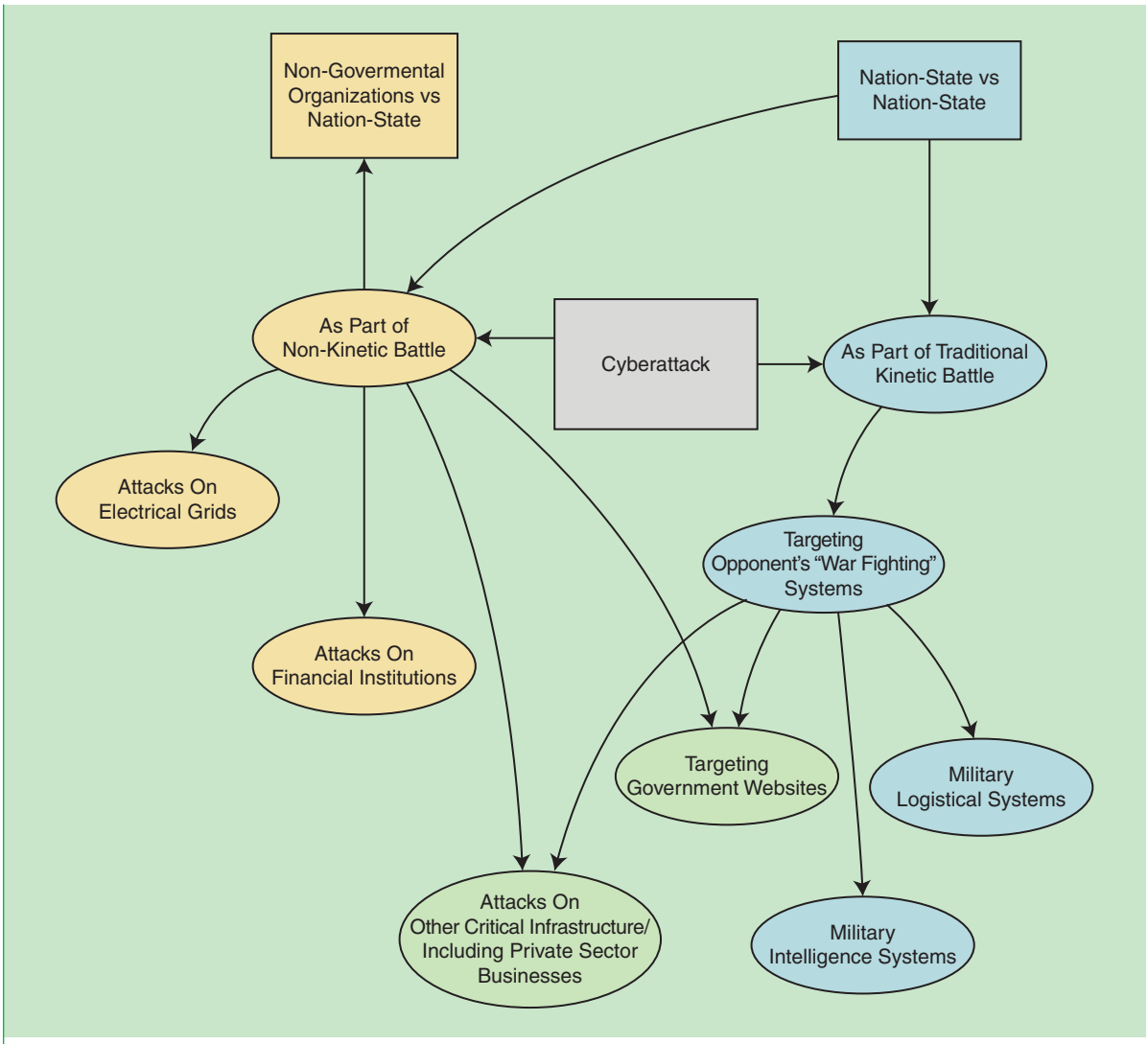

Fig. 1. Cyberattacks and organizational typology.

attacks in cyberspace more prevalent. In this type of environment, the impact of a Law of Cyberwarfare, as a regulatory mechanism, may therefore be limited. The *Tallinn Manual* defines cyberwar as a cyberattack, in either an offensive or defensive cyber operation, that is reasonably expected to cause death to persons, damage, or cause destruction to objects. Excluded from this definition, are psychological cyber-operations or cyberespionage [3]. A major drawback with this definition is its use of the term cyberattack, which is often synonymous with cyberwar and with the accompanying narrow definition of cyberwar. For example, it excludes cyber-operations designed to destabilize a nation-state's financial system, since the attack did not directly result in death or physical destruction.

Traditionally, violence has been viewed as a necessary correlate of a cyberattack, placing cyberwar within the context of an armed conflict. The focus was the equivalence of the effects of a cyberattack to the effects of an armed attack using physical means [2]. This approach to cyberwar has been adapted by those who view cyberattacks in military campaigns as a motive to target an opponent's communications, intelligence, as well as other Internet or network-based logistic operations [4]. The linkage of cyberwar with the use of force and armed conflict may be the current prevailing position in some international sectors. However, it fails to take into account the extent of non-physical damage that can be inflicted through cyberspace in a world that is becoming increasingly networked, up to and including nuclear facilities.

The Geneva Center for the Democratic Control of Armed Forces (DCAF) adopted a more inclusive definition of cyberattacks in its *DCAF Horizons 2015 Working Paper.* This definition distinguishes between state-sponsored and non-state-sponsored cyberattacks, and also includes cybervandalism, cybercrime, and cyberespionage within its definition of cyberattacks [1]. The DCAF defines cyberwar as warlike conduct conducted in virtual space

using information, communications technology, and networks, with the intention of disruption or destruction of the enemy's information and communications systems. It is targeted at influencing the decision-making capacity of an opponent's political leadership and armed forces [1]. It is, therefore, distinguished in two key areas. First, it recognizes that there is a non-physical impact to cyberwar, and second, it recognizes the significance of political leaders in making this determination.

> It is virtually impossible to identify every cyberattack that occurs.

A pure military-target definition of cyberwar is no longer realistic in the context of modern geo-political instabilities and a global environment of asymmetrical warfare. When a smaller force is in conflict with a larger entity, an armed conflict will most likely not be successful for the smaller force. In addition, the reality of the conflict proves that the determinations of when a nation-state declares war, and the precursor interpretation of events leading up to that determination, are decisions made by its political leadership. As a result, the terms cyberattack and cyberwar must be decoupled so that cyberattacks are not defined exclusively in terms of the use or effect of physical force causing death, damage, or destruction. Or, if the terms cyberattack and cyberwar are going to continue to be synonymous, then it's important to acknowledge that cyberattacks, and hence cyberwar, can include non-kinetic cyber activity without a co-requirement of kinetic military action.

Table I
Top 15 Source Countries for Cyberattacks in May 2013 [5]

Source of Attack	Number of Attacks
Russian Federation	1 153 032
United States	867 933
Germany	831 218
Taiwan	764 141
Bulgaria	358 505
Hungary	271 949
Poland	269 626
China, The Peoples' Republic of	254 221
Italy	205 196
Argentina	167 379
Romania	153 894
Venezuela, Bolivarian Republic of	140 559
Brazil	140 281
Colombia	124 851
Australia	120 157

When Does Cyberwar Occur?

It is virtually impossible to identify every cyberattack that occurs. Some can operate undetected for years. Others are brief, but still leave no detectable trace. This section describes a European-based effort aimed at measuring the frequency and source of attempted infiltrations over a one-month period. It also describes a few selected global examples of cyberattacks. Growing concerns with the security of Supervisory Control and Data Acquisition (SCADA) systems are discussed later in this article.

Frequency of Cyberattacks

Deutsche Telekom AG (DTAG), a German Telecommunications company, established a network of 97 sensors to serve as an early warning system to provide a real-time picture of ongoing cyberattacks. Although the majority of the sensors are located in Germany, DTAG also locates honeypots and sensors in other non-European countries. The top fifteen countries recorded as the source of cyberattacks by the DTAG sensors are listed in Table I. Approximately, 20% of the cyberattacks listed originated in the Russian Federation. The first four countries listed, including the U.S., Germany, and Taiwan, accounted for 62% of the cyberattacks represented. These instances provide a snapshot in time of attacks primarily targeted towards a particular geographic area, in this instance, Europe.

On a broader international and historical scale, the *DCAF Horizons 2015 Working Paper* describes historical instances of what they identify as cyber conflict and which clearly should be considered as cyberattacks. The attacks have been summarized in Table II. It should be noted that, for many of the cyberattacks described, the perpetrator is indicated as "alleged." This reflects the difficulty in ascertaining responsibility.

Of the fourteen cyberattacks described in Table II, five occurred within the context of an actual kinetic or "hot" war, one occurred within the context of a "cold" war, and the remainder occurred within the context of ongoing tensions between nation-states, or between a nation-state and non-state actors that may or may not have been supported by another nation-state. The temporal trend in these identified conflicts is the utilization of cyberattacks in the absence of a kinetic battle. When considered with the subsequent cyber occurrences described in Table III, the trend is towards attacks against a nation-state's critical infrastructure [24].

Why Does Cyberwar Occur?

For smaller nations, or terrorist organizations, the use of DDoS attacks are much cheaper to launch than conventional warfare tools against an enemy possessing

Table II
History of Cyberattacks as Reported by the Center For the Democratic Control of Armed Forces (DCAF) [1]

Year	Perpetrator	Target	Incident
1982	United States	(then) Soviet Union	Embedded logic bombs caused malfunctions in pump speeds and valve settings in oil pipelines [note: The CIA "permitted" the software to be stolen by the Soviets in Canada].
1991	United States	Iraq (first Iraq War)	Airstrikes against Iraq's command and control systems, telecommunications systems, and portions of its national infrastructure; supported by communication and satellite systems.
1994	Pro-Chechen separatist movement and pro-Russian forces		Both sides engaged in a virtual Internet war simultaneously with a kinetic ground war.
1997 – 2001	(breakaway region of) Chechnya and the Russian Federation		Simultaneous with a kinetic war – use of Internet for propaganda by both sides. Russia also accused of hacking into Chechen websites.
2002	Russian Federation (alleged)	Chechnya	The Russian Federal Security System allegedly knocked out two Chechen websites hosted in the U.S. immediately prior to the Russian Spetsnaz Special Forces storming a Moscow theater that was under siege by Chechen terrorists.
1999 – 2002	Israeli and Palestinian cyberconflict		Israeli teen hackers launching a sustained Distributed Denial of Service (DDoS) attack that successfully jammed six websites operated by the Hezbollah and Hamas organizations in Lebanon and the Palestinian National Authority. In response, hackers attacked sites belonging to the Israeli Parliament, the Ministry of Foreign Affairs, and the Israeli Defense Force information site; later striking the Israeli Prime Minister's Office, the Bank of Israel, and the Tel Aviv Stock Exchange.
April – May, 2007	Russian Federation (alleged)	Estonia	Series of DDoS attacks first against Estonian government agencies, and then private sites and servers. Some attacks lasted weeks. The botnet utilized in the DDoS attacks employed up to 100 000 zombie PCs.
August 2007	The People's Republic of China (alleged)	England France Germany	Intrusions into government networks.
September 6, 2007	Israel	Syria	Israeli airstrike destroyed a nuclear reactor under construction to process plutonium. It is alleged that prior to the airstrike Syria's air defense network was deactivated by Israel activating a secret built-in switch.
June – July, 2008	Russian nationalist hackers	Lithuania	Hacking of hundreds of Lithuanian government and corporate websites some of which were covered in digital Soviet-era graffiti.
August 2008	Russian Federation (attacks also launched from Lithuania)	Georgia	Cyberattack directly coordinated with a kinetic land, sea and air attack. Main attack vectors: Botnets attacked Georgian media, DDoS attacks targeted command and control systems. DDoS, Structured Query Language (SQL) injection, and cross-site scripting (XSS). Main targets: Government websites, financial and educational institutions, business associations, news media websites (including the BBC and CNN).
January 2009	Russian Federation (alleged)	Kyrgyzstan	DDoS attacks focused on three of the four Internet Service Providers (ISP) in Kyrgyzstan disrupting all internet traffic. Russia was the source of most of the DDoS attacks.

(Continued)

Table II
(Continued)

Year	Perpetrator	Target	Incident
July 4 – 8, 2009	Unknown – North Korea has been suggested since the attacks begin on the date of a North Korean missile test launch and concluded on the 15th anniversary of the death of North Korea's Kim II Sung.	South Korea & United States	Coordinated attacks against South Korean and U.S. government and business websites, including the public websites for the U.S. stock exchanges: New York Stock Exchange (NYSE) and NASDAQ. A botnet built using the early 2004 MyDoom worm, and rudimentary DDoS attacks were used. The attacks originated from 86 IP addresses in 16 countries.
2009 – 2010	Unknown	Iran	Stuxnet, a cyber worm, caused damage to centrifuges of Iran's nuclear reactors. Stuxnet attacked and disabled Siemens type Supervisory Control and Data Acquisition (SCADA) systems in a manner that disguises the damage from the operators until it is too late to correct.

greater resources in terms of weapons, money, and troops. Imagine a drone, not only intercepted, but also then re-routed back towards its originator. Fewer resources are required, but yet, on the other hand, increased specialized training is required. Cyberattack for hire is a lucrative business for those who have been previously overlooked as merely cybercriminals. As noted by many, including Richard Clarke, former National Coordinator for Security, Infrastructure Protection, and Counterterrorism for the United States, cybercriminals can become rental cyberwarriors [8]. This easy transition from cybercriminality

Table III
Recent Cyberattacks on Critical Infrastructure

Year	Perpetrator	Target	Cyberattack
2010 [first discovered]	Unknown	Iran and other parts of the Middle East	Flame has been described as a backdoor with Trojan and worm-like characteristics. Its purpose was to gather information from infected PCs. After gathering the information it uploads it to command and control computers. It is more complex and is believed to be much more dangerous than the Stuxnet virus. Flame can attack critical infrastructure and the United Nations International Telecommunications Union has warned other nations to be on/ the alert for its appearance [19].
2012	Originated in the Middle East	United States	For a one week period in September 2012 five major U.S. banks were subjected to ongoing Distributed Denials of Service (DDoS) attacks which prohibited customers from accessing their bank's website. These attacks were believed to be part of an ongoing and continuing attack on the financial sector of the US [20].
2012	"The Cutting Sword of Justice" (claimed responsibility)	Saudi Arabia's state oil company ARAMCO	The Sharmoon virus infected 30 000 ARAMCO computers is a form of malware that overwrites the Master Boot Record (MBO) placing the data with a jpg file, in this instance, a picture of a burning American flag [21]–[22].
2012	Unknown	Qatar state owned oil company RasGas	Sharmoon virus [22].

to cyberwarriors for hire suggests that reliance on a strict delineation between the two activities. Cybercrime and cyberattacks may, in the long run, lead to increased cyberattacks.

Cyberattacks have the ability to disrupt the way in which ordinary individuals live their lives (e.g., the chaos that would arise if none of the automatic teller machines (ATMs) in a country were operational). The interconnectedness of global financial institutions, enabled by modern communications technology, increases this risk [23]. A few years ago, we witnessed the impact of the 2003 northeastern blackout in the U.S. that affected electrical grids spanning from Ohio to New York, and even stretching to the Canadian province of Ontario. While it lasted for only a few days, it's important to ask what would be the impact of something similar, or on a larger scale, that was deliberately caused for a prolonged period of time. When Estonia was subjected to a barrage of cyberattacks, it was forced to cut its external Internet connections so that people within the country could continue to use their conventional services [9]. With external Internet service access disabled, an Estonian traveler in another country could not retrieve money from an ATM machine or use a bank issued credit card. Despite taking 30 000 computers off-line, the Sharmoon virus was ultimately not successful in that it did not significantly disrupt oil production in either Saudi Arabia or Qatar. But, what if it had? What would the impacts have been?

Cyberattacks use a variety of vectors, both technological and organizational.

The United States has identified cyberattacks on its critical infrastructure as a matter of national security, and has declared cyberspace a domain of war [10]. Critical infrastructures are physical or virtual systems and assets that are so crucial to a nation that any harm done to them will have a drastic effect on security, national economic security, national public health, or safety [11]. Specifically, these attacks are referring to agriculture, food, water, public health, emergency services, government, defense, industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industries, and postal and shipping systems [12]. It is the potential destabilizing effects of disruptions to these infrastructures that concern the political decision-makers who ultimately label such disruptions as a cyberattack or a cyberwar. This is why cyberattacks, or cyberwar, often extend beyond a physical battlefield. Although the above-mentioned disruptions cause no physical injury or damage, they can nevertheless be considered acts of war (i.e., by political leaders).

How Cyberwar Occurs

Cyberattacks use a variety of vectors, both technological and organizational. They seek out vulnerabilities in any of the entities that comprise cyberspace. Moura found that certain types of attacks were more likely to originate from certain nations or regions. For instance, 75% of the Internet Service Providers (ISPs) containing the most *phishing* scams are located in the United States. Ordinary spam primarily originates in India and Vietnam, while the largest concentration of spammers per Internet address is in Nigeria [15]. Moura argues that analyzing where malicious hosts are concentrated could enhance prediction of future attacks.

Several technological methods are used to launch attacks in cyberspace. In this section, we briefly present some methods used for attacks in cyberspace. We also present a sample heuristic diagram for the classification of cyberattack types.

Methodological Approaches

The DTAG honeypot system also identified the five most popular types of attacks detected in May 2013. These tended to be targeted towards cyber or Internet technologies. As illustrated in Table IV, 78% of these attacks were on Server Message Block (SMB) protocols. SCADA systems are particularly vulnerable to attacks, and hence attractive to potential cyberattackers. Known as the "workhorses of the information age," computer control systems are also the weak link in critical infrastructure systems [10], [24]. These systems regulate the operation of the infrastructure. For instance, they manage the flow of natural gas through a pipeline, or they manage the production of chemicals, etc. SCADA systems are increasingly being connected to other networks, including the Internet, making them vulnerable to external cyberattacks. Given the extent of damages, such as serious injuries, deaths, unavailability of crucial daily services that can result if the operations of a SCADA system are disrupted, it is not surprising that these attacks are considered cyberterrorism or cyberwar. SCADA systems

Table IV
Top 5 Attack Types in May 2013 [5]

Description	Number of Attacks
Attack on Server Message Block (SMB) protocol	5 970 973
Attack on Secure Shell (SSH) protocol	660 350
Honeytrap Attacker on Port 161	439 981
Attack on Port 5353	288 136
Attack on Netbios protocol	269 211

operate electrical grids, open and close dams, as well as regulate a host of other unseen yet vital, critical infrastructure operations. It was the SCADA system in Iran's nuclear centrifuge facility that was successfully targeted by Stuxnet. The danger for highly industrialized countries is that their computerized critical infrastructure makes them vulnerable to similar attacks. The United States has one of the most developed, computerized critical infrastructure systems in the world, making it highly vulnerable [8]. Cyberattacks are not the only danger to these systems. Among the SCADA attacks worldwide that have made it to court, many have been found to be the work of a disgruntled employee with no political motivation [24].

A recurring question is whether there may be instances where DDoS attacks could be considered acts of war. For those requiring a military context, it has been argued that cyberwar can be understood through the context of maritime commerce warfare [16]. Waterways are the most efficient mechanism for transporting tangible goods. The Internet is the most efficient mechanism for transporting intangible goods. Therefore, just as naval blockades and attacks on shipping lanes were considered acts of war in both World Wars because they prevented the transport of tangible goods, DDoS attacks block the transport of intangible goods [16]. This definition, while still analogous to traditional warfare, provides a definition for cyberwar, which circumvents the co-requisite of a kinetic battle.

Manipulation of increasingly automated information systems, insecurity of the supply chain, and cross-platform malware are among the emerging cyberthreats identified for 2013 [17]. The ability to manipulate automated information systems is a direct threat to the security of any nation's supply chain. Few people are aware of the extent to which agribusiness, the process by which food is harvested, transported, and sold in stores, is automated. When combined with a "just in time" marketing system designed to deliver produce and supplies to the stores with little or no surplus, manipulation of a distributor's information system can result in deliveries not being made. This can potentially lead to food shortages in some locales. Cross-platform malware has also become more common. This can be partially attributed to the rapid increase in the number of smart phones and other hand-held, mobile devices, along with the emergence of applications. Many of the applications are designed to infect the device and transfer the malware wirelessly to other devices. Unrelated to cyberattacks, but also present, are internal end-user vulnerabilities confronting critical infrastructure.

Heuristic Classification of Cyberattacks

Cyberattacks are launched at multiple levels. This list is not intended to be hierarchical, or all-inclusive. Among the levels where cyberattacks can occur are:

- Government versus Government (within the context of a kinetic battle)
- Asymmetrical warfare: Non-state actor versus the agencies or contractors of its own, or another government
- Government against another Government's critical infrastructure (non-kinetic battle)
- Criminally inspired hackers versus individual users

As previously stated, cyberattacks between nation-states can occur within the context of kinetic and non-kinetic battles. This overlap is illustrated in Fig. 1. In the case of the nation-state of Georgia, described in Table II, while the cyberattacks occurred as adjunct to a kinetic war with the Russian Federation, it was believed that Russia had hired virtually every criminal hacker in Europe, both to assist in perpetrating the cyberattacks, as well as to deprive Georgia of an opportunity to retaliate in kind [18].

Non-Kinetic Cyberattacks Increasing

Non-kinetic cyberattacks appear to be increasing both in frequency and in severity in terms of the potential damage they cause. It is particularly feared that terrorists fighting an asymmetrical war against a larger, more powerful opponent, will utilize this attack mechanism. They may or may not occur within the context of a traditional kinetic war. Nation-states have also been accused of utilizing cyberattacks, both during, and in the absence of a kinetic battle. An important emerging distinction is that political leaders and military leaders do not necessarily utilize the same definitions. Political leaders are more apt to consider non-kinetic cyber-operations, targeting government, financial, or other critical national infrastructure as cyberattacks, and hence cyberwar, even in the absence of the use of force, injury, death, or physical damage.

At present, the greatest difficulty nation-states and organizations face is identifying perpetrators with confidence. In the absence of an admission, all that is initially available is speculation. To date, despite frequent allegations by nation-states as to who did what, or rhetoric from the political leaders of those nation-states, no nation-state has yet responded to a non-kinetic cyberattack with a kinetic operation. While the future of cyberwarfare in the 21st century will likely show cyberattacks that occur, not in conjunction with traditional armed conflict, but rather stand alone in a non-kinetic battle, it is equally as likely that these increased non-kinetic battles will have kinetic repercussions.

Author Information

Angelyn Flowers is a Professor and the Graduate Program Director of the Homeland Security Program at the University of the District of Columbia, Washington, DC. Email: aflowers@udc.edu.

Sherali Zeadally is an Associate Professor in the College of Communication and Information at the University of Kentucky, Lexington, KY. Email: szeadally@uky.edu.

Acknowledgment

The authors express gratitude to Katina Michael and to the anonymous reviewers for their useful comments and suggestions, which helped us to improve the quality and presentation of this paper.

References

[1] F. Schreier, *On Cyberwarfare: DCAF Horizons 2015 Working Paper.* Geneva: Defense Center for Armed Forces, 2013.

[2] J. Lewis, "Cyberwar thresholds and effects," *IEEE Security and Privacy*, pp. 23–29, Sept./Oct. 2011.

[3] M. Schmitt, Ed., *Tallinn Manual on The International Law Applicable to Cyberwarfare*, Cambridge, U.K.: Cambridge Univ. Press, 2013.

[4] W. Jones, "Declarations of cyberwar: What the revelations about the U.S.-Israeli origin of Stuxnet mean for warfare," *IEEE Spectrum*, pp. 18, Aug. 2012.

[5] Deutsche Telekom AG, "Overview of current cyber attacks;" http://www.sicherheitstacho.eu/, accessed June 6, 2013.

[7] Daily Mail Reporter, "Cyber attacks now fourth biggest threat to global stability," *Mail Online*, Jan. 12, 2012; http://www.dailymail.co.uk/news/article-2085876/Cyber-attacks-fourth-biggest-threat-global-stability-says-World-Economic-Forum.html, accessed June 6, 2013].

[8] R. Clarke and R. Knake, *Cyberwar: The Next Threat to National Security and What to Do AboutIt*. New York, NY: Harper Collins, 2010.

[9] M. Lesk, "The new front line: Estonia under cyberassault," *IEEE Security and Privacy*, vol. 5, no. 4, pp. 76–79, July-Aug. 2007.

[10] R. O'Harrow, Jr., *Zero Day: The Threat in Cyberspace*. New York, NY: Diversion Books, Washington Post E-Book, 2013.

[11] B. Obama, "Executive order 13636: Improving critical infrastructure cybersecurity," *Federal Register*, vol. 78, no. 33, part III, Feb.19, 2013.

[12] D. Warfield, "Critical infrastructures: IT security and threats from private sector ownership," *Information Security J.: A Global Perspective*, vol. 21, no. 3, pp. 127–136, 2012.

[15] G. Moreira Moura, *Internet Bad Neighborhoods*. The Netherlands, University of Twente, dissertation, 2013.

[16] J. Laprise, "Cyberwarfare seen through a mariner's spyglass," *IEEE Technology and Society Mag.*, vol. 25, no. 3, pp. 26–33, 2006.

[17] Georgia Tech Information Security Center and the Georgia Tech Research Institute, Emerging Cyber Threats Report 2013, presented at the Georgia Tech Cyber Security Summit, 2012.

[18] R. Haddick, "This week at war: Lessons from cyberwar I," *Foreign Policy*, Jan. 28, 2011; http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i?print=yes&hidecomments=yes&page=full, accessed May 21, 2013.

[19] J. Newman, "The Flame Virus: Your FAQS answered," *PC World,* May 30, 2012; http://www.pcworld.com/article/256508/the_flame_virus_your_faqs_answered.html, accessed June 4, 2013.

[20] J. Menn, "Middle East cyber attacks on US banks were highly sophisticated," *Huffington Post*, Oct. 2, 2012; http://www.huffingtonpost.com/2012/10/02/middle-east-cyber-attacks-us-banks_n_1933943.html, accessed May 23, 2013.

[21] N. Perlroth, "In cyberattack on Saudi firm, U.S. sees Iran striking back," *NY Times,* Oct. 23, 2012; http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all, accessed June 8, 2013.

[22] D. Sanger, and N. Perloth, "Cyberattacks against U.S. corporations are on the rise," *NY Times,* May 12, 2013; http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&_r=0, accessed June 5, 2013.

[23] L. Orman, "Technology as Risk," *IEEE Technology and Society Magazine*, pp. 23–31, Summer 2013.

[24] J. Clough, *Principles of Cybercrime*. New York, NY: Cambridge Univ. Press, 2012.