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?

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

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]?

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

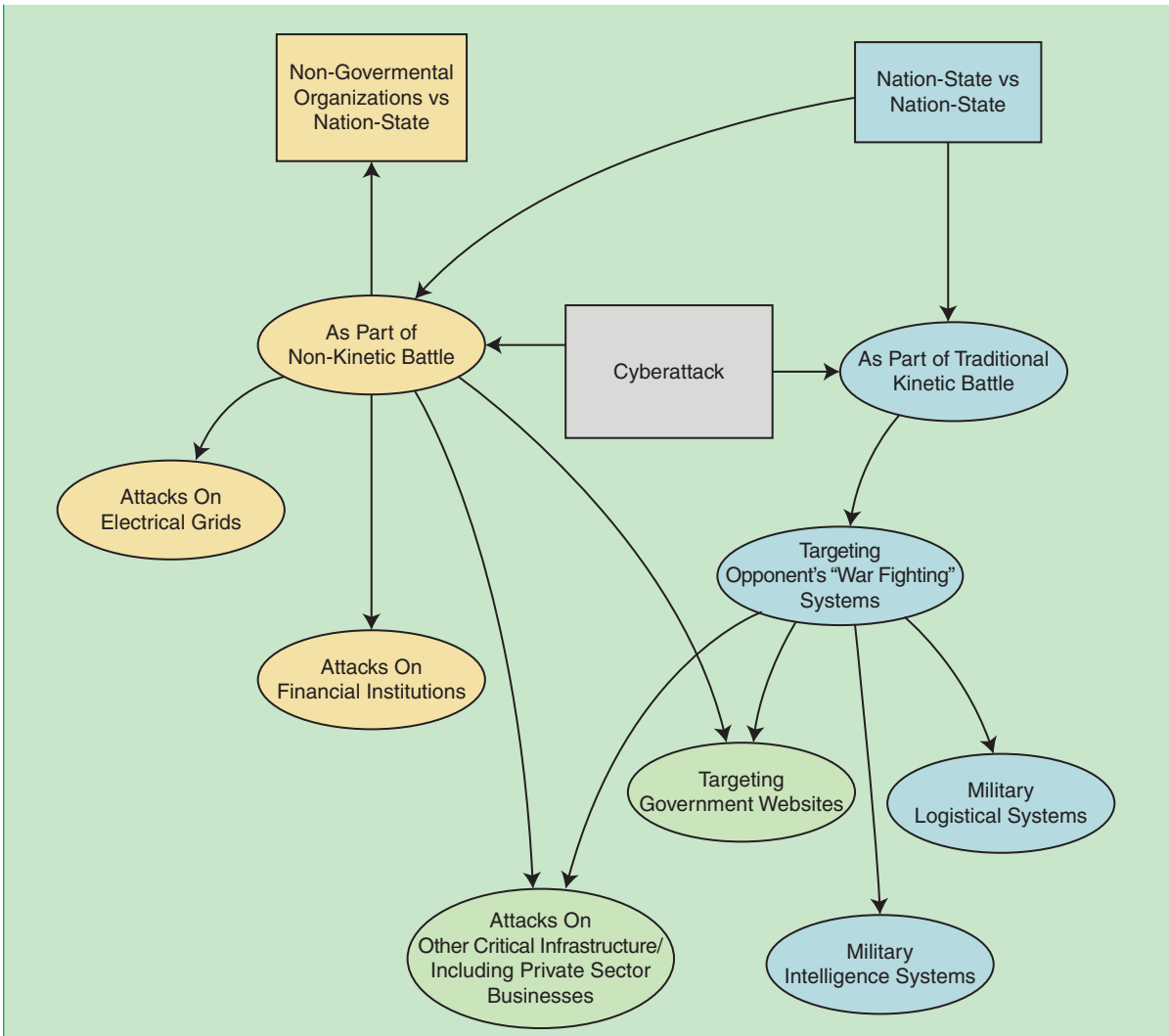

Fig. 1. Cyberattacks and organizational typology.

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

[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 cyber-

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.

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 Il 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].

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.