Johan Sigholm, Captain, Ph.D. student, Swedish National Defence College

NON-STATE ACTORS IN CYBERSPACE OPERATIONS

Abstract

The growing importance of cyberspace to modern society, and its increasing use as an arena for dispute, is becoming a national security concern for governments and armed forces globally. The special characteristics of cyberspace, such as its asymmetric nature, the lack of attribution, the low cost of entry, the legal ambiguity, and its role as an efficient medium for protest, crime, espionage and military aggression, makes it an attractive domain for nation-states as well as non-state actors in cyber conflict.

This paper studies the various non-state actors who coexist in cyberspace, examines their motives and incitements, and analyzes how and when their objectives coincide with those of nation-states. Literature suggests that many nations are currently pursuing cyberwarfare capabilities, oftentimes by leveraging criminal organizations and irregular forces. Employment of such non-state actors as hacktivists, patriot hackers, and cybermilitia in state-on-state cyberspace operations has also proved to be a usable model for conducting cyberattacks. The paper concludes that cyberspace is emerging as a new tool for state power that will likely reshape future warfare. However, due to the lack of concrete cyberwarfare experience, and the limited encounters of legitimate cyberattacks, it is hard to precisely assess future effects, risks and potentials.

Keywords
Non-state actors, cyber, cyberspace, cyberwar, cyberactions, cyberattack

1. Introduction

The world is becoming completely hooked on information and communications technology (ICT). Almost alarmingly so. Large parts of our daily lives are shaped

by computers, smartphones, the Internet and scores of unseen ICT-dependent societal services that we take for granted, such as electricity, clean water and sewage, food, healthcare, mass transit, heating, and security. The increasing integration of computer and network technology into the critical infrastructures supporting these services, and the complex interdependencies created by sector-spanning information requirements, certainly makes the offered services, efficient, accessible and "smart", but at the same time vulnerable to single points of failure and adversary attacks. During the last decade, between 2000 and 2010, global Internet usage increased by over 500 %, growing from 360 million to 2 billion users [61]. As more people are getting online, cyberspace is becoming a defining feature of modern life, where individuals and communities are socializing and organizing themselves across national borders and traditional sociocultural boundaries.

Cyberspace has also brought with it several new threats. The fact that cyber-dependency has become so widespread in society, with complex interconnections between various sectors, has increased vulnerability to attacks against both civilian and military infrastructures. We have thus seen an increased focus on cyberdefense within armed forces and national security organizations in many parts of the world. Within the military, cyberspace has been identified as a new fifth arena, besides land, sea, air and space, in which military operations can be performed [44]. These operations, called cyberspace operations, include both offensive and defensive measures, and may be performed independently or as a complement to conventional warfare.

Although nation-states might seem to be the most likely main players in a future full-scale cyberwar, recent events have shown that non-state actors might also play key roles during such events, and almost certainly will do so during low-intensive cyber-skirmishes. The often cited "cyberattacks" (see later discussion on definitions below) on targets in Estonia in the spring of 2007 is an example of where volunteers actively took part in an open cyberconflict [48], acting as a sort of cybermilitia, by rallying to overload various cyberspace resources, such as Estonian

government and commercial web services. Another example is Anonymous, a collective of so-called “hacktivists”, who have been claiming responsibility for several widely publicized web defacements, information leaks, denial-of-service attacks, and other cyberactions sometimes related to national security or military affairs [15].

Rogue malware authors and organized cyber criminals have also been very active during the last few years, motivated primarily by economic gain [66]. In 2009, it was discovered that a cyberespionage network called “GhostNet” had accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world [14]. It has been claimed that the software, which apparently was controlled by servers located on the island of Hainan, China, was a tool of that government [42]. However, as China has officially denied all responsibility for GhostNet, and there is no conclusive evidence that the Chinese government is involved in its operation, others mean that direct accusations should be avoided [10].

As the concept of cyberwarfare is becoming gradually more relevant for many nation-states, the need of quickly achieving a military cyberspace operation capability has become a top priority for armed forces and intelligence agencies around the world. In early 2013 the U.S. Department of Defense approved a major expansion of its Cyber Command, increasing its size more than fivefold to nearly 5000 troops and civilians [43]. Similar cyber-mobilization trends can be seen in many countries. While well-developed countries might primarily see the need of a defensive capability, protecting vulnerable digital resources, such as command and control systems, developing countries may instead recognize cyberspace operations as an attractive method, relatively inexpensive and politically risk-free, to wage war against an enemy with kinetic battlefield superiority. Non-state actors are thus increasingly being approached by many governments globally, who seek to benefit from their experience and leverage their cyber know-how to attain this sought-after capability [71][72][46]. This could be a possible explanation in the case of GhostNet, and was also posited in relation to the 2010 Stuxnet attacks [26]

(although they were later attributed to the United States and Israel [55]). This is an interesting development, which further underlines the growing importance of the various non-state actors in cyberspace.

This paper analyzes the use of cyberspace for armed conflict, with a focus on non-state actors and their relation to nation-states, and the involvement of non-state actors in cyberspace operations. The question of what exactly cyberwarfare is, and how it differs from classic kinetic warfare, requires some initial attention. Moreover, the nature of the cyberspace environment makes evaluation of whether certain activity is to be regarded as an act of war extremely precarious. To address these questions, the paper thus commences with a section on definitions, and presents a review of some basic warfare principles to differentiate cyberwar from armed conflict in the traditional sense.

The rest of this is paper is structured as follows; Section 2 presents related work previously done in the area. Section 3 offers an attempt at defining the concept of cyberwar, in relation to its physical-world counterpart of conventional kinetic war, and tries to disaggregate the various cyberactions that are commonly, sometimes quite carelessly, bundled into the concept of cyberattack. Section 4 describes the main relevant non-state actors in cyberconflict, and section 5 presents some benefits and drawbacks of nation-states employing these actors. A discussion of the relevance of non-state actors in cyberspace operations is given in section 6. Some concluding remarks are offered in section 7.

2. Previous work

Since “cyber” has become a veritable hot-topic within several different research areas during the past few years, quite a lot of recent work has been done on the subject in several sub-fields. The fast-paced technical advancement and the rapid development of new military doctrines, public policy and various legislation, does however make the area quite volatile and subject to constant change.

Of the available textbooks on the subject of cyberwarfare, worth mentioning is "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" [2] by Jason Andress and Steve Winterfeld which offers a thorough introduction to cyberspace, its conflicts and actors. "Inside Cyber Warfare" [12] by Jeffrey Carr gives some good insights into the specifics of the major cyber-events that occurred between 2002 and 2009. The series of books including "Access Denied" [17], "Access Controlled" [16], and "Access Contested" [15] edited by Ron Deibert et al. gives a comprehensive view of the ongoing struggle for control of cyberspace, and the resistance it meets in many parts of the world. The anthology "Cyber Power and National Security" [32] edited by Kramer et al. of the National Defense University consists of a collection of two dozen papers on policy issues, governance, theories, and trends related to cyberwarfare that are relevant in order to understand the perspectives of the U.S. and NATO.

When considering the most influential paper authors in the area, Professors John Arquilla and Dorothy E. Denning, both at the department of Defense Analysis at the Naval Postgraduate School, have written several frequently cited papers about cyberspace security and conflict since the mid-1990s [4][5][18][19]. Regarding the evolving nature of cyberconflict and cyberwarfare, one of the more productive contemporary authors is James A. Lewis, senior fellow at the Center for Strategic and International Studies [34][35][36][37]. Professor Ron Deibert director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto, has contributed to the understanding of how power is exercised in cyberspace through several books and publications [14][15][16][17]. The use of irregular forces in cyberspace operations has been extensively covered by Dr. Rain Ottis of the NATO Cooperative Cyber Defence Centre of Excellence, Estonia [48][49][50].

3. Definitions and principles

The use of various types of cyber-related actions during an armed conflict is inevitable, but what is an actual cyberwar, what will it look like and under what circumstances will militaries use cyberattacks? In media, as well as in various

government reports and even scientific papers, one can read about cyberwarfare, which includes a broad range of malicious actions in cyberspace. The identities of those who engage in these activities are usually vague, and their intent is most often ambiguous. However, this uncertainty about attacker and motive does not justify a similar imprecision in describing the performed actions, the method of execution and the consequences. It is unconstructive and misleading to label every "bad thing" happening on the Internet as "cyberwarfare" or "cyberterrorism," and this type of imprecise nomenclature hampers serious discussion on the subject, if the terms are not properly defined.

The thresholds for an attack in cyberspace, or an all-out war, should not be much different than those in the physical world. We can thus reduce imprecision by clearly separating the different kinds of malicious activities in cyberspace from one another, and defining the probable outcomes of these activities more carefully. In order to refine discussion, the following definitions are offered;

Cyberspace is the global, virtual, ICT-based environment, including the Internet, which directly or indirectly interconnects systems, networks and other infrastructures critical to the needs of society.

Cyberactions are a collection of predominately illegal activities in cyberspace, carried out by non-state actors, causing damage or disruption, in pursuit of various political, economic or personal goals.

Cyberspace operations are military activities employing cyberspace capabilities in order to achieve strategic objectives or effects in or through cyberspace.

Cyberattacks are a subset of cyberspace operations employing the hostile use of cyberspace capabilities, by nation-states or non-state actors acting on their behalf, to cause damage, destruction, or casualties in order to achieve military or political goals.

Cyberwar occurs when cyberattacks reach the threshold of hostilities commonly recognized as war by the international community and as defined by international law.

The definitions above should not be seen as definite, and are primarily given as a basis for further use in this paper. They consist of incrementally improved versions of, and in part, amalgamation of several previous definitions [65][11][7]. While the first four definitions are relatively straightforward and easy to deduce, the concept of cyberwar is still somewhat elusive. One might reason that cyberwar is simply warfare in the cyberspace environment. However, this interpretation turns out to be an unhelpful oversimplification. As an example, the bombing of an Internet exchange point – an important infrastructure hub in which communications links of Internet Service Providers are interconnected in order to exchange data flowing between their respective customers – does not by itself meet the criteria of constituting cyberwar. Neither does defacing a government website or unleashing a massive distributed denial-of-service attack (DDoS), such as the ones directed towards Estonia in 2007 (at least not unless the attacks were sufficiently extensive and prolonged to have an effect similar to that of a naval blockade on the target country's commerce [56]). Moreover, such a simple definition of cyberwar would ignore the complexity of applying the more fundamental legal aspects of war to cyberspace.

According to the classic Clauswitzian perception, war is "nothing but a continuation of political intercourse, with a mixture of other means," and "an act of violence intended to compel our opponent to fulfill our will." [13] The use of violence, or the threat of violence, requires the use of force, which in turn involves inflicting physical harm or exercising coercion [35]. International law addresses the concept of "act of war" in terms of a "threat or use of force," in accordance with the wording of the United Nations (UN) Charter [63]. A determination of what is a "threat or use of force" in cyberspace must thus, as in the physical world, be made in the context in which the performed actions occurs, and it involves an analysis by the affected states of the effect and purpose of the actions in question [62]. Certain

actions conducted in cyberspace on a regular basis could probably constitute acts of war according to the UN Charter, and consequently allow legitimate use of force in self-defense. However, if the actions do not include violence, or the threat of violence, they cannot be defined as attacks.

Discovering that your network has been penetrated, your computer's security mechanisms circumvented, and that valuable or sensitive information has been compromised, as in the case of the previously mentioned GhostNet, could be intimidating to say the least. It is, however, important to differentiate between covert cyberspace operations that entail the use of force or violence, such as manipulating the chemical concentrations of a major water treatment plant, and pure cyber espionage. If the malware used for illicit information collection is intended to go undetected, and if the exploit does not cause any damage, destruction, or casualties, it cannot be considered to be intimidation, the use of force, or a cyberattack (according to the previously given definition). Nevertheless, there is still a quite extensive gray zone in cyberspace operations, especially when considering disruptive actions, and drawing the line when disruptive actions rise to the level of use of force, which could legally constitute cyberwar without actual cyberattacks [7].

Cyberwarfare will likely involve a plethora of actions, ranging from attacks to critical infrastructure, inflicting physical damage and casualties, to disruptive and psychological actions, bordering to the wider concept of information warfare, creating uncertainty and doubt among the opposing forces and its political leaders. The stand-off nature of cyberattacks allows for striking tactical as well as strategic targets from large distances, using comparatively inexpensive technology. However, there are simultaneously some considerable disadvantages of using cyberattacks. A major drawback is the lack of control and estimation of collateral damage in the targeting process, especially when comparing to conventional kinetic attacks. The complex, interdependent nature of cyberspace makes it hard to evaluate if a cyberattack disabling a certain military network could also entail extensive unintended consequences to non-combatants, civilians, neutrals, or

possibly even the attacker himself. This unpredictability creates significant political risk as unexpected collateral damage carries the danger of conflict escalation, may weaken the legitimacy of one's cause in the eyes of the international community, can generate negative domestic reactions, and reinforce resistance in the targeted country or equivalent body. These disadvantages will likely constrain nation-states' use of cyberattacks.

A way of resolving the aforementioned political backlashes of cyberattacks, besides exploiting the covert nature of cyberspace to circumvent attribution, is the employment of non-state actors in cyberspace operations. Some of the most common actors in cyberspace are discussed in the following section.

4. Actors in cyberspace

Cyberspace is a global domain, available for almost anyone with access to a computer with an internet connection, a smartphone or any other type of uplinked multimedia device. In this domain many different actors exist in parallel, with varying needs, goals and intentions. Some act alone, others in loosely connected networks or more formal structures. The roles may also vary depending on the situation, and may overlap. Actors can move between categories over time and depending on their current aims and goals.

1989	**The WANK worm** An infiltration of NASA's computer network in protest of nuclear weapons and the use of radioactive plutonium to fuel the Galileo probe's booster system.
1995	**The Strano Network sit-in** A "netstrike" strike action directed against French government computers to protest policies on nuclear and social issues.
1998	**UrBaN Ka0s hackings** Defacement of Indonesian government web sites focusing on the oppression of the people of East Timor.
1998	**Electronic Disturbance Theater's "Web sit-ins"** Denial-of-service attacks against the web sites of the Pentagon and Mexican government in support of the Zapatistas.
1999	**Team Spl0it anti-war hackings** Web defacement calling for an end to the Kosovo conflict.

Table 1. Early examples of non-state "hacktivism" cyberactions.

Besides all positive things cyberspace has begot, it has simultaneously been a medium used in conflict for more than two decades. In cyberspace, rivaling hacker gangs actively confront one another, protest groups voice their opinions through virtual vandalism, criminal organizations disseminate malware in pursuit of easy profits, and shady actors engage in illicit intelligence gathering. As shown in Table 1, early instances of cyberactions (see previous definition) date back to late 1980s, and continue on during the 1990s. However, none of these were committed by governments or were clearly tied to state-level conflicts. Rather, they were committed by non-state groups quarrelling with their own kind and with international governments.

Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decisionmakers or innocent victims	Protests via web page defacements or DDoS attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDoS for blackmail
Corporations	Financial gain	ICT-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

Table 2. Main non-state actors in cyber conflict.

During the late 1990s, when access to and use of Internet had become

commonplace, physical-world conflicts triggered many state-targeted cyberactions, primarily conducted by non-state actors. Hackers with nationalistic tendencies aimed their cyberactions against foreign countries, commonly in support of their domestic governments, which could be seen at several occasions during the Kosovo conflict. For example, a group of Serbian-based patriot hackers known as Black Hand (named after the pre-World War I Serbian military society) defaced a Kosovo Albanian website and threatened to sabotage military computers of NATO countries [18]. Similar hacker groups from China targeted various U.S. websites after the Chinese embassy in Belgrade was accidently bombed during airstrikes in May 1999 [4]. The Kosovo conflict came to be characterized, by some, as the "the first Internet war" [18], although others conflicts, such as the Iraq War [27] and the Estonia attacks [45] have later also been awarded the same epithet. In the case of the Kosovo conflict, its label as an "Internet war" was given in recognition of not only the actual cyberactions, which per se do not meet up to the requirements of being actual acts of war, but also to reflect the broader role played by the Internet in spreading information about the conflict to the general public.

During the first decade of the 21th century, cyberspace itself progressively came to be a source of major conflict. The areas of dispute were closely tied to the nature of cyberspace and the use, and misuse, and control of information within its domain. The conflicts involved disagreement on subjects such as intellectual property right and file sharing, the limits of free speech, the balance between privacy and security online, and Internet governance and net neutrality [16]. Cyberspace can facilitate and accelerate all types of clashes stemming from the physical world, from street protests coordinated through social media to full-scale wars where cyberspace is leveraged to disseminate information to the warfighter as well as to the general public in promotion of ones cause. As a target of conflict, both the infrastructure of cyberspace, and the resources of its users, are exposed the consequences of these conflicts [36].

Some of the most common cyberspace actors are defined in Table 2, grouped in categories by motivation, target in focus, employed methods, and exploited attack vectors. They are further elaborated on below.

4.1. Ordinary citizens

The most common actor in cyberspace is, quite naturally, the ordinary citizen, using the Internet for various lawful purposes, such as browsing the web and using online services. In this category one will find home end-users as well as employees of companies, organizations or governments, with the common trait that their actions and motives are purely individual, and mostly benign. When it comes to cyberactions this actor category is mostly passive, or acts indirectly, e.g. as a "zombified" victim of a botnet (a collection of Internet-connected computers whose security defenses have been breached and control ceded to a malicious party), or as a more conscious actor voluntarily letting own resources be used by others in a cyberaction.

4.2. Script kiddies

Script kiddies can be said to be the vandals, or perhaps graffiti artists, of the Internet. It is a quite derogative term, commonly used to describe someone with an inferior knowledge of programming or security technologies, expressing a juvenile or an immature behavior. The competence of the individual script kiddie may of course vary, but in general it is the person's devotion (or rather lack thereof) that is defining. A script kiddie does not want to spend a long time to fully understand how "hacking" really works, but is rather in it for the quick rewards and the bragging rights, motivated by short-term ego-gratification. If access to a web server is obtained, a script kiddie will usually seize every opportunity to deface its web pages, later showing off the achievement in a common Internet Relay Chat (IRC) channel, on Twitter, or a similar social forum.

The typical script kiddy searches for existing, frequently well-known and easy to find malware, pre-made scripts, or more advanced security auditing and penetration

testing tools (such as Metasploit [41]) that they can use to identify and exploit weaknesses in remote computers, networks or other resources in cyberspace. At first glance this actor category might seem relatively harmless, but unfortunately they can and will do real damage to any network or computer resource they gain access to. The damage is also indiscriminate, often random and with little care, or even understanding, of the potentially harmful consequences. No difference is made between attacking assets belonging to a large government agency or that of a small business owner.

4.3. Hacktivists

Hacktivism is the use of cyberspace resources, in legal or (perhaps more commonly) illegal ways, as a means of general protest or to promote an expressed ideology or a political agenda. Hacktivism can also, indirectly, be used as a method to reach underlying, hidden political, military or commercial goals. Tools used by hacktivists include web site defacements, internet resource redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins and various forms of cyber- sabotage. Hacktivists can, in some sense, be seen as a cyberspace equivalent to Greenpeace activists or other groups carrying out acts civil disobedience.

The loosely associated “Anonymous” collective is many times seen as an archetype of a hacktivist actor [47]. It consists of a mixed group of people, ranging from script kiddies to professional black hats (see below), connected through a variety of non-mainstream social networking services such as the anonymous “4chan” and “711chan” forums, the “Encyclopaedia Dramatica” wiki and specific chat channels in the IRC network [8]. They have taken responsibility for several significant, widely publicized cyberactions in recent years, gaining them widespread attention [39]. These attacks include the “war” on Scientology, various support actions during the Arab Spring, and attacks on companies such as Louis Vuitton, Sony, Mastercard and U.S. government websites.

Although hacktivists are generally thought to be ethically motivated, their activities span many political ideals and issues. Hacktivist collectives have sometimes been described as a flock of birds, where at any given moment more birds can join, leave, or peel off in another direction entirely. Individual members of a hacktivist collective can thus have varying loyalties, and simultaneously be part of other actor formations.

4.4. Hackers

Hackers are people with deep knowledge and thorough understanding of computer technology, and how computer hardware, software and networking interact. They are commonly concerned with subtle details of operating systems, algorithms and system configurations. Hackers are generally thought of as an elite collective of well-trained and highly ambitious people, spending large parts of their lives in front of computer monitors. They may be motivated by a multitude of incentives, such as curiosity, economic gain, political agendas, attraction to technical challenge, or pure boredom. Although the term "hacking" has broadly come to denote any type of illegal computer-related activities, the original term only described a general technical aptitude, whereas the epithet "cracker" was given to hackers with a malicious intent [38]. However, contemporary categorizing of hackers by intent and motivation is usually done by "hat color". Depending on their motives, hackers are sub-categorized into black-hat hackers, white-hat hackers, and grey-hat hackers.

Black-hat hackers are the malevolent types of hackers originally dubbed "crackers". They are people who exploit computer systems and networks for their own benefit. For example, they may hack into an online store's computer system and steal stored credit card numbers. They may then use the stolen information to purchase merchandise, technical equipment or sell the credit card numbers to a third party. Black-hat hackers are commonly viewed as the most malign actors in the hacker sphere, acting without respect for the law or the result that their actions may result in for their victims.

White-hat hackers, or "ethical hackers", are hackers who have high moral standards, relative to common societal norms. They specialize in penetration testing and validation methodologies in order to ensure the security of an organization's information systems, and are commonly employed by government agencies or by companies specializing in information security consulting. White-hats commonly alert and advise software vendors of the vulnerabilities that they discover, so that they may be patched.

Gray-hat hackers are hackers who conform to white-hat standards most of the time, but who may also wear a metaphoric black hat once in a while. For example, if their interests are targeted by an attack, they might opt to take the matter into their own hands, rather than to report the incident to proper law-enforcing agencies. Grey-hats may also either consciously or inadvertently violate the law in an effort to study or improve system design and security.

4.5. Patriot hackers

Patriot hackers are hackers whose main motives are to aid or support one's own nation-state in an ongoing real-world conflict or war, by carrying out various disruptive actions in cyberspace directed towards the enemy of the state. Chinese hackers have traditionally been especially inclined toward patriotic hacking [30]. Known as the "Red Hacker Alliance" or the "Honker Union of China", they have published an open manifesto, expressing their patriotic mission [1]. Several cyberactions undertaken by these groups have been two-way "hacker wars" between the Chinese-based hackers and their antagonists in other countries.

Russia has also been home to an active patriot hacker collective. This became evident during the 2007 denial-of-service attacks targeting Estonia [19], in the wake of the Soviet-era war memorial relocation controversy, and again in 2008, when Georgia was the target of similar attacks in conjunction with a conventional military confrontation with Russian forces [49]. Russian patriot hackers were also implicated for several web defacements during the 1999 Kosovo conflict, such as

those previously mentioned above, and for various cyberactions against Israel, Chechnya, Belarus, Kyrgyzstan, and others during the past decade [31].

4.6. Cyber insiders

Cyber insiders are actors who have legitimate access to computer and network resources, including information residing in associated systems, but who are disloyal to their employer, hiring party or constituent, and are willing to betray them for monetary benefits or other reasons. The cyber insider may plant logical bombs or open backdoors in programs they help develop, or steal sensitive data by use of small, portable and easily concealed storage devices. They may act as script kiddies in the sense that they attack internal resources to provoke a reaction from the employer, to enact personal vendettas, or as a cyber-espionage agent to collect and publicly disclose classified information or to sell corporate secrets to a competitor or foreign intelligence agency. Studies have shown that although the proportion of security incidents related to cyber insiders have decreased, the financial impact and operating losses due to insider intrusions are increasing [25].

The cyber insider threat is unlike other vulnerability based attacks in that the action taken by the initiator is not based on unauthorized access, but rather by authorized access by authorized objects (people or system processes), within the organizations security boundary. Any illicit actions instigated by a cyber insider will thus not be perceived as anomalous by intrusion detection systems, logging or expert systems, making them highly difficult to mitigate. The U.S. Defense Advanced Research Projects Agency (DARPA) has an ongoing project called CINDER (an abbreviation for “The Cyber Insider Threat”) [60]. This project aims to combat such insider-induced intelligence leaks as the so-called “Afghan War documents” and the diplomatic cables of “Cablegate”, which were publicly disclosed to media outlets by Julian Assange and Wikileaks [24].

4.7. Cyber terrorists

Terrorists are extremists who do not hesitate to make use of extreme means, such as brutal violence towards the innocent or mass destruction of public property, in pursuit of their political goals or ideological agendas. Cyber terrorists are terrorists who use computer and network technologies to carry out their attacks and cause public fear. Cyber terrorism has been a much debated topic during the last few years. It has also been a rather emotionally charged subject, in which expert opinions on the realism of the threat have been divided. Some experts claim that cyber terror is one of our times most potential and alarming dangers [59][6], whereas others mean that the fear of cyber terrorism has been greatly exaggerated and is largely blown out of proportion [53][68], perhaps at the expense of more plausible and possible cyber problems [23].

There have not yet been any reported cases of cyberterror attacks, and it has been argued that cyberterrorism does not exist [34]. In reports that have been published on cyber terrorism, the so-called terrorists are regularly “ordinary” hackers, or other actors, mistaken for terrorists [68]. However, if terrorists would manage to conduct such attacks in cyberspace, the consequences might be significant and thus cannot completely be ignored.

4.8. Malware authors

Malware authors can be seen as a form of specialized black-hat hackers, who develop original software for antagonistic or criminal purposes. They are usually relatively highly skilled in computer programming and especially knowledgeable of methods to evade detection by common antivirus, anti-spyware and spam-filtering software. There are, however, less sophisticated malware authors, who utilize readily available malware “creation kits”. These frameworks allow for the creating of customized malware by choosing from a set of available delivery methods, payloads and means of propagation [52]. Creators of malware using such

means are usually grouped into the same category as script kiddies, as utilizing these tools does not require any specific programming skills.

4.9. Cyber scammers

Scammers are usually considered to be the least skilled actors in cyberspace. The ordinary cyber scammers are similar to the real-world, analog counterparts, but instead employ information technology to defraud their victims. These scammers commonly make use of random spamming, trying to get the attention of victims by advertising fake lottery winnings, a recently discovered large inheritance, or a job offering with an unreasonably high salary, while masquerading as a trustworthy entity. This approach is sometimes called “phishing”, a term influenced by the related term “phreaking”, a portmanteau of the words phone and freak. Phishing refers to the use of tempting “baits”, in hopes that the potential victim will be tempted to “bite”, and thus fall for the scam. The motives of cyber scammers are almost universally pure economic gain, by deceiving the ones who respond to the scams into disclosing credit card details or other valuable information. However, there are more sophisticated and subtle scammers who target their victims carefully, perhaps after analyzing lists of stolen bank statements, open source intelligence gathering of personally identifiable information. This type if scam, sometimes called “spear phishing”, includes the use of advanced social engineering schemes to separate the victims with from whatever items of value that they may have.

4.10. Organized cybercriminals

Organized crime in cyberspace can, in some sense, be seen as the analog of its counterpart in the real world. However, the borderless and anonymous nature of cyberspace allows otherwise unassociated individuals in different parts of the world to connect and form criminal networks sharing a common goal or interest [64]. Some further, significant differences between cybercrime and its real-world equivalent include the immature status of cyber law enforcement, the low

thresholds for entry into “market”, and the easy access to large groups of potential targets. These factors all contribute to facilitate the work of organized cybercrime syndicates.

Many of the activities defined in this paper as cyberactions are deemed illegal by national legislation as well as international treaties, including the previously mentioned phenomenons hacking, scamming and executing denial-of-service attacks. There are, however, also many other types of problematic crimes committed in cyberspace, such as identity theft, harassment, extortion, child pornography and human trafficking. Of all these criminal activities that occur in cyberspace, some 80 percent are estimated to originate in some form of organized activity [40]. These groups tend to be quite small, commonly consisting of less than a dozen people, are more loosely structured than groups involved in other forms of organized crime, and include members that are older and less tech-savvy than commonly believed [40][64].

Although cybercrime may be committed from any part of the world, certain regions have been implicated as particularly active cybercrime hubs, including Eastern Europe and West Africa [64]. Organized cyber criminals are usually motivated by money and power, i.e. significant economic return on invested resources, and acquiring control of the market. However, another explanation for regions such as the above mentioned having a high degree of organized cybercrime could be that in areas where unemployment rates are high and salaries are low, previously lawful citizens with sufficient technical skills turn to organized cybercrime as a way of leveraging oneself out of poverty [28][9]. Since cybercrime in many cases has shown to be highly lucrative, and most developing countries are not actively or efficiently sanctioning these actions, cybercrime is seen as a viable, and sometimes even commended, career path.

Organized cybercriminals, as in other organized crime generating large revenues, may many times have the potential to be on even footing with even the strongest enemy, such as law enforcement agencies and nation states when it comes to

available resources. The profits are in some cases truly immense. According to a study made by the security company Sophos, cybercriminals in Brazil managed to steal $900 million during 2010 [58]. When considering the cost of cybercrime on a global scale, the anti-virus software company Symantec has estimated it at staggering $114 billion. It is thus "significantly more than the annual global market for marijuana, cocaine and heroin combined [54]."

4.11. Corporations

Corporations acting in cyberspace are usually thought to be law-abiding entities, as serious transgressions may lead to sizeable economic sanctions or even personal accountability for key officials within the organization. This fact is normally what separates the corporation from an organized crime syndicate, since they both share the motives of economic profit and market control. Corporations carrying out acts in cyberwarfare are thus usually doing so at the request of a nation-state, either by being on a government contract or by more autonomous actions under the government's blessing [21]. Intelligence agencies may also use corporate fronts as a cover for cyber espionage operations [2]. Large international corporations doing business in many different countries may find themselves in a precarious situation during a cyberconflict, finding themselves on both sides of the front line. An example of this is Google's Chinese subsidiary, which in 2010 was permanently moved from Mainland China to Hong Kong, after Chinese-originated cyber-attacks against Google and other U.S. corporations was discovered [22].

4.12. Cyber espionage agents

The concepts of intelligence and espionage are closely related. While intelligence gathering in general is not considered to be illegal, the subset of actions that fall within espionage is commonly deemed to be crimes under the legal code of many nations. Espionage involves obtaining classified or sensitive information without the permission of the holder of the information, and can be committed by an agent in employ by military forces of a certain country, a government institution, a

commercial corporation, a criminal organization or by an individual acting autonomously [33].

In cyber espionage, agents make use of cyberspace resources for intelligence collection. They intercept information that passes through, or resides in, computer networks or computer systems of special interest, by using cracking and infiltration techniques, software and hardware tools for surveillance, or other similar approaches. The gathered data is analyzed and utilized in the preparation of intelligence reports for the commissioning entity. Cyber espionage may also entail the collection and analysis of open source information, publicly available on Internet web pages or via social media networks such as Facebook, Twitter, blogs, discussion boards and forums.

Whether the purpose of the cyber espionage is military, political or economic, a distinction that can be made between cyber espionage agents and other actors, such as cyber criminals, is that the former act lawfully or with the tacit approval of a sponsoring nation-state, at least in relation to the laws of that state. In some views, cyber espionage is regarded as a necessary part of global economic competition, and monitoring of cyber capabilities of adversaries is considered to be essential to national security [70]. Although cyber espionage agents are commonly associated with national intelligence agencies, military units or similar organizations tied to nation-states, cyber espionage agents can also act autonomously, as rogue entities.

4.13. Cybermilitias

A cybermilitia may be defined as a group of volunteers who are willing and able to use cyberattacks (or perhaps disruptive cyberactions as defined in this paper) in order to achieve a political goal [49]. They utilize a common communications channel, such as an Internet forum or a social media service, and take measures to hide their true identities. Furthermore, it is understood that members of a cybermilitia do not get any monetary rewards for their services, nor are they bound by any contractual obligation [49]. Regular military cyber-units, or a national cyber

reserve forces, are in this context not considered to be cybermilitia, although they could consist of “cyber mercenaries”, actors who take part of military actions in cyberspace essentially by the desire for private gain, or people who are part of a cybermilitia in their spare time. The members of a cybermilitia are either loosely connected in real life, or completely lack away-from-keyboard relations to one another.

The involvement of civilians in recent cyber-conflicts has created a sizeable gray area between hacktivists, political hackers and legitimate combatants backed by nation-states. The debate has been fierce concerning if these people are individual and independent actors, motivated by political or nationalistic goals, or participants in covert government-orchestrated campaigns with the purpose to further the strategic political or military objective of the instigating state [3]. Most cases of politically motivated cyberactions that have occurred during recent years have been attributed to unidentified radical hackers, or hacktivists. Such actions have ranged from mere annoyances, e.g. the defacement of websites in Japan in reaction to new anti-piracy legislation [51], to full-scale digital blockades of the target country. In cases such as the attacks on Estonian cyberspace resources in 2007, an intense debate continues as to whether the attacks were instigated by a nation-state, if they were the work of independent patriot hackers defending their country’s honor, or if an organized cybermilitia was responsible [50][3].

As cyberattacks can be launched by proxy, using trojanized unsuspecting end-users’ computers, proving whether nation-states are engaging in cyberwarfare is naturally difficult. Cyber-militias have been suspected of performing several recent high-profile cyberactions that were, at least in part, sanctioned by nation-states. The list of nations engaging in political hacking includes Iran, Turkey, Israel, and North and South Korea [3]. Two examples of nations involved in these types of attacks are the People’s Republic of China and the Russian Federation. Both of these countries are rapidly building cyberwarfare capabilities, and have developed large bodies of doctrine and technology in support of this new concept [12].

5. Employing non-state actors in cyberspace operations

As cyberspace, unlike other arenas associated with warfare, provides a high level of anonymity, attackers can carry out actions in this domain with little or no risk of attribution. Nation-states thus have little or no incentive to support a legally binding definition of cyberwar, which would limit their freedom of action, or to formally take responsibility for executed cyberattacks. Furthermore, cyberattacks can be carried out inexpensively, and can, at least in theory, cause extensive damage or at least trigger severe disruptions to ICT-based services. In addition, if a nation-state can covertly initiate, fund, or control such attacks, relying on non-state actors to carry out the attacks in their stead, they can reduce the already low risk of political implications, and potentially achieve their objectives without the burden of adhering to the Law of Armed Conflict. This gives an attacker a tremendous asymmetric advantage, especially for smaller nations that cannot prevail on a kinetic battlefield. As a result, employment of non-state actors in cyberspace operations is likely a very attractive option for nation-states or an equivalent body, especially when pursuing limited strategic goals.

Benefits	Drawbacks
Gaining the initiative – element of surprise	No direct control of non-state actors
Plausible deniability	Risk of unintended collateral damage
Can choose target and attack vector	Targeting of own resources
Determinate scale and duration of attack	Escalation to conventional war
Exploit legal uncertainties	Labeling as sponsor of terrorism
Possibility of rapid attacking-by-proxy	Backlashes (blackmailing etc.)

Table 3. Benefits and drawbacks of using non-state actors in cyberspace operations

Some of the main "pros and cons" of engaging in cyberwarfare, and employing non-state actors in the associated cyberspace operations, has been summarized in Table 3 above. The benefits and drawbacks are also further explained and motivated below.

5.1. Benefits

- The attacker gains the initiative and can most often conduct cyberattacks covertly, offering the advantage of surprise as well as the benefit of plausible deniability. By being the one who initiates the attack, the defender is forced to respond, often in a predictable way.

- The attacker can launch the cyberattack at the exact time, and against the target, of their own choosing, using appropriate attack methods. The attacker may need only a single computer to conduct an attack, whereas the defender must efficiently shield all its cyber-resources, which can be prohibitively expensive.

- The attacker can decide the attack mode, scale and duration in order to cause desired effects. Besides conducting the attacks themselves, they can enlist allies, magnifying both the scale of the attack, and the effects of plausible deniability.

- Even if attribution is successful, i.e. the attacker is identified by the defender, the lack of applicable international laws covering cyberwarfare creates a useful shield of legal ambiguity.

- The attacker can outsource cyberattacks to cyber militias, organized cyber criminals, or mercenary hackers. Although employing non-state actors in this manner might raise suspicion in the international community, the lack of any hard evidence will protect the attacker political ramifications. Thus, the threat of a counterstrike is negligible.

- By recruiting non-state actors from previously identified Internet forums and social networks, rapid mobilization of a considerable, suitably

motivated, and technically competent force can be achieved at little or no cost.

5.2. Drawbacks

- Although the attacker may give directives as to what targets and methods that should be in focus during a cyberattack, the actual control of non-state actors in cyberspace operations can be ineffective, as unacceptable behavior is hard to curb, and ongoing attacks difficult to thwart.

- The attacker risks creating unwanted collateral damage, by hitting unintended targets. Attacks could also grow beyond the intended size and scope. Overly zealous members of cybermilitias, not limited by the restrictions that govern military organizations, could opt to target civilian targets without thought of possible consequences.

- Attacks initiated by non-state actors could affect the attackers network or resources negatively, by overloading common infrastructures, such as Internet backbone connections.

- Even though the laws of war are unclear concerning cyberspace, attacks that are linked back to the initiating nation-state could be politically devastating. Escalation may also lead to retaliation through conventional means [35].

- If cyberattacks are directed against civilian systems, as is most likely in one way or another, the initiating state could be accused of committing war crimes, or being branded as a sponsor of cyberterrorism, becoming pariah as far as international relations are concerned.

- Employing non-state actors can potentially be risky in the long term, even though the immediate attacks are successful, as these might be unreliable. Criminals might try to blackmail a government in order not to disclose sensitive details, and contracted cyber espionage agents might defect to the opposing nation if offered political asylum.

5.3. Legal issues

The legal issues surrounding cyberwarfare are vast, especially when it comes to the frameworks that currently govern state-to-state warfare. Although the main focus of this paper is not to study the quirks and twists of international law in any great detail, it is still relevant to acknowledge the current uncertainties in existing legislation and international conventions, and to observe how this uncertainty affects the employment of non-state actors in state-sponsored cyberconflict.

The use of cyberattacks would likely violate, if not the direct tenets, at least the spirit of the Law of Armed Conflict [67]. That is assuming that such laws are at all applicable to cyberwarfare. Even other, less destructive cyberactions, could probably constitute acts of war according to the UN Charter [56], and consequently allow legitimate use of force in self-defense. However, as previously established, if the actions do not include violence, or the threat of violence, they cannot be defined as cyberattacks. Because of the prevailing uncertainty regarding cyberspace as a battlefield, it is probably in many nation-states' interest to keep such laws from becoming applicable to cyberwarfare. The reason is that it would be likely be impossible to carry out cyberattacks while remaining within the legal framework. Nevertheless, should new conventions on cyberwarfare be universally ratified, covertly outsourcing cyberattacks to cyber-militias could be a viable option. In any case, the current ambiguity in international law strongly favors the attacker, and does not seem to offer any resort to cyberattack victims.

Another relevant question is if an individual who conducts a cyberattack legally can be considered to be a combatant? According to the Third Geneva Convention there are two types of combatants – privileged and unprivileged [20]. Privileged combatants are members of the armed forces of a party to the conflict who (i) are being commanded by a person responsible for his subordinates, (ii) have a fixed, distinctive sign recognizable at a distance, (iii) carry arms openly, and (iv) conduct their operations in accordance with the laws and customs of war. Most non-state actors, including hackers, criminals, and terrorists clearly do not fall within the

constraints of this definition. It could be argued that state-sponsored cyber-militias, patriot hackers or cyber espionage agents are being commanded by a person responsible for subordinates. However, it is quite obvious that they do not wear a fixed, distinctive sign or carry arms openly. Furthermore, many of their actions could be interpreted as being in direct violation of the laws and customs of war.

In addition, even members of regular military cyberforces might fail to meet the requirements of the Geneva Convention. Although they are afforded privileged combatant status when engaged in conventional hostilities, conducting cyberattacks could potentially deprive them of that status. While members of regular armed forces might be wearing uniforms when conducting a cyberattack, the victims of their attack will not be able see it. Carrying arms openly is also quite unlikely as most cyberattacks are, if at all detectable, virtually impossible to track to their original source. Combatants who engage in actions that violate the laws of war, such as deliberately targeting civilian resources, automatically lose that privileged combatant status. At least in theory, this precludes using commercial infrastructure for delivery of cyberattacks. Whereas privileged combatants are entitled to treatment as a prisoner of war, unprivileged combatants might be subject to punishment under the civilian laws of the detaining power.

As the risk of capture is very unlikely in cyberwarfare, incentives for attackers to adhere to the laws of war in order to gain privileged combatant status must be assumed to be fairly weak. Especially since the victims are oblivious to the combatant status of the one who instigated the attack. This is somewhat similar to other weapons that provide great standoff distances, such as intercontinental ballistic missiles (ICBM) or unmanned aerial vehicle (UAV) drones. However, those weapons usually leave quite obvious evidence of the attacks originating nation, while the anonymity that cyberweapons afford attackers is almost absolute.

Even if an indisputable connection is established between a non-state proxy and a nation-state, such a connection does not legally grant the attacking individuals combatant status. As an example, in the cyber-conflict between Russia and Georgia

of August 2008, plausible evidence linked the "StopGeorgia.ru" website, where attack instructions against Georgian government systems were given, to the Kremlin by way of Russian intelligence services (GRU) and the national youth association "Nashi" [12]. It can thus be argued that the Russian government-commissioned "non-state" hacktivists to accomplish its objectives. Even though the individual hacktivists may have been enjoying backing from a nation-state, they cannot legally be considered to be combatants, but rather as cybercriminals, albeit somewhat doubtfully so.

All in all, the Russian government's employment of non-state actors in the cyberconflict with Georgia demonstrated a usable model for conducting limited-scope cyberattacks. By use of patriot hackers or cybermilitias, recruited through informal channels appealing to nationalistic zeal, the instigating nation-state could escape recrimination while simultaneously, at least partially, reaching its strategic objectives.

6. Discussion

The true nature of cyberwarfare, cyberconflict, and the actors engaging in these activities, has unfortunately been heavily obscured by the frequent use of vague terminology in media and contemporary literature, the employment of sensationalist rhetoric by politicians and corporate proponents, a lack of solid empirical datasets, and a lingering notion that these new concepts are unique in their characteristics, rather than constituting yet another set of new and improved technologies applied to the art of war. The goal of this paper has been to study the various non-state actors who coexist in cyberspace and their employment by nation-states in cyberspace operations. The distinctions between these actors may perhaps appear somewhat artificial. Boundaries between, for example, script kiddies and hacktivists, between cybermilitias and patriot hackers, or between cybercriminals and cyberespionage agents, may admittingly be somewhat blurry. Similarly, individual actors can of course participate in multiple activities. However, the distinctions between the actors are useful for analytical purposes.

Although the imminent threat of an all-out cyberwar is not very likely, the prospect of bringing warfare to the cyber arena nevertheless promises significant asymmetric advantages to a limited resource nation-state, especially if the attacker can remain anonymous. Moreover, if the instigating nation covertly employs cybermilitias and hacktivists to carry out cyberattacks, this will provide an efficient shield against subsequent blame and political ramifications, while simultaneously allowing strategic political objectives to be achieved. If traced to the source, such attacks will legally be seen as criminal activity, possibly even in the unlikely scenario where comprehensive and irrefutable evidence can be provided, linking the nation-state and the attacker, as blame can always be passed around.

Nation-states have little incentive to openly take credit for cyberattacks. Doing so could lead to political or military recrimination, and might expose individuals to criminal prosecution if their responsibility for committed illicit actions was deemed to be against the laws and customs of war. While some nation-states might favor ratifying a novel legal framework defining acts of aggression in cyberspace, it seems likely that many others would find it far more beneficial to maintain the current ambiguity that surrounds cyberwarfare, and perhaps even actively undermine such efforts, as the asymmetric nature of cyberwarfare benefits those who lack the ability to dominate in conventional arenas. Even if the international community were successful in codifying cyberwarfare into alignment with international law, and thereby implement limitations of its use, it would probably still not be very effective as the employment of non-state actors in cyberspace operations is still in effect a gray area.

Due to these asymmetric advantages that may be leveraged in cyberspace, this arena will likely grow in importance over the coming decades as the Internet becomes even more pervasive throughout developing countries of Asia and Africa, and the critical infrastructures of these countries evolve. Politically motivated cyberactions will likely escalate in both frequency and scale, and attribution for these acts is likely to remain infeasible because of the anonymity the Internet

provides. As the number of global Internet users grows, problematic cyberactions related to such actors as cyber scammers and script kiddies are also like likely to increase. The fact that there are quite a lot of people in this category, namely those interested or curious about exploiting cyberspace resources for private gain, in combination with the amount of readily available tools for security vulnerability exploitation, and the generally low awareness of how to establish adequate information security in society, makes these users more than a nuisance.

An interesting question is what it would take for the nation-states that currently dominate use and development of cyberspace to intervene in reaction to this trend. Whereas attacks such as those previously mentioned, directed at Estonia and Georgia, have primarily resulted in discussion, it is conceivable that an extensive and damaging attack conducted against a nation-state, such as a cyberterror attack, could motivate the international community to create a legal framework to address this issue, or incite a rapid technical development that would limit or prevent future attacks.

Given that the response to an extensive cyberterror attack would follow the same reaction logics as a conventional terror attack, it is fair to assume that the response would also be of a similar nature, resulting in an overall heightened security posture, and possibly also retaliation against those thought to be responsible or in plausible support of the attacks. We might also begin to see the erection of virtual walls, formation of controlled cyber borders and stricter logical or physical separations of cyberspace domains. If the cyberterror attack was serious enough we might even see the end of the Internet as we know it today, and the creation of a replacement with a more rigorous and fundamental security design. One such proposed scenario is “cyber-balkanization” [29], referring to the splintering of the Internet into subnets for specific functions such as critical infrastructure management or internal government communications. While that scenario is fiercely opposed by the advocates of “net neutrality” [69], others call for the creation of a new secure Internet infrastructure to reduce the threat of cyberattacks

[57]. If this theoretical development would be for the better or worse can thus surely be debated at lengths.

7. Conclusion

Although cyberspace conflicts are predominately a non-state activity, they are drawing the attention of those who wish to leverage them to promote their own purposes. Cyberconflicts can be seen as a mirror of their real-world counterparts, but also increasingly as completely independent disputes, clashes, attacks and perhaps acts of war in an emerging arena. In most cases, as we have seen, cyberactions involve various non-state actors. However, the overlapping gray-zone between these actor categories and legitimate state-backed cyberwarriors are a source of concern since no legal definition of cyberwarfare, or agreement on what constitutes an "act or war" in cyberspace, currently exists. It also seems unlikely that such conventions will be forthcoming in the immediate future, creating a window of opportunity for resource-limited actors who cannot prevail on a kinetic battlefield.

The covert or overt employment of non-state actors in cyberspace operations, as volunteers in state-to-state conflicts, cybermilitas, cyber-mercenaries or organized cyber-criminals raises many new questions, and is an interesting trend which deserves further study. Although there have not yet been any concrete instances where cyberactions, or cyberattacks, have resulted in physical injury or extended destruction of property, the heavy cyber-dependency of modern western countries makes more damaging cyberattacks plausible or even probable in future scenarios. Finding ways to mitigate these types of hazardous events, before they evolve into real threats to national security, are thus an increasingly pressing issue for academia, as well as practitioners, involved in the study of cyberdefense.

As the ongoing "War on Terror" is slowly coming to an end, focus increasingly seems to be shifting towards the cyber arena. Terrorism as a phenomenon is most certainly not eradicated, in Afghanistan or elsewhere, and as next-generation will-

be cyberterrorists are growing up with computers and smartphones, the advent of cyberattacks of magnitudes greater than those previously witnessed, could be approaching. In the other corner, the global defense industry is likely picking up the scent of significant military spending coming their way. This makes for an interesting, if perhaps somewhat disquieting development in the coming years, where one could probably only hope for a balanced and sensible approach from all involved actors.

References

[1] Amorosi, D., "Chinese State of Denial," Infosecurity, Vol 8 Issue 6, Elsevier, Nov.-Dec. 2011.

[2] Andress, J. and Winterfeld, S., "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners," Elsevier, 2011, p. 199.

[3] Applegate, S. D., "Cybermilitias and Political Hackers: Use of Irregular Forces in cyberwarfare," IEEE Security & Privacy, Volume 9, Issue 5, Sep.-Oct. 2011.

[4] Arquilla, J. and Ronfeldt D. F., "Networks and Netwars: The Future of Terror, Crime, and Militancy," RAND Corporation, 2001.

[5] Arquilla, J. and Ronfeldt, D., "In Athena's Camp: Preparing for Conflict in the Information Age," RAND Corporation, 1997.

[6] BBC News, "US prepares first-strike cyber-forces," BBC News Technology, Oct. 12, 2012. Available: http://www.bbc.co.uk/news/technology-19922421

[7] Beidleman, S. W., "Defining and Deterring Cyber War", Strategy Research Project, U.S. Army War College, Jan. 2009.

[8] Bernstein, M. S., Monroy-Hernández, Harry D., Andreé, P., Panovich, K. and Vargas, G., "4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community," In Proc. Fifth International AAAI Conference on Weblogs and Social Media (ICWSM-11), Jul. 2011.

[9] Bhattacharjee, Y., "How a Remote Town in Romania Has Become Cybercrime Central," Wired Magazine, Jan. 31 2011. Available: http://www.wired.com/magazine/2011/01/ff_hackerville_romania/

[10] Bradbury, D., "The Spy Who Hacked Me," Infosecurity, Vol 8 Issue 5, Elsevier, Sep./Oct. 2011.

[11] Cabinet Office of the United Kingdom, "Cyber Security Strategy of the United Kingdom," Nov. 25 2011.

[12] Carr, J. "Inside Cyber Warfare," O'Reilly, 2010.

[13] Clausewitz, C. von, “On War”, originally Vom Kriege (3 vols., Berlin: 1832-34), translated by J. J. Graham,Wordsworth Editions Limited, Hertfordshire, U.K., 1997.
[14] Deibert, R. and Rohozinski, R., “Tracking GhostNet: Investigating a Cyber Espionage Network,” Information Warfare Monitor, University of Toronto, Munk Centre for International Studies at Trinity College, Toronto, Mar. 2009.
[15] Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (Eds.), “Access Contested: Security, Identity and Resistance in Asian Cyberspace”, MIT Press, 2011.
[16] Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (Eds.), “Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,” The MIT Press, Apr. 2010.
[17] Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (Eds.), “Access Denied: The Practice and Policy of Global Internet Filtering,” The MIT Press, Apr. 2008.
[18] Denning, D. E., “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”, The Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, Nautilus Institute, Dec. 1999.
[19] Denning, D. E., “Cyber Conflict as an Emergent Social Phenomenon,” Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (T. Hold and B. Schell eds.), IGI Global, 2011.
[20] Diplomatic Conference of Geneva of 1949, “Convention (III) relative to the Treatment of Prisoners of War”. Available: http://www.icrc.org/ihl.nsf/FULL/375
[21] Drew, C. and Markoff, J., “Contractors Vie for Plum Work, Hacking for U.S.,” The New York Times, May 30, 2009. Available: www.nytimes.com/2009/05/31/ us/31cyber.html
[22] Drummond, D., “A new approach to China: an update,” Google Official Blog, Mar. 22 2010. Available: http://googleblog.blogspot.se/2010/03/new-approach-to-china-update.html
[23] Dunn Cavelty, M., “The Militarisation of Cyberspace: Why Less May Be Better,” in Proc. 4th International Conference on Cyber Conflict (CYCON 2012), Tallinn, Estonia, Jun. 2012.
[24] Greenberg, A., “WikiLeaks’ Julian Assange Wants To Spill Your Corporate Secrets,” Forbes Magazine, Dec. 2010. Available: http://www.forbes.com/sites/ andygreenberg/2010/11/29/wikileaks-julian-assange-wants-to-spill-your-corporate-secrets/
[25] Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., Hull, T. D., “Combating the Insider Cyber Threat,” IEEE Security & Privacy, Volume 6, Issue 1, Jan.-Feb. 2008.
[26] Hållén, J. and Dahlin N., ”Undergroundhackare skapade Stuxnet” (Underground hackers created Stuxnet), Ny Teknik, Jan. 19 2011.
[27] Harlan Reynolds, G., “The Blogs of War,” The National Interest, spring issue, Mar. 2004.

[28] Hassan, A. B., Funmi, D. L., and Makinde, J., "Cybercrime in Nigeria: Causes, Effects and the Way Out," ARPN Journal of Science and Technology, Vol. 2, No. 7, Aug. 2012.
[29] Healey, J., "The Five Futures of Cyber Conflict and Cooperation," Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, Special issue, 2011.
[30] Hvistendahl, M., "China's Hacker Army," Foreign Policy, Mar. 3 2010. Available: http://www.foreignpolicy.com/articles/2010/03/03/china_s_hacker_army
[31] Karatgozianni, A., "Blame It on the Russians: Tracking the Portrayal of Russian Hackers during Cyber Conflict Incidents," Digital Icons: Studies in Russian, Eurasian and Central European New Media, Issue 4, 2010.
[32] Kramer, D., Starr, S. H, and Wentz, L. K. (Eds.), "Cyber Power and National Security," National Defense University Press, Washington, D.C., 2009.
[33] Lachow, I., "Cyber Terrorism: Menace or Myth?" in F. D. Kramer, S. H. Starr & L. K. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, Washington, D.C., 2009.
[34] Lewis, J. A. "Cyberwarfare and its impact on international security," United Nations Office for Disarmament Affairs, UNODA Occasional Papers, No. 19, Jun. 2010.
[35] Lewis, J. A., "Cyberwar Thresholds and Effects," IEEE Security & Privacy, Volume 9, Issue 5, Sep.-Oct. 2011.
[36] Lewis, J. A., "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict," Center for Strategic and International Studies, Washington, D.C, Oct. 2009.
[37] Lewis, J. A., "The Cyber War Has Not Begun," Center for Strategic and International Studies, Mar. 2010.
[38] Malkin, G., "Internet Users' Glossary," Request for Comments: 1983, Internet Engineering Task Force, Aug. 1996.
[39] Mansfield-Devine, S., "Anonymous: serious threat or mere annoyance?" Elsevier Network Security, Volume 2011, Issue 1, Jan. 2011.
[40] McGuire, M., "Organised Crime in the Digital Age," research report, John Grieve Centre for Policing and Community Safety, London Metropolitan University, Mar. 2012.
[41] Metasploit. Available: http://www.metasploit.com/
[42] Muñiz Jr., J., "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors," Master's Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, Jun. 2009.
[43] Nakashima, E., "Pentagon to boost cybersecurity force," The Washington Post, Jan. 27 2013.
[44] Netherlands Ministry of Defence, "The Defence Cyber Strategy," Jun. 27 2012.

[45] Nicola, S., “The World's First Internet War,” United Press International, Aug. 6 2007. Available: http://www.upi.com/Emerging_Threats/2007/08/06/Analysis-The-worlds-first-Internet-war/UPI-93861186432610/

[46] O’Leary, A., “Worries Over Defense Department Money for ‘Hackerspaces’,” The New York Times, Oct. 5 2012.

[47] Olson, P., “We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency,” Little, Brown and Company, Jun. 2012.

[48] Ottis, R., “From Pitch Forks to Laptops: Volunteers in Cyber Conflicts.” In Czosseck, C. and Podins, K. (Eds.) Conference on Cyber Conflict. Proceedings 2010. Tallinn: CCD COE Publications, pp. 97-109.

[49] Ottis, R., “Proactive Defense Tactics Against On-Line Cyber Militia,” in the proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010), Thessaloniki, Greece, Jul. 2010.

[50] Ottis, R., “Theoretical Offensive Cyber Militia Models,” in Proc. 6th International Conference on Information Warfare and Security (ICIW), Washington, D.C., USA, Mar. 2011.

[51] Phneah, E., “Anonymous hacks Japanese govt sites,” ZDNet, Jun. 28 2012. Available: http://www.zdnet.com/anonymous-hacks-japanese-govt-sites-2062305268/

[52] Roberts, P., “UK’s top ecrime investigator describes a life fighting cybercrime,” Sophos Naked Security, Sep. 25 2012. Available: http://nakedsecurity.sophos.com/2012/09/25/interview-bob-burls/

[53] Schneier, B., “Threat of ‘cyberwar’ has been hugely hyped,” CNN, Jul. 7, 2010. Available: http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/

[54] Serrano, A. F., “Cyber Crime Pays: A $114 Billion Industry,” The Fiscal Times, Sep. 14, 2011. Available: http://www.thefiscaltimes.com/Articles/2011/09/14/ Cyber-Crime-Pays-A-114-Billion-Industry.aspx

[55] Shane, S., “Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials,” The New York Times, Sep. 26 2012.

[56] Simma, B., “The Charter of the United Nations: A Commentary,” Second Edition, Oxford University Press, 2002.

[57] Sternstein, A., “Former CIA Director: Build a new Internet to improve cybersecurity,” Nextgov, Jul. 6 2011. Available: http://www.nextgov.com/cybersecurity/2011/07/former-cia-director-build-a-new-internet-to-improve-cybersecurity/49354/

[58] Theriault, C., “Brazil’s cybercrime evolution - it doesn’t look pretty,” Sophos Naked Security, Oct. 5 2011. Available: http://nakedsecurity.sophos.com/2011/10/05/brazils-cybercrime-evolution-it-doesnt-look-pretty/

[59] Thibodeau, P., “Cyberattacks an ‘existential threat’ to U.S., FBI says,” Computerworld, March 24 2010. Available: http://www.computerworld.com/s/article/9173967/Cyberattacks_an_existential_threat_to_U.S._FBI_says

[60] U.S. Defense Advanced Research Projects Agency (DARPA), Cyber-Insider Threat (CINDER) program. Available: http://www.darpa.mil/Our_Work/I2O/Programs/Cyber-Insider_Threat_(CINDER).aspx

[61] U.S. Department of Defense, "Strategy for Operating in Cyberspace," July 2011.

[62] U.S. Department of Defense, Department of Defense Cyberspace Policy Report, Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, Nov. 2011.

[63] United Nations Charter, Article 2(4). Available: http://www.un.org/aboutun/charter/

[64] United Nations Office on Drugs and Crime (UNODC), "The Globalization of Crime: A Transnational Organized Crime Threat Assessment," United Nations publication E.10.IV.6, 2010.

[65] United States Department of Defense, "Dictionary of Military and Associated Terms," Joint Publication 1-02, Nov. 8, 2010.

[66] Verizon Business Inc., "The 2012 Data Breach Investigations Report." Available: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[67] Watts, S., "Combatant Status and Computer Network Attack," Virginia Journal of International Law, Vol. 50, No. 2, 2010.

[68] Weimann, G., "Cyberterrorism: How Real is the Threat?" United States Institute of Peace, special report, May 2004.

[69] Werbach, K., "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart," UC Davis Law Review, Vol. 42, 2009.

[70] Wilson, C., "Cyber Crime," in F. D. Kramer, S. H. Starr & L. K. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, Washington, D.C., 2009.

[71] Wittman, G. H., "China's Cyber Militia," The American Spectator, Oct. 21 2011. Available: http://spectator.org/archives/2011/10/21/chinas-cyber-militia

[72] Yoon, S., "North Korea recruits hackers at school," Al Jazeera, Jun. 20 2011. Available: http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html