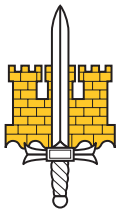


CYBER WARFARE

Editor Jouko Vankka

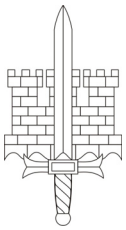
National Defence University
Department of Military Technology
Series 1, No. 34

CYBER WARFARE

Editor Jouko Vankka

National Defence University
Department of Military Technology

Series 1
No. 34



HELSINKI 2013

Prof. Jouko Vankka (ed.): Cyber Warfare
Maanpuolustuskorkeakoulu, Sotatekniikan laitos
Julkaisusarja 1: No. 34
National Defence University, Department of Military Technology
Series 1: No. 34

Most recent publications in pdf-format:
http://www.doria.fi/

Maanpuolustuskorkeakoulu – National Defence University,
Sotatekniikan laitos – Department of Military Technology

ISBN 978-951-25-2455-6 (nid.)
ISBN 978-951-25-2456-3 (PDF)
ISSN 1796-4059

Juvenes Print
Tampere 2013

Preface

A postgraduate seminar series with a title Cyber Warfare held at the Department of Military Technology of the National Defence University in the fall of 2012. This book is a collection of some of talks that were presented in the seminar. The papers address computer network defence in military cognitive networks, computer network exploitation, non-state actors in cyberspace operations, offensive cyber-capabilities against critical infrastructure and adapting the current national defence doctrine to cyber domain. This set of papers tries to give some insight to current issues of the cyber warfare.

The seminar has always made a publication of the papers but this has been an internal publication of the Finnish Defence Forces and has not hindered publication of the papers in international conferences. Publication of these papers in peer reviewed conferences has indeed been always the goal of the seminar, since it teaches writing conference level papers. We still hope that an internal publication in the department series is useful to the Finnish Defence Forces by offering an easy access to these papers.

Editor

Contents

Computer Network Defence in Military Cognitive Networks

Anssi Kärkkäinen
Defence Command Finland
anssi.karkkainen@mil.fi

Abstract

For complex computer networks, the task of configuring the ideal network operating parameters is challenging. In near future, Cognitive Network (CN) is seen as an answer to improve the performance of these networks. CN is defined as a network with a cognitive process that can understands current conditions, plan, decide, act on those conditions, and learn from the results of actions. A key factor in the process of learning is the ability to take advantage of the previous decisions. Cognitive network is seen to have significant benefits in military networks. At the same time, cyber threats have grown tremendously and become a global threat as a result of networked infrastructures. Various technologies and technical solutions are developed to guarantee cyber security on communications networks and the Internet. Traditionally, the Computer Network Defence (CND) capability is mainly based on an individual (technical) security controls with static configurations. At worst, the security controls have been implemented afterwards. Previously, information systems and networks are not typically built in cyber security terms.

This paper presents a new approach to build the CND capabilities from a cognitive process point of view. For this cognitive process, situation awareness (SA) and management is a critical capability. The paper proposes a model to build network security services and capabilities using a dynamic and adaptive approach. Security controls are established and modified according to decisions made by a cognitive process. The model consists of two important elements; SA establishment and management, and network security control. The SA element provides awareness of the system and environment state, and the control part modifies updates and configures network settings and parameters. The security control element adjusts configurable security controls in a cognitive network node. The model proposes active defence capabilities which enable a cognitive service and capability allocation in which the system configuration varies randomly resulting in a non-static target for an attacker. The paper also discusses evaluation and implementation challenges of the model.

Keywords

Cognitive networks, computer network defence, network security, security architecture, cyber threat

1. Introduction

Networks and information services play as a major role on the future battlefield. Information sharing and networked systems bring advantages to modern war fighters. Increasing amount of information and its accuracy helps decision-makers to make faster and more precise decisions. Future communication and network technologies will provide more capacity and security to support the mobile and agile operations. The technologies do not solve all the challenges of network centric operations challenges but it brings more opportunities to information sharing and processing.

One of the critical requirements for the military networks is cyber security. Information security means that information could not be stolen or modified, networks function as desired, and information availability is guaranteed. Information security sets controls to protect information in the systems but cyber security includes all the aspects how an adversary could use information networks to cause desired effects in a target systems. This means that information is not an only protected object. Through cyber security the information system should be protected against all imaginable attacks so that the system is able to provide services continuously.

Expansion of cyberspace has created new and increasing threats to military communications. Cyberspace can be seen as an electronic medium of computer networks in which online communication and information sharing takes place. Thus all military equipment with a programmable micro circuit or computer creates a new attack surface to be exploited by an adversary. The purpose of a cyber attack may be e.g. information espionage and sabotage or physical damage. Information espionage is the act of obtaining sensitive, proprietary or classified information. Physical damage is a result of cyberspace attack in which the target is to affect SCADA systems so that the control of industrial or infrastructure processes is disturbed.

From military perspective, information and network protection could be seen as military operations. Computer Network Operations (CNO) is a broad term to describe the operations used primarily to disrupt, disable, degrade or deceive an adversary's command and control, thus disabling the adversary's ability to make effective and timely decisions, while protecting and preserving friendly command and control. Computer Network Defence (CND) is a defensive part of

CNO. CND consists of actions in cyberspace to monitor, detect, analyse response and protect hostile activity.

Cognitive Network (CN) is a new research field that is seen as an answer to also the performance of the military networks. CN provides learning and adaptation features which will be key functionalities for a future complex and massive information and networking system because the task of configuring the network operating parameters is challenging in complex computer networks. CN is defined as a network with a cognitive process that can understands current conditions, plan, decide, act on those conditions, and learn from the results of actions. A key factor in the process of learning is the ability to take advantage of the previous decisions. Cognitive networks is seen a promising solution to improve military communications and networking. At least in theory, the cognitive networks provide:

- improved robustness and adaptability
- improved usability and comprehensibility,
- improved security and stability, and
- reduced human intervention for operation and configuration.[1]

Growing cyber threat requires new type of approach when implementing military and commercial information and communication systems. This study presents this new approach to build CND capabilities into cognitive military networks. The paper proposes an architectural model to implement network services and capabilities using a dynamic and adaptive method. A cognitive process is used to establish and modify user and network services, and also security services or controls. The proposed model consists of two main elements; SA establishment and management, and network control. Situation Awareness (SA) is a critical functionality for CN to provide understanding surrounding environment and system internal state. The network control manages an adjustable network platform which adapts network parameters according to the made decisions.

The content of the paper is following. Section 2 discusses on major elements and requirements of building CND. Section 3 gives an overview of cognitive networks and cyber threat on them. Section 4 proposes a new model for cognitive CND, and in section 5, the model is evaluated and some implementation challenges are presented. Section 6 concludes this paper.

2. Computer Network Defence

Computer Network Defence (CND) is about how to secure information and data from hostile attacks. CND could be applied into both military and civilian environments, but the term Computer Network Defence is typically used within military operations. CND illustrates defensive aspects of Computer Network Opera-

tions (CNO). CNO also includes Computer Network Attack (CNA) and Computer Network Exploitation (CNE). CNA includes all the actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and networks. CNE uses computer networks to gather data from target or adversary automated information systems or networks for intelligence and operations. [2]

2.1 Definition of computer network defence

The term Computer Network Defence (CND) was created to describe defensive operations on networks. According to DoD [3] Computer Network Defence includes all the actions taken through the use of computer networks to protect, monitor, analyse, detect and respond to unauthorized activity within Department of Defence information systems and computer networks. Naturally, this definition talks about the DoD's systems and networks. Removing the DoD aspect the definition of CND can be stated as:

Computer Network Defence includes actions taken via computer networks to protect, monitor, analyse, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defence information systems and networks. [4]

As the definition shows the general idea is to protect the information systems against unauthorized use. The definition does not seem to bring up any new aspects if the definition is compared to traditional information and network security. The CND definition has more operational view to securing information and may also include some active measures as counterattacks and pre-emptive attacks [2].

Once we consider network defence, we often see the term of Information Assurance (IA). Information Assurance is tightly related to information security but IA consists more of the strategic risk assessment and management of information systems rather than the implementation of security controls. In addition to defending against malicious code and network attacks, IA planners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems. IA integrates an organized, manned, equipped and trained workforce to guard, secure and secure information and information systems by providing the security services/attributes of availability, authentication, confidentiality, integrity and non-repudiation. [5]

IA is also an interdisciplinary field requiring expertise in accounting, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to computer science. Thus IA is best thought to be as an umbrella term for information security and in that way also for CND in a broader context.

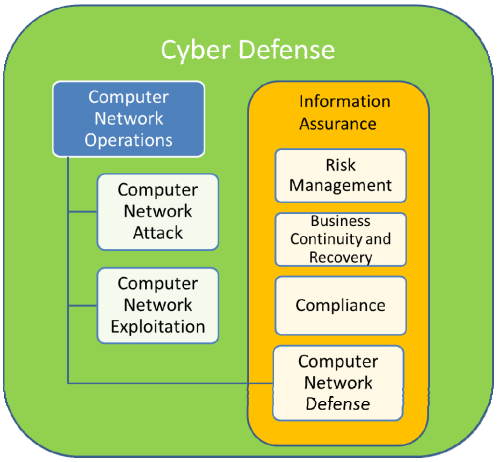


Figure 1. The definitions and their relationships

Figure 1 illustrates relationships between cyber defence, CND, and IA. Cyber defence is thought to be a high-level term for all protective means for information systems and networks. It includes both CND and IA. CND is part of Computer Network Operations but at the same time it is an element of IA. Information Assurance also includes risk management, business recovery and continuity, and compliance.

2.2 Passive and active defence

Although the purpose of CND is to protect information services and infrastructure, CND also includes some CNA and CNE capabilities because defence requires both passive and active methods. For example through CNE operations the defender receives intelligence information that could be used for counteractions during the attacks or even before them. As in traditional war fighting and thus pass includes could be approached with passive or active security implementation.

The passive controls typically consist of firewalls, antivirus applications, access control and vulnerability patching [6]. The primary objective of firewalls is to control the incoming and outgoing network traffic by examining the data packets and determining whether it should be allowed through or not, based on a preconfigured rule set. A major challenge is to keep the rule set updated. An effective firewall also requires updates to ensure it can recognize and exclude newly discovered threats. Thus, a firewall is only as good as the system administrator who runs it. First-generation firewalls were basically packet filters, and nowadays third-generation firewalls proceed application filtering as they monitor certain applications and protocols.

Antivirus applications are used to prevent, detect and remove malicious code and malware. A typical antivirus application is based on a signature detection in which known patterns of data within executable code are searched. Signature libraries are updated according to new viruses. A problem is that a virus must be

found before a specific signature is developed. Thus, heuristic approaches can be used to counter such so-called zero-day threats.

Access control provides a capability to prevent unauthorized party to access private information. Access control systems provide the essential services of identification and authentication, authorization, and auditing which in chronology order provide the chain of access control (see Figure 2). [2]

The authentication process is for verifying the identity of an individual or system against a presented set of credentials. This is typically delivered using username/password combination, RSA SecureID, or PKI-cards. In the future these might include biometric identifiers, such as fingerprints, iris scans, or other means based on physical attributes. The authorization process open Activities that particular identity is allowed to carry out, known as authorization. A simple design principle is that only the minimum level of privilege that is needed for it to operate properly is given for each user. The auditing process has a capability to monitor what activities have taken place on an information system. [2]

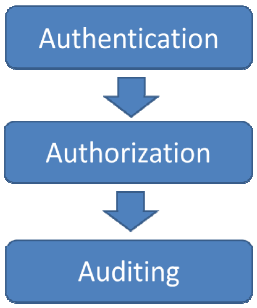


Figure 2. The access control chain

Patching is a common process to fix problems with, or update a computer program its supporting data. Patching is mainly conducted to fix critical or other security vulnerabilities, but it also includes fixing other bugs and improving the system usability or performance. Poorly designed and implemented patches can sometimes cause new unknown problems.

IDS (Intrusion Detection System) is a device or software application which monitors network traffic or system functionality for malicious behaviour. IPS (Intrusion Prevention System) is an extension of IDS providing ability to actively prevent or block intrusions that are detected. Intrusion detection and prevention systems are mainly designed for identifying possible incidents, logging information about them, and reporting attempts. [7]

Active defence can be divided into three categories according to the type of activity. These are pre-emptive attacks, counterattacks, and active deception. [6] Pre-emptive attacks may have only little effects to an adversary‘s CNA capabilities, if these remain isolated from the Internet until actually beginning their at-

tack. A challenge is to discover possible attack sources and know that that adversary is going to use the source against friendly systems. The purpose of the preemptive attacks is to affect the adversary before attacks are launched.

Counterattacks are more promising, but these attacks must begin early enough to authorize all preparatory activities to be completed before the adversary‘s CNA is completed. Active deception also shows promise, but only when attacks can be perceived quickly and accurately, and adversaries’ attacks could be redirected into dummy or fake networks and services (honey nets). Active deception tries to channel an attack away from the defender‘s information system and into dummy networks. The defender leads the attackers to believe the attacks are successful, when in fact the attacks are neutralized. Active and passive defence measures can work side by side to strengthen one another.

2.3 Security measures

The purpose of cyber security and defence is to protect information in all forms. In a military context, information exposition may have greater consequences than information of other (e.g. civilian) areas. In a military environment, lives can be lost on a large scale or the balance of power can be shifted significantly. Protected information incudes e.g. operations orders, war plans, troop movements, technical specifications for weapons or intelligence collection systems, identities of undercover intelligence agents, and any number of other items critical to the functioning of military and government.

There are several measures that are used when information is being protected. Commonly known measures are confidentiality, integrity and availability. However, in [8] four other measures are presented. These seven measures are listed in Table 1. The ITU-T X.805 [9] standard describes eight security dimensions that include some of those presented in Table 1, but the standard also introduces a few new dimensions. The ITU-T dimensions are access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy.

Table 1. The security measures and their purpose

Measure	Purpose	Threat	Protection methods
Availability	Data can be accessed when needed to do so	Corrupt or delete data, DoS	Robust environment (system outages, communication problems, power issues) Use of redundancy and backups
Accuracy	Data is free from mistakes or errors	Data modification in all forms	Encryption (difficult to successfully manipulate data without the proper authorization) Hashes or message digests (e.g. MD5 and SHA1)
Authenticity	Data is kept authentic (data is in the same state in which it was created, stored, or transferred)	Data modification in all forms	
Confidentiality	Keeping data out of the hands of those that should not be seeing it	Information disclosure	Access controls Encryption
Integrity	Prevent data from being manipulated in an unauthorized manner	Altered to reverse their meaning or to alter the outcome of decisions based on the data in question	Encryption Hashes or message digests
Possession	Data is owned or controlled by a proper user	Data removal from the secure environment, data theft	Physical security, access control
Utility	Data has value for some purpose or end	Data modification in all forms	Encryption Hashes or message digests

2.4 Cyber Situational Awareness

Cyber Situational Awareness (SA) is very critical for all kinds of defensive actions including CND. As in traditional warfare, also CND requires high quality security awareness. Situational awareness is established in human brains, which means that SA technology attempts to provide understandable information of an operating environment. When we consider cyber SA of the CND assets, we face with at least seven aspects [10]:

1. Awareness of the current situation
2. Awareness of the attack impact
3. Awareness of how situations develop
4. Awareness of adversary behaviour
5. Awareness of why and how the current situation is caused. This aspect includes causality analysis (back-tracking) and forensics
6. Awareness of the quality (and trustworthiness) of the collected situation awareness information items
7. Evaluation of possible futures of the current situation.

Cyber security situation awareness can be regarded as a three phase process [11] in which the previous aspects are included. The phases are situation recognition (observations), situation comprehension (understanding) and situation projection (prediction). Smart CND solutions require technologies to support these process phases when a goal is to produce automated cyber defence systems. However, in practice, current cyber SA with hardware sensors and advanced computer programs do not operate without mental processes of human beings making advanced decisions [11].

2.5 Defence in depth

Defence in depth is an old military concept which describes a layered approach to defence [2]. In cyber security context, defence in depth means security controls and solutions are layered so that an attacker must penetrate several layer to reach target data or location. An example of the layered defence is shown in Figure 3. In this example case there are defences at the network level, the host level, the application level, and the data level. Critical information is located at the center of all these layers of defence. Security measures and controls at each layer may be different according to the environment in question, but the basic principles will remain the same.

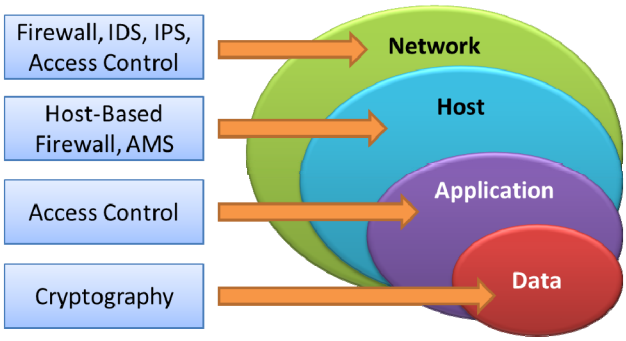


Figure 3. An example of layered defences

Layered defences should be configured so that it slows an attacker as much as the defender has time to detect and defend successfully the attacks. It is very unrealistic to expect that we can build an impenetrable system which is secure forever. By using segmentation and access restrictions, we can mitigate some of the risks of an adversary being able to penetrate, steal information and get back out. Figure 3 also shows some examples of security controls and mechanisms related to each defence layers. At the data layer, cryptography is an important method. The application layer includes access control mechanisms to prevent unauthorized accesses. The methods at the host and network layers consist of firewalls, IDS/IPSs, access controls and AMSs (Application Management Services).

3. Cognitive Networks

In [12] and [13] Cognitive Networks (CN) are described as:

> ”A cognitive network is a network with a cognitive process that can perceive current network conditions, and then plan, decide, and act on those conditions. The network can learn from these adaptations and use them to make future decisions, all while taking into account end-to-end goals.”

The cognitive aspect of this description is similar to those used to describe a cognitive radio and broadly includes many simple models of cognition and learning. Unlike cognitive radios, cognitive network do not restrict its scope in radio spectrum. CN tries to exactly perceive the current network situation and plan and decide to meet the end-to-end goals in an entire network aspect. CN learns through this adaptation and uses information of these previous actions in future decisions. As new aspects, the definition introduces the terms network and end-to-end goal. Without the network and end-to-end approach, the system may only perform as a cognitive device or network layer, but not as a cognitive network in a wide scale.

In the definition end-to-end represents all the network elements involved in the transmission of a data flow. In military communications, this includes e.g. the tactical radios, radio relays, routers, switches, virtual connections, encryption devices, interfaces, or SDR waveforms. The end-to-end goal which is typically defined by a client-server type of service, gives a cognitive network its network-wide scope. This separates the scheme from other adaptation approaches, which usually have a scope of single element, layer or resource.

3.1 Cognitive process and system framework

A cognitive process in such networks could be viewed as the commonly known OODA loop [14] in which the network observes, orients, decides and acts. Figure 4 shows the phases of the OODA loop in context of cognitive networking. The observation phase is critical because the effect of a cognitive network’s decisions on the network performance depends on how much network state information is available. If a cognitive network has knowledge of the entire network’s state, cognitive decisions should be more “correct” than those made in ignorance. For a large, complicated system such as military tactical networks, it is unlikely that the cognitive network would know the total system state. It could be very high costly to communicate status information beyond those network elements requiring it, meaning CN will have to work with less than a complete picture of the network resource status.

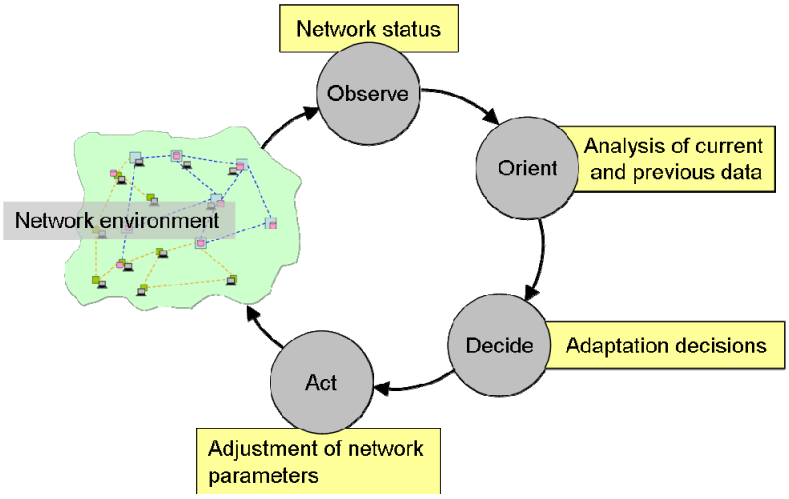


Figure 4. The "OODA" loop in context of cognitive networking

The orientation phase also plays an important role in the cognitive process. In this phase all observed information and previous knowledge are add together and analysed. Filters and weighting are examples of methods used in the orientation phase. In the decision phase the best decision for the required end-to-end data flow capability is made. Finally, actions are taken in the Acting phase. Action includes modifications of cognitive network elements. These elements associated with each data flow are allowed to act selfishly and independently (in the context of the entire network) to achieve local goals. The actions taken have straight effect to the observed environment or network state, thus a feedback loop is created in which past interactions with the environment guide current and future interactions.

Figure 5 illustrates a cognitive system framework [12] which consists of three functional levels. The end-to-end level includes applications, users and resources which form the end-to-end goals to be achieved at an appropriate service level. The cognitive level consists of three components: the specification language, cognition layer, and network status sensors. These components provide the actual intelligence of the cognitive level, and allow the level to interface with the configurable network elements and the users and applications on the end-to-end level.

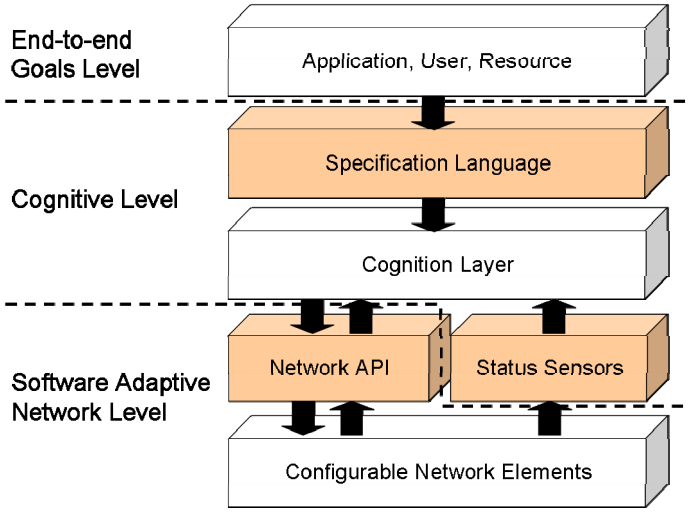


Figure 5. A cognitive system framework

For connecting the top level requirements to the cognitive level, an interface layer must exist. Information about the goal must not be globally known but needs to be communicated between the source of the requirements and the local cognitive process. Other requirements for the specification language include at least support for distributed or centralized operation including the sharing of data between multiple cognition layers. The specification language does not actually perform the cognitive process which is done by the cognition layer, but the language is required to translate application level requirements for the cognitive layer.

The cognitive process of the network can be either centralized or distributed. In the military environment, the requirements for high-resilience mean that each node should be able to maintain a cognitive process, providing an argument against the centralized solution. The cognition layer contains the cognitive element of the framework. Typically, cognition is provided through various machine learning algorithms as neural networks, genetic algorithms, artificial intelligence, Kalman filters and learning automata algorithms [12]. The network status sensors provide feedback from the network to the cognition layer, and the sensors also allow the cognition layer to observe patterns, trends, and thresholds in the network for possible action. To be able to report connection status sensors must have ability manage the sensor. The sensor layer is also capable to distribute their information to the entire network.

The software adaptive network layer consists of the network application programming interface (API) and configurable network elements. The network API provides a generic interface to adjust network parameters according to actions decided by the cognitive layer. Another responsibility of the API is to notify the cognitive network of what the operating states of the network elements are. Many modifications to the network stack require that all the links and nodes are synchronized and operating in the same mode. The communication required to syn-

chronize these states is the responsibility of the software adaptive platform and could be realized either in or out of channel.

3.2 Cyber threats on cognitive networks

Security of CN is discussed in [15], [16], [17], [18}] and [19]. Although, the most of the traditional cyber threats (e.g. TCP/IP threats, man-in-the-middle, etc.) are valid, cognitive networks also face some unique security challenges not faced by conventional wireless or wired networks. In an ideal CN, security of the network is provided as a result of a cognitive process, which generates new threats. For instance, incomplete situation awareness or a disturbed decision-making process may lead to the decision not to use any security controls for certain communications although it is extremely required. Table 2 presents three new cyber security threats related to cognitive networking.

Table 2. Major security threats in cognitive networks

Threat	Description	Implication
Sensor Input Violation	Sensor data is altered by an attacker or other means	Learning and decisions are made according to false SA which results faulty performance.
Information Sharing Violation	Information sharing between network nodes is damaged	SA of the surrounding environment is false.
Data Storage Attack	Data storages are injured	History data, as a basis for decision-making, is incorrect.

In the cognitive network, locally-collected and exchanged information is used to construct a perceived information environment that will influence both current and future behaviours. By violating sensor data, information sharing and history data (databases), an attacker is able to change the information environment. Training with the incorrectly perceived environment will cause the CN to adapt incorrectly, which affects short-term behaviour. Unfortunately, the CN uses these adaptation experiences as a basis for new decisions. Thus, if the malicious attack perpetrator is clever enough to disguise their actions from detection, they have the opportunity for long-term impact on behaviour. Furthermore, the CN collaborates with its fellow nodes to determine behaviour. Consequently, this provides an opportunity to propagate a behaviour through the network in much the same way that a malicious worm.

In cognitive networks, one of the main concerns is an attacker spoofing faulty sensor information, causing a network node to select an undesired configuration.

By manipulating the receiving information the attacker can cause faulty statistics data to be appeared in the knowledge database of a network node.

The cyber threat on CN can also be considered by analysing the objectives of a cyber attack and the ultimate outcome the attack may have. The effects of cyber attack align generally into four areas [19]:

- *Loss of Integrity*. Data integrity is a basic security requirement for end users, but it is also very critical for CN behaviour. If the loss of data integrity is not corrected, continued use of the corrupted data could result in inaccuracy, fraud, or incorrect decisions in a cognitive process.
- *Loss of Availability*. If a mission-critical network is attacked and all services are made unavailable to its end users, the mission or operation will most likely be affected. Loss of system functionality and operational effectiveness may result in loss of productive time, or military decision-making. In CNs, loss of availability also means that information and services are not available for the cognitive process.
- *Loss of Confidentiality*. Successful military operations require high information confidentiality. CN should provide appropriate confidentiality services so that operational data is kept secret as desired. Communication channels, data processes and databases must be secured against untrusted parties. Confidentiality is also critical to the cognitive process because stolen information could be used against the process.
- *Physical Destruction*. Physical destruction is possible through cognitive networking when the CN provides a platform for supervisory control and data acquisition (SCADA) systems.

4. Cognitive Computer Network Defence Model

Cognitive networks provide new opportunities to design and build security features and functions into the networking system. Learning and decision-making capabilities are key factors to create automated, resource-efficient and, especially in a military context, secure communications networks and services. In next section, a new architectural model for cognitive computer network defence is presented. The model describes high-level elements of the cognitive CND system.

4.1 Model overview

The overview of the cognitive CND model is depicted in Figure 6. The figure shows the main elements of the model which are security situational awareness (SA), decision-making, and security control management, and active defence. The decision-making element is a core of the cognitive system. The decision-making gets inputs from the SA element, and the history database, and based on the desired (security) goal performs a computational process that ends up with a

decision. The end-to-end security goal is defined by a network user or service (application).

The task of the SA element is to provide high-quality situational understanding. The element receives sensor data from each system layer. In this model, the cognitive network is divided into four functional layers that are Network, Host, Application and Data. The security control management element configures and updates security controls at each layer. These controls include a large variety of traditional, and in the future, new security mechanisms. The security control management element transforms incoming decisions into updated security parameter values, and configures those values into the system.

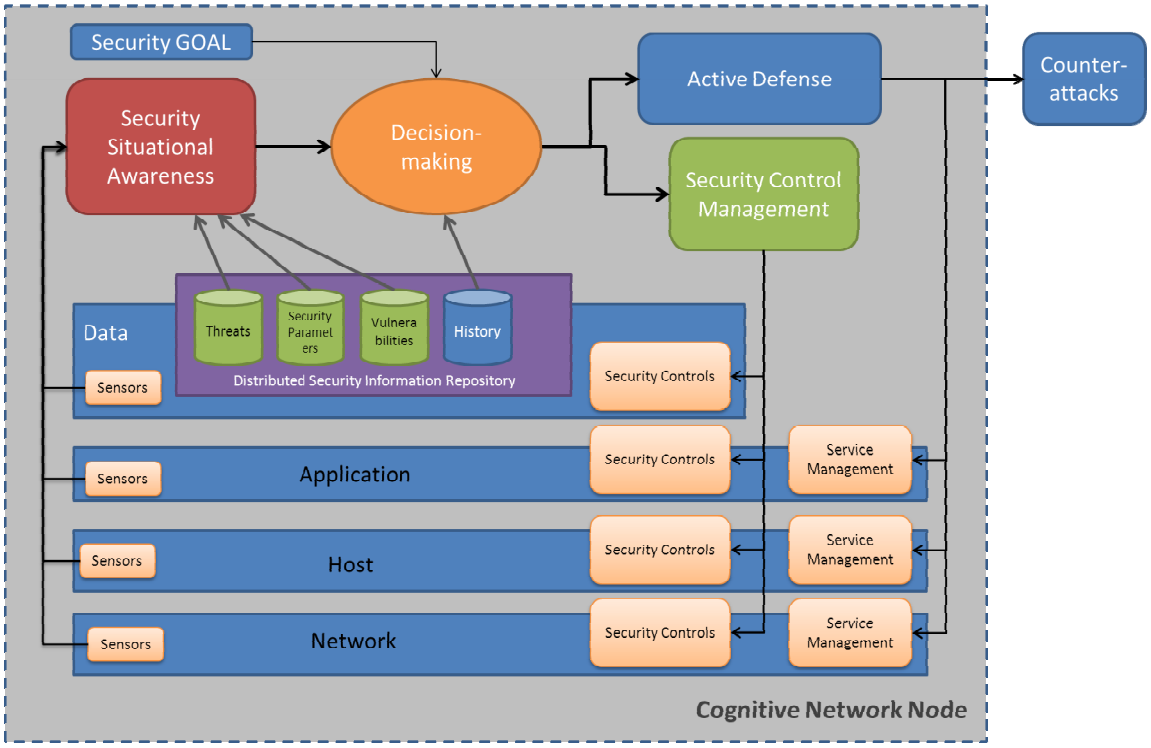


Figure 6. Overview of the model

The purpose of the active defence element is to execute active defence operations as part of cognitive CND. In this model, active defence means both counteractions against an adversary, and active service configuring in the cognitive nodes. The counteractions can be pre-emptive or reactive as described in Section 2.2. The purpose is to eliminate attack sources beforehand or during attacks. Active service configuring could be seen as part of deception operations. The idea is to actively change service configuration, and thus make an attacker's destination system as a moving target. This means that the target configuration is already changed during attack preparations (after intelligence data collection). Configure changes might include e.g. application versions, operating system (OS) types, port configurations, process access structures, etc.

Distributed Security Information Repository consists of different databases that are distributed among the network nodes. The databases include history data (e.g. previous decisions and conditions), vulnerability and threat libraries, and current security parameters of the other nodes.

4.2 Situation Awareness

Situation Awareness (SA) is a very critical part of the cognitive process and network. The quality of decisions depends on the level of SA. The SA element consists of four main elements; sensors data collection, threat management, vulnerability management and SA engine. Figure 7 illustrates the SA element of the model.

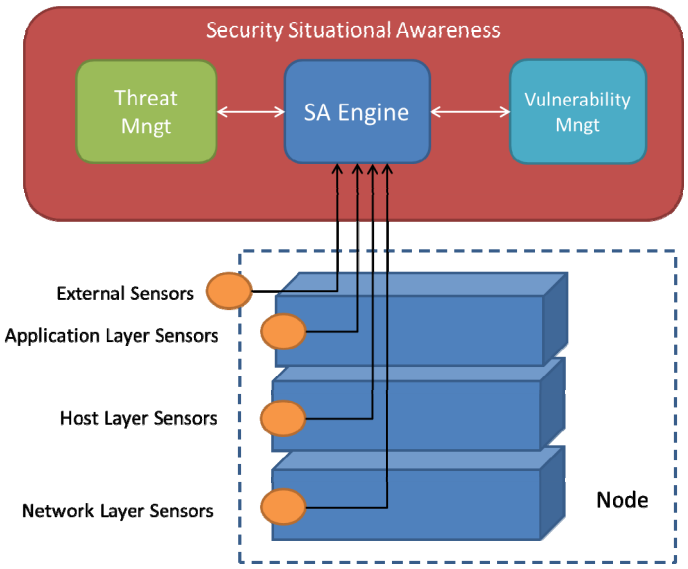


Figure 7. The SA element

The purpose of sensor data collection is to collect all SA related information for data analysis and fusion. The sensor data sources include both internal and external sensors. The node internal state sensors collect security and service performance data about the internal state of each network node. At the network layer, collected internal parameter data includes cryptography algorithms and key lengths, IDS/IPS rules and policies, anomalous traffic alerts, incidents DMZ configurations, allocated links, etc. At the host layer, internal parameter data consists of access control lists (valid users and services), tunnelling parameters, authentication information, access blockages etc. At the application layer, collected data concerns end-to-end encryption settings, application security configurations, authorized code lists, etc.

The external sensors monitor environmental conditions outside of the node. These conditions include such as temperature, physical security, and especially in cognitive radios, spectrum usage conditions.

The threat management element adds risk assessment capabilities to the cognitive CND. The purpose is to build and maintain SA of risks and risk levels in a cognitive network. The threat management element includes a threat management process and a threat database in each cognitive network node. The management process described in [20] consists of threat identification, risk assessment and mitigation trade-off sub processes as shown in Figure 8. The threat identification element receives information from several security sensors and databases, and then calculates and enumerates the threats and sets out intrusion/attack scenarios, and identifies the relevant vulnerabilities.

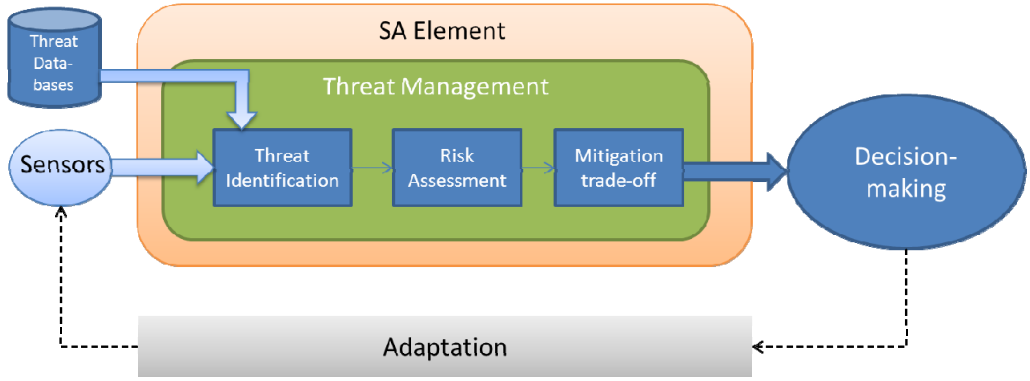


Figure 8. The threat management element

The risk assessment sub process quantifies the risk for each intrusion scenario through the use of event history databases, and policies and mitigation strategies. Quantifying the risk can be done using historical data or statistical sampling. Also, an expert opinion may be needed when relevant data is missing, but in the CN context this manual evaluation is not desired. The cyber event or incident may not always result in the same consequences. A number of consequences with differing probabilities (for instance, an attack on a network may result in a temporary outage of one workstation at one extreme, and a complete extended loss of the network at the other) may exists. In this cognitive network context, the expected damage from the event or incident is then the sum of the probabilities of each possible consequence.

At the final stage the mitigation trade-off sub process calculates the trade-off cost of mitigation against the risks. The process provides an adaptation map in which different responses to an incident are shown in a sense of costs. The costs of mitigation include such attributes as service availability, connectivity, security levels, etc.

The purpose of the vulnerability management element is to provide knowledge about a current system configuration and vulnerability situation within this configuration. The management element has an ability to identify, classify, remediate, and mitigate vulnerabilities [21]. In this model, this refers to software vulnerabilities in the computing systems of a cognitive network. In practice, the vul-

nerability management provides an automated software patching system for a cognitive networking system. Knowledge of vulnerabilities is also used for the previously described threat management. Vulnerabilities allow an attacker to design and execute hostile actions against the defended system.

The SA engine collects information from the threat and vulnerability management elements, and from all sensors. Based on all available information the SA engine generates the best possible situational understanding. A number of different techniques can be used for data-mining, correlation, neural computing, and other data processing applications.

4.3 Security control management

The function of the network security control management is to adapt and configure all security controls throughout the entire network. The security control management consists of a management element and configurable security controls. The main task of the management element is to shape a decision into new parameters for security controls of each layer. After the new parameters are generated, the parameters are distributed and updated to the security controls.

Table 3. Security controls at each layer

Layer	Security controls	Purpose	Parameters to be configured
Network	Demilitarized Zone (DMZ)	Provide a proxy between trusted and untrusted networks.	Proxy configuration
	Intrusion Protection System (IPS)	Detect anomalous traffic by using data mining, pattern matching, and decision-making (IDS). Filter and drop undesired packets (firewall).	Pattern models, decision rules, attack signatures. Packet filtering rules.
	Link cryptography	Protect transmission links	Algorithms, keys
	Packet Level Authentication (PLA) [25]	Ensure that all the packets transported are from a trusted source	Authentication keys
	Physical layer protection	Prevent interception	Frequency hopping, spread spectrum
Host	Access Control	Prevent unauthorized access	Access lists, service authorization lists
	Tunneling	Provide confidentiality and integrity	Tunnel settings, protocols, algorithms
	Authentication		
	Service configuration	Protect CN by a dynamic service configuration (non-static target environment)	Used applications, protocols, addresses, etc.
Application	End-to-end encryption	Protect data traffic through all the layers between server and client	Algorithms, keys
	Signed code	Prevent to execute malicious code. Code must have a valid signature.	Authentication keys
	Controlled Execution Environment [26]	Prevent execution of malicious code or applications	Lists of trusted code or applications

Security controls are provided with a large variety of security mechanisms and methods [22]. Each mechanism efforts to protect the system against cyber at-

tacks, and thus meet the goal of the security measures (confidentiality, availability, integrity, etc.). The cognitive CND model do not describe exactly all the relevant security methods. Within the model, it is possible to use traditional or new security control techniques. A basic requirement is that a security control is adjustable by software. Thus, for example firewall rules, cryptography key lengths or service access lists must be modifiable through the cognitive process.

Table 3 illustrates examples of security controls at each layer. The list is not complete, but it shows that there are many mechanisms to enhance security in communications networks. In a cognitive environment, parameter adjustability is a important function. The last column of the table considers these parameters that are to be adjusted during the cognitive process.

One of the key issues with the cognitive CND model is how to protect the cognitive process itself. Network-wide cognitive behaviour depends on information sharing between the network nodes. This information sharing must also meet all the security requirements. Of course, all the security controls are available, but a challenge is the performance of a mobile node. Control information causes lots of "overhead" on communication links, which may lead to link capacity and e.g. battery life-time problems specially in mobile wireless nodes.

5. Evaluation and Implementation Challenges

This section discusses on architecture evaluation and implementation challenges within the proposed model. Security architecture evaluation is important to ensure that the architectural model meets all critical requirements before the model is implemented and tested in a real-life environment.

5.1 About architecture evaluation techniques

Reference [23] introduces four types of architectural assessment for evaluation. These are mathematical modelling, simulation-based, scenario-based and experience-based assessment. Mathematical modelling can be appropriate for attributes where the requirement defines the exact desired system behaviour (e.g. performance). It could be impossible to develop a mathematical model which accurately measures the level of security provided by an architectural model.

Simulation is usually conducted using an executable model of the software architecture. The technique requires that simulated attacks are relevant, and because the overall architecture is an incomplete, a complete penetration testing with the full range of potential attacks cannot be carried out.

Scenario-based evaluation is based on a set of scenarios that are developed to convey the actual meaning of the security requirement. For network security evaluation, scenarios are typically attack scenarios that describe certain attack

types or techniques. The effectiveness of the scenario-based evaluation relies on the accuracy of the representative scenarios. In experience-based assessment, security experts use their experience and intuition to logically validate certain design decisions. The method is more subjective than the others, but it can be beneficial if it is combined with a scenario-based method.

In this paper, a full-scale evaluation is no conducted because of limited space, and no specific evaluation method is chosen. Further research could include scenario-based evaluation with e.g. the scenarios of node-capture, sensor violation, and Denial-of-Service attacks. However, some evaluation is provided by considering defence in depth aspect.

5.2 Defence in depth

Security requirements, goals, and operating environment are key issues when we evaluate the architectural model. Applicability of security mechanisms depends primarily on where security requirements are located throughout the cognitive network, and what those requirements are. Reference [22] introduces a security zones approach for security evaluation which is depicted in Figure 9. There may be requirements and cyber security goals for different levels of security, coupled to certain user groups, their applications and devices. Each security zone has specific security requirements and thus implemented security controls.

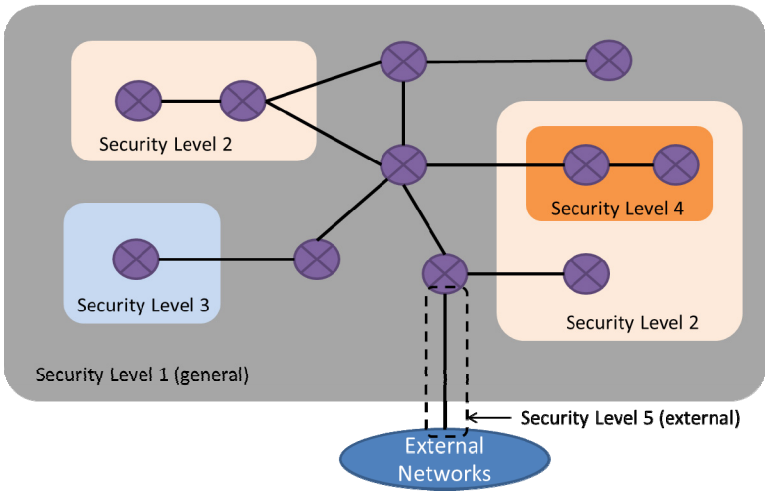


Figure 9. Security evaluation using security zones

The first zone (Level 1) covers the entire cognitive network and provides a general level of security to all users, applications, and devices. The second, third and fourth (Levels 2, 3, and 4) zone provides a higher level of security for a group of users, applications, or devices, whose security requirements are different from the rest of the network. For example, processed and shared data has a higher classification level, and thus more security controls are needed. The fifth zone (Level

5) provides a higher security between this cognitive network and all external networks.

The security zones approach meets the defence in depth requirements when access to the most critical data is layered so that a user must bypass several security control layers to reach critical data. Figure 9 shows an example of three defensive control layers at the network level (nodes L1-L3). At each layer (node), appropriate security controls are implemented to slow an attacker's movement towards critical data. Once the attacker reaches the destination node there are still the next layer security controls to penetrate (see Figure 3).

5.3 Implementation challenges

The implementation of the proposed architectural model meets number of challenges. The main challenges are targeted to the cognitive process which requires well-functioning decision-making. Major challenges are described in the following.

Decision process is based on algorithms which should generate the best decision for each situation. Automated decision-making is always related to quality and amount of input information. Human-based decision-making is much more effective compared to a computational process. The automated decision-making is typically an optimizing problem [24]. Several optimization schemes based on learning are available in the literature, like neural networks, genetic algorithms, ant-colony optimization, etc., but the use of them requires further analysis and research.

Learning process is in a key role when devices' or networks' behavior is improved by learning from past decisions. The design of the appropriate learning algorithm represents a challenge already by itself, and measurements which should be employed by learning open even new issues related to which measurements to use and how to perform them.

Situational Awareness establishment is critical for decision-making. Thus, it is vital to create formal and unambiguous SA for decision-making algorithms. Different SA input sources (vulnerabilities, threats, security parameters, etc.) must be shape into a common format.

Threat and vulnerability management faces a challenge of information updating. Threat and vulnerability management should be based more on anomalous behaviour than signature libraries. In a complex system it could be challenging to maintain coherent threat and vulnerability libraries distributed among the network nodes. Attacker may use zero-day attacks which are not detected by signature-based IPSs.

Data repository replication should be accurate, reliable and light-weight. Keeping distributed data synchronized in a dynamic military network is very resource-consuming. To provide ideal replication between the databases, the nodes should remain connectivity and sufficient bandwidth capacity continuously. Bandwidth requirements are high when data must be kept synchronized in millisecond periods. That requires a real-time replication mechanism. Lots of methods are developed for replication, but most of them are not very effective in dynamic environments.

System complexity creates new attack surfaces for an attacker. The more complex systems are the more they include software code, configurable parameters, interfaces, and running processes. In some cases, it could not be possible to evaluate and test the entire system against all possible threats. Continuous attack development means that there are always unknown threats existing.

6. Conclusion

Cognitive networks are a promising research area for future military networking. In theory, the cognitive networks will improve network performance, resilience, and self-organizing, and security. Situational Awareness (SA) and adaptation capabilities are the key enablers to enhance the level of security.

Cyber threats are growing, and new vulnerabilities are found continuously. At the same time, criminals and other actors develop new cyber weapons that exploit those vulnerabilities in networks, devices and applications. Cognitive networks will open new potential attack surfaces such as situational awareness, decision-making and adaptation processes. The performance of the cognitive networks depends on these complex processes and all control information shared between cognitive nodes.

Computer Network Defence (CND) sets high-level requirements for military communication networks. Failing to protect classified information may cause severe consequences in military operations. Due to the growing cyber threats, a CND architectural model for the cognitive military networks must be designed outside the box. This paper proposed a model in which the main functionalities are the SA, Network Security Control elements and Active Defence elements. All the elements are part of the cognitive process. The SA element collects security related information for decision-making. Based on decisions, the control element adjusts security control parameters in a network node. Similarly, the active defence element (randomly) adjusts device and application configurations to make an attacker's target non-static.

The proposed model is a rough approach, and still faces several implementation challenges and future research areas. The model must be evaluated using different scenarios with the most likely and dangerous situations. The evaluation is

critical when proving the ability of the model or architecture to meet the security requirements. Further research includes sensors types, decision-making algorithms, adjustable security controls, and performance calculations. Also information sharing in the cognitive process needs more research as it is seen a weak point of the cognitive system. The idea of dynamic, continuously changing service configuration is interesting, but requires more studying. Especially, configuration rules and potential applications should be considered.

References

[1] Mahmoud, Q., Cognitive Networks: Towards Self-Aware Networks, Wiley-Interscience, 2007.

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

[3] Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, 2010 (As Amended Through 15 July 2012).

[4] http://en.wikipedia.org/wiki/Computer_network_operations, cited 4.10.2012.

[5] Willett, K. D., Information Assurance Architecture, Taylor & Francis, 2008.

[6] Holdaway, E. J., Active Computer Network Defense: An Assessment, Research Report, Air Command and Staff College Air University Maxwell AFB, USA, April 2001.

[7] Newman, R. C., Computer Security: Protecting Digital Resources, Jones & Bartlett Learning, 2009. Retrieved June 2010.

[8] Whitman, M. E. and Mattord, H. J., Principles of Information Security, Cengage Learning, 2011.

[9] Security architecture for systems providing end-to-end communications, ITU-T Recommendation X.805, 10/2003.

[10] Jajodia, S., Liu, P., Swarup V. and Wang C. (ed.), *Cyber Situational Awareness: Issues and* Research, Volume 46, Springer, 2010.

[11] Onwubiko, C. and Owens, T., Situational Awareness in Computer Network Defense: Principles, Methods and Applications, IGI Global Snippet, 2012.

[12] Thomas R.W., DaSilva L.A. and MacKenzie A.B., *Cognitive Networks*, Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005.

[13] Thomas R.W., Friend D.H., Dasilva L.A. and Mackenzie A.B., Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives, IEEE Communications Magazine, Volume 44, Issue 12, 2006.

[14] Boyd J., A discourse on winning and losing: Patterns of conflict, briefing, 1986.

[15] Mody, A.N., Reddy, R., Kiernan, T. and Brown, T.X., *Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard*, IEEE Military Communications Conference (MILCOM), pp 1 – 7, 2009.

[16] Prasad, N., *Secure cognitive networks*, European Conference on Wireless Technology, pp 107 – 110, 2008.

[17] Burbank, J., *Security in cognitive radio networks: the required evolution in approaches to wireless network security*, 3rd International Conference on

Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp 1- 7, 2008.

[18] Chaczko, Z., Wickramasooriya, R., Klempous, R. and Nikodem, J., *Security threats in cognitive radio applications*, 14th International Conference on Intelligent Engineering Systems (INES), pp 209 – 214, 2010.

[19] Clancy, T.C. and Goergen, N., *Security in cognitive radio networks: threats and mitigation*, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp 1 – 8, 2008.

[19] *Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02, US Army Training and Doctrine Command, August 2005.

[20] Kärkkäinen, A., *Cyber Threat Management in Cognitive Networks*, Proceedings of 11th European Conference on Information Warfare and Security (ECIW), 2012.

[21] Foreman, P., Vulnerability Management, Taylor & Francis Group, 2010.

[22] Joshi, J.B.D., *Network Security: Know It All*, Morgan Kaufmann, 2008.

[23] Alkussayer, A. and Allen, W.H., *A scenario-based framework for the security evaluation of software architecture*, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.

[24] Pawełczak P., *Technical Challenges of Cognitive Radio-Related Systems*, First Annual Conference of Competition and Regulation in Network Industries, Brussels, 2008.

[25] Kärkkäinen, A. and Candolin, C., Ensuring privacy in a network centric environment, Proceedings of 7th European Conference on Information Warfare and Security (ECIW), 2008.

[26] Pfleeger, C.P. and Pfleeger, S.L., *Security in Computing (3rd Edition)*, Prentice Hall, 2002.

Computer Network Exploitation

Jan Lucénius
Aalto University
jan.lucenius@aalto.fi

Abstract

The term Computer Network Exploitation (CNE) is a part of cyber warfare, where the final aim is to gather intelligence from the target network and systems. This article describes briefly the process, phases and tools for CNE. We notice, that CNE in many ways is similar to attacks used by hackers/crackers, but there are differences also. Especially when the target is military or other state authority, the CNE process must be carried out carefully, so that it is not detected. This means, that it needs a lot of time and resources, as the target network is highly secured.

Design/methodology/approach

The article is basically based on the book [2], which was dedicated for this seminar. Information from a few other sources is added.

Findings

This is a pure literature study any new findings are not introduced.

Keywords

Cyber warfare, computer networks, exploitation, security, intelligence, reconnaissance, surveillance, counter-intelligence

1. Introduction

Generally, in the field of IT security, there is a competition between the crackers and other hostile people and organizations, who tries to break in to systems, and the "good" ones, who try to build more secure systems, put up barriers, try to discover what is happen and last but not least, patch the existing security holes, as soon as they are found. Computer Network Exploitation (CNE) in military context is not only about breaking in to systems, but it is indeed a part of it. Also the growth and integration of various systems and network services, bringing new dimensions to the way people work, sometimes even introducing new paradigms, may introduce new security holes, either caused by the systems themselves, their interaction or contradictions between on one hand openness, ability to communicate and perform task better, and on the other hand various security measures. Even simple examples – either from traditional way of using systems and components, or from world-wide social networks, also indicates that security measures are not unambiguous. Solving one problem may introduce another. Just think about encrypting data on a media. If the password, passphrase, or whatever used to enable use of the media gets lost or is forgotten, the data is lost, unless we have a backup, which is reasonable up to date, and which is accessible when the data is required.

What is CNE? In [1] it is defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks". In other words, we can think of CNE as a cyber warfare equivalent of spying [2]. In the cyber world, there is less need for the spies and intruders to be physically present in the counter-parts sites, but it seems that many similar methods are applied also here. Or let's say, the process does not necessarily involve only sitting behind a computer; the most effective CNE operations may be a combination of traditional intelligence and hacking/cracking.

As a thread of this article, chapter 8 of the course book [2] assigned for this seminar is applied. Additionally I have looked at some of the tools. A more detailed examination of the tools, not to mention practicing CNE methods, require, however, much more time, resources and to be "useful" on inter-state level, experience preferable as a full-time worker in these tasks. On the other hand, a"spy" or full-time cracker with access to top-secret information could neither for his own safety nor because of his secrecy obligation reveal hardly anything at all for a publication like this.

In section 2 the topic is described in more detail and the parties involved are explained. Additionally, some related concepts are defined. Section 3 describes

Open source Intelligence (OSINT), section 4 reconnaissance and Section 5 surveillance, including advanced persistence threat.

2. Research Work

2.1 The concept CNE and its scope

The term *computer network exploitation* (CNE) is related to the terms *computer network attack* (CNA) and *computer network defence* (CND). Together these three form *computer network operations* (CNO) [1].

Computer network attack (CNA) is defined in [1] as "actions taken through the use of computer networks to disrupt, eny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves".

Computer network defence (CND) consists of "actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defence information systems and computer networks". Let's still repeat the definition of CNE: "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks"

Particularly, the book [2] notes that CNE is not about gaining privileges or shells on the remote systems, as some crackers who misuse other's computers usually tend to do when they send out spam or carry out distributed denial of service (DDoS) attacks. Nevertheless, this statement did not quite convince me, and I rather feel that this kind of hacking, or something close to it, actually is a part of CNE. But indeed, CNE is a larger concept.

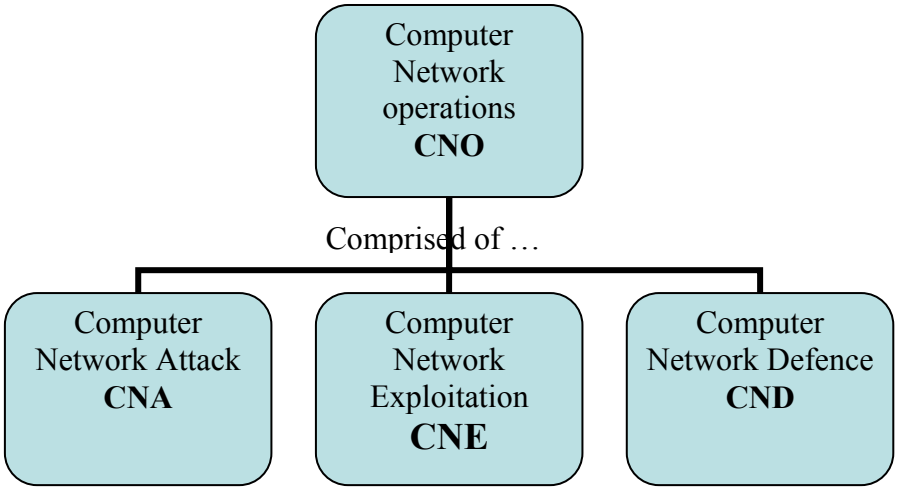


Figure 1. Relation between CNO and CNE

Even if civil crackers have advanced from the script kids type to international criminals, who carry out directed attacks, in order to bring an organization or to gain economic winnings, there are differences between these CNE, particularly when we look at it in a military context. Civil attacks are usually discovered, when something happens, i.e. the intruders have successfully carried out their operation. They also make use of badly protected systems and users, who haven't the capabilities to defend themselves against these attacks, and certainly don't even understand when and where they are exposed to dangers. On the other hand, even highly authorized persons are still humans and there is no reason why they couldn't make similar mistakes. Comparing attacks in general and CNE,I see two main differences:

1. Critical information systems are highly protected, and their connections to the Internet are often indirect [2, 3, 4]. Actions and connections are monitored in order to detect and defend against attacks and other misuse. Also, vulnerabilities, which may not be patched on commercial systems are likely to be patched in critical environments. All this makes it much more difficult for the attacker.

2. In CNE, it is preferable if the operations leave as little tracks as possible, that would enable the counter-part to detect, or even suspect that anything is being carried out. Where the intention of an attack, either in civil context or in warfare, may be to cause damage, the intention in exploitation operations is reversed. If damage would happen, it is likely that the operation would be discovered and would be discontinued. If furthermore the actors are discovered, it is likely that they will run into disputes.

In other words, it is like comparing bank robbery and spying in the physical world.

2.2 Sources of cyber attacks?

The endpoint(s) from where the attack seems to originate, may be only a compromised intermediate system, acting as a proxy for the attack. The attacker may use a botnet or some kind of anonymous service, which disguises both identity and origin [2]. More, if these intermediate networks enable splitting up communication, it may be difficult to find the origin even based on logs. If the attack is not interactive, but the compromised proxy is instructed to operate later, like in a typical Denial of Service (DoS) attack, it may not at all be possible to find the origin. Even if the intermediate network is more straightforward, the attacker would likely use a chain of proxies, preferably in different locations, and such which don't necessarily keep any log of their traffic. The longer the chain is, the harder it is to find the originating attacker, of course.

Acting directly, without unstable intermediate systems may in some cases be more effective and particularly faster, but it is also risky, as the Internet Service Provider (ISP) may shut down the connection for the attacker, if an attack is reported [2]. This is the case at least in some countries.

We could of course argue, isn't it self-evident that a connection from which attacks or "illegal" traffic is generated should be shut down? The network operator would do so temporarily, in order to resume stable operation of network or the target's system. In that case they should also inform the owner of the connection, and reconnect the line when the problem is solved. As we see above, the users behind that connection may be guilty of performing attacks, but as well completely unaware of their system being compromised.

In cyber warfare the attackers may be roughly categorized in

- Governmental/state organizations or actors, which are sponsored by states and operate on behalf of states, and
- Non-government sponsored organizations, e.g. political, activist or terrorist organizations, corporations, criminals, or even individuals.

2.3 Phases of CNE

The book [2] divided cyber reconnaissance into three categories, which roughly could be considered as three phases: *open source intelligence* (OSINT), *passive reconnaissance* and *advanced persistent threat* (APT).

The limits between these three categories are not sharp. We can actually consider a growing degree of intrusion along the CNE process. As the actor digs deeper into the target's systems and networks, the risk that the reconnaissance is detected also grows. Additionally, the actor's methods also become more illegal, and thus, the consequences are also more serious in case the target part detects suspicious traffic or actions on the systems. (Even if it would be difficult to point out the actor, the target organization would at least take preventing/defending actions.) An alternative taxonomy of CNE methods would be to add an additional category "*active reconnaissance"* between passive reconnaissance and APT.

APT in indeed more advanced than the former ones, as it is the "final goal" here, and merely surveillance instead of reconnaissance. What's the difference? That will be clarified in the more detailed descriptions of the CNE categories in the following sections.

3. OSINT

3.1 Public information

Open Source Intelligence (OSINT) is the initial phase of cyber warfare related CNE. Here, the actor starts to use public information, which is available in newspapers, publically, or almost publically available reports, and similar sources. It is also possible to watch people moving to and from the target organization's premises, find out if they are working for the organization or otherwise have contacts. IT system related transports to the target's premises might reveal some hint of which makes of systems the organization uses. However, the actor has to act carefully, that their interest is not revealed.

3.2 Professional information

In addition to publically known information, the actor may also have access to job related information, like military magazines, conference proceedings and classified information – if not secret information of an enemy, anyway more insider information than in public magazines.

3.3 Internet searching

Those sources mentioned above did not yet include the Internet. Nowadays searching robots in Internet (Google, etc.) is the fastest way to find information. Choosing the right search terms is important in free text search, otherwise there

is either zero or very few search results, or so many that it may be difficult to pick those of value. Metadata based search can be more effective.

3.4 Social media and cloud computing

As sources of information, we should not forget the web 2.0 paradigm in the Internet. The two categories, which I have in mind here are various cloud computing and social media.

I do not here try to give any definition of cloud computing, neither will I go very deep into the science on how these may be used for CNO. Anyway, various kind of information may be stored in the Internet on some server, which location is not necessarily even known, most likely in a virtual server– which is perhaps doesn't matter here, as the data anyway has to be stored somewhere. The level and categories vary, but data may anyway be private, shared (among a group or dedicated users), or it may be public.

Take Dropbox as an example [15]. Usually the files are encrypted and requires authentication. It is also possible to share files through web, but only if the owner decides to do that. Conceptually that sounds very good. Yet, it is not considered completely trustworthy, because security has at some point of time been temporarily broken, and the files would at that point have been potentially accessible by anyone, see for example [16].

Especially among young people, various social media services are much used. Social media sites may of course also, if not mostly be variants of cloud services, so the two types of services are certainly overlapping. Naturally, when computing, communication and information move from stationary devices to clouds, the crackers and other parties, which try to misuse information, earn on it or otherwise make harm, also move there. Obviously, it is easy to spread malware through social media, and if some user in the target organization happens to download it, the attacker may be in.

Employers' attitude towards social media as professional communication channels varies from forbidding to promoting. As the phenomenon is fairly new, there may not even be clear guidelines for how social media should be used. For CNE/CNO actors, we shall not either underestimate cloud and social media services as sources of information. Say, the CNE actor knows from his work activity, that A is a highly authorized insider person in the target organization. From various social media it could be find out who are A's friends, his/her interests, etc. Even if A should not disclose any confidential data on such sources, this may still happen, directly if A does not care, know or understand the importance or classification of some fact, or indirectly if for example some of

A's friends or friends' friend may have revealed a bit too much. Alternatively the actor may find several small facts, which put together can be used to find out about the target.

3.5 DNS, etc.

In CNE, it is more important to find out about the systems and networks, and finding out about the people is only an intermediate phase. To find DNS information is the next step. Tools and commands, which can be used here are:

- nslookup (especially in interactive mode)
- dig
- whois
- finger
- dnsenum

The list below shows an example of what can be retrieved using the whois command:

```
whois 130.188.4.36
#
# Query terms are ambiguous.  The query is assumed
to be:
#     "n 130.188.4.36"
#
# Use "?" to get help.
#
…
… (Information about ARIN and whois deleted)
…
% Note: this output has been filtered.
% To receive output for a database update, use
  the "-B" flag.

% Information related to '130.188.0.0 -
130.188.255.255'

inetnum:   130.188.0.0 - 130.188.255.255
remarks:

remarks:   This inetnum has been transfered
           as part of the ERX.
```

```
remarks:    It was present in both the ARIN and
            RIPE databases, so
remarks:    the information from both databases
            has been merged.
remarks:    If you are the mntner of this
            object, please update it
remarks:    to reflect the correct information.
remarks:
remarks:    Please see the information for this
process:
remarks:    http://www.ripe.net/projects/erx/
            erx-ip/network130.html
remarks:
remarks:    **** INFORMATION FROM ARIN OBJECT ****
remarks:    netname: VTTNET
descr:      Technical Research Centre of Finland
descr:      Vuorimiehentie 5
descr:      Espoo, 02044 VTT
remarks:    country: FI
admin-c:    VS1745-RIPE
tech-c:     VS1745-RIPE
remarks:    changed: hostmaster@arin.net 19880919
remarks:    changed: hostmaster@arin.net 20000728
remarks:    **** INFORMATION FROM RIPE OBJECT ****
netname:    VTTNET
descr:      Finnish State Research Centre
descr:      FINLAND
country:    FI
admin-c:    JR2592-RIPE
tech-c:     VS1745-RIPE
remarks:    rev-srv:        vtt.fi
remarks:    rev-srv:        hydra.helsinki.fi
mnt-by:     AS565-MNT
status:     EARLY-REGISTRATION
source:     RIPE # Filtered
remarks:    rev-srv attribute deprecated by
            RIPE NCC on 02/09/2009

person:     Jan Rautalin
address:    Vuorimiehentie 5

phone:      +358 20 722 4107
nic-hdl:    JR2592-RIPE
```

```
source:     RIPE # Filtered

person:     Veikko Suutari
address:    VTT
            Vuorimiehentie 5
address:    02044 VTT
phone:      +358405899147
nic-hdl:    VS1745-RIPE
source:     RIPE # Filtered

% Information related to '130.188.0.0/16AS565'

route:      130.188.0.0/16
descr:      VTTNET
origin:     AS565
mnt-by:     AS565-MNT
source:     RIPE # Filtered
% This query was served by the RIPE Database Query
Service version 1.19.5 (WHOIS2)
```

Figure 2. Use of whois command

The information, which can be retrieved from various name servers and hosts using these commands vary, but the actor may anyway find out a lot about the network hierarchy, etc. Even if this is public information, there is a risk that an excessive investigation of a specific organization's network may be noticed, thus it would be safer for the actor to either hide behind for example *The Onion Router* (Tor), or to use web services, where these services are implemented.

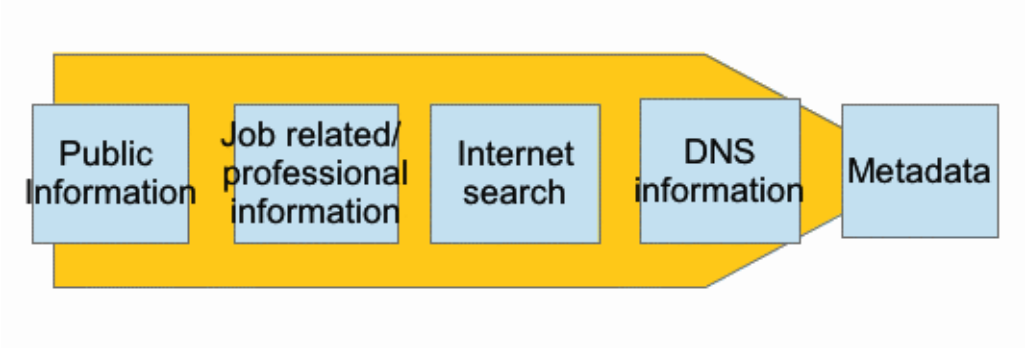


Figure 3. OSINT process [2]

3.6 SIGINT

In addition to OSINT, also signals intelligence (SIGINT) may be used to capture information [5].If the actor can get physically close enough, eavesdropping is an effective method. Copper or fiber cables may be difficult to access, but wireless LANs could be easily eavesdropped. Of course, traffic is encrypted, but media access control (MAC) addresses are anyway possible to find out. The MAC address reveals also the manufacturer of the network interface card [6].

4. Reconnaissance

4.1 Characteristics of reconnaissance

The intention of the reconnaissance phases is to invent and enumerate the target network and systems and do reconnaissance on it in more detail, until it is possible to access vulnerabilities. In [2] the actions described in this section are referred to as passive reconnaissance, as they are not attacks against the target system itself. An example mentioned is compromising a router, and slowing down other routes in order to route the target's traffic through the compromised router. Reconnaissance involves more direct actions to extract information from the target than OSINT. Information gathered with OSINT means may be utilized in this phase.

Even if the reconnaissance actions at least in initial steps are passive, they may be considered as attacks. The example of compromising a router is certainly an illegal action. As this also will alter the traffic pattern, it may be detected, either by the target (that at some point of time will recognize that their traffic is slowed down or uses other routes than generally) or the network operator, which also through network management notices the performance changes. A way for the attacker to hide the action would be to interfere with some event, which naturally causes a change in the traffic pattern, for example when some router is down or a new system is tested.

4.2 How to avoid detection

Generally, as mentioned in section 2, the actor should spread the actions, so that they seem to originate from varying IP addresses, preferably geographically in different countries. The actions can also be spread over a longer period of time than would be done in usual attacks, or when legally testing. Together, this would probably make the actions immune to intrusion detection systems (IDS) and intrusion prevention systems (IPS) [2].

Of course, traffic analyzing theory and more practically, knowledge of what is general traffic and what is not, is increasing by time. According to this increased knowledge, IDSs and IPSs can be better programmed and tuned, but still, distinguish normal traffic variations from attacks is difficult. A too paranoid tuning of the IDSs and IPSs would result in a lot of false positives.

4.3 Phases in reconnaissance

The reconnaissance process goes as follows [2]:

1. Enumeration of the environment. This means making a scheme of the network architecture of the target: the routes and addresses. Information from the OSINT phases helps here but also eavesdropping or wire-tapping. Network sniffers and various scanning tools will be used.
2. Use of port scanner(s) to find open ports.nmap is a commonly used port scanner program.
3. Testing of services on the open ports.
4. Fingerprint operation system(s)
5. Finally the actor accesses vulnerabilities. A useful tool for this step is Nessus.

4.4 Vulnerabilities

In critical environments it is likely that commonly known vulnerabilities are patched (not all, however, Microsoft's Internet Explorer seems still to suffer from the vulnerability mentioned in [7]. Not even their latest patch prevents one from jamming it.) In general, the actor trying to access vulnerabilities has to look for zero day vulnerabilities, i.e. such which are not commonly known.

Tools used in addition to port scanners are specific fingerprinting tools and banner grabbing tools [8]. The latter are used to list services. Some common tools, which may be used in CNE are listed in [9].

4.5 CNE process steps and intrusiveness

Figure 4 lists some CNE actions starting from such described in the OSINT section and ending with advanced persistent threat (APT), which is the "final goal" described in next section. The position on the Y-axis indicates intrusiveness versus openness of the action. The figure shall not be used to give objective values for how intrusive an action is, it is more of ordering the actions or methods mutually. Of course, this ordering is not either fixed, the actor may return to a previous method if needed, or of course pass some method if it is not worth the effort. The order is partly based on the figures in [2] and partly on my

subjective opinions. As already stated, the more intrusive the actions are, the bigger risk it is also for the actor. Roughly, the actor would also more seriously break the law when the CNE advances. Exceptions may be service interrogation and OS fingerprinting, which may vary from case to case. Systematic port scanning is certainly illegal.

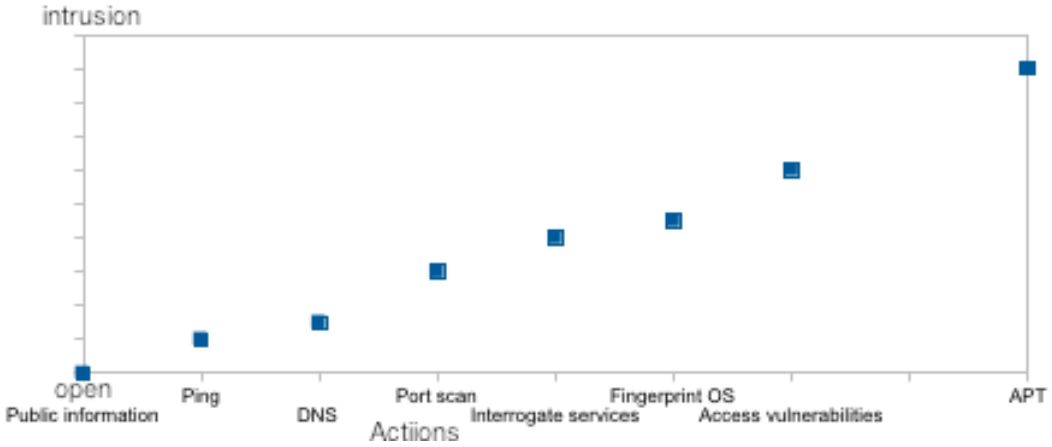


Figure 4. Some actions in the CNE process in a growing scale of intrusiveness. The scale is not intended to be linear or objectively measured

5. Surveillance

5.1 Reconnaissance vs. surveillance

After finding vulnerabilities in the target's network, CNE will gradually be extended towards surveillance. The difference between reconnaissance and surveillance is that reconnaissance implies single observations of the target environment, whereas surveillance is implies ongoing observations [2, 11]. It usually takes several months or even years, before the attacker withdraws or the attack is detected [13]. At least some of the tools and techniques, which are used for reconnaissance, could in principle also be used for surveillance, but in continuous use, there is a higher risk that they are discovered. Examples of surveillance actions are WikiLeaks's exfiltration of U.S. State information and the Night Dragon APT [13]. In addition to states, surveillance may also be domestic, for example industry espionage.

Surveillance of voice and data communication needs insertion of software and/or hardware into the target environment. Wire-tapping is regulated by law, but network centers have tools for lawful interception. This is used when the police

needs to wiretap phone calls and SMSs of suspected criminals, and certainly also to find possible terrorists. Can we trust in authorities that they do not misuse lawful interception? Probably not, it depends on the country. Foreign calls may be a significant risk as well as domestic traffic routed via foreign countries. According to [2], laws are not necessarily followed to letter, or it may be completely ignored.

5.2 Advanced persistent threat

Advanced persistent threat (APT) is a form of surveillance, defined as "an organized long term attack, designed to access and exfiltrate information from the target systems" [2]. The role of the actor is considerable more active than during the reconnaissance phase. Actually, APT is similar to an attack in general. In both cases, the attacker exploits one or more vulnerabilities in the target system, and possible inserts malware. The difference is that, when general crackers' attacks often cause significant damage, this is usually avoided in APT. The attacker wants still to operate unnoticed, as it then would be possible to conduct the surveillance for a longer time, once the target system is successfully attacked. The attacker's final goal is to be able to extract the intelligence continuously.

APT involves three steps [2]

- attack
- escalate
- exfiltrate.

5.2.1 Attack phase

The attack may occur at the client side, and/or custom malware may be used. If the vulnerability is not commonly known, and the malware is new, programmed and tuned for this specific purpose, it is very possible that the attack would be successful, especially if it is not too aggressive.

Botnets may be used for the attack. The principle of botnets is explained in [10]. The *bot* or *robot* means here a program that either executes small repetitive tasks on its own or acts as an agent, performing tasks controlled by the attacker. When the bot somehow, for example via a download or an email attachment, is loaded to a computer, the attacker may instruct the bot to execute tasks without the owner of the computer knowing it. When several computers are infected by the same bot, they form a botnet. A computer in the botnet is also called *zombie*.

The attacker, also called *botherder* instructs the bots via a command and control infrastructure (C&C), see figure 5. Typical attacks are sending spam, DDoS attacks, spreading of itself and other malware.

5.2.2 Escalation phase

In the escalation phase, the actor tries to get access to the desired information, which usually means rising the credentials. It may not be necessary to have root access, it is more important to gain just the rights needed. In some cases, it is also possible that the attacker gets directly enough rights to access the desired information, and escalation is not needed.

This may involve password cracking. Tools like *Cain and Abel*, *hydra* and *john the ripper* may be used for this. A tools, which combines several attack methods is *Metasploit.*

5.2.3 Exfiltration phase

The last phase of APT is exfiltration of the information. This means that information which interests the attacker (or the mandatory of the attacker) must be collected, temporarily stored and finally somehow transferred out of the target system.

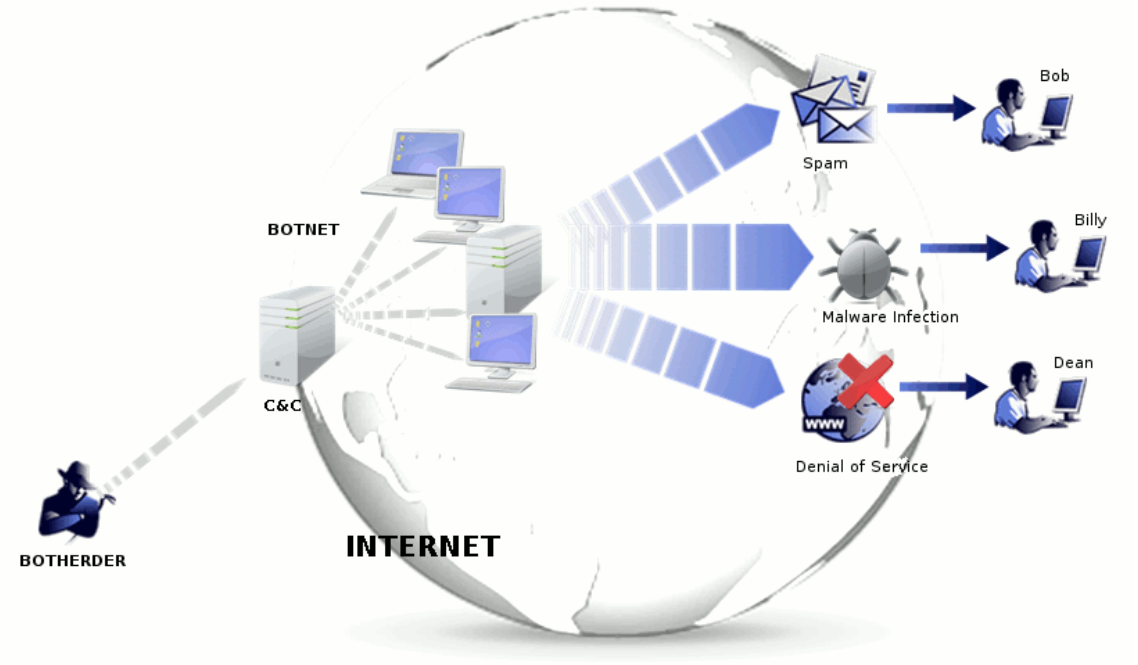


Figure 5. Botnet

The ways the attackers can use for exfiltration of information is described in [12]. As in the previous phases, the attacker may not hurry, but wait for the best time to start the exfiltration. They may store the data in password protected compressed archives.

Usually the same channel is not used for breaking in to the system and exfiltrate data [12]. A problem in getting the data out from highly secured systems is that most ports may be blocked. Sometimes the attacker may install a malicious program on the target system for email, FTP or HTTP communication. It is, however, likely that even these generic protocols cannot be used directly in highly secured networks, but only through special arrangements, like terminal servers. To use them, the attacker should thus have the credentials of some real user. But even if the ports would be open, such channels are likely to be monitored. It is safer for the attacker to use some covert channel. Such a channel is DNS exfiltration, which is outlined in [13].

A method to hide information mentioned in [12] is to use automated time delays between packets. Another method – especially useful if not covered channels are used – is steganography. There is for example a program named Steghide [14], which can be used to hide a file inside a picture or other huge file, where it is difficult to detect. A drawback with this method is that the size of the file needs to be much bigger than the actual information, in which the attacker is interested. Thus it is more usable in cases where the information transfer itself can occur quite fast. In covert channels, the affective bandwidth may be quite low.

6. Conclusion

We have realized, that CNE against a military or otherwise highly secured network or system requires a lot of work. On the other hand, there are the most fancy tools available even for free, which a skillful hacker may use. They also have the knowledge about vulnerabilities, which are not yet patched or maybe design flaws in the systems. Specific skills which the crackers have, is to increase their rights in the way that they can access almost any information, and go around almost any security measure.

We have seen that the CNE process starts with OSINT, and more exactly public and job related information available, both in the physical world and in the Internet. It continues with DNS related information and similar open network intelligence. The next step is reconnaissance, involving scanning of target systems. To get into the last phase, surveillance, the target system is attacked. The attacker insert tools, which can be used to exfiltrate intelligence from the

target. Thus, CNE is slowly advancing intrusion, which from the start to the end should be hidden if it's going to be successful. But the intention of CNE is not to damage the target system as attacks in general.

References

[1] What are Information Operations. Cyberspace and information operations study center. 2010. http://www.au.af.mil/info-ops/what.htm [Accessed 30.09.2012]

[2] Jason Andress and Steve Winterfield. Cyber Warfare, Techniques, Tactics amd Tools for Security Practitioners. ISBN 978-1-59749-637-7. Syngress, 2011.

[3] http://www.helsinki.fi/aleksanteri/civpro/publications/publications.htm

[4] Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia. Valtioneuvoston periaatepäätös 23.11.2006. Puolustusministeriö. ISBN 951-25-1727-2 (In Finnish)

[5] Signals Intelligence. Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Signals_intelligence [Accessed 6.10.2012]

[6] http://standards.ieee.org/develop/regauth/oui/oui.txt [Accessed 6.10.2012]

[7] Jan Lucénius. SECURITY COLLABORATION TOOLS FOR AUTHORITIES. COLLABORATION TOOLS IN THE MILITARY ENVIRONMENT. National Defence University. Department of Military Technology. ISBN 978-951-25-2124-1. Helsinki 2010

[8] Banner grabbing. Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Banner_grabbing [Accessed 7.10.2012]

[9] Top 15 Security/Hacking Tools & Utilities. http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/ [Accessed 7.10.2102]

[10] About Botnets. F-Secure. http://www.f-secure.com/en/web/labs_global/articles/about_botnets [Accessed 7.10.2102]

[11] U.S. Marine Corps. Imagery Intelligence. MCWP2-15.4. http://www.scribd.com/doc/9698904/US-Marine-Corps-Imagery-Intelligence-IMINT-MCWP-2154 [Accessed 8.10.2012]

[12] Exfiltration: How Hackers Get the Data Out. Host Exploit. October 08, 2012. http://news.hostexploit.com/cybercrime-news/4877-exfiltration-how-hackers-get-the-data-out.html

[13] Kenton Born. Browser-Based Covert Data Exfiltration. Kansas State University. Proceedings of the 9th Annual Security Conference. Las Vegas, Nevada. April 7-8, 2010. http://www.kentonborn.com/browser_data_exfiltration [Accessed 8.10.2012]

[14] Steghide http://steghide.sourceforge.net/ [Accessed 8.10.2012]

[15] Dropbox http://www.dropbox.com [Accessed 9.10.2012]

[16] Dropbox confirms user info was stolen, adds new security measures. http://www.engadget.com/2012/08/01/dropbox-confirms-security-breach-new-measures/ [Accessed 9.10.2012]

Non-State Actors in Cyberspace Operations

Johan Sigholm
Swedish National Defence College
johan.sigholm@fhs.se

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 cyber warfare capabilities, oftentimes by leveraging criminal organizations and irregular forces. Employment of such non-state actors as hacktivists, patriot hackers, and cyber militia in state-on-state cyberspace operations has also proved to be a usable model for conducting cyber attacks. 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 cyber warfare experience, and the limited encounters of legitimate cyber attacks, it is hard to precisely assess future effects, risks and potentials.

Keywords

Non-state actors, cyber, cyberspace, cyber war, cyber actions, cyber attack

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 [60]. 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 is thus becoming increasingly woven into the fabric of everyday life, and has brought with it many opportunities and positive changes as well as new threats to our society.

For private as well as public sectors, cyberspace has rapidly become an important environment, generating new business models and offering easy access to people, in their roles as customers and citizens. Large parts of trade, media distribution and social services around the globe are now dependent on pervasive communications networks, such as the Internet, or various forms of cloud-based infrastructures. Through its high-speed development cycles, cyberspace has become an incubator for ever evolving forms of entrepreneurship, technology advancement and spread of free speech that reflects the proliferation of democratic values and principles.

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 cyber defence 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 [43]. 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 cyber war, 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 "cyber attacks" (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 cyber conflict [47], acting as a sort of cyber militia, 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 cyber actions 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 [65]. In 2009, it was discovered that a cyber espionage 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 cyber warfare 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. 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][45]. 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 [54]). 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 cyber warfare 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 cyber war 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 cyber war, in relation to its physical-world counterpart of conventional kinetic war, and tries to disaggregate the various cyber actions that are commonly, sometimes quite carelessly, bundled into the concept of cyber attack. Section 4 describes the main relevant non-state actors in cyber conflict, and section 5 presents some benefits and drawbacks of nation-states employing these actors, such as questions regarding their combatant status. 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 cyber warfare, 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 cyber warfare 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 cyber conflict and cyber warfare, 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 [47][48][49].

3. Definitions and Principles

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

government reports and even scientific papers, one can read about cyber warfare, 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 "cyber warfare" or "cyber terrorism," 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.

Cyber actions 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.

Cyber attacks 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.

Cyber war occurs when cyber attacks 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 [64][11][7]. While the first four definitions are relatively straightforward and easy to deduce, the concept of cyber war is still somewhat elusive. One might reason that cyber war 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 cyber war. 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 [55]). Moreover, such a simple definition of cyber war 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 [62]. 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 [61]. 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 cyber attack (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 cyber war without actual cyber attacks [7].

Cyber warfare 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 cyber attacks 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 cyber attacks. A major drawback is the lack of control and estimation of

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" cyber actions

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 cyber attack 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 cyber attacks.

A way of resolving the aforementioned political backlashes of cyber attacks, 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.

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

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	Decision makers 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

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 above, early instances of cyber actions (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.

During the late 1990s, when access to and use of Internet had become commonplace, physical-world conflicts triggered many state-targeted cyber actions, primarily conducted by non-state actors. Hackers with nationalistic tendencies aimed their cyber actions 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 [44] 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 cyber actions, 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 above, 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 cyber actions 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 cyber action.

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.

Hackers with hats of all colors (see below) view script kiddies with alarm and contempt since they do nothing to advance the "art" of hacking, and sometimes incur the wrath of authorities on the entire hacker community. While a hacker takes pride in the quality or originality of an attack – commonly leaving no trace of an intrusion – a script kiddie may aim at pure quantity, seeing the number of successfully compromised servers, Trojanized clients, or stolen credit cards as a way to obtain attention and notoriety. Script kiddies are sometimes portrayed in media as bored, lonely teenagers seeking recognition from their peers.

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 [46]. 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 cyber actions 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.

The stereotypic hacker, as portrayed in movies and through popular culture, is a young “nerdy” male, dressed in black clothes, an enthusiastic fan of the science fiction genre, lacking general social skills and preferring fast food and high-caffeine content soft drinks. Although this might once have held some measure of truth, the concept of a hacker has expanded greatly and includes wide ranges of people, including self-taught computer specialists, computer science college students and security professionals of many occupations. These hackers 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. This approach stands in contrast to that of black-hat hackers, who usually keep their findings to themselves, in order to develop exploits targeting the specific, unknown vulnerability (also called zero-day attacks).

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 cyber actions 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 [48]. Russian patriot hackers were also implicated for several web defacements during the 1999 Kosovo conflict, such as those previously mentioned above, and for various cyber actions 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") [59]. 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 [58][6], whereas others mean that the fear of cyber terrorism has been greatly exaggerated and is largely blown out of proportion [52][68], perhaps at the expense of more plausible and possible cyber problems [23].

There have not yet been any reported cases of cyber terror attacks, and it has been argued that cyber terrorism 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. After the 9/11 terror attacks in the United States, it became apparent that the country was quite ill-prepared for preventing those types of events. Later investigations showed that part of the responsibility for this inability could be attributed to "the stovepiping of intelligence that allowed the attack to go unmitigated." [2] This was subsequently addressed by enacting new laws and empowering certain authorities to allow for harsher monitoring and surveillance, so that greater amounts of information could be collected to feed the various intelligence agencies.

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 [51]. 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 cyber criminals

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 [63]. 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 cyber actions 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][63].

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 [63]. 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 [57]. 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 [53]."

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 cyber warfare 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 cyber conflict, 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.

The National Security Agency (NSA) and the Central Intelligence Agency (CIA) are two of the largest intelligence organizations within the United States government. Besides having a large number of intelligence analysts, these organizations frequently employ prominent mathematicians and computer scientists to study encryption algorithms and to develop cryptanalysis tools. This sort of work has significantly helped to win battles and to end wars, and is thus considered to be of very high importance to national security and the armed forces [66]. In 2010 the United States Cyber Command, co-located with the NSA, gained operational capability. The command's main purpose is to organize and coordinate the U.S. cyber resources, and to ensure U.S. and allied freedom of action in cyberspace and deny the same to its adversaries. Similar military organizations are being established in many countries, as cyberspace is increasingly being recognized as an important arena for military operations. Cyber espionage agents are thus a key asset which is essential in maintaining information dominance.

4.13 Cyber militias

A cyber militia may be defined as a group of volunteers who are willing and able to use cyber attacks (or perhaps disruptive cyber actions as defined in this paper) in order to achieve a political goal [48]. 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 cyber militia do not get any monetary rewards for their services, nor are they bound by any contractual obligation [48]. Regular military cyber-units, or a national cyber reserve forces, are in this context not considered to be cyber militia, 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 cyber militia in their spare time. The members of a cyber militia 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 cyber actions 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 [50], 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 cyber militia was responsible [49][3].

As cyber attacks can be launched by proxy, using trojanized unsuspecting end-users' computers, proving whether nation-states are engaging in cyber warfare is naturally difficult. Cyber-militias have been suspected of performing several recent high-profile cyber actions 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 cyber warfare 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 cyber war, which would limit their freedom of action, or to formally take responsibility for executed cyber attacks. Furthermore, cyber attacks 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.

Some of the main "pros and cons" of engaging in cyber warfare, 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.

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

5.1 Benefits

The attacker gains the initiative and can most often conduct cyber attacks 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 cyber attack 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 cyber warfare creates a useful shield of legal ambiguity.

The attacker can outsource cyber attacks 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 cyber attack, 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 cyber militias, 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 cyber attacks 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 cyber terrorism, 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 cyber warfare 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 cyber conflict.

The use of cyber attacks 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 cyber warfare. Even other, less destructive cyber actions, could probably constitute acts of war according to the UN Charter [55], 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 cyber attacks. 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 cyber warfare. The reason is that it would be likely be impossible to carry out cyber attacks while remaining within the legal framework. Nevertheless, should new conventions on cyber warfare be universally ratified, covertly outsourcing cyber attacks 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 cyber attack victims.

Another relevant question is if an individual who conducts a cyber attack 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 cyber forces might fail to meet the requirements of the Geneva Convention. Although they are afforded privileged combatant status when engaged in conventional hostilities, conducting cyber attacks could potentially deprive them of that status. While members of regular armed forces might be wearing uniforms when conducting a cyber attack, the victims of their attack will not be able see it. Carrying arms openly is also quite unlikely as most cyber attacks 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 cyber attacks. 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 cyber warfare, 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 cyber weapons 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 cyber conflict with Georgia demonstrated a usable model for conducting limited-scope cyber attacks. By use of patriot hackers or cyber militias, 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 artificial nature of the cyber environment is one of the fundamental differences between cyber warfare and kinetic warfare. Conventional warfare is carried out in the physical world, governed by the familiar laws of physics that we know and understand with respect to warfare. Cyber warfare, on the other hand, takes place in an artificial world, created by humans, in a state of constant change. While some principles of kinetic warfare can be employed in cyber warfare, others have minor or no meaning in cyberspace. Some concrete examples are the concepts of distance, time and targeting, which are essential in the planning and execution of conventional warfare. The principles of cyber warfare are thus fundamentally different from those of kinetic warfare. This fact highlights the need for a new military approach when considering cyber war, including the development of strategy, tactics, tools and specializations to suit the needs of future operations in cyberspace.

The true nature of cyber warfare, cyber conflict, 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, hacktivists and patriot hackers, or between cybercriminals and cyber espionage 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.

As we have seen, the threat of an imminent all-out cyber war is not very likely. The prospect of bringing warfare to the cyber arena does nevertheless promise significant asymmetric advantages to a limited resource nation-state, especially if the attacker can remain anonymous. Moreover, if the instigating nation covertly employs cyber militias and hacktivists to carry out cyber attacks, 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 cyber attacks. 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 cyber warfare, and perhaps even actively undermine such efforts, as the asymmetric nature of cyber warfare benefits those who lack the ability to dominate in conventional arenas. Even if the international community were successful in codifying cyber warfare 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 cyber actions 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 cyber actions 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 cyber terror 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 cyber terror 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 cyber terror 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 cyber attacks [56]. 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. Cyber conflicts 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, cyber actions involve various non-state actors. However, the overlapping gray-zone between these actor categories and legitimate state-backed cyber warriors are a source of concern since no legal definition of cyber warfare, 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, cyber militias, 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 cyber actions, or cyber attacks, have resulted in physical injury or extended destruction of property, the heavy cyber-dependency of modern western countries makes more damaging cyber attacks 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 cyber defense.

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 cyber terrorists are growing up with computers and smartphones, the advent of cyber attacks 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., “Organized 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] Netherlands Ministry of Defence, “The Defence Cyber Strategy”, Jun. 27 2012.

[44] 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/

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

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

[47] 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.

[48] 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.

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

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

[51] 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/

[52] 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/

[53] 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

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

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

[56] 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/

[57] Theriault, C., “Brazil's cybercrime evolution - it doesn't look pretty,” Sophos Naked Security, Oct. 5 2011.

[58] 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

[59] 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

[60] U.S. Department of Defense, “Strategy for Operating in Cyberspace”, July 2011.

[61] 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, November 2011.

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

[63] 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.

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

[65] 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

[66] Wang, J., “Computer Network Security: Theory and Practice,” Springer-Verlag Berlin Heidelberg, 2009.

[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

Offensive Cyber-capabilities against Critical Infrastructure

Timo Kiravuo,
Aalto University
timo.kiravuo@aalto.fi

Abstract

The Stuxnet worm changed the picture of cyber war from abstract to concrete in an undeniable way. This paper studies the implications of recent discovery of Stuxnet and other self-replicating cyber weapons. We describe the state of art in known cyber weaponry and extrapolate the requirements and attributes for potential weapons. From this understanding of the weapons we discuss some aspects of future cyber doctrine.

1. Introduction

This paper studies the structure and use of cyber weapons that are targeted against the critical infrastructure of a modern society. Digitalization of the infrastructure has provided a large number of vulnerabilities and by analyzing and understanding them we can envision potential cyber weapons to use against these vulnerabilities. Understanding the behavior and capabilities of these weapons enables us to design defense against them.

Cyber war itself is a new concept that is still looking for its meaning. We think that a recognized war between nations, which is fought only over computer networks is not a likely occurrence in near future. More likely is that cyber operations will be used during conventional war, where they form one supporting theater, similar in concept to air war. And, as one of the characteristics of cyber weapons is deniability, clandestine cyber operations will take place but as the perpetrator is not known, a war will not be declared.

No commonly agreed definition of cyber security exists yet; for this paper we define “cyber security” as *security of all kinds of digital systems* and “cyber weapons” as *computer based capabilities against digital systems*. The purpose of the first definition is to emphasize that our digital infrastructure includes devices that are not commonly viewed as “computers”, such as the power grid, traffic lights and cars. The second definition emphasizes the nature of cyber weapons as a collection of tools and modules rather than individual pieces of software or

hardware. We also think that "cyber war" could be defined as *operations against a nation's digital systems, which threaten its national and economic security*.

2. Critical Digital Infrastructure

The digital systems on which the modern society is based have been built with reliability and industrial safety in mind. Threat of an intentional adversary has usually not been included in planning and, when realized, has usually been countered by isolating these systems to their own networks.

Those parts of the infrastructure that are vital to the workings of a nation can be considered the *critical infrastructure* and with the digitalization of these systems part of this infrastructure is the *critical digital infrastructure*. When computers and digital automation are used to control systems, their actions are fast and invisible, unlike a human controller's. Many parts of the modern infrastructure are also very complex. This leaves an opening for an attacker that wishes to harm the society. Conventional attacks require human presence at the system one wishes to influence; digital attacks can be performed over networks or by autonomous software without physical presence.

The lack of need to be present is what distinguishes cyber warfare mostly from conventional warfare. Computer networks, like the Internet are in effect almost "zero-dimensional", any point in the network can be reached from any other point and the effort is not dependent on the distance between the points.

The purpose of a nation's military forces is usually to protect the existence of the nation and its people. As the vulnerabilities created by the digitalization of the infrastructure become more clear, the demands for the military grow. How the need to protect the infrastructure affects the mission of the military will be an interesting question that needs to be answered in many countries in the near future.

2.1 Automation systems in critical infrastructure

Industrial automation has progressed steadily from fixed, mechanical automation via more flexible digital automation to centrally controlled systems. For example the water supply for a city could be run from a reservoir to water towers and to residential areas and be controlled with mechanical valves that are controlled by floats and levers that sense water levels. The water towers guarantee a sufficient water pressure to the homes, but a large amount of water is stored in the system, getting stale and possibly polluted by bacteria. Replacing the towers with pumps and smart controllers lessens the amount of water in system, increasing quality and offering better overall control, but removes the automatic redundancy from the system and makes it more vulnerable to loss of control.

A town's water supply is a relatively simple control process, with basically one product flowing in one direction with little processing. Many critical systems are more complex and require much more control. For example the processes required to turn raw oil to fuels, lubricants and various chemicals for other industries are complex. Centralized control helps in tuning these processes to be very efficient, enabling a continuous flow of materials and lowering the cost of process, but the removal of intermediate storage and fine tuning of various steps have created a process that can not be controlled manually any longer. A modern chemical plant is worthless without its automation systems.

Modern automation systems are networked. Typically a process is controlled by a local control unit that may just transmit signals to and fro, but often also includes some logic capabilities. For example a programmable logic controller (PLC) may monitor and control the temperature or speed of a process. These units are then connected to a central control unit that monitors the overall process, called a distributed control system (DCS) or supervisory control and data acquisition (SCADA) system. These central controllers are usually connected to database servers and operator workstations using Ethernet and Internet technologies. [1]

When automation technologies were developing, safety concerns were raised and while a hundred years ago an employee who lost important body parts to machines was considered careless, today's automation is controlled both by laws and by a culture of safety and even minor incidents are a cause of inquiry. However, this culture of safety does not consider intentional harm. The situation is very analogous to computer security. Before the spread of Internet computer security was a theoretical field, with practical interest only to military and banks. When Internet became ubiquitous security became every person's practical concern. Current automated systems are connected to the Internet, directly or indirectly, and the shift to security thinking has not yet happened in the profession. This is the very reason why the infrastructure of all developed nations is vulnerable.

2.2 Targeting the critical infra

Lewis [9] presents the critical infrastructure of a nation as 11 interdependent sectors, such as telecommunications, finance, postal service and chemical industries. His analysis points out that attacking any sector will likely affect several of other sectors. Transportation requires communications and fuel for daily operations, but also spare parts and food and water for drivers. Lewis categorizes the challenges of protecting this infrastructure to seven categories: size of national infrastructure, unclear command structure involving public and private sector, lack of information sharing, lack of knowledge on the complex infrastructure, interdependencies between the sectors, inadequate analysis tools

and the asymmetricity between a defender trying to defend everything and an attacker being able to pick any target.

It should be noted that while Lewis stresses the interdependence of the critical infrastructure, actual governments often consider these sectors independent. For example the Finnish national security strategy charges Ministry of Traffic and communications with the responsibility for electric data and communications infrastructure, but Ministry of Employment and the Economy with providing the needed power. [2]

For analyzing and solving the problem of protecting the infrastructure of a nation, Lewis recommends an approach that models properties of the infrastructure as a network. This enables the analysis of interdependencies and can bring out features of the infrastructure, such as critical links and nodes, cascade behavior (failures that spread causing other parts of the network to fail, too), or resiliency to failures. Once the network is understood, its parts can also be analyzed for threats and vulnerabilities.

Lewis's approach is particularly useful when analyzing a new area of national security. Governments have national security strategies, but for example the current Finnish strategy [2] is a static list of protection areas and tasks to be taken to protect them.

3. Actors

Several groups of people may have an interest in damaging the infrastructure of a nation or performing other types of cyber attacks. [13]

Nation states can see a possibility to reach their goals without resorting to military action. What is considered a war in cyberspace is not yet clear, nor is how to respond to acts of cyber war. The governmental actors may be from military or intelligence, or government controlled activists.

Organized crime has found the networked society useful for criminal activities, such as extortion by threatening to perform denial of service attacks on web sites, simple blackmail by gaining access to information or encrypting data and demanding money for the decryption key. Cyber-physical systems provide an extension for these activities.

Corporations might find that the anonymity of cyberspace lowers the risk of detection of disturbing the competition. Losses in production, defects in quality or disruption of logistics can make a difference to the competition. Corporations may also be aided by their national governments. The wellbeing and worth of a

nation is no longer as tied to the land area it controls, but to the wealth and profitability of its corporations and residents.

Terrorists and **politically motivated hactivists** are likely to take advantage of the asymmetry provided by the digital environment. Their goal may be to damage the society or to get attention to their political message.

Hobbyist hackers and script kiddies may damage the infrastructure just out of curiosity or neglect.

Unhappy employees are traditionally known to be a sizeable threat segment in security. They have usually both knowledge of and access to systems and various motivations to cause them to use this knowledge for harmful activities.

It should be noted that while protection from attacks from other nations and possibly terrorists falls under the military area, similar attacks from other parties are clearly a civilian law enforcement matter, even if there is no difference in act and damage.

4. Cyber Weapons

When the Stuxnet worm came to light in 2010, it ignited the field of cyber security. Previous cyber attacks had been mostly politically motivated web site defacements or shutdowns, such as the Bronze soldier attacks against Estonia in 2007 or the various attacks during the South Ossetian war in 2008.

Stuxnet, however, was a different type of a beast. A carefully crafted software worm aimed at a single, specific target. At an assumed cost of millions of dollars, it was beyond the capabilities of hobbyist troublemakers, but extremely cheap by military standards. After Stuxnet the risk of a targeted, well resourced cyber attack can no longer be ignored.

4.1 Protest attacks

The Bronze Soldier attacks were targeted against Estonian web sites at 2007 and were related to moving a Soviet era statue in Tallinn. The effect of the attack was denial of service by traffic overload at web server and some servers were broken into and defaced. Similar attacks happened during the South Ossetian war in 2008.
These attacks had mostly nuisance value. When a web server is overloaded, it will return to normal use once the attack stops. Depending on network architecture, continuous attacks may be blocked by the network operator before they reach the target server. Defaced web sites are usually fairly easy to replace

from backups onto new server platforms that don't have the vulnerabilities that let the attacker into the first server.

Thus on the strategic level the attacks achieved nothing and on tactical level they tied up some resources and prevented use of web pages for a while. However, attacks of this type should not be considered insignificant. They are the equivalent of light cavalry or skirmishers, which do not have the power to win a battle, but can not be ignored either. Attacks of this type have a low cost, can hunt for targets of opportunity and tie up opponent's resources.

4.2 Advanced persistent threat

Titan Rain is the US name for series of persistent, targeted attacks against US computer systems, especially in the defense industry 2003-2005. [12] The goal of these attacks appears to be to get access to sensitive information at specific targets. Attacks of this type have given rise to the concept of advanced persistent threat (APT), where the attacker sets a specific goal and keeps on trying to reach that goal, over a long period of time and using different methods. Unlike the nuisance attacks, ATP operations serve a strategic goal.

4.3 Stuxnet

Stuxnet is a carefully crafted worm targeted specifically against the Iranian Natanz nuclear enrichment plant [5]. It is designed to be transported inside the plant on a USB thumb drive where it will penetrate the controlling SCADA servers using known Windows vulnerabilities. After penetration the code will run on the server and program the controllers of the enrichment centrifuges to change their speed, which causes the high-speed centrifuges to break. To avoid detection the program reports false centrifuge speeds to the management system of the centrifuges, thus hiding the reason of centrifuge breaks.

Stuxnet was created by United States and Israel [14] and it served two political goals: to slow down or stop the Iranian nuclear weapons program and to avoid using conventional military force in this. While the details of the Stuxnet program are not public, it has been estimated that the project might have been realized with only perhaps a dozen programmers and analysts and a budget in the order of millions of dollars [8]. Before the administration of United States decided to reveal their involvement, Stuxnet provided also plausible deniability, unlike a kinetic attack would have.

The Stuxnet attack was a multiyear project preceded by careful reconnaissance of the target plant. Several versions of the worm were created and deployed. The attack followed the advanced persistent threat (APT) concept, where the attacker selects the target and keeps on working towards their goal, using high level of technology.

4.4 Other autonomous cyber weapons

Besides Stuxnet, several other autonomous cyber weapons have been observed. We present Duqu and Flame, that are assumed to be linked to cyber operations by the United States.

4.4.1 Duqu

Duqu is a intelligence gathering Trojan horse that shares some components with the Stuxnet. Most likely it has been developed in same organization that has developed Stuxnet, too. [3, 4, 8]

The general insertion method might vary, in one instance Duqu is known to have been inserted via e-mailed Word document. Duqu has several methods to make its detection harder: it may be recompiled differently for each insertion, after insertion Duqu waits for a 10 minute period of user inactivity before starting to install itself to the operating system, installation uses signed installation files making Duqu appear legitimate and after 30 days Duqu uninstalls itself unless instructed to remain.

Duqu downloads the payload modules after installation. Observed functionalities include keylogging (keyboard capture), screen capture and transmitting selected files from the target host to the C&C server. Payloads can browse file shares and their download can be instructed from the C&C server, thus designating Duqu as an intelligence gathering platform is based on its use, not its capabilities.

4.4.2 Flame

Flame is a sophisticated modular attack toolkit, deployed to the Middle East in 2010. Flame appears not to have any direct relation with Stuxnet, but it may be a separate approach by the same organization. The malware is large, about 20 MB in all, modular and communicates with its command and control servers. The payloads deployed have shown intelligence gathering features, capturing screenshots and keyboard input, recording audio and listening to network traffic. Flame has also its own SQL database for storing information and it uses a scripting language called LUA. [6, 16]

Flame is an actively run piece of malware. Several versions have been found, which means that the code is being developed and updated. Various instances can have different modules deployed. Dozens of C&C servers are deployed around the world. Flame seems to collect AutoCAD drawings, e-mails, PDF-documents and sends them or summaries of them to the control servers. For spreading to new hosts, Flame uses several methods, one of which is masquerading as a Microsoft Windows Update server and sends itself to the target machine as a Windows Gadget update [7].

5. From Cyber Weapons to Cyber-capability

The previously presented examples show that existing cyber weapons are already modular and form a family of weapons that share some components and have other modules tailored for a particular task. We consider that a cyber weapon is just an instance created from a larger pool of cyber-capability. An individual tool has tactical and operational significance, a toolbox from which these tools are created has strategic significance. Based on what we know about existing cyber weapons and malware in general, we can describe a likely toolbox for future cyber operations.

5.1 Independent component capabilities

To be able to have a "cyber-capability", the components must exist and be ready for use. The actual weapon is then integrated according to operational requirements.

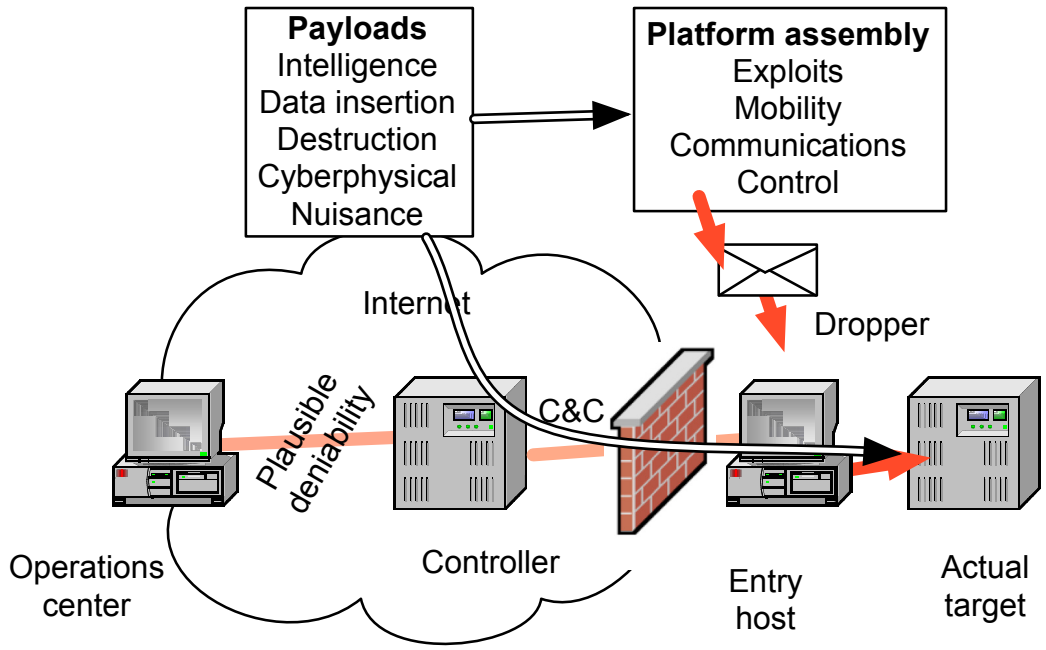


Figure 1. Assembly and deployment of a cyber weapon

5.1.1 Payloads

Payload is the actual reason for the weapon, rest of the system serves it. Different types of payloads are needed for different missions.

Intelligence gathering payloads can look for files based on name or content, analyze the network to which the host machine is connected, use the microphone and web camera in the system, collect data from keyboard and display and so on. This intelligence can then be sent back to the controller of the operation using the command and control channels available. If network connectivity is not available, the data may be attached to the weapon itself and transported along with the weapon's code as a virus.

Misinformation payloads may be used for information warfare. These may take different forms but are likely to be targeted against specific systems, such as cyber-physical monitoring systems, centers for monitoring any vital resources or planning documents. Payloads of this type have a huge potential if they can control the information the leaders of the opposition see. Actual operations can be hidden, false ones created, logistics misdirected, equipment miscontrolled and so on.

Destructive sabotage payloads may delete data from databases and files and format hard disks. They may also target cyber-physical systems. For the latter purpose the cyber-capability should include knowledge of potential target systems and how to control them. Part of building the cyber-capability may include collecting automation hardware from sources such as eBay for analysis.
Nuisance payloads such as resource consuming denial of service (DoS) payloads may be used to attract attention and to consume both computing and human resources.

To maintain operational security, the payload may be encrypted and the decryption key delivered later.

5.1.2 Exploits

A library of vulnerabilities in software and matching methods to use them (exploits) is needed to enter the target systems. According to current reports the price of a new, unpublished vulnerability (so called zero-day vulnerability) is in the order of hundreds of thousands of dollars for popular operating systems. Defense products companies, such as Vupen[1] are already purchasing and selling these. [15]

5.1.3 Mobility module

If the system to be penetrated is protected by a firewall, air gap (no direct network connectivity) or some other method preventing direct access from the command and control servers, self-replicating, mobile code may be used, making the weapon in effect a worm or virus. The code must know what to copy and

[1] http://www.vupen.com

where in the new system, how to decide where to go, identify itself to avoid conflicting with itself. However, the viral mobility of the weapon makes it more likely to be detected and thus there is a case for leaving the mobility out, reducing the weapon to a Trojan horse.

5.1.4 Command, control and communications module

A cyber weapon may operate autonomously or have tight or loose control. An autonomous weapon must have its own logic programmed to control its payload activities and mobility, including the decision of whether to trigger the payload or not. Being able to control the weapon increases operator's possibilities to react to findings, for example new modules may be loaded to the weapon. However, the control channel adds the risk of detection and may not be always technically possible.

If the cyber weapon is deployed to a host that has network connectivity, it can communicate with the command and control (C&C) server (described in next section). The capabilities of this control channel depend on the properties of the path. Firewalls or intrusion prevention systems may limit the protocols or volume available. Hiding the existence and traffic on this channel is usually desirable. The channel may be masqueraded as a video game protocol or ordinary web browsing. Botnets consisting of a large amount of synchronized computers use often the Internet Relay Chat (IRC) as control channel, as it allows spreading information fast to large amounts of nodes.

If direct network connectivity is not available, the weapon may use other methods, for example part of the weapon may be on an isolated network and connect using USB media to another part in an Internet connected network. Or the audio components of a computer may be used to communicate with another computer.

A command and control channel is used to steer the cyber weapon and to receive data from it, and also to provide separation between the weapon and its users. A properly constructed command and control system includes sufficient number of cutouts to provide deniability to the owner of the weapon.

5.1.5 Command and control servers

Cyber attacks may be controlled from the attacker's own computers (leading to easy detection) or, more preferably, from deniable computers, either captured third party computers or legally acquired hosts.

A suitable controller would be a server host from a cloud server, easily acquired at low cost. Any competent intelligence organization should be able to organize a

process for acquiring a set of untraceable servers spread internationally to different places.

The weapon code must carry some address that enables it to locate the control server. This could be the IP address or DNS name of the server or some more complicated method, like IRC channel name, Bittorrent hash table or a WWW URL. This will be found when the weapon is found and dissected, thus the need for a deniable server and additional cut-outs even when connecting to that server (e.g. making all connections over public WLAN).

5.1.6 Droppers

To deliver the viral software to the target system, a dropper component can be used. The dropper enables packaging the rest of the software to an e-mail message, web page, software update, auto-executable file on a USB drive or other initial delivery vector. When activated, the dropper installs the viral code to the target system, where it activates and starts its own activities. (Applies also to Trojan horses, explain terminology somewhere.)

The actual code for the software can be included in the same package as the dropper, or it can be downloaded from elsewhere. As seen in the case of Duqu the dropper can contain its own stealth methods, such as waiting for a period of no keyboard activity to initiate its operations.

To give an example, one of the methods used to inject the commercial FinFisher[2] surveillance product to the target workstation is to send an e-mail message with the program included. To avoid the recipient to notice that the attachment is a program, it is named gjp.1bajaR.exe, with the Unicode “right-to-left override” character as first character, causing the file name to appear as exe.Rajab1.jpg. [10]

5.2 Integrated components and capabilities

In addition to the prepared modules, there are features useful for a cyber weapon, that do not form their own software module.

5.2.1 Stealth

In general low probability of detection is a desirable feature in cyber weapons. This is not a property of any individual component, but a property that emerges from overall design and operation of the weapon. Detection can be avoided by features such as slow propagation rate, small size, ability to hide in the operating system and low activity level when human are operators present. A common way

[2] http://www.finfisher.com

for intruders and malware to hide in the operating system is to masquerade as utility programs, device drivers, software libraries and such, and to modify or replace analysis tools with versions that do not show the processes and files of the malware or the intruder. Stealth during the installation may be assisted by acquiring valid installation certificates for the cyber weapon.

5.2.2 Hidden components

To avoid analysis parts of the malware can be encrypted without including the decryption key in the malware itself. The key to activate the encrypted portion may be transmitted from operations center or may be created (via a cryptographic hash) from environmental parameters the weapon will encounter only when it reaches the target system.

5.2.3 Removal of tracks

To avoid detection and analysis a cyber weapon may want to remove its tracks in various ways. A sensible guideline would be to remove any component, like the dropper, when it is no longer needed. If possible, the weapon should analyze the backup service in the target system and to try to avoid being included in the backup.

5.2.4 Kill switch

For various reasons it may be desirable that the operation of a cyber weapon to be halted. For weapons that are able to connect to the Internet, this may be a message from the control server. To protect the weapon, this message may be cryptographically signed to verify its authenticity (using asymmetric encryption means that detection of the decryption key does not matter). One method to kill the weapon would be to prepare an identification string and removal instructions for anti-viral software, to be published if needed.

5.2.5 Countermeasures after detection

To avoid analysis and to gain time future cyber weapons may include functionality to defend itself from detection. There is no trivial way to identify detection, but access to the weapon’s files or processes may indicate an attempt to detect it, as does use of system tools. If the weapon estimates that it has been detected or detection is likely, it can activate countermeasures such as spreading rapidly virally, mutate itself to avoid analysis or even spawn a hidden copy of itself or a different weapon. The goal is not so much to avoid detection, but to gain time by increasing the defender’s work load. Human detection and analysis move at human speed, while software moves at subsecond time frame. Depending on the mission, the weapon might gain mission success even after initial detection, by avoiding analysis and keeping the defenders occupied.

5.3 Operational integration

As discussed above, a modular architecture is a likely solution to be employed for creating a cyber weapons capability in the long run. Modularity allows the actual weapons to be crafted according to the needs, increasing flexibility and decreasing costs. However, modularity is not without its own issues.
For a modular system to work, the interfaces between the components and the architecture need to be well defined. Ideally it should be possible to create a weapon just by selecting its desired functionality and assembling the components, in practice this might be challenging if cloaking from anti-viral detectors is also desired. Depending on the architecture, there may be a need for integration testing.

Thorough testing takes time that may not be available. It can be assumed that any cyber weapon will have defects and some of these defects will cause unintended consequences. For example an autonomous cyber weapon may start to spread more rapidly and widely than intended or it may target wrong systems, including the operator's own systems.

To make detection harder, a compiler can be created that randomizes the structure of code thus making each instance of the weapon unique and more difficult to be recognized by antiviral software and other tools. There could be several libraries that are randomly used to implement same higher layer primitives or different machine language operands can be used for same low level function. In a similar way dropper programs may be created in a way, that makes them appear unique. Each target system could then be targeted with an individual binary.

6. Cyber Doctrine

From the study of existing cyber weapons, we propose some insight that could be included when creating a cyber doctrine.

6.1 Defensive cyber strategy for the nation and its military

The military forces of a nation exist only to protect it, thus the cyber strategy must protect the nation, not just its military forces. As shown, the digital civilian infrastructure presents a great vulnerability to modern society and requires protection. However, the national defense strategy does not necessarily require this part of defense to be under the military. This cyber defense may be considered part of civil defense, instead of military defense, thus also being more likely to be considered unlawful target for military actions. [17]

Credibility of cyber defense is not based on the amount of servers, firewalls or technicians, as the attacker can select the point of attack. We think that the most effective way of providing credible cyber defense is to show that a nation has a comprehensive cyber security program that covers all areas of critical infrastructure. Such a program would include recognizing and analyzing the critical infrastructure, educating its operators, setting standards and requirements and auditing the results. A nation thusly protected is likely to survive a cyber attack and less likely to be attacked in the first place. If the program is in civilian hands, it enables the claim that their infrastructure is not a lawful target.

6.2 Offensive cyber strategy

Offensive strategy is not as necessary as defense. Retaliation against cyber attacks with similar attacks is not a sound strategy, as the source of attacks is likely to be very hard to identify.

The basis of an offensive strategy is a constant creation of cyber-capabilities and targets. Computer and cyber-physical systems can change rather rapidly and the time it takes to develop a weapon from scratch may close the time window to hit that target.

However, since the industrial automation sector is very conservative in deploying updates to operating systems and other software, in fear of disturbing the process being controlled, there is a permanent window of opportunity between release of a security update and its deployment. During this window the supplier of the automation system and its users are verifying that the new patch does not disturb the control systems and the attacker may reverse engineer the update and develop an exploit to be used before the update is deployed.

Targeting is likely to require creation of intelligence gathering operations to support he cyber operations. If the target is civilian infrastructure, information can often be easily obtained from public sources, such as tenders for automation systems or company websites.

A long term strategic process can be described: Learn the capabilities of cyber weapons. Create a cyber-command leadership that understands these capabilities. Communicate these capabilities to other branches in the military and intelligence community. Make sure enough knowledge is available to the planning of military operations. Knowledge of cyber-capabilities should be available to planners so that cyber operations can be used to support or replace conventional operations.

6.3 Cyber deterrence

The concept of deterrence is based on the ability to inflict retaliatory force on an adversary at will and using this ability to force the opponent to refrain from some

actions. For example nuclear deterrent is based on the capability of being able detect development of nuclear weapons and to deliver unilateral destruction that the target can not prevent.

Credible defense deflects the deterrence. Resource consuming denial of service attacks can be thwarted by deploying more resources. Logical attacks, in turn, can be thwarted by removing systems off-line, maintaining proper security practices and distributing systems so that exploiting the remaining vulnerabilities does not ensure catastrophic failure of systems. Thus using cyber weapons to threat other parties is likely to not be very effective. (For opposing viewpoint see Mazanec [12].)

Existence of conventional military capabilities can often be detected, as such devices take physical space and large projects to create. Cyber-capabilities can be developed by a team of tens and the knowledge be kept to hundreds of people and their existence hidden inside any large bureaucracy with ease. This means that non-proliferation of cyber weapons is in practice hard or impossible to monitor and verify, unlike with conventional weapons, such as inter-continental missiles.

6.4 Defensive cyber operations

Due to the asymmetry of cyber conflict, the situation is analogous of defense of a medieval castle, where the defender must protect the perimeter everywhere and the attacker may decide where to focus force. In cyber defense, there are additional challenges. The defender is likely to not notice the attack in the first place, especially if it is logical by nature. The defender can not deflect the attack easily by moving resources inside the perimeter, as only a limited amount of people can work on one system. Each attack that penetrates the perimeter requires sanitizing its target computing environment while preventing the attack to reoccur. This process may require shutting down services or whole cyber-physical production systems and may take weeks or months.

Our recommendation for the defensive cyber doctrine is to identify critical systems and nodes in the cyber systems of the defender. Lewis [9] provides a model based on network analysis for this. As the cyber attack may preclude a conventional attack, it is not enough to protect just operational military systems, but the analysis should cover military support systems and the critical infrastructure of the nation. The defender must take into account the effects that a large scale disarray in civilian infrastructure will have to the ability of the military to operate.

A wealth of literature exists on computer and network security. New cyber attacks do not change the practices described in the literature, but give rise to some adjustments. The attacker may have the resources of a nation state in use.

Following the APT model means that the attacker may spend a lot of resources using various means on a specific target. The realization that the target may not be Web servers, but the entire digital infrastructure of a society, networked or not, enlargers the target area. Together all of these mean that a nation has a large domain to protect and at the current time much of the cyber-physical systems are without protection.

There is no current clear vision on when to consider that cyber attacks form a cyber war. This might potentially depend on if the attacks can be recognized in the first place, or even confirmed as actual intentional attacks, the identity of the attackers, if identified, the scale of operations, the chosen targets and possibly several other parameters. The difference between an attack and a war is a significant issue as the rules of engagement and control of the defense might shift from the law enforcement or other civilian entities to the military forces. A proper cyber doctrine should define these issues in a manner that does not disturb the defense by changing the command structure in the middle of operations.

We think at this point that a sensible doctrine would charge the owners of digital infrastructure with their protection and have a civilian agency in charge of controlling the protection, even in time of war. The military would then be in charge of protecting its own infrastructure and possible offensive operations.

6.5 Offensive cyber operations

Continuously collecting vulnerabilities and exploits and building the platforms to use them is necessary in preparation for offensive operations. Also building a network of deniable hosts on the Internet is necessary to maintain secrecy of the operator. As these are low cost operations, it can be claimed that these preparations should be made even if the strategic doctrine does not include use of offensive capabilities.

The modules should be built by different teams using different styles and tools, and the deployment of integrated modules should be recorded, to avoid traceability from re-use of components. It should be assumed that any deployed weapon will be found and reverse-engineered and analyzed.

One of the challenges of offensive cyber operations is evaluating their effectiveness. Martino [11] recommends forming a baseline prior to the attack and evaluating the changes caused by the attack. Martino also recommends using network analysis to identify the effect of an attack at connected nodes.

Time behaves differently in cyber operations than in conventional operations. Operations like Suxnet may be run over several years, while a prepared, targeted operation may be executed in seconds. We evaluate that the following time scales should be applied to cyber operations:

- Creating modules: months to years
- Running operations: days to years
- Defensive operations: minutes to days
- Detection of an attack: seconds to years
- Analysis after weapon capture: days to months

6.6 Defensive cyber tactics

The practicalities of defending cyber systems can be found in common data security practices that should be extended to cyber-physical systems, too. To thwart attacks it is useful to be able to detect them, however this might be impossible if the attack is well planned. We have not yet seen use of multiple simultaneous coordinated attacks in cyber war, in such a case tactical leadership and maintaining situational awareness becomes very important. The author's experience from security incidents is that specialists tend to become very focused on handling particular incidents and the larger picture is easily lost, leaving systems unmonitored. The cyber doctrine should include a model for handling cyber incidents and in case of a cyber war it is likely that these incidents will have an intensity that greatly exceeds conventional data security incidents.

6.7 Offensive cyber tactics

As discussed earlier, cyber weapons may have intelligence, misinformation, destructive or nuisance capabilities. These weapons may be used alone or in combination with other weapons, but also in combined arms operations to support conventional military forces. Cyber attacks prior to a conventional attack may disturb logistics and other support services, weakening the defender.

During the conventional attack coordinated cyber attacks may be used to distract the defender, give wrong information on the target of the attack and to gain information on the defender, even possibly by monitoring defender's actions via CCTV cameras.

We propose that conventional leaders should view their cyber-capability as light cavalry. A force for reconnaissance, distracting the enemy, probing attacks and operations behind the lines.

7. Conclusion

We have presented a modular architecture for cyber weapons and argue that strategic offensive cyber-capability is the ability to construct various weapons from prepared modules within a reasonable time frame. For defense against these weapons we point to traditional data security practices and network analysis to identify the critical points in the digital infrastructure. We also have shown how

cyber operations can be used to support conventional military operations, or to replace them, depending on the intended goal.

However, we feel that our study creates more questions than answers. Should cyber defense be in the hands of the military or civilians? What are lawful targets for cyber operations and are cyber defenders combatants or civilians? While it seems impossible to prevent the development of cyber weapons, what are proper ways to retaliate against their development or use?

The study of cyber warfare is still in its infancy. When the needs and wishes of nations clash, cyberspace may grow to be as important a dimension as the air became, a century ago.

References

[1] *Teollisuusautomaation tietoturva, verkottumisen riskit ja niiden hallinta*. Suomen Automaatioseura ry, 2010.

[2] *Yhteiskunnan turvallisuusstrategia: Valtioneuvoston periaatepäätös 16.12.2010*. Puolustusministeriö, 2010.

[3] W32.Duqu: The precursor to the next stuxnet. Online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf, 2011. Retrieved Sep 20, 2012.

[4] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi. Duqu: Analysis, detection, and lessons learned. *Proceedings of 2012 European Workshop on System Security*, April 2012.

[5] N. Falliere, L. Murchu, and E. Chien. W32.Stuxnet dossier. Online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2010. Retrieved Oct 24, 2011.

[6] A. Gostev. The Flame: Questions and answers. Online: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, May 2012. Retrieved Aug 30, 2012.

[7] A. Gostev. 'gadget' in the middle: Flame malware spreading vector identified. Online: http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified, 2012. Retrieved Sep 20, 2012.

[8] A. Gostev, I. Soumenkov, and V. Kamluk. The mystery of Duqu: Parts 1-10. Online, 2011. Retrieved Sep 20, 2012.

[9] T. G. Lewis. *Critical Infrastructure Protection in Homeland Security*. Wiley, 2006.

[10] M. Marquis-Boire. From Bahrain with love: FinFisher's spy kit exposed? Online: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/, July 2012. Retrieved Sep 23, 2012.

[11] R. A. Martino. Leveraging traditional battle damage assessment procedures to measure effects from a computer network attack. Graduate research project, Department of the Air Force, Air University, 2011.

[12] B. Mazanec. The art of (cyber) war. *Journal of International Security Affairs*, (16):84, 2009.

[13] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. SCADA security in the light of cyber-warfare. *Computers & Security*, 31(4):418 – 436, 2012.

[14] D. E. Sanger. Obama order sped up wave of cyberattacks against Iran. *New York Times*, June 2012. Retrieved Aug 9, 2012.

[15] B. Schneier. The vulnerabilities market and the future of security. *Forbes*, May 2012. Retrieved Sep 21, 2012.

[16] sKyWIper Analysis Team. sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks, v1.05. Online: http://www.crysys.hu/skywiper/skywiper.pdf, 2012. Retrieved Sep 20, 2012.

[17] T. Tuukkanen. Adapting the current national defence doctrine to cyber domain, August 2012. Seminar presentation at Finnish National Defence University.

Notification

Due to copyright laws this article (*Topi Tuukkanen - Adapting the Current National Defence Doctrine to Cyber Domain*) cannot be published on the internet.

Please contact the library of National Defence University for full printed version of this publication!

Authors

Jouko Vankka is a professor in the Department of Military Technology in the Finnish National Defence University (NDU) since 2012. He received the M.S. and Ph.D. degrees in electrical engineering from Helsinki University of Technology in 1991 and 2000, respectively. He received the Degree of Bachelor of Social Sciences from Helsinki University in 1994. Since 2005 he has been with the Finnish Defence Forces.

Anssi Kärkkäinen is a captain in the Finnish Defence Forces (FDF). He holds an officer degree since 2000 and graduated a M.Sc. (Eng.) degree at Helsinki University of Technology in 2005. He has served in various communications development positions in FDF since 2000.

Jan Lucénius is a M.Sc. (Eng) from Helsinki University of Technology (TKK). He worked formerly as research scientist at Technical Research Centre of Finland (VTT) and Finnish National Defence University. He is also a post-graduate student at Aalto university.

Johan Sigholm, Captain, is a Ph.D. student in Military Technology at the Swedish National Defence College in Stockholm, Sweden, and the National Defence University in Helsinki, Finland. He is an officer in the Swedish Air Force and received his M.Sc. degree in Computer Science and Engineering from Linköping University, Sweden.

Timo Kiravuo is a M.Sc. (Eng) from Helsinki University of Technology (TKK). Among his experiences are formulating the Internet security policy for the government of Finland (1998), administering DNS for Telecom Finland (1996), operating the Internet backbone for the Kingdom of Saudi Arabia and transferring the knowledge to local staff (1999-2000) and participating in the design of a content charging system (2000-2002). He is the vice chairman for Internet Society's Finnish chapter and a member of Finnish Information Processing Association Working Group on Ethics. He is also a post-graduate student at Aalto university.

Topi Tuukkanen, Commander, is a senior staff officer serving in the Finnish Ministry of Defence. He is a post-graduate student at University of Oulu.

National Defence University
Department of Military Technology
P.O. BOX 7, FI-00861
Helsinki ▸ Finland

Tel. +358 299 800
www.mpkk.fi

ISSN 1796-4059
978-951-25-2455-6 (pbk)
978-951-25-2456-3 (PDF)