Journal of Computations & Modelling, vol.7, no.1, 2017, 29-56
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2017

Cyber Warfare Affecting Land, Sea, Air and Space Operations

Sozon A. Leventopoulos and Nikolaos Benias

Abstract

This paper aims to inform the target audience about the impact that cyber-attacks could have on land, sea, air and space military operations. The methodology that will take place is an academic overview of the hitherto known cyber-attacks that have been successfully used in the recent past, the analysis of several NATO scenarios that were examined so far in CC (Cyber Coalition) exercises and the potential use of cyber threats in several (not that much) imaginary attacks (case study). The main results of the paper should be to raise awareness of the aforementioned cyber threats, to present an overview of cyber defence capabilities, to emerge the legal framework that is still vague in several cases and, finally, to suggest several necessary measures that need to be implemented in military cyber defence. The predecessor of INTERNET, called ARPANET, started as a project of U.S. Department of Defence in 1969. Since then, both hardware and software have changed rapidly, with the former following Moore's law. Nowadays, we have reached the age of the so called Internet of Things, which is receiving a lot of criticism and controversies. The major issues involve privacy, autonomy and control, security, design and environmental issues. Alongside with the aforementioned revolution, expert computer users began to grow in numbers, resulting some of them to gradually transform and become malicious, also known as hackers. Viruses, trojans and other malware types of infectious software are their main weapons of choice, which in conjunction with good to

Article Info: *Received* : October 15, 2015. *Revised* : January 12, 2016.
Published online : January 20, 2017.

excellent social engineering skills, enables them to be considered as a great asymmetric threat, free of any kind of identity. The effectiveness of attacks is based on some -discrete- factors such as limited or non-existent legal framework, lack of forensics procedures that those responsible are brought to justice and the ability of anonymity that Internet offers. The cyber incidents that occurred in Estonia during 2007 and in Georgia in 2008 are considered the first examples of a new form of warfare, with the latter to be considered the first time in history where a cyber-attack coincided with a shooting war.

1 Introduction

Every era in the human history was dominated by a key event that had radical and profound impact in humanity's life and culture. In the ancient years we had, stone (“Stone Age”), Bronze (“Bronze Age”), the Iron (“Iron Age”) etc. Many years later we have the industrial revolution, which set the foundation for the world we know today. Our era is dominated by the need for accurate, prompt and timely information. The basic mean for collecting, analysing and exploiting the vast amount of information we collect every day is the INTERNET and the WORLD WIDE WEB. Today, we are experiencing the revolution of the Internet in what it is now called “The Internet of Things”. Soon we will pass to “Internet of Everything” where all devices (from our smartphones to refrigerators, cars, airplanes, etc) will be interoperable and connected creating a new reality.

This evolution, and for many revolution, could not have let the armed forces and military operations unaffected. The military is one of the few organizations in the world that from the beginning of their existence they were deeply dependant in the presence of accurate information or better, intelligence. Many authors throughout the years tried to measure the connection between intelligence and victory, but in our belief it was *Carl Von Clausewitz*[2] that described it better as

[2] Carl Phillip Gottfried von Clausewitz (1 June 1780 – 16 November 1831). A Prussian general and theorist. His most notable work is “Vom Kriege” (On War) which was pub-

"the fog of war".

While in the past few years the means needed to collect the amount of intelligence which was necessary to conduct military operations successfully, have increased both in numbers and capabilities, the military organizations came up against four challenges:

- ✓ The amount of information gathered by all those means is so vast that its processing takes a rather large amount of time, which in returns makes the information useless by violating the need for prompt and timely intelligence.
- ✓ The framework and means needed in order to distribute that amount of information is not yet fully developed, creating conjunction which leads again in violation of the timely aspect of intelligence.
- ✓ The military are growing almost fully dependant from the presence of this intelligence in order to take decisions in such a scale that tend to forget all the other aspects of military art.
- ✓ This intelligence is also available to parties outside of the moral and ethical framework that the western civilization is based in and it is used for criminal or other non-legitimate usage (terrorist attacks, crime, etc).

All of the above challenges are sharing a common factor. All of them are vulnerable to the effects of cyber warfare in provisional or global scale.

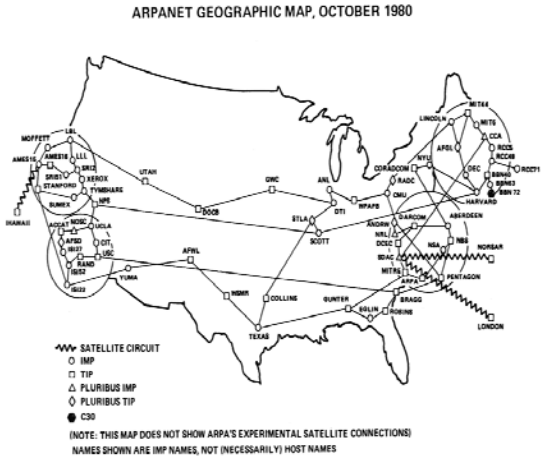
Already the volume of information that is distributed and managed every day in the internet is huge and reflects the growing dependence of modern day societies in exactly that information not only for their everyday operation, but also in maintaining their social and economic structures. As a result – since the dawn of the 21st century – a growing number of government organizations and civil and private ventures and enterprises of all sizes have endorsed the internet in their operational structures, using Big Data technologies.

---

lished after his death. He was one of the first military theorists that described the impact of moral and political aspects in the conduct of war.

2 The Internet and the World Wide Web

2.1



In the middle of the 1960's various scientists around the world (mainly in UK and USA) came up with the idea of "packet switching", a method that could lead to reliable digital data communication between computers. One of the first implementations of the new technology was ARPANET (Advanced Research Projects Agency Network) which interconnected various institutions around the United States. The ARPANET is consider the predecessor of the INTERNET. During the 1980's the technology of the micro-processors together with the implementation of a new protocol, the TCP/IP, created the basis for the future development of the INTERNET. Furthermore the invention of the World Wide Web (WWW) by *Sir Timothy Burners Lee*[3], together with the successful implementation of Hyper Text Transfer Protocol (HTTP) for the interconnection of a client and server computer via the internet was the dawn of a new era. Less than two decades later the Internet and the World Wide Web is dominating our everyday living.

[3] Sir Timothy John "Tim" Berners-Lee (OM, KBE, FRS, FREng, FRSA, DFBCS) (Born8 June 1955) is an English computer scientist. He is considered as the inventor of the World Wide Web as he managed to successfully communicate between a client computer and a server which were connected over the Internet using Hypertext Transfer Protocol, then well-known now HTTP.

2.2

Today we live in a world of interconnected devices which form a gigantic network of input and output spots for information distribution. The social media, the cloud, the online shops are transferring our reality into a virtual layer, the **cyberspace**. Like in real world this virtual one is also a space for non-legitimate acts and actors with revenues from criminal and illegal acts reaching billions of US dollars. Furthermore, our dependence on the Internet and WWW, along with the lack of awareness about the danger lurking inside this – virtual – world is making us extremely vulnerable.

2.3

A clarification between The Internet and the World Wide Web is needed in order to create a distinction between the two technologies, because many people nowadays tend to confuse Internet and WWW.

2.3.1 The Internet is a space or – if you would like an alternative term - a community of interconnected devices (end-users). Those end-users (or clients) could be desktop or laptop computers, smartphones, printers or even servers that are connected to other end-users, which in return could be other servers, computers etc. All these devices are connected through various means (cables of all kinds, wireless, optical, etc) and other devices (routers, modems, multi-layer switches) which ensure the proper direction of the packets (that's the information). All these devices and means need a common language or protocol in order to communicate accurately and timely. An example of this common language is the TCP/IP protocol. The three major factors that play a vital role in Internet's operation are:

- ✓ **Bandwidth**. A precise definition could be "*the width of the frequency*

spectrum of a signal measured in Hertz[4]". It also safe to suggest another term as "*the rate at which data can be sent over a given channel measured in bits per second"*.

✓ **Throughput**. In general terms, throughput is "*the rate of production or the rate at which something can be processed*".

✓ **Latency**. Generally speaking, latency is a time interval between the stimulation and response, or, from a more general point of view, as a time delay between the cause and the effect of some physical change in the system being observed. Physically speaking, is a consequence of the limited velocity with which any physical interaction can propagate. In communications, the lower limit of latency is determined by the medium being used. In reliable two-way communication systems, latency limits the maximum rate that information can be transmitted, as there is often a limit on the amount of information that is "in-flight" at any one moment.

2.3.2 On the other hand the WWW is an environment where documents and other web resources (internet banking, e-commerce, etc) are identified by URLs, interlinked by hypertext links, and can be accessed via the Internet using suitable browsing programs.

2.3.3 So, in order to sum up, when you connect your computer to the router you are connected to the Internet via a service provided by certain Internet Service Providers or also known as ISPs. When you use a service (search engines, e-commerce, etc) then you are connected to the WWW, which «lives» inside the Internet.

2.3.4 Finally, a brief description of IP address in also needed. One should consider the use of the IP address as his personal home or business address, which distinct him from the rest of the world. This address is personal and comes to the form of four 3-digit number, like 192.168.0.1. These addresses are divided into private and public. The private ones are used in order to interconnect devices

[4] John F. Pane and Leland Joe, Making Better Use of Bandwidth.

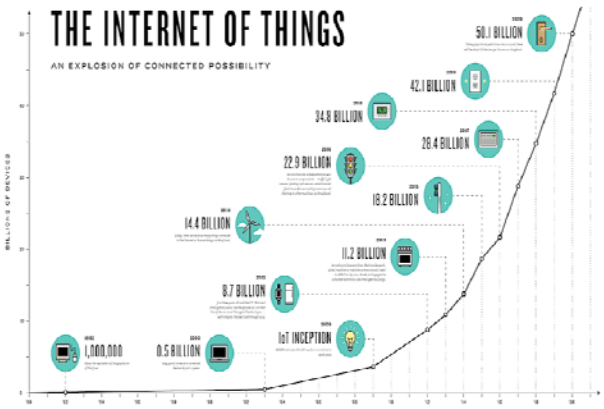
inside a network which is not connected to the Internet. For example when you connect more than two devices in your home's router, private IPs are going to be allocated while when your router is connected to the internet a public IP is going to be provided. Here we should clarify that the personal computer or other end-user device is not directly connected to the internet but the connection is established through the modem/router which is responsible to determine the best possible pathway to the desire destination. The public addresses could be:

a. Static: A static IP remains the same through time.

b. Dynamic: A dynamic IP changes through time (usually the interval is one week).

2.4 Internet of Things

The Internet of Things (IoT) is a new concept which describes the possibilities by having any kind of device (from smartphones and computers to refrigerators and weather monitoring devices) connected to the Internet and exchanging data. This proposal – if and when will be fully operational - could create a revolution in how we will be able to understand and interact with our environment. The first examples of this technology are already present (like RFID tags, wearables, IP security solutions, etc).



2.5 Networks

As mentioned above, the existence of Internet itself lies in the networks.

While the definition of Networks is not part of the present paper, a brief description is needed in order to define those specific elements that affecting them we can affect the whole system. It is crucial to understand that in order to have communication between devices (or end-users) we need to establish a form of a network. But what are those network characteristics needed?

2.5.1 Network Characteristics

Topology There are two major topologies. The one is the **physical** one, which is the actual arrangement of cables, devices and end-systems that comprise the network. The other one is the **logical** one, which is the actual path that the signal should travel through the above actual arrangement in order to reach its destination.

Speed How fast the signal is reaching its destination.

Availability The actual time that we can use a network. The formula that describes the availability of any given network is described below:

$$Availability = \frac{timeactualavailable}{totaltimeofoperation} * 100(inordertohaveapercentage)$$

Security Describes the security of our network. How easy it is for someone to penetrate our network, how easy it is for someone to deny the services provided, how certain we are that data transmitted over our network reaches the proper destination.

Scalability How easy (and cost effective) it is to expand our network in order to come up with future needs or developments.

Reliability While sometimes it is mistaken or confused with availability the reliability defines how well our means are working. It is often measured in Mean Time Before Failures (MTBF).

Redundancy How well our network behaves in failures. What alternates are implemented in order to immune our network to failures.

At this point it should be clear that compromising any of the above

characteristics leads to the failure of our network. It is crucial to understand that cyber warfare targets all of the above characteristics (as we will examine later on) and that network security is a complex task.

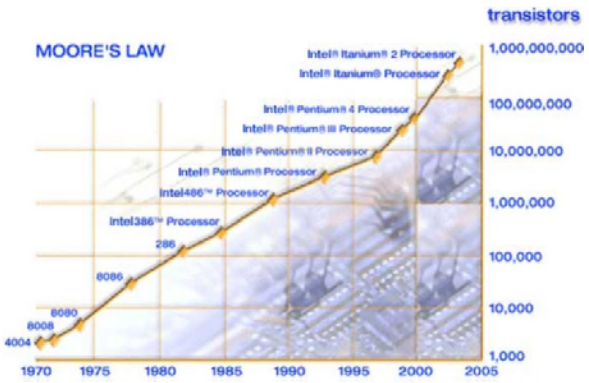
3 Computer Technology

3.1

Ever since computers were invented, they have changed our daily lives and even the route of mankind. These general-purpose devices can be programmed to carry out a set of arithmetic or logical operations automatically and since a sequence of operations can be readily changed, computers can solve more than one kind of problems. Nowadays, computers are used for almost everything, making us completely dependent on them.

3.2

According to Moore's Law[5], "*the number of transistors in a dense integrated circuit doubles approximately every two years*". This prediction proved accurate for several decades, and the law was used in the semiconductor industry to guide long-term planning and to set targets for research and development. The period is often quoted as 18 months, because of Intel executive David House, who predicted that chip performance would double every 18 months (being a combination of the effect of more transistors and the transistors being faster).



[5]Gordon Earle Moore (born January 3, 1929) is an American businessman, co-founder and Chairman Emeritus of Intel Corporation.

3.3

There is active research to make computers out of many promising new types of technology, such as optical computers, DNA computers, neural computers, and quantum computers. Most computers are universal and able to calculate any computable function, limited only by their memory capacity and operating speed. However, different designs of computers can give very different performance for particular problems; for example quantum computers can potentially break some modern encryption algorithms (by quantum factoring) very quickly. The above mentioned types will clearly change the landscape of computer science, once developed.

4 The Implementation of Networking in Military Affairs

4.1

While the ARPANET started as a – at least partially – funded military project, quickly the management and implementation of various technologies slipped away from military control. The development of computers and networks, especially during the last decades, is unimaginable and – for many – the fasted developing technologies in all human history[6].

4.2

As mentioned above our era is the era of Information. Over the years of

[6]During the '80s it was said that if aviation technologies where developing with the same rate, now (in the 80s) we should be able to circumnavigate the earth with an aeroplane in less than 2 hours, and that was in the 80s!

military history the main concern of all military commanders was the need of valid information about the enemy and in the same time the denial of that information from the enemy. While various military writers (like Thoukididis, Sun Tzu, etc) described that reality it was Clausewitz that offered the most accurate description when he talked about the “fog of war”. If you are not familiar with the term you can check – almost all – strategy games. The clouds around you are the visualization of Clausewitz definition.

4.3

Inevitable, the military operations could not stay unaffected. The main characteristics of today's and future battlefields will be the non linearity and the chaotic form making the need for timely, prompt and accurate information crucial. Furthermore our battle against terrorism, a battle that will not end easily or in the near future and the need to confront the non-symmetrical threats which introduced themselves with the most emphatic way during 9/11, will stretch today's networks to their limits. During the 70's many declared space as the 4th and final dimension of warfare. Today it is clear that this declaration was far from being true and a new dimension – the 5th – was created in order to describe a new – virtual – environment, the ***cyber space***. Today it is safe to declare that dominating the warfare in the 5th dimension and the electro-magnetic spectrum is *sin non qua7* for dominating a future warfare. We should not wait for the info-war to be declared. We are already fighting it furiously.

4.4

During the past years a vast number of studies proposed the need for

[7]Formal terminology for "but-for" causation.

technologically advanced weapons in order to prevail in the future battlefield. Technologies like High Energy Weapons (i.e laser, MW, magnetic rail guns, etc), nano and bio technologies that will offer advanced systems, robotics, artificial intelligence and many more where proposed. On the other hand all of the above systems are dependent in networks and computers for their operation, a fact that many forgot.

4.5 The Digital Battlefield

4.5.1 During all of mankind's conflicts, either peripheral or global in nature, the key players need information regarding three basic pillars:

4.5.1.1 Information about the enemy, its strength, its tactics, its morale was crucial in order to decide the amount of force needed to repel the threat or to decide the proper action plan.

4.5.1.2 Information about the weather is also needed in order to prepare your forces (clothing, support, etc) and in order to decide about the use of the proper means in every occasion.

4.5.1.3 Finally information about the terrain leads in choosing the right equipment in order to fight a battle (it is well known around the military the effect of terrain not suitable for tanks and how that can affect the operations) or to avoid certain

areas that give the advantage to the opponent.

4.5.1.4 One excellent example of how knowledge about the three pillars can affect the outcome of an operation is the destruction of the Spanish Armada outside Britain. The Spanish were able to create a spectacular naval and army force with battle experience and high morale against the British who could mobilize a small militia force and off course – their navy. Although the Spanish took every precaution when they prepared their forces, they failed to collect a single piece of information about the enemy. If they have done so, they would have known that the British had introduced a new ship model more capable for naval warfare than the Spanish galleons, (which stayed almost the same since the Roman Empire) that gave them the advantage. Additionally, they had no idea about the weather or the terrain and in fact the leader of the naval forces had never met with the leader of the land forces, with which had to conduct a highly complicated operation (lack of interoperability?)

4.5.2 As mentioned above and in order to overcome all of the difficulties that are profound in a field that lucks linearity and structure, the military authorities all over the globe (with various attempts and depth) are trying to create was is now known as the **Digital Battlefield**. In order to create such an environment someone should follow some basic rules:

4.5.2.1 At first, you need to establish a series of sensors whether those would be electro-optical devices, ground or airborne radars, satellites, sonars, friend or foe systems and many more, that will create a “recognized picture” of the battlefield. That data should be updated in a “real-time” basis (or at least near real time) in order to fulfil the timely factors as described above.

4.5.2.2 Secondly, you need a system of systems that will interconnect all of those devises and will ensure their interoperability.

4.5.2.3 Thirdly, you need a way to distribute that information to the actual players (from government officials and actors down to the field commanders and foot soldiers) and at the same time you need the means in order to mobilize those

forces in a specific point in time and space.

4.5.2.4 Finally, you need a method to engage the desire targets with the exact force in order to minimize cost, risk and increase efficiency.

4.6 The C4I (or ISTAR)

4.6.1 The answer to all of the above challenges was the creation of what is well known as the C4I (Command, Control, Communication, Computers, Intelligence) or its ancestor the ISTAR (Intelligence, Surveillance, Targeting, Acquisition and Reconnaissance).

4.6.2 In order to create such systems you need to define the architectural frameworks in place. Some of the most commons are the “IEEE 1471 meta-architecture framework”, the “Zackhman Framework”, the “US DoD Architecture Framework” and many more. Furthermore you have to define the Architecture Description Languages that should be used in order to design and create such environments.

4.6.3 Key Features

4.6.3.1 As mentioned earlier the key purpose of any C4ISR system is to provide data regarding

i. Weather
ii. Enemy
iii. Terrain

The intelligence gathered should in turn answer some fundamental questions like who, how, when, where, what, and why. The non-ending intelligence processing is best described in the following picture.

4.6.3.2 The C4ISR should also

i. Create and manage a common picture of the theatre of operations

ii. Give geospatial intel

iii. Dominate the info war

iv. Plan, execute & control joint military ops

v. Enhance co-operation between military & civil partners

4.6.3.3 In order to provide all of the above and taking into account the framework architectures and best practises when designing any given C4ISR system the following should be observed.

Security: Security comes through:

Authentication

Integrity

Non-disclosure

Access control

Confidentiality

Availability: Availability is ensured when you create a system with:

Stability

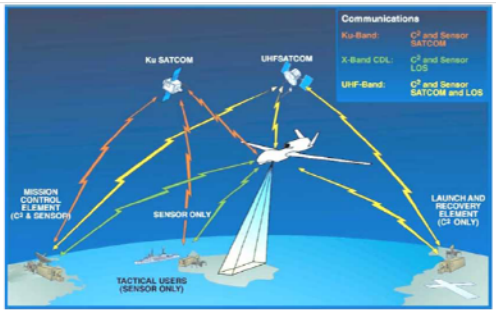
Continuity

Consistency

Recovery

4.6.4 Dependence on Space and Cyberspace

4.6.4.1 One of the key lessons learned from the conflicts that took place since the 80's is the growing dependence on access to satellites, for navigation purposes through the use of the Global Positioning System (GPS) constellation



* Northrop Grumman Corporation, "RQ-4A Global Hawk High Altitude Endurance Unmanned Reconnaissance System," November 16, 1999, Slide 2.

of satellites, the use of satellite communications and the use of various imaging satellite systems for data and geospatial information gathering (i.e. in order to create highly accurate 3D digital maps needed for the Terrain Following systems of cruise missiles).

4.6.4.2 Additionally the dependence of high speed and bandwidth networks in order to transfer and exploit all data gathered by various sensors and courses had increased rapidly. It is noted to mention that a – single – Predator orbit requires data rates up to 6.4 million bits/second and can create data up to 274 Mbps.

4.6.5 Future Needs

4.6.5.1 In the future, all military aspects, from foot soldiers to aircraft carriers shall be incorporated into a single network. The advances in micro-electronics and computer processors will introduce new abilities and in the same time will decrease the size and power consumption. The future Unmanned Vehicles (Land, Sea, Air) will require additional networks in order to smoothly operate alongside manned means. The size of data gathered will require additional means (computers, networks, etc). The dependence in satellites (for communications and early warning) will increase.

4.6.5.2 In the past years we witness what was described by many authors and theorists as the Revolution in Military affairs[8]. In order to give the magnitude of this revolution, in the Operation Desert Storm in 1991 almost 92 percent of the 230.000 ammunitions used in the campaign where unguided or “dump”. Almost a decade later during the Operation Iraqi Freedom the ammunitions launched during the air operations was reduced to 28.000 with 65% of them being guided or “smart”. This difference in numbers represents a huge increase in efficiency and

[8] According to Krepinevich’s assessment in 1994, RMA is “what occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict by producing a dramatic increase in the combat potential and military effectiveness of armed forces”

cost management.

5 The Threat

5.1

In the above paragraphs we described a brief view of the future needs in the area of information. Already, from that brief description, the basic challenges regarding the security aspects and needs of present and future military networks have already arose. The key features and elements of networks both in military and civil usage are the ones vulnerable to the threat.

5.2

As we described above, our era is dominated by the use of the Internet and the WWW. In such an environment it was just a matter of time to see the first non-legitimate actions. One of the major advantages of the Internet is that it provides its users anonymity and in many cases absence of punishment for any non-legitimate act. The influence of the social networks in everyday life of most of use is a phenomenon yet to be explained, in particular why people that are very concerned about their privacy are willing to voluntary give away private and in many cases sensitive information about their life and whereabouts.

5.3 Describing the Threat

5.3.1 As mentioned above, the major advantage of the Internet is the anonymity it offers to the users, and we do not refer to the usage of specialized programs or techniques, like usage of proxy setting, TOR browsers, etc., but simple that

everyone has the potential to be someone else. Furthermore, the potential profit from such non-legitimate acts, together with the limited or non-existent law framework, makes the Internet a very attractive place for criminals. Additionally, the “foggy” law environment and the reluctance that many nations show due to their own agenda (that is the usage of the Internet in their favour) offers criminals that roaming the Internet – or better The Cyber Space – a multi-billion dollar industry.

5.3.2 Those follow the computer science (both its software and hardware parts) are familiar with the evolution of computer threats. In the beginning computer threats like viruses and other harmful software were part of “case studies”, “a way to prove someone’s abilities” etc. Soon what started like a game proved to be very expensive and dangerous. Today we do not see too many viruses or at least their effects are very limited. The malicious software lies now to trojan's, malware programs, sniffer's, etc which in many cases are extremely sophisticated and well written computer software. New malicious software has even the ability to evolve according to the environment or even react to it. Today's malicious software is able to understand the difference between a live and a virtual machine and thus alter its behaviour accordingly.

5.3.3 Terms and Definitions

5.3.3.1 Cyber space: The cyberspace is the environment that inside it “lives” the Internet, all kind of networks, the software, the hardware, the users together with the user's actions.

5.3.3.2 Cyber security: Is the sum of all tools, security policies, doctrines, risks assessments, training, best practises and everything else that can be used in order to protect the cyberspace and its infrastructure.

5.3.3.3 Cyber defence: It is the ability to provide and administer such means inside and outside cyber space in order to immediately possible real threats against

it.

5.3.3.4 Communication Systems and IT Systems Security: It is the ability to protect the confidentiality, integrity and availability of data that resides in such systems.

5.3.3.5 Cyber space defensive operations: It is the sum of all actions taken in order to detect, analyse and confront any kind of cyber threat.

5.3.3.6 Cybercrime: Unfortunately – for reasons explained earlier – we still lack a firm and coherent definition of what cybercrime is and every nation deals with the issue per case and according with its interests.

5.4 The Problem of Security

5.4.1 According to a vast number of published papers and thesis (including the famous Church – Turing Theorem) the possibility to have a completely secure computer system is practically none. The main – and only law – that there is regarding cyber security is this:

YOU CAN NEVER HAVE A COMPLETELY SECURE SYSTEM

$$
\begin{array}{ll}
[1] & \forall M \forall V \\
[2] & (M,V) \in VS \text{ iff} \\
[3] & \quad [V \in TS] \text{ and } [M \in TM] \text{ and} \\
[4] & \quad [\forall v \in V [\forall H_M \\
[5] & \quad [\forall t \forall j \\
[6] & \quad\quad [\quad P_M(t) = j \text{ and} \\
[7] & \quad\quad\quad\quad S_M(t) = S_{MO} \text{ and} \\
[8] & \quad\quad\quad\quad (\square_M(t.j) \ldots . \square_M(t.j - |v| \quad 1)) = v \\
[9] & \quad\quad] \Rightarrow \\
[10] & \quad\quad [\quad \exists v' \in V [\exists t' > t [\exists j' \\
[11] & \quad\quad\quad\quad [\quad [[(j' - |v'|) \leq j] \text{ or } [(j - |v|) \leq j']] \text{ and} \\
[12] & \quad\quad\quad\quad\quad\quad (\square_M(t'.j'), \ldots, \square_M(t'.j' + |v'| - 1)) = v' \text{ and} \\
[13] & \quad\quad\quad\quad\quad\quad [\exists t'' \text{s.t.} [t < t'' < t'] \text{ and} \\
[14] & \quad\quad\quad\quad\quad\quad\quad\quad [P_M(t'') \in \{j', \ldots, j' + |v'| - 1\}]] \\
[15] & \quad\quad]]] \;] \qquad]
\end{array}
$$

5.4.2 Amongst the ranks of all computer enthusiasts there is an anecdote which describes the pointless efforts of creating a completely secure system. In this anecdote, the user is directed to unplug his computer from the net, close it inside a vault that he does not know the combination

Church - Turing Thesis 1

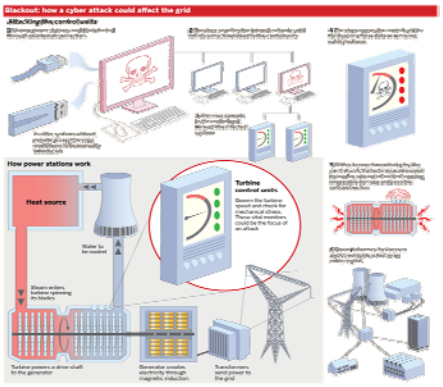
and then throw it into the ocean. While this for many people seems a rather good idea, it lacks availability. The point here is that after all we should create such an environment where we have adequate security, but also availability and ease of use.

5.4.3 We should never forget that one of the best hackers of all times, *Kevin Mitnick*[9], was not an excellent programmer, but an excellent social engineer. The way Mitnick managed to acquire passwords and user's IDs is frankly remarkable and perhaps why the social media have that impact in western societies.

5.4.4 The problem that computer and network specialist are facing right now is to balance between the need of availability and security. One common problem that many network administrators may find it familiar is how many locked accounts had to unlock because the user forgot his/hers password. Of course, it could be very easy to go by 123qwerty but that is not very hard to guess or crack.

5.4.5 Finally, another problem that security authorities are facing comes from the Internet itself. Today it's very easy to find cracking programs, instructions, best practices, online communities to attend or reach out for help or even "enterprises" that are willing to spread your non-legitimate software, for a couple of dollars.

5.5 The Power Grid Challenge



5.5.1 While we have mentioned many aspects of today's threats we deliberately left the power grid challenge for last. For many years now the western civilization lives in a more-or-less safe environment where many things are taken for

[9] Kevin David Mitnick (Born 6 August 1963). He is an American computer security consultant and author but he is also known as one of the best hackers of all times. He is well known for his excellent implementation of social engineering tactics and methods rather than his computer programming skills.

granted, like the uninterrupted flow of food supplies, the supply of fresh water and most importantly the supply of electricity. Our western civilization is based upon the flawless supply of electricity, that trail of moving electrons. Forget about petrol. We have already found alternatives for that resource, but when it comes to electricity. Take for example how everyone feels when a power failure or power outage takes place. It is like our whole life comes to a halt. Imagine now all those systems that are vital for our existence and that depends. Hospitals, banks, the Internet, industries that provide our food, everything runs on electricity.

5.5.2 The way to attack such an infrastructure is not of the present paper, but the following picture summarizes adequately the process. The effects of a sustain power failure cannot be documented easily.

6 How Cyber Warfare can Affect Military Operations

6.1

Earlier in this paper we described the need for a C4ISR system. Besides that the need for interoperable connected networks and systems are vital for everyday military life and more importantly for the conduct of operations. It is clear that those systems are making us more effective, more capable and in the same time could decrease running costs. Furthermore, we live and operate in a globalized environment where borders have little or no importance. In order to bring distant places closer and erase all limitations caused by distances, we rely on networks and computer systems.

6.2 Affecting the Military Operations

Someone can affect the conduct of military operations with two ways: Directly and Indirectly.

6.2.1 The Direct Way

The direct way includes all those actions taken in order to limit or deny the use of computer systems, networks, sensors, etc. Actually there are numerous ways to do that. The easiest definition is by HARD or SOFT kill. The HARD kill describes those methods that the use of deadly or destructive force is taken in order to achieve certain goals. The HARD kill could be an attack with conventional weapons (including cruise missiles or other “smart” munitions), an attack with nuclear or biological/chemical weapons, and the attack with suicide bombers or other acts of terrorism. While the HARD kill is a very effective method it is in parallel and a high profile one, which in most cases leads to acts of retaliation which in return can escalate a conflict.

6.2.2 The Indirect Way

On the other hand, the indirect way includes all those methods that can deny the services of certain systems. Electronic warfare is one of those methods, but attacks in the IT and C4ISR systems of the enemy is less provocative and highly anonymous act, and even though the origins of the attacks can be traced, it is very difficult to enable government authorities and states in these acts. Additionally, it is possible to attack vital civilian infrastructures, like electricity (as we described above), water supply, banking and stock exchange networks and facilities creating a critical situation which will enable the military forces into relief and civil support operations thus making them unable to respond – at least into a certain limited time frame – against a conventional military act.

7 The Solution?

7.1

In order to describe and even implement a solution we first need to define the

problem and there lays the biggest challenge. Even today people in all levels, including military officials and civil parters are unaware of the actual battle that takes place in the cyber space. Still, the cyber warfare is a term that creates more confusion than clarification. The proposed measures in order to confront or mitigate the effects of a cyber-attack are:

I. Define and describe the problem in details.
II. Have always in mind the one and only law regarding computer systems security: **“You will NEVER have a completely secure system”.**
III. The end user will always be the weakest link in the chain of security.
IV. Training, training, training and when in doubt... training.
V. All critical data should be encrypted.
VI. Alternate and back-up systems should be implemented.
VII. Cyber forensic procedures should be established and more importanly followed.
VIII. There should be constant surveillance of systems and critical infrastructures.
IX. Emergency Response Teams for computer systems and networks should be created with mission to confront cyber-attacks or to aid and support other players in confronting those attacks.
X. Certain steps should be taken in order to create software and hardware that can actually understand and respond to cyber-attacks.
XI. Implementation of a strict security policy which will be audited constantly in order to be upgraded and adapted to future needs and realities.
XII. There should be certain measures in order to ensure the fragmentation and access denial to the whole network structure. The whole network/data/system should be visible only to a few selected members.
XIII. Finally certain measures should be taken in order to monitor the «health» of friendly cyber society (including hackers and various other players – even non-legitimate ones) because it can give certain evidence about an incoming

cyber-attack. It is clear that in cases of emergency a country or nation can rely on its cyber community for repelling or counter cyber-attacks.

8 Case Studies

8.1 Estonia (2007)

8.1.1 The cyber-attacks in Estonia are the first well documented incident of a new model of warfare and that is why it poses a significant element in the study of cyber warfare.

8.1.2 The cyber-attacks in Estonia was a series of various types of attacks against a plethora of government and civil sector organizations. The attacks began on 27 April 2007 amid a disagreement between Estonia and Russia about the relocation of a WWII era monument commemorating Soviet soldiers in the city of Tallinn.

8.1.3 Various Estonian authorities were attacked including the Estonian Parliament, banks, ministries, newspapers and broadcasters, including various attacks in individual users. The preferred method was DDoS (Distributed Denial of Service), spam mails, ping floods, etc together with the activation of several botnets. The attacks were limited in denying the service of certain authorities (as described above) and also limited defacements were noticed. The attacks did not caused much trouble in everyday life and critical infrastructures stayed unharmed.

8.1.4 While the Estonian government launched a criminal investigation under the Estonian penal code, only one person was found guilty and that after years of investigation. The main reason for the actual failure of the investigation was the denial of cooperation by the Russian authorities, even though most of the attacks were originated from Russian Federation.

8.1.5 Lessons Learned

8.1.5.1 The majority of attacks was DDoS. Botnets (actually expensive rentals)

were also used, but mainly for spam mail distribution.

8.1.5.2 The attacks did not affect (deliberately?) critical infrastructures while the attackers had the abilities to do so.

8.1.5.3 After years of investigations the Estonian government failed to present valid technical data regarding the origins of the attacks.

8.1.5.4 In order to successfully attack critical systems a co-operation of state authorities and large telecom companies is required.

8.1.5.5 The international legal background is – at minimum – foggy, thus every state driven attack could easily be hidden behind bureaucracy or any other excuse.

8.2 Georgia (2008)

8.2.1 For several years after the fall of Soviet Union, the Russian Federation and Georgia were engaging over a number of territorial disputes (like South Ossetia and Abkhazia). The conflict escalated in August 2008 after several weeks of arguments regarding the future of the South Ossetian territory. The conflict started after the Georgian armed forces launched an attack (including artillery bombardment) against targets in South Ossetia and Tskhinvali. In return the Russian armed forces launched a massive joint attack against Georgia.

8.2.2 Several weeks prior, the Russian armed forces assault a series of cyber-attacks occurred against various government and civil authorities. The number and intensity of attacks escalated as the date of attack was closing in.

8.2.3 Various attacks against all kind of targets (newspapers, re-routing of internet traffic, etc) occurred during the war including a highly sophisticated one against the Baku-Tbilisi-Ceyhan pipeline on August 5, which led to increased pressure and explosion.

8.2.4 The attacks continued several weeks after the cease fire agreement.

8.2.5 Lessons Learned

8.2.5.1 It was the first time in history that a war was fought in 4 dimensions, land, sea, air and cyber space and it was the first time that cyber-attacks were co-ordinated with conventional attacks on the ground.

8.2.5.2 Cyber-attacks targeted also the Georgian cyber community thus Georgia's response to the attacks was practically none.

8.2.5.3 While cyber-attacks were vast in number and complexity, they did not target critical infrastructures (except one case), which would had led Georgia to chaos.

8.2.5.4 While cyber-attacks were co-ordinated with land assaults, no lethal force was used in order to attack critical internet infrastructures. The reasons for that may rely on the decision from the Russian authorities not to clearly show their involvement or because that infrastructure was critical for the success of the attacks.

8.2.5.5 For one more time after Estonia no-one took responsibility or was prosecuted for those attacks due to the lack of firm law background.

9 Conclusion

It is clear that cyber warfare is a reality and is happening as we speak. The motivations behind the attacks could be anything, from egoism to profit or sabotage. We also know that cyber-attacks can be co-ordinated together with military action affecting the conduct of operations and it should be cleared that you cannot create an invincible online or interconnected system. Additionally the effects of a full scale cyber-attack are not well measured and could be similar to those of a nuclear war by turning as back to the "Stone Age". The only way to protect ourselves and our systems is by creating and implementing a "security culture" in all aspects of our life and operations. In this paper we have not

examined the impact of the social networks and – most importantly – the escalation of the technologies and capabilities of smartphones and tablets which are proving rather vulnerable. Today the majority of attacks and malicious code is intended for the smartphones, but since they are not operated within the scope of military operations there were excluded from any further analysis.

References

[1] Carl Von Clausewitz, “Von Kriege” (On War). Everyman’s Library, Published by Alfred A. Knopf.

[2] Sun Tzu, “The Art of War” (Greek Edition, Publish by MINOAS Publications).

[3] Luke Harding, “The Snowden Files (The Inside Story of the World’s Most Wanted Man), First Published in 2014 by Guardian Books and Faber & Faber Ltd (copyright “The Guardian”).

[4] War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?, *The Economist*, (01 July 2010).

[5] Center for Strategic and Budgetary Assessments (CBSA), The Maturing Revolution in Military Affairs (by Barry D. Watts), 2011.

[6] Markoff, John, Before the Gunfire, Cyberattacks, *The New York Times*, (12 Aug 2008).

[7] Wentworth, Travis, How Russia May Have Attacked Georgia’s Internet, *Newsweek*, (23 Aug 2008).

[8] Kathryn Kerr, *Putting Cyberterrorism into Context*.

[9] Glossary of Information Warfare Terms, available at www.psycom.net/war.2.html

[10] Rex B. Hughes, NATO and Cyber Defence, Mission Accomplished? Ar:2009nr1/4.

[11] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand and D. Boyle,

From Machine-to-Machine to the Introduction to a New Age of Intelligence.

[12] Commission of the European Communities, Internet of Things — An action plan for Europe, (18 June 2009).

[13] Stephen J. Blank, (Preparing for the Next War: Reflections on the Revolution in Military Affairs, Chapters 3 and 4).

[14] Tim Berners-Lee and the Development of the World Wide Web (Unlocking the Secrets of Science), Ann Gaines (Mitchell Lane Publishers, 2001).

[15] National Cyber Security Framework Manual, Edited by Alexander Klimburg, NATO Cooperative Cyber Defence Centre of Excellence.

[16] Kevin Mitnick, Simon William L., *The Art of Deception: Controlling the Human Element of Security*, Wiley Books.

[17] Kaspersky Lab Report: Financial cyber threats in 2013.

[18] Kimberly Tam, Salahuddin J. Khan, Aristide Fattoriy and Lorenzo Cavallaro, CopperDroid: Automatic Reconstruction of Android Malware Behaviors.

[19] Yajin Zhou, Xuxian Jiang, Dissecting Android Malware: Characterization and Evolution.

[20] The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, (July 2013).

[21] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data.

[22] Hackers' Bazaar" (RAND publications).

[23] Barbara Guttman and Edward A. Roback, An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12.