Cyber Weapons: a Profiling Framework

Maathuis, Clara; Pieters, Wolter; van den Berg, Jan

Publication date
2016

Published in
Proceedings of International conference on cyber conflict

Citation (APA)
Maathuis, C., Pieters, W., & van den Berg, J. (2016). Cyber Weapons: a Profiling Framework. In *Proceedings of International conference on cyber conflict: Protecting the future* IEEE.

Cyber Weapons: a Profiling Framework

Clara Maathuis, Wolter Pieters, Jan van den Berg

***Abstract*—In the last decades we witnessed the creation of a virtual world: cyberspace, which offers plenty of opportunities and challenges. Meanwhile, we are confronted with many conflict situations between different groups of people or countries. In the last years, several events have been described in terms of cyber warfare or the use of cyber weapons, leading to critical international security concerns. At the same time, there is little research on the definitions of what constitutes a cyber weapon and how it can be profiled.The present article gives an answer to the question "How to define cyber weapons?" and proposes a conceptual framework that defines and profiles cyber weapons from a multidisciplinary perspective: cyber and military, considering legal aspects as well. This framework establishes the context of use and the life cycle of cyber weapons, defines them, presents their structure and proposes a way to profile them. The aim of this article is to support decision makers and academia that have to deal with the implications and consequences of cyber weapons. Therefore, to evaluate our framework, we propose a profiling matrix for Stuxnet, Operation Orchard and Black Energy and we conduct an exploratory case study on Stuxnet based on the existing literature and reports. We conclude by presenting our future research.**

***Index Terms*—cyberspace, cyber weapon, cyber warfare, impact.**

I. Introduction

IT is well known known that the human genome, the DNA, consists of 3 billion base pairs. According to the last statistics there are around 3 billion different users in cyberspace [1]**.** It is interesting to consider that as being part of nature, humans had the need, will and power to create a totally new space, the cyberspace, which has become "the dominant platform for life in the 21st century" [2], an environment resulting from the interaction between technology, services and people [3], [4], [5] "the space of cyber activities" [6]. By being officially recognized as a new battlefield and domain of warfare next to the land, sea, air and space [7], cyberspace is still under development and is shaping its existence.

A crucial moment in the 21st century history was the 9/11 event. This represents a trigger moment in realizing the importance of security and the role that cyber capabilities can play. Different countries have invested in their resources, strategies and capabilities and have considered the possibility of a Cyber 9/11 or a Cyber Pearl Harbour [8]. More than 30 countries have integrated cyber capabilities in their armed forces [9] and more than 140 countries invest in new ones [10].

In 2010 Stuxnet was discovered and shocked the whole world. This was an awareness moment at global level of the existence and utilization of a mean or capacity created completely out of code, which can impact beyond borders of cyberspace. More countries have joined this new battlefield, realize the important role that Cyber Security plays in the national and international security [11], [12] by investing in their strategies, policies and programs [13] and by preparing for possible conflict situations by creating new plans of cyber weapons implementation and use. We are now in a time of struggle trying to understand what they mean, how they can be used and how they can impact our society and our lives. At international level, cyber weapons are an uncertain concept due to the fact that there is no accepted global definition and there is a lack of research concerning their profile, action and impact from a multidisciplinary or interdisciplinary perspective. We are able to define and profile conventional weapons such as melee weapons, archery weapons, firearms and explosives or unconventional weapons like weapons of mass destruction e.g. chemical, biological, nuclear or radiological and improvised weapons; we should also be able to do the same thing concerning cyber weapons. That being said, decision makers have a difficult mission when they have to deal with the impact of cyber weapons utilization. Therefore, we propose a conceptual framework that helps understanding, profiling and dealing with cyber weapons.

This article is organized as follows. The second section introduces a conceptual design model that discusses the context of use of cyber weapons and represents the settlement in describing their life cycle. The third section proposes a definition for cyber weapons from a cyber and military perspective. For a better understanding, the structure of cyber weapons will be analysed. The fourth section presents characteristics and classification criteria of cyber weapons as necessary components in realizing their profile. In order to exemplify and validate the framework. In the fifth and the sixth sections we evaluate this framework by proposing a profiling matrix for Stuxnet, Operation Orchard and Black Energy and by conducting an exploratory case study on Stuxnet. It is estimated that more warriors will come in this battlefield; therefore, in the end we briefly present our future

C.M. Author is currently doing her multidisciplinary PhD in Cyber Operations and Cyber Security at Delft Technical University, Netherlands Defense Academy and TNO in The Netherlands (e-mail: clara.maathuis@tudelft.nl).

W.P. Author is currently Assistant Professor in Cyber Risk at Delft University of Technology in The Netherlands (e-mail: w.pieters@tudelft.nl).

J.v.d.B Author is currently Full Professor in Cyber Security at Delft University of Technology and Leiden University in The Netherlands (e-mail: j.vandenberg@tudelft.nl).

research.

II. Context Of Use Of Cyber Weapons

Sun Tzu, Chinese general, military strategist and philosopher claimed that "The supreme art of war is to subdue the enemy without fighting" [14]. Due to the evolution of technology, warfare can be extended in this man-made domain - cyberspace - by making use of cyber weapons, during cyber warfare by either supporting or amplifying the conflict [15] which makes it a real threat to the national security [16] that needs international cooperation in providing optimal solutions [17]. In this settlement, we illustrate in the following figure a conceptual design model that represents the context of use of cyber weapons and we continue by explaining each component of it.

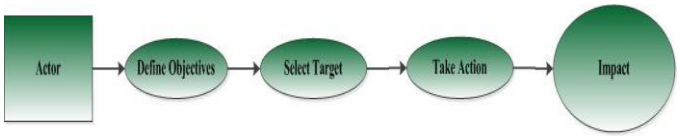

Fig. 1. Conceptual design model of context of use of cyber weapons.

- Actor: is responsible for conducting cyber operations or activities having a purpose in achieving military objectives [18].
  a) State actors: are states, their governments or institutions that have the power, knowledge and resources to authorize cyber weapons at a highly sophisticated level. Normally in this case many procedures have to be designed, followed and implemented. This process can take longer time, some times longer than expected, be less flexible and less dynamic than by a process organized by a non - state actor. However, the difference between state and non - state actors can be seen in the availability of resources (intelligence, personnel, equipment etc.) and consequently maybe in the quality, innovation and intelligent methods used to implement cyber weapons [19]. The available evidence seems to suggest that Stuxnet had a "sophisticated design, which a state could afford" [20].
  b) Non - state actors: are non - state or non - governmental institutions, groups or organisations of people that decide to organize, implement and use cyber weapons on their own, without being associated to any state actor. Examples of non - state actors are: hacktivists, individual professionals, security researchers, private organisations or institutions [21], [22]. They can have other types of motivations, such as personal, economical, ideological or ethical. Due to the fact that anyone can now have access to advanced knowledge and technology, the level of sophistication of state actors can also be reached sometimes by non - state actors by dealing with a diffusion of power in cyberspace [23].
  c) Hybrid actors: are represented by a combination of state and non - state actors, either a state actor supported by a non - state actor or a non - state actor supported by a state actor.

Actors involved in cyber warfare make use of their cyber power as the main informational instrument of power [24] by creating and employing different tools and techniques as means and methods to gain advantage on their adversaries [25], [26] inside and/or outside cyberspace.

- Define Objectives: objectives are defined goals that an actor wants to achieve (inside or outside cyberspace). In order to do that, he will define and select the right targets, take the action that will fulfil his ambition and reach the end state.
- Select Target: target is an entity, an object or a person that can be engaged in order to achieve advantage on the adversary. In other words, targets are engaged to achieve objectives or desired types of impact by an actor. The process that deals with selecting and prioritizing targets is called targeting process. Hence, an analysis is conducted to decide if executing a set of actions contributes to achieving the desired end state.
- Take Action: once an actor has defined and planned its objectives and targets, he will employ a cyber weapon. This will conduce to a set of different types of effects, the impact of an operation or activity.
- Impact: is a physical or a non-physical result/effect of an action or another effect. We define desire or intent as criteria of classification and we consider expectation as dimension of classification for each category since some results can be expected and others unexpected. Based on this, we describe the following categories of impact or effects of cyber weapon use:
  a) Desired impact: this category of impact describes the results that are desired or intended and that will contribute to a desired end state, achieving the mission.
  b) Undesired impact: this category of impact describes the undesired results that negatively influence achieving the desired end state. When planning and engaging into an operation, collateral damage should be considered. An estimation (before the employment of a cyber weapon) and assessment (after the employment of a cyber weapon) of collateral damage is done by remaining in the boundaries of the LOAC (the Law of Armed Conflict). The available literature on Stuxnet suggests that its intention was to limit collateral damage [27].

Considering expectation dimension we define the following categories that apply to both desired and undesired impact:

a) Expected effects: this category of impact describes the expected results even if was or wasn't intended from the beginning.
b) Unexpected effects: this category of impact describes the unexpected results that can have multiple consequences concerning dimensions like social, economic, politic etc.

We have described the context of use of cyber weapons. However, they have their own life cycle that needs to be analysed in order to be able to define and profile them. This process begins with the initial phase when the cyber weapon is

only a concept or an idea, and goes to the final phase when the cyber weapon exists and has been used. Practically it corresponds with the *Action* component from the model that we have just introduced and will be evaluated with the analysis that we will do on three cyber weapons in the last section. Based on analysing the approaches presented in [28] - [35], we distinguish the following phases of the life cycle of a cyber weapon:

- Phase I - *Project Definition*: in this phase the concept of the cyber weapon is defined from both a strategic and managerial perspective. Therefore the architecture of a cyber weapon is created and the main functionality is identified [28].
- Phase II - *Reconnaissance:* in this phase a research about the target is done in order to find possible existing vulnerabilities that can be exploited by collecting useful data and information. This phase is about learning and gaining as much information as possible about the system selected to be attacked [29].
- Phase III - *Design*: in this phase the design of cyber weapon is described. Detailed functionalities, specifications, tasks and deadlines for every module or component are translated and presented by making use of different diagrams, models and use cases that will help engineers to understand what and how they have to implement the project [30], [31].
- Phase IV - *Development*: in this phase engineers will implement the code of the cyber weapon by using diverse programming and/or scripting languages, as well as use cases and test cases that will be used in the testing phase.
- Phase V - *Testing*: in this phase engineers will make use of the use cases and test cases defined in the previous phase, will prepare a testing environment that should be a mirror or as close as possible to the esential part or component of the real environment where the cyber weapon will be launched in order to simulate the real situation of attack. This phase is a *condicio sine qua non* meaning that it is essential and very important that testing procedures are defined and implemented to see if the desired objectives are achieved. [32]. There are experts consider that Stuxnet was tested before it was used. One of them has declared for The New York Times that "the reason the worm has been effective is that the Israelis tried it out" [33].
- Phase VI - *Validation*: in this phase results from phase V are compared to objectives and functionalities defined in phases I and III. If the result of this comparison is positive, then the cyber weapon can be prepared to intrude the target system, otherwise patches should be done by going back to Phase III, IV and V.
- Phase VII - *Intrusion and Control*: Since the cyber weapon was validated and ready to be launched in the previous phase, in this phase two processes are involved. The first process represents the actual intrusion, more precise the moment when the cyber weapon gets inside the target system. The intrusion can be realised by having physical or remote access to the system. The second process is getting control of the system in order to monitor it and decide when is the right moment to launch the attack [34].
- Phase VIII - *Attack*: in this phase the attack is launched by activating (remotely or not and automatically or not) the most important part of the cyber weapon, the payload that will continue to fulfill its objective.
- Phase IX - *Maintenance*: in this phase the action of the cyber weapon is monitored in order to be sure that desired effects are achieved. If things that are not according to the plan are happening, measures will be taken to solve the problem and continue the attack or directly going to Phase X when the chance of being discovered becomes too big.
- Phase X - *Exfiltration:* this phase the life cycle of the cyber weapon ends and the cyber weapon is removed from the target system. We consider three cases of exfiltration. In the first case, it is in the interest of the attackers that they proactively delete any traces of their intrusion and attack on the target. In the second case, maybe it is not in the interest of the attackers to delete the traces of their actions since the goals are achieved and the problem of attribution in cyberspace is persistent [11]. In the third case, the attackers don't want to delete their traces in order to make a point about their presence and actions. When conducting digital forensic actions in order to detect attacker's identity and the impact of his actions, time plays an important role since it can offer details about the process of creation, launching, utilization and stopping the action of a cyber weapon. Attackers on a Ukrainian energy plant that have used Black Energy have tried to cover their traces and to look as if they were not in the systems by destroying some of the computers. However, some Ukrainian security experts have succedeed on pointing the attack to the Russian government [35].

III. Defining Cyber Weapons

As we have seen in the previous section, in the model that we have introduced, in order to achieve his objectives and get advantage against adversaries, an actor will select one or more targets and take action by using a cyber weapon. We consider this our starting point in the interest of presenting our definition of cyber weapons.

Before we do that, we will dissect the *cyber weapon* concept and analyse the meaning of each term. It is important to mention that there is no globally accepted definition for the concept *cyber* or terms that contain the concept *cyber*. The Oxford Dictionary explains the etymology of the word *cyber* as a word derived from the Ancient Greek κυβερεω (kybereo) that means to steer or to control, and it is used as an attribute or adjective next to other words. The same source defines the word *weapon* as "a thing designed or used for inflicting bodily harm or physical damage" [36]. Along these lines, the "Tallinn Manual on the International Law Applicable to Cyber Warfare" [37] sees cyber weapons as one of the cyber means of warfare "capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects". Since

intelligence, espionage tools have the purpose to collect data and intelligence and are not intended to produce direct physical damage, we exclude them from the beginning as being cyber weapons. Along similar lines, [38] argues that "Weaponry is not a tool of espionage."

For the purpose of this article, we propose the following definition for a cyber weapon:

A computer program created and/or used to alter or damage (an ICT component of) a system in order to achieve (military) objectives against adversaries inside and/or outside cyberspace.

We continue by explaining each component of the given definition:

Computer program can either be a software application or a script because programming and scripting languages allow control of both data and hardware that serve diverse roles.

Created or used because a cyber weapon can be created (designed and implemented) and used by the same state, group, organization or person or used because someone can buy a cyber weapon according to his needs. Later in this section we will elaborate this subject.

To alter or damage because the purpose of a cyber weapon is to change or to damage temporary or permanent a target e.g. a system or an application, in the physical or in the digital world.

A system or an ICT component of a system because the target can be an ICT system e.g. application, data, device or it can be a non - ICT system that contains an ICT component that represents practically the carrier to the desired target.

To achieve (military) objectives against adversaries since it is aimed at reaching specific goals and targets. However, the impact can be on neutral or allied parties and even on those who deployed it.

Inside and/or outside cyberspace because the impact can be: a) inside or outside cyberspace, b) considering geographical dimension, at local (domestic or national) level or global (at international) level. The impact can be limited to the targeted systems or it can spread to others, even to the human domain, altering the behaviour of people and organisations.

Taking into account the fact that we have described the context of use of cyber weapons and we have defined them, to be able to profile them, we also need to have knowledge of their structure. Therefore, we continue by defining and analysing their structure. We are performing that by having in mind the relation between objectives, action and impact, and we are mapping this vision to a layered structure that contains three components: the first layer is the access, the second layer is the transport and the third layer is represented by the payload.

- The *access* layer is based on a vulnerability that can be exploited; it is practically the enabler and the gate into the system for a cyber weapon in order to achieve the attacker's goals [11], [22]. The nature of access can be:
  a) Software: vulnerabilities (bugs) that have not been patched even if their existence was known or unknown.
  b) Hardware: vulnerabilities in design of hardware or channel components.
  c) Configurations: mistakes in installing, configuring or updating/upgrading a system.
  d) Other: mainly related to the human factor by giving access not in a proper manner to another entity or by allowing access to another entity without knowing that the system can become vulnerable. Edward Snowden and NSA files show that the insider threat is the biggest threat since someone that is strongly related to a system is able to find the deepest and most critical vulnerabilities or to make use of information that should remain secret, inside the company or institution [2].

There is support for the claim that vulnerabilities and cyber weapons are for sale on the black market [39] - [41]. On this market, cyber weapons are created by different groups (individuals or specialized companies), distributed by secret and very connected networks and bought and used by others - the attackers. Vupen is a company founded in 2004 by Chaouki Bekrar and does research and development in the area of zero-day vulnerabilities in different platforms and applications that are sold to law enforcement and intelligence agencies [42]. One of its biggest customers was NSA [43]. Recently Bekrar launched a new company named Zerodium that sells exploits respecting "international regulations, we only sell to trusted countries and trusted democracies. We do not sell to oppressive countries" [44].

- The *transport* layer represents the mechanism of delivering and propagating the software components of a cyber weapon in the attacked system. The transport can be realized at: a) logic or data level via websites, certificates, phishing etc. [19] and b) physical level where the transport is realized using external devices like CDs, DVDs, USB sticks etc.
- The *payload* layer is a software application or a script designed, created or used to compromise data or a system target. Since the payload is constructed and used by thinking to the impact, [45] considers it as the *raison d'être* of a cyber weapon. The payload can have one of the next architectures:
  a) Single - module architecture: it is the case of a simple single objective or function that the cyber weapon has to achieve.
  b) Multi - module architecture: it is the case of a complex objective or multiple objectives or functions that the cyber weapon has to achieve.

IV. Profiling Cyber Weapons

In the previous sections of this article we have seen that the reason behind the creation and utilization of cyber weapons is the idea of achieving ones objectives in a conflict situation. In this section we continue by creating a multidimensional profile of cyber weapons. We are pursuing that by having a look at the characteristics and criteria of classification of cyber weapons.

Based on our findings, we determine the following characteristics of cyber weapons:

- Target specific: cyber weapons are addressed to specific targets in order to achieve desired objectives. Stuxnet targeted the Iranian uranium program and attacked the nuclear facility from Natanz that "caused the centrifuges to break down without any notice or apparent reason" [46]. Behind target and objectives are motivation and interests.
- Intangible: cyber weapons have a logic nature that makes them virtual and intangible to the physical world. They are non - kinetical weapons that can have kinetical effects and non - kinetical effects.
- Diversity of knowledge: when creating and using cyber weapons, one must know diverse and deep information about its target and objectives.
- Less expensive: in many cases cyber weapons represent a cheaper alternative to conventional weapons having "minimal expenses in lives and resources" [47] - [49].
- Configurable: cyber weapons can have one or more variants depending on the vulnerabilities that they exploit:
  a) Single: this is the case when only one variant of a cyber weapon is created based on an existing vulnerability and then used.
  b) Multi: this is the case when more variants of a cyber weapon are created based on an existing vulnerability and then used. It is possible that a cyber weapon can have more variants depending on the target, objectives and mission.
- No re-use: cyber weapons have well defined functionality and once they are used, they can be considered exposed. In case of taking proper countermeasures, they cannot be used in the same way again [27]. However, if countermeasures are not taken, it is possible to use the same cyber weapon again.
- Violent nature: in [27] the author argues that if an attack in cyberspace causes physical damage, then it can be considered a violent act.

We propose the following classification criteria of use of cyber weapons:

- Purpose:
  a) Offensive: to attack an adversary.
  b) Defensive: to defend from an adversary.
  c) Multipurpose: in [48], the author considers that it is another class of cyber weapons that can be used for both offense and defence.
- Use:
  a) Single: the case where only one cyber weapon is used.
  b) System: while [50 - 51] consider a cyber weapon system as "a combination of one of more offensive cyber capabilities ", [52 - 53] and the older version [54] consider a weapon system as "a combination of one or more weapons" having "related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency" [50 - 54] For the purpose of this article we will comply with the second vision and we will consider a cyber weapon system as being a combination of offensive, defensive or multipurpose cyber weapons that are designed and function as a whole system.
- Sophistication:
  a) Highly sophisticated: in case of investing large amounts of resources in the process of acquisition or implementation of a cyber weapon. It can correspond to an actor that can invest extensive resources and use innovative and intelligent methods and technologies.
  b) Lowly sophisticated: in case of investing a reduced amount of resources in the process of acquisition or implementation of a cyber weapon. It can correspond to an actor that uses only open sources platforms and applications or less innovative and intelligent methods and technologies.
- Area of action:
  a) Local: is the case where only the targeted system is affected.
  b) Regional: is the case where effects can be seen in more systems in the nation of the targeted system.
  c) Global: is the case where more systems are affected at global level.

In cyberspace it is difficult to speak about borders. We can think of Stuxnet that had a global impact even if it is supposed to be designed to act locally.

V. Profiling Matrix For Three Cyber Weapons

In this section we will analyse and profile three cyber weapons, Stuxnet, Operation Orchard and Black Energy. Before we picture the profile matrix that we have created, we briefly introduce each cyber weapon. Stuxnet was discovered in 2010 by a Belarus company called VirusBlockAda; after long investigations, international experts have concluded that it was meant to target the Natanz nuclear facility in Iran and has damaged around 1000 centrifuges. Operation Orchard was discovered in 2007 in Syria; after investigations, international experts have agreed that it was used to neutralize Syrian radar systems in order to destroy a Syrian nuclear facility in the Deir ez-Zor region by an aerial attack. Black Energy was discovered in 2015 in Ukraine; international experts have concluded that it was used to target the energy plant in the Ivano - Frankivsk region and many cities were left without energy for some hours, computers and phone lines were destroyed.

We are conducting this analysis with the intention of illustrating and evaluating our conceptual profiling framework that we have defined. Furthermore, in the table below we present our profiling matrix that helps decision makers and academia better understand what cyber weapons mean and what the impact scale is.

TABLE I
Cyber Weapons Profiling Matrix

Name Parameter	**Stuxnet**	**Operation Orchard**	**Black Energy**
Purpose	Offensive	Offensive	Offensive
Sophistication	Highly-sophisticated. Some experts	Highly-sophisticated. Some experts	Highly-sophisticated. Some experts

	have concluded that it was created and orchestrated by US and Israel [55].	have concluded that it was created and orchestrated by Israel [59].	have concluded that it was created and orchestrated by the Russian hacking group Sandworm Team [61] - [63].
Target specificity	Iran's nuclear program	Syria's nuclear program to build a nuclear reactor	Ukraine's energy system
Configurable	According to Hamid Alipour, deputy head of Iran's Information Technology Company, it had more versions [56].	Single	According to Kaspersky it's one of the Black Energy APT cyber attack family that goes back to 2014 [64].
Diversity of knowledge	Strong technical skills: exploited a Windows vulnerability, had advanced knowledge of PLCs and Siemens systems, nuclear processes and was tested in a mirror environment [27], [34], [57].	Strong technical skills: advanced and specific knowledge of electronic warfare and air defence [59].	Strong technical and social engineering skills: exploiting the network and getting access to the ICSs and UPSs systems, plus advanced knowledge of ICS, power and electrical systems [62].
Use	Single	Single	System: against three distribution centres..
Time	Roots have been found since 2009. However, it was discovered in June 2010.	Used in 2007, but planted one year before [60].	Used on December 23, 2015. Was fast discovered and analysed.
Area of action	Global: Indonesia, India, U.S. and other countries [58].	Local: Al Kabir complex in Syria [59].	Regional: affected half of the people from Ivano-Frankivsk region, Ukraine [62].
Violent nature	Yes	Yes	Yes

This analysis reflects the effectiveness and applicability of this framework: it does not matter where or when these cyber weapons were created or used, nor by whom, they all follow the same pattern that we have captured and expressed.

VI. Case Study: Profiling Stuxnet

We have introduced Stuxnet in the previous section; we will continue in this section by applying the components of our framework to it in order to reflect a more in depth analysis of a cyber weapon, create a concise profile of it and emphasize the applicability of our framework.

By being considered the first "peacetime act of cyberwar" [65] or the first cyber weapon that was designed, implemented and used against a specific target [28] - a critical infrastructure system of a state actor [19 - 20] - Stuxnet was a computer program written in multiple programming languages, a combination of high level and low level programming languages: C/C++ and Assembler, it was compiled in Microsoft Visual Studio 2005 and Microsoft Visual Studio 2008 by a professional team of engineers who probably worked at its development and testing somewhere between six months and one year; it has proved an impressive amount of knowledge and experience on working with Industrial Control Systems, more precise Programmable Logic Controllers produced by Siemens and used in the Natanz nuclear facility [34], [66]. Stuxnet had a multi - module architecture that reflects a layered, structured and systemic way of thinking and implementing in order to map an advanced and complex objective to a set of multiple simpler objectives and functions that should be accomplished [34], [45].

Although we do not know for sure who is really behind Stuxnet, the grade of knowledge, professionalism and investment behind of it reveals the implication of state actors: in this regard some experts opinions suggest the involvement and collaboration between state nations like U.S. and Israel [20], [55], others suggest state nations like India and Russia [67]. There is an ample amount of literature and reports on Stuxnet's objective: to sabotage the nuclear facility from Natanz [23], [41] that targeted the nuclear program of Iran [55], [68]. This was possible by intruding the network with an infected USB and by successfully exploiting four existing Windows vulnerabilities [23] on systems that run WinCC and Step 7 dedicated software from SIMATIC which allows programming and controlling PLCs of physical processes. In other words, ICT entities (both hardware and software) such as an USB stick (transport layer) and four software vulnerabilities (access layer) represent the carriers to a non-ICT system that can still be targeted by containing ICT components that can be altered or damaged to achieve ones objectives.

The payload layer had a multi modular architecture as well and contained two components: the first payload to change the rotation rates of the nuclear centrifuges from Iran's facility by causing physical damage to the machines and the second payload to open and close the valves to flow gas to other centrifuges by influencing the quality of the products of the refinement process without being noticed on the operator interfaces [34]. Stuxnet could update itself by communicating with a Command and Control server via HTTP or by a call to a RPC server in a peer to peer communication [55]. Despite the fact that Stuxnet was a targeted attack with a precise objective, designed and developed to limit possible collateral damage, it had a global impact by infecting 100.000 computer systems from countries like Iran, Indonesia, India, Pakistan, Uzbekistan and other countries [66].

As we have seen from the evaluation conducted in the previous and current section, this conceptual framework contributes and helps decision makers and academia in better understanding and dealing with the impact of different cyber activities or events considered cyber warfare or situations of cyber weapons use by defining and profiling them.

VII. Conclusion

In 2011 the U.S. Department of Defence has pointed that there is "no international consensus regarding the definition of 'cyber weapon'". Although cyber weapons have become reality, five years later we are in the same situation. In this article we propose a multidisciplinary conceptual framework that defines and profiles cyber weapons. This framework brings a contribution to decision makers and academia from the military, cyber and legal domains when they have to understand and deal with the implications and consequences of cyber weapon phenomenon. Therefore, to illustrate our framework, we have conducted an exploratory case study and proposed a profiling matrix in order to prove that our framework can cross time dimension by being applied on three different moments of time and in three different situations of cyber weapon utilization.

When thinking about writing pages of the future, we have to keep in mind that cyberspace is a global common [69], both a military and a civilian domain [70] where time and space have different meanings than in other domains. Philosopher Eric Hoffer believed that "The only way to predict the future is to have power to shape the future." Shaping the future poses great challenges considering the growing advancement of technology and the freedom of access it. Everyone can download Stuxnet's source code, modify it and create new cyber weapons. Scholars and experts claim that this is already happening since the blueprint is provided. Predicting the future, a future of a strongly interconnected human - machine world, makes us want to investigate the role cyber weapons will play in it and the way they will impact coordinates of our lives. This is our mission for the near future.

Acknowledgment

We would like to thank to prof. dr. Paul Ducheine BG and drs. Rudi Gouweleeuw MA for their valuable feedback in the process of reviewing this article.

References

[1] Internet Live Stats. "Internet Users" [Online]. Available: http://www.internetlivestats.com/internet-users/. [July 07, 2016].
[2] P.W. Singer and A. Friedman, "Cybersecurity and cyberwar: what everyone needs to know", Oxford University Press, 2014.
[3] ISO/IEC 27032:2012, *Information technology - Security techniques - Guidelines for Cybersecurity*, ISO, 2012.
[4] P. Cornish et al. "On Cyber Warfare", London: Chatham House, 2010.
[5] United States Army Joint Publication 3-12 (R). *Cyberspace Operations*, 2013.
[6] J. van den Berg et al. "On (the Emergency of) Cyber Security Science and its Challenges for Cyber Security Education", NATO STO/IST 122 Symposium, 2014.
[7] W.J. Lynn III. (2010, September/October). *Defending a New Domain: The Pentagon's Cyberstrategy* [Online]. Available: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain
[8] D. Jennings (2015, September 1). *Homeland Security Preparing for 'Cyber Pearl Harbor'* [Online]. Available: http://www.offthegridnews.com/current-events/homeland-security-preparing-for-cyber-pearl-harbor/
[9] R. Berlk and M. Noyes, "On the Use of Offensive Cyber Capabilities", The Office of Naval Research, U.S., 2012.
[10] P. Suciu (2014, December 21). *Why cyberwarfare is so attractive to small nations* [Online]. Available: http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/
[11] United States Air Force 3-12. *Cyberspace Operations*, United States Army, 2011.
[12] F. Harre, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?", NATO CCDCOE.
[13] K. Geers, "Cyberspace as Battlespace", Black Hat Webcast, 2014.
[14] S. Tzu, "The art of war".
[15] P. Shakarian et al, "Introduction to Cyber Warfare: a Multidisciplinary Approach", Elsevier, 2013.
[16] K. Geers, "Sun Tzu and Cyber War", NATO CCDCOE, 2011.
[17] K. Geers, "Pandemonium: Nation States, National Security, and the Internet", NATO CCDCOE, 2014.
[18] United States Department of Defense. *The DoD Cyber Strategy*, 2015.
[19] T. Herr and E. Armbrust, "Identification and Implication of State Authored Malicious Software", The George Washington University, 2015.
[20] S. Shaheen, "Offence - Defence balance in Cyber Warfare" [Cyberspace and International Relations, Springer, p. 77-93, 2014].
[21] NSCS, *Cyber Security Assessment Netherlands 2015*, National Cyber Security Centre, 2015.
[22] J. Andress and S. Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", Elsevier, 2011.
[23] J.S. Nye, "Power and National Security in Cyberspace" [America's Cyber Future: Security and Prosperity in the Information Age, vol. 2, c. 1, p. 5-24, 2011].
[24] J.J. Wirtz, "Cyber War and Strategic Culture: the Russian Integration of Cyber Power into Grand Strategy" [K. Geers, Cyber War in Perspective: Russian Aggression Against Ukraine, c. 3, p. 29 – 37, NATO CCDCOE, 2015].
[25] H. Lin, "Cyber Conflict and International Humanitarian Law", International Review of the Red Cross, vol. 94, no. 886, 2012.
[26] S. H. Starr, "Towards an Evolving Theory of Cyberpower", 1st International Conference on Cyber Conflict, 2009.
[27] M. Turner, "Is there such a thing as violent act in cyberspace?". International Security and Intelligence Summer School, University of Cambridge, 2013.
[28] J. Dougherty (2015, November 9). *The Pentagon is developing cyber weapons that are extremely lethal* [Online]. Available: http://www.cyberwar.news/2015-11-09-the-pentagon-is-developing-cyber-weapons-that-are-extremely-lethal.html
[29] F. Schreier, "On cyberwarfare", DCAF Working paper, 2015.
[30] K.A. Demir, "Challenges of weapon systems software development", Journal of Naval Science and Engineering, vol. 5, no. 3, p. 104-116, 2009.
[31] E. Iasiello, "Are cyber weapons military effective tools?", Journal of Military and Strategic Affairs, vol. 7, no. 1, 2015.
[32] E. Tyugu, "Command and control of cyber weapons", 4th International Conference on Cyber Conflict, 2012.
[33] W. J. Broad et al (2011, January 15). *Israeli test on worm called crucial in Iran nuclear delay* [Online]. Available: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0
[34] N. Falliere et al, *W32. Stuxnet Dossier*, Symented, 2011.
[35] K. Zetter (2016, January 20). *Everything we know about the Ukrainian power plant hack* [Online]. Available: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/
[36] Oxford Dictionary, Oxford University Press.
[37] M. N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University Press, 2013.
[38] T. Herr, "PrEP: A Framework for Malware & Cyber Weapons", The Journal of Information Warfare, vol. 13, no.1, p. 87-106, 2014.
[39] M. Baer, "Toward Criteria for International Cyber Weapons Bans", East West Institute - The Global Cyberspace Cooperation Summit, 2015.
[40] P. N. Stockton and M. Golabek-Goldman, "Curbing the Market for Cyber Weapons", Yale Law & Policy Review, vol. 32, art. 1, 2013.
[41] H. Shane (2014, March 25). *Black Market for Malware and Cyber Weapons is Thriving* [Online]. Available: http://foreignpolicy.com/2014/03/25/black-market-for-malware-and-cyber-weapons-is-thriving/
[42] WikiLeaks, *Vupen: Threat Protection Program*, 2011.
[43] M. J. Schwartz (2013, September 17). *NSA Contracted With Zero - Day Vendor Vupen* [Online]. Available: http://www.darkreading.com/risk-management/nsa-contracted-with-zero-day-vendor-vupen/d/d-id/1111564?

[44] D. Fisher (2015, July 24). Vupen Founder Launches New Zero - Day Acquisition Firm Zerodium [Online]. Available: https://threatpost.com/vupen-launches-new-zero-day-acquisition-firm-zerodium/113933/

[45] T. Herr and P. Rosenzweig, "Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP model", The Journal of National Security, Law & Policy, vol. 8, no. 2, 2015.

[46] SANS Institute, "Information warfare: cyber warfare is the future warfare", Global Information Assurance Certification Paper, 2004.

[47] R.M. Rustici, "Cyberweapons: Leveling the International Playing Field", The U.S. Strategic Studies Institute, 2011.

[48] S. Mele, "Cyber-weapons: legal and strategic aspects", Istituto Italiano di Studi Strategici, 2013.

[49] D. Denning, "Reflection on Cyberweapons Controls", Computer Security Journal, vol 16, no. 4. pp. 43-53, 2000.

[50] United States Department of Defense. *Joint Terminology for Cyberspace Operations*, United States Army, 2010.

[51] United States Strategic Command. *The Cyber Warfare lexicon*, United States Department of Defense, 2009.

[52] United States Army Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, United States Army, 2016.

[53] United States Army Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, United States Army, 2009.

[54] United States Army Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, United States Army, 1994.

[55] A. Thabet, "Stuxnet Malware Analysis Paper", Code Project, 2011.

[56] S. Writers (2010, September 27). Stuxnet worm rampaging through Iran: IT official [Online]. Available: http://www.spacedaily.com/reports/Stuxnet_mutating_rampaging_through_Iran_IT_official_999.html

[57] R. Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve", The Langner Group, 2013.

[58] J. Shearer, "W32.Stuxnet", Symantec, 2010.

[59] R. Clements (2014, September 06). How a Syrian nuclear facility was destroyed by the Israeli Air Force 7 years ago today [Online]. Available: https://theaviationist.com/2014/09/06/operation-orchard-anniversary/

[60] K. Zetter (2009, March 11). *Mossad Hacked Syrian Official's Computer Before Bombing Mysterious Facility* [Online]. Available: https://www.wired.com/2009/11/mossad-hack/

[61] SANS ICS, "Analysts of the Cyber Attack on the Ukranian Power Grid: Defense Use case", ICS SANS, 2016.

[62] Fire Eye Industry Intelligence Report, "Cyber Attacks on the Ukranian grid: what you should know", Fire Eye, 2016.

[63] J. Stone (2016, January 08). *Russian Hacking Group Sandworm Targeted US Tefore Knocking Out Power In Ukraine* [Online]. Available: http://www.ibtimes.com/russian-hacking-group-sandworm-targeted-us-knocking-out-power-ukraine-2257194

[64] GReAT - SECURELIST Kaspersky Lab. "Black Energy APT Attacks in Ukraine employ spear phishing with Word documents", Kaspersky Lab, 2016.

[65] A. C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate", 2012.

[66] A. Matrosov et al. "Stuxnet under the microscope", Esset, 2011.

[67] H. Porteous, "The Stuxnet Worm: Just Another Computer Attack or a Game Changer", Canada Library of Parliament, 2010.

[68] Kaspersky Lab. "Stuxnet Spotlight", Kaspersky Lab, 2011.

[69] S. Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law", University of Pennsylvania Law School, 2012.

[70] B. Mueller, "On the need for a treaty concerning cyber conflict", The London School of Economics and Political Science, 2014.