Effects Assessment for Targeting Decisions Support in Military Cyber Operations

Maathuis, E.C.

DOI
10.4233/uuid:c46af1d3-77b7-40f8-9e0a-3ad634bbdb47

Publication date
2020

Document Version
Final published version

Citation (APA)
Maathuis, E. C. (2020). *Effects Assessment for Targeting Decisions Support in Military Cyber Operations*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:c46af1d3-77b7-40f8-9e0a-3ad634bbdb47

Effects Assessment for Targeting Decisions Support in Military Cyber Operations

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus Prof. dr. ir. T.H.J.J. van der Hagen, voorzitter
van het College voor Promoties,
in het openbaar te verdedigen op 18.09.2020 om 15:00 uur

door

Emanuela-Clara Maathuis

Master of Science in Intelligent Systems – Artificial Intelligence

This dissertation has been approved by:

Promotor: Prof. dr. ir. J. van den Berg
Promotor: Assoc. Prof. dr. ir. W. Pieters

Composition of the doctoral committee

Rector Magnificus	Chairman
Prof. dr. ir. J. van den Berg	Promotor, TU Delft Leiden University
Assoc. Prof. dr. ir. W. Pieters	Promotor, TU Delft

Independent members

Dr. E. Armistead	Journal of Information Warfare
Prof. dr. B. van den Berg	Leiden University
Prof. dr. P.A.L. Ducheine	Netherlands Defense Academy University of Amsterdam
Prof. dr. ir. P.H.A.J.M. van Gelder	TU Delft
Prof. dr. ir. M.F.W.H.A. Janssen	TU Delft

Keywords: cyber security, cyber operations, cyber warfare, cyber weapons, artificial intelligence, intelligent systems, fuzzy logic, ontology, military operations, war, targeting, collateral damage, laws of war.

This research was funded by TNO and the Netherlands Ministry of Defense under a grant of the Netherlands Defense Ministry of Defense, in cooperation with the Netherlands Defense Academy, and Delft University of Technology.

Cover design: Clara Maathuis

Printed by: Gildeprint

Distributed by Delft University of Technology, Faculty of Technology, Policy and Management, Jaffalaan 5, 2628BX Delft, the Netherlands.

In memory of the ones I lost,
but always love…

“Life is a waterfall
We're one in the river
And one again after the fall.
Swimming through the void
We hear the word
We lose ourselves
But we find it all?”
(System of a Down - Aerials)

Acknowledgements

"If you know the enemy and know yourself,
You need not fear the result of a hundred battles.
If you know yourself, but not the enemy,
For every victory gained, you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle."
(Sun Tzu – The Art of War, musical interpretation: Sabaton – The Art of War)

Perhaps it is because I grew up in the heavy years after the fall of the communist regime which were full of painful stories regarding resistance, deportation, and immigration, that studying conflicts, and in particular wars, has always been one of my passions... maybe this brought me here. Perhaps it is because my biggest childhood loves were mathematics, air and space technologies, music, and drawing…maybe these brought me here. Or perhaps it is just a combination thereof.

This PhD journey was like learning an amazing, yet heavy dance where sometimes you have to be guided to make the right movements, other times you learn that there are no right movements, and ultimately you learn that you need to have control to be able to further guide. Now, at the end, I see that I have changed in so many ways.

These years have been among the heaviest of my life. Having to bury my father and uncle in the beginning of the final phase of my PhD, living in-between worlds, and being confronted with different challenges was difficult. Then I recall Therion – Rise of Sodom and Gomorrah: the song whose melodic line captures this journey.

Learning this dance was possible because of many intelligent and amazing people that I had the chance to work with and get in touch with. Thank you all, and I apologize for not being able to mention all your names here.

Paul, I am grateful to you for starting the initiative behind this research (SRO Cyber Operations) and materializing it together with TNO and TUD. Thank you for your guidance, support, and for showing me the importance of fundamental military-legal aspects in (cyber) warfare. I am also thankful to you for connecting me with other military experts from MoD.

Jan and Wolter, I am grateful to you for your guidance and support you showed me through this journey in research and science, although I know that you have also gone through difficult times. I am also thankful to you for connecting me with scientists from Denmark and U.K. in different settings.

Rudi, I am grateful to you for your guidance, support, encouragement, and for sharing your office with me although I had many questions during my military learning process. I am also thankful to you for showing me how beautiful science joints and supports applied science and practice, and connecting me with other military experts from TNO and MoD.

Dear supervision team: I am thankful to you all. In this journey, we have been through sunny moments of enthusiasm and cloudy moments of despair. Because of you, I have learned a lot and changed in many ways.

I am grateful to the members of my Graduation Committee for their willingness, availability, and time for reading my thesis and providing me valuable feedback.

I am also thankful to all the editors and reviewers of my publications for taking time to reading them and providing me useful feedback, as well as to all the participants that I met in different scientific settings for the interesting and insightful discussions we had.

I am also thankful to all TNO and MoD experts that I met, discussed with, worked with, and participated in the design and evaluation phases of my artefacts. I would also like to thank to all military experts from Canada, France, Germany, the Netherlands, and U.S. The brotherhood, support, and determination that I found here impressed me and changed me.

"…En het is zo stil in mij, ik heb nergens woorden voor
Het is zo stil in mij en de wereld draait maar door..."
(Van Dik Hout – Stil in Mij)

To all my roommate friends, ceai (i.e. tea) friends, PhD peer group friends as well as to all friends and colleagues from ICT section, TPM/TUD, TNO, and MoD, thank you for sharing good and bad moments with me, and finding time and space for our experiences, thoughts, and ideas over different topics: I wish you all further a wonderful career.

I am grateful for the support of TPM, TNO, and MoD secretaries and support services. I am also thankful for the nice discussions we had.

Dear family, friends, the ones I lost, and teachers that previously formed and inspired me, thank you all: you have contributed to who I am now.

Inima mea, everything I do, I do it for you: Thom Hanreich – Pina (Main Theme).

Clara,
Delft, Den Haag, Breda, Utrecht

Table of Contents

Chapter 1. Introduction

"Hello darkness, my old friend
I've come to talk with you again
Because of a vision softly creeping
Left its seeds while I was sleeping
And the vision that was planted in my brain
Still remains
Within the sound of silence."
(Simon and Garfunkel – The Sound of Silence)

1.1. Introduction

"Leven we in een droom wereld of is dit de realiteit?" ("Do we live in a dream world or is this the reality?") asks Mark Jansen (Jansen, 2006) at the beginning of a symphonic metal masterpiece played by Epica. Is this a dream world whose brain (software) is able to influence, disturb, or damage perceptions, processes, and systems? This research does not provide a direct answer to this question, but reflects on a type of war of whose existence and meaning totally depends on software: Cyber War. This new type of war, Cyber War – otherwise said, the execution of military Cyber Operations – has the ability to support or amplify different types of ongoing or future conflicts by altering, disturbing, damaging, or destroying different entities (actors and/or systems) in order to achieve the aim of one or more actors.

Cyber War(fare), is not anymore a new concept or phenomenon. It has already a history of more than a decade and is constantly present in the academic, professional (e.g. political, military, technical), and media discourses. However, each incident that is labelled as such, surprises again and again with its impact different audiences at global level. This can be exemplified when thinking about Cyber Operations like Operation Orchard used to neutralize a Syrian radar system in Syria in 2007, the ones conducted in Georgia during the Russian–Georgian war in 2008 used to undermine Georgian governmental expression capabilities at national and international levels, and Operation Olympic Games (Stuxnet) discovered in 2010 used to delay Iran's nuclear program. Such incidents continue to consternate global audiences due to the lack of understanding, awareness, and readiness in regards to the phenomena themselves as well as their effects.

Stuxnet is considered "a game changer…perhaps the first peacetime act of cyber war" (Foltz, 2012). It was a Cyber Operation conducted by U.S. and Israeli intelligence helped by Dutch intelligence (NLTimes, 2019), that was ordered and started under President George W. Bush and continued under President Barack Obama. Stuxnet was executed with a supportive role to other politic and diplomatic means while no war was going on between the parties/actors involved (Foltz, 2012; NLTimes, 2019; Stevens, 2019), and aimed at delaying the ongoing nuclear program of Iran. In order to do that, its creators exploited software and human vulnerabilities, and built Stuxnet as a malware type named worm that targeted specific PLCs (Programmable Logic Controllers) with the intention of altering and by that damaging some nuclear processes in Iranian nuclear facilities without being noticed on operators' interfaces (Falliere et al., 2011). Several investigations (Langner, 2013; Falliere et al., 2011; McDonald, 2013; Albright, 2012; Zetter, 2015) assessed that Stuxnet achieved its intended effects on its

targets and reached its aim, and through the damage produced, it could be seen as an act of Cyber War. Although countermeasures for limiting its unintended effects were taken, other systems were infected by Stuxnet at the level of performance and availability of their resources. The scale of Stuxnet's impact was global since it infected around 100.000 systems in countries such as India, Indonesia, and U.S. This led to long debates at international level towards understanding the context where this Cyber Operation was conducted, its nature, and meaning of its effects.

Since the number of Cyber Operations is increasing and their means and methods to produce effects are advancing by becoming more intelligent, automated, and adaptive, it is likely that they represent a realistic option to different actors against their adversaries (Maathuis et al., 2018) by targeting them and employing against them cyber weapons/capabilities/means (Boothby, 2012). However, correspondent models and methodologies for understanding Cyber Operations and assessing their effects do not exist yet. From the vast space of contexts of Cyber Operations (e.g. political, military, economic), to narrow down the scope of this research, we focus on the military domain. And to be able to address this gap inside the military domain, we aim in this research to assess the effects of Cyber Operations in order to support targeting decisions of military Commanders and members of his/her team (e.g. cyber advisors and military intelligence) in Cyber Operations with adequate decision support information. These decisions concern the proportionality assessment as well as further preparations for targets' engagement in Cyber Operations. To do that, we propose a set of five artefacts packaged into a modelling framework.

To be able to assess the effects of Cyber Operations, we first need to understand what are the means to producing them: cyber weapons. For the purpose of this research we define a cyber weapon as follows (Maathuis et al., 2016):

> 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.

The effects resulted from targets' engagement using cyber weapons could be found inside cyberspace (e.g. degradation with impact on availability of ICT systems) or outside cyberspace (e.g. human injury or destruction of non-ICT systems such as buildings). The way how we have classified and defined the effects considered is presented in Section 1.2.2. Furthermore, for supporting targeting decisions we have adopted the definition of the principle of proportionality which considers that an attack that can "cause incidental loss of civilian life, injury to civilians, damage to

civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" is disproportional, thus it must be banned (AP I Art.51(5)(b), 1977). To support targeting decisions, we have considered two perspectives or contexts of use: military-legal and military-operational, both further addressed in Section 1.2.2. To the end, our goal is to contribute to the integration of Cyber Operations as military operations that could be considered in military training, exercises, and operations in a war context.

1.2. Research Background and Motivation

In the next two sub-sections the background and motivation of this research are addressed in more detail. In order to capture knowledge from the cyber security domain for modelling Cyber Operations and their effects by considering, for instance, the layers of cyberspace and corresponding elements contained, we use a historical perspective described in Section 1.2.1. Next, to be able to capture knowledge from the military domain for modelling Cyber Operations as military operations and assessing their effects in a war context, we address the military targeting process and its corresponding military-legal dimensions in Section 1.2.2. These two dimensions form the context and background of this research.

1.2.1. From Cyber to Cyber Operations and their effects

"We do not see with our eyes, but with our mind. If the mind is empty, our eyes look without seeing.'' (Stefan Odobleja)

In this section we first establish the origins of concepts such as cyber, we go further to discussing what cyberspace means, and how it is structured as it is important to understand the places where the effects of Cyber Operations are aimed at and/or where they could be found. Finally, we address specific activities or incidents that were labelled as Cyber Operations or Cyber Warfare operations.

The cyber concept

In the mid-1990s took place the rise and salience of the concept 'cyber' as referring to ICT (Warner, 2012) technologies and techniques proposed and developed since decades before. As a term, 'cyber' or 'cyberspace' finds its origins in the Ancient Greek κυβερνήτης (kybernētēs) which means steersman, governor, or pilot, and relies on the following two foundational books (Pohoata, 2016; Vlada & Adascalitei, 2017):

- The first one is “Psychologie consonantiste” published in two volumes in 1938/9 (Odobleja, 1938; Odobleja, 1939) and written by the Romanian scientist Stefan Odobleja. Considered as the founder of consonantism and generalized cybernetics, Stefan Odobleja was educated and trained as medical doctor and military officer. In his book, he discusses cybernetics, systems thinking, and control.
- The second one is “Cybernetics: or control and communication in the animal and the machine” published in 1948 (Wiener, 1948) and written by the American mathematician and philosopher Norbert Wiener. Considered as the founder of the notion of feedback (as in engineering fields) and cybernetics, Norbert Wiener was educated in mathematics, zoology, and philosophy. In his book, he discusses cybernetics and feedback in relation to servomechanisms.

Cyberspace

Although there are no globally officially recognized definitions for cyberspace or for different cyber-terms, cyberspace is generally perceived as the environment resulting from the interaction between technology, services, and people (ISO, 2012; Maathuis et al., 2016; Cornish, 2012; U.S. Army, 2013). The ITU (International Communications Union) considers that cyberspace describes “systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks” (ITU, 2011). In this research, we consider that the core of cyberspace is captured in the definition provided by ITU since the key functional components of cyberspace are formed by physical-based systems and software-based solutions. On top of this, we consider that the first definition extends the ITU definition by including the human element since people’s role, their ICT-enabled activities, and their representation in cyberspace (e.g. identity) are as important as the technological infrastructure. Further in this research we address the human dimension of cyberspace (i.e. the people component of the first definition) by considering Cyber Operations as cyber activities executed by military actors. This means that we embed both perspectives of conceptualizing cyberspace.

After having explained what we understand by cyberspace, it is helpful to know how it is structured to be able to further address operations conducted in this man-created space (i.e. Cyber Operations) and their effects. There are several interpretations on structuring the technical core of cyberspace which find roots in the earliest vision on structuring computer networks using the OSI (Open Systems Interconnection) model-seven layers that define communication systems (Bryant, 2016). However, this structure is extended by incorporating the human/social dimension as well. Furthermore, a series of models for structuring cyberspace are discussed:

- (Libicki, 2009) as physical ("boxes and wires"), syntactic (instructions and protocols), and semantic ("the information that the machine contains").
- (U.S. Army, 2013; U.S. Army, 2018) as physical network (infrastructure and devices), logical network (software applications and network processes), and cyber-persona (direct reflection of the human element through digital representations of people that incorporate e.g. personal or organizational data such as e-mail accounts, phone numbers, social networks identities etc.).
- (Berg et al., 2014; Berg, 2019) as technical (the OSI layers), socio-technical (the layer of cyber activities), and governance.
- (U.S. Army, 2016b) as physical (geographic and physical network components), logical (logical network components), and social (persona and cyber persona components).

We can see that these representations are largely aligned with and extend with the OSI and ITU interpretations, and that there is a set of mappings between them which can be defined as follows:

- A physical mapping containing the physical infrastructure that supports cyberspace which can be found in the physical layer (Libicki, 2009), in the physical network layer (U.S. Army, 2013; U.S. Army, 2018), in the technical layer (Berg el al., 2014; Berg, 2019), and in the physical layer (U.S. Army, 2016b).
- A software mapping containing the logic-based applications that allow the physical layer to exist and function which can be found in the syntactic layer (Libicki, 2009), in the logical network layer (U.S. Army, 2013; U.S. Army, 2018), in the technical layer (Berg et al., 2014; Berg, 2019), and in the logical layer (U.S. Army, 2016b).
- An informational and social mapping with the information representation (e.g. of people) and flow between the hardware and software processes. This mapping is found between the semantic layer (Libicki, 2009), cyber-persona layer (U.S. Army, 2013; U.S. Army, 2018), soctio-technical and governance layers (Berg et al., 2014; Berg, 2019), and social layer ((U.S. Army, 2016b).

We have considered using the mapping between the structures abovementioned as it shows where these effects can be found and how they are defined on each of its layers (Chapter 5). Even more than that, the three-layered structure is helpful for understanding the operations/attacks conducted (Libicki, 2009) using the underlying ICT-based services in moments such as:

- When an actor is or is positioned as an attacker/offender and needs to fulfil its aim and by that finding a target to attack/engage using cyber weapons/capabilities/means, thus a-priori to executing a Cyber Operation. Taking into consideration the abovementioned layered structure of cyberspace as well as its defining and actionable aspects (ICT-based or ICT-embedding systems), a target can belong to the following layers. Firstly, to the first two layers of cyberspace which means that it has directly a physical or a logical/software nature and contains ICT elements that could be directly be engaged in a Cyber Operation. Secondly, to the third layer of cyberspace (semantic/persona) but is engaged through one or both of the other layers (physical and logical/software) since information and people through their representations cannot be directly engaged in a Cyber Operation if an ICT-based or ICT-embedding element is missing.
- When an actor is a defender, a neutral actor (e.g. researcher, in most cases), or an attacker/offender trying to take actions regarding a Cyber Operation or an entity (i.e. target or collateral). Such actions could be considered at one or more of the each considered layers, and could imply to: prevent, deter, protect, assess its impact/effects together with other implications and consequences, as well as respond and recover.

Cyber Operations and their effects

Considering their actor, aim, and nature, cyber incidents are sometimes classified in the following (limited set of) categories: cyber espionage (e.g. collection of sensitive data), cyber crime (e.g. internet banking fraud), Cyber Warfare (e.g.. military system degradation), and cyber terrorism (i.e. harming personal civilian values) (Brenner, 2006; INTEL.GOV; Weissbrodt, 2013).

From this set, we focus in this dissertation on Cyber Operations which we define as military operations conducted by one or more actors that intend to achieve their military aims using cyber capabilities/weapons/means (Maathuis et al., 2016) in the detriment of other actor(s) by deploying them through the physical and logical layers of cyberspace, and from there experiencing effects not only on these two levels, but also on the other levels. Thus, we refer to intentionally planned Cyber Operations. Such incidents happened in the last two decades in different places around the Globe. For instance, in 2008 against Georgia during the Russian-Georgian war, Stuxnet in Iran in 2010, as well as Black Energy and Not Petya conducted in 2015 and 2017, respectively.

In the light of these events, as well as their raise in significance and current global situation, developments, and threats, NATO (and earlier the U.S.) recognized cyberspace as a warfare domain i.e. "domain of operations" (NATO, 2016b), in other words "a man-made theatre of war" (ICRC, 2011).

During the years, due to technological advancements and flexibility or easiness of accessing them, cyberspace became the space of operations where state actors are not acting alone using digital resources against their adversaries, but also non-state or hybrid actors. Known non-state or hybrid actors are different groups or organizations such as Sandworm, Anonymous, or Daesh/Islamic State, and are ranging from script kiddies to highly skilled engineers (U.K. MoD, 2016) who are determined and active to reaching their aims against their enemies (Jensen & Banks, 2018). Cyber Operations are conducted by different actors to achieve their aims also outside of war (Schmitt, 2017; Sander, 2019), for instance, as the external involvement and interference with the U.S. presidential elections in 2016 (Gioe, 2018). In this way, two different contexts or regimes are considered for Cyber Operations conducted by states: i) inside war time with a supportive or amplifier role to other military operations, and ii) during peacetime, in other words, outside war time. This means that different legal frameworks are applicable with the exception of the Human Rights Law which is always applicable (Gill & Fleck, 2011). Fitton (2016) considers that an additional context or state is the 'gray zone' between war and peace, and argues that this is 'the primary characteristic of modern conflicts', and positions here the (hybrid) operations conducted by Russia in Ukraine (Fitton, 2016). To narrow down the scope of this research, we are positioned in the context of war. This fact implies that different perspectives of use for Cyber Operations and their means to produce effects (cyber weapons) are embedded in this research aligned with the i) context (war regime). These perspectives of use will be further addressed in Section 1.2.2.

We consider that Cyber War not only is coming, as Ronfeld announced it in 1993 (Arquilla & Ronfeldt, 1993), but it is already here to stay in the present and (near) future. It should then be perceived and understood through deeper and more dimensions than classical kinetical or non-kinetical warfare and classical laws of war because "it represents a radical shift in the nature of the wartime battlefield" due to its characteristics such as dynamism, anonymity, and offensive's advantage (Solce, 2008). This vision is aligned with the one of (Stone, 2013) which argues that Cyber War is real and will happen, as in contradiction to the famous Rid's (Rid, 2012) which argues (through historical and political lenses) that Cyber War will not take place.

Hence, the logical flow of Cyber Operations starts with actors who try to achieve their political and/or military goals by employing cyber weapons/capabilities (Boothby, 2012) against their adversaries (Maathuis et al., 2018). This is technically possible by exploiting one or more vulnerabilities of target(s) (Smart, 2010). Since more than 30 countries have included cyber weapons/capabilities in their military forces (Brown & Owen, 2012), among them all the current military super-powers e.g. U.S. (Vinik, 2015), the U.K. (Hopkins, 2011), and Russia (Raboin, 2011), this reflects their great potential as well as impact or effects in the form of implications and consequences.

Since we focus on military Cyber Operations in time of war and on the assessment of their effects, we now present our understanding on their effects. An effect is considered to be "a change in the state of a system (or system element), that results from one or more actions, or other causes" (NATO, 2013). As argued by (U.S. DoD, 2019), an effect can also be the result, outcome, or consequence of another effect. In the context of Cyber Operations, their effects are produced as the results of the action(s) of cyber weapon/capabilities. In this context two main criteria can be used to classify the effects of Cyber Operations (Maathuis et al., 2016; Maathuis et. al., 2018): intention and nature. For the intention criterion, the effects are classified as intended and unintended effects, and for the nature criterion the effects are classified as military and civilian. For scoping this research, the effects of Cyber Operations are addressed through technical and military lenses since this research is conducted using technical and military knowledge. Other types of effects such as political and economic are outside the scope of this research. The classes of effects of Cyber Operations are further elaborated in the next section as well as in Chapters 4 and 5 in the context of targeting in Cyber Operations.

1.2.2. Targeting in Military Operations

In this section, to discuss the military context of our research, we address targeting in military operations and the military targeting process. Furthermore, we briefly discuss the military legal principles relevant in a war context and the ones relevant in this research in particular. Next, we define the perspectives or contexts of use as well as our definitions for the effects of Cyber Operations considered in this research.

Military Operations

The complexity of wars has grown in the last centuries (Oliveira, 2010), and is directly reflected in the instantiations of the classical military

OODA (Observe, Orient, Decide, Act). The loop starts from the wars of the 17th century, going to WWII, and into incipient and future wars. Firstly, the Observe concept moved from telescope (wars of the 17th century), to radio and radar (WWII), and is going to network (future wars). Secondly, the Orient concept moved from weeks (wars of the 17th century), to hours (WWII), and is going to be continuous (future wars). Thirdly, the Decide concept changed from months (wars of the 17th century), to days (WWII), and is going to be immediate (future war). Fourthly, the Act concept transformed from according to the season (wars of the 17th century), to weeks (WWII), and is going to be done in minutes (future wars) (Lehto, 2016). These recollections and prognostics are done based on known data from historical events and anticipations for future ones, respectively. However, what is considered to be a reflection of future wars in the abovementioned illustration has already begun because new, fast, precise, and more intelligent and adaptive means and methods of warfare are continuously being designed, developed, and used by different entities (e.g. state or non-state actors). As (Gray, 2007) argues, this is possible since "war is waged with the products of technology" and technological advancements play a significant role in the way how military operations are planned, executed, and assessed.

In the view of Clausewitz, "war is the continuation of politics by other means" (Clausewitz & Maude, 1982). In other words, war stars with political goals that translate to military aims that need to be achieved by defining and shaping the scope, participants, conditions, intensity, duration, limits, restrictions, and choices that need to be established and done while conducting wars/military operations (HQ Department of the Army, 1991; Department of the Army, 1978). Clausewitz sees war as "nothing but a duel on an extensive scale….War therefore is an act of violence intended to compel our opponent to fulfil our will…the compulsory submission of the enemy to our will is the ultimate object….Two motives lead men to war: instinctive hostility and hostile intention" (Clausewitz & Maude, 1982). Furthermore, "the necessity of fighting very soon led men to special inventions to turn the advantage in it in their own favour: in consequence of these the mode of fighting has undergone great alterations; but in whatever way it is conducted its conception remains unaltered and fighting is that which constitutes war" (Clausewitz & Maude, 1982). In order to fight, actors (nation states) rely on their instruments of power such as diplomatic, information, military, and economic (Hillson, 2009). Nevertheless, this research focuses only on the information and military instruments of power (i.e. means and capacity available to governments to achieve own objectives) (Worley, 2012). That is because we are focusing on the military cyber domain and cyberspace itself is considered to be a part of the

information domain. From there, we concentrate on Cyber Operations as military operations conducted by military actors to achieve their aims.

Military targeting

To fight against different opponent actors and achieve goals, military operations are conducted in order to influence their target(s) in several ways (e.g. alter the behaviour of a target audience, disrupt communications processes, damage a system). The core of this phenomenon and process is represented by what is called military targeting. (NATO, 2016; U.S. Army, 2013) define military targeting as the process of selecting and prioritizing targets and matching the appropriate response to them while considering operational requirements and capabilities. The characteristics or principles of targeting are as follows (NATO, 2016):

- Objective based: achieving objectives in efficient and effective ways.
- Effects driven: creating physical and psychological effects that contribute to achieving objectives.
- Multidisciplinary: requiring coordinated and integrated efforts from multiple disciplines and capabilities.
- Timeliness: time is important and often targeting is time critical which implies the need for a fast information flow from source to destination.
- Centrally controlled and coordinated: maintaining a system of centralized and coordinated control.
- Information: accessibility and security: the necessary information such as target intelligence and collateral damage estimation needs to be properly stored, available, and accessible in different moments.

Furthermore, two main types or methods of targeting exist (NATO, 2016; U.S. Army, 2013):

- Deliberate targeting implies engaging planned targets using different lethal or non-lethal actions scheduled against them.
- Dynamic targeting denotes engaging unexpected or planned targets which were not included in sufficient time in the deliberate targeting process or need to go through target development, validation, and prioritization, respectively.

As this research aims at assessing the effects of Cyber Operations is relevant in both deliberate targeting when sufficient time is taken to go through the whole process as well as in dynamic targeting when on-call resources are used in less time.

Targeting is considered to link strategic-level direction and guidance to tactical-level activities through an operational-level targeting cycle in order to create effects that support the achievement of military objectives and end state of the mission. (Boothby, 2012) sees targeting as "the *sine qua non* of warfare". The targeting cycle contains six phases as depicted in Figure 1.1. In this figure, two blocks have been marked using rectangles. The first one is 'Preparations to decide' which depicts preparations made for choosing the possible target to engage followed by the weapon which could be deployed to engage the target. The second one is 'Decide and execute' which depicts Commander's decision making and moment of execution once the target and weapon are properly chosen. These phases have been marked in this figure as they represent the place where this research is mainly positioned. These phases contain several processes and actions, and further are briefly described (NATO, 2016; Boothby, 2012; Melzer, 2008; Ducheine & Gill, 2018; NATO, 2013; ICRC, 2013):

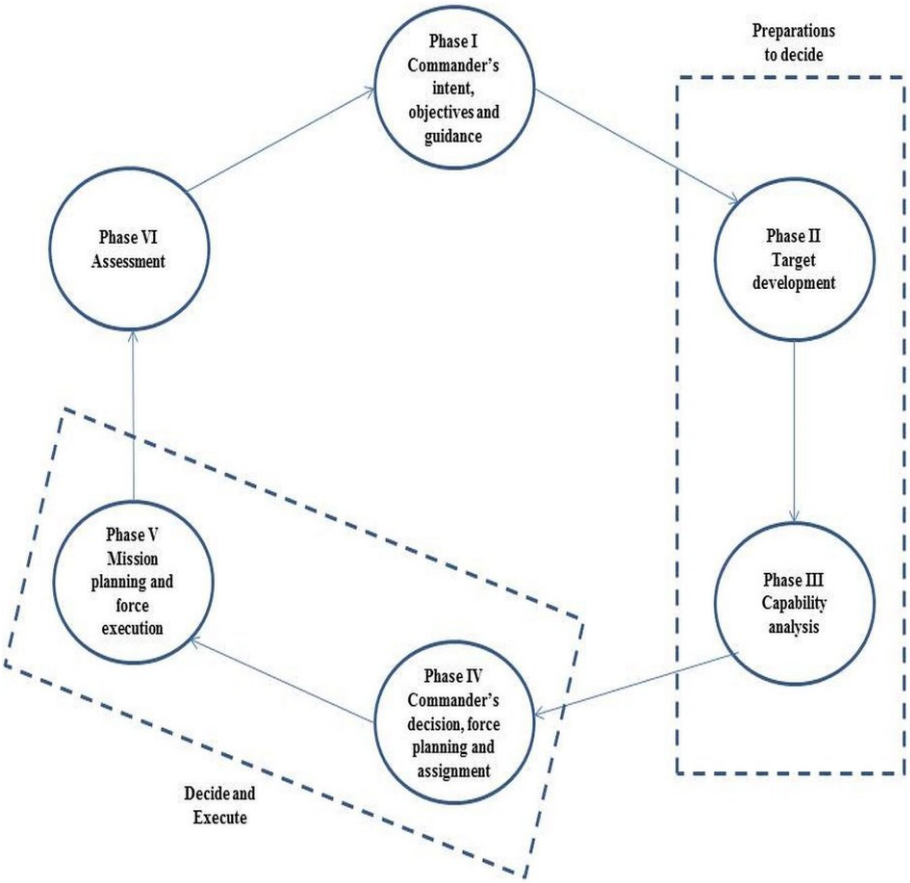


Figure 1.1. Targeting cycle (as in NATO, 2016)

- Phase I (Commander's intent, objectives, and guidance/Effects and guidance): political and strategic direction and guidance is provided to identify clear and well-defined objectives as well as under what circumstances, actions, and parameters these objectives can be achieved. Moreover, operational tasks are defined and targets of whom engagement would support the accomplishment of objectives are nominated together with probable Courses of Actions (CoAs) that could be considered.
- Phase II (Target development/Target selection): eligible targets are identified in order to impact them and achieve the objectives. These targets have to be military objectives (i.e. military targets) in the legal sense which implies that the "attacks shall be limited strictly to military objectives" (AP I Art.57(2), 1977; AP I Art.52(2), 1977). Furthermore, the identified targets are analysed, vetted, validated, and prioritized producing a prioritized target list that integrates the estimation of collateral damage-Collateral Damage Estimation (CDE). CDE is a methodology that begins in Phase II and is relevant and continued in Phase III and V, which provides an estimation of collateral damage, thus not a certainty.
- Phase III (Capabilities analysis/Weapons taxation): the targets included in the developed prioritized list, are further analysed and matched with appropriate lethal and non-lethal capabilities in order to generate intended effects and achieve the objectives defined while minimizing collateral damage. (AP I Art.57, 1977) imposes questioning if engaging a particular military target with a specific weapon produces collateral damage (in the sense of being foreseeable and expected). Moreover, the proportionality assessment is conducted by the Commander in order to analyse if collateral damage (based on CDE) "is excessive in relation to the concrete and direct military advantage anticipated" (AP I Art.57, 1977). Hence, if capabilities produce or targets of whose engagement produce disproportionate collateral damage, then they should not be used or engaged, instead other options should be considered or the attack should be "cancelled or suspended" (AP I Art.57(2), 1977). Otherwise, when capabilities do not produce or targets of whose engagement does not produce disproportionate collateral damage, then the military targets can be further prepared for engagement in the next phase.

  For engaging targets in military operations and reach their aims, more weaponry options in the CoA Development process according to Phase I. This process signifies developing, analysing, and comparing different paths to mission achievement by incorporating and weighting both the expected intended and unintended effects.

- Phase IV (Commander's decision, force planning and assignment/Weapons allocation): the results obtained in the previous phase are assigned for further planning and execution while taking into consideration any relevant constraints and restraints.
- Phase V (Mission planning and force execution/Execution): the mission is further planned at tactical level and prepared for execution while a final target positive identification (PID) based on AP I Art.57(2)) is conducted together with other information checks and collateral damage avoidance or minimization, as precautionary measures. Moreover, force execution consists of six (Find, Fix, Track, Target, Engage, Exploit, with Assess done in Phase VI). Here, two situations are possible: the first one, when the military target can be engaged, and the second one, when the military target cannot be engaged due to last-minute findings (e.g. it is not a military target anymore or it produces disproportionate collateral damage).
- Phase VI (Assessment/Evaluation): the effects produced are evaluated together with the achievement of objectives based on collected information. This also supports a possible re-engagement decision which could imply using a completely different engagement capability. Additionally, this also further contributes to wider assessments, lessons learned, or input for other missions.

Main Military Targeting Perspectives or Contexts of Use

From the description provided above for the targeting cycle, two major perspectives/contexts of use (NATO, 2013; ICRC, 2013) are of particular relevance in this research. These perspectives/contexts of use are the following ones:

- The first perspective is of *military-legal nature (*phases III-V) and is based on the interpretation of the proportionality assessment (as already introduced and further elaborated in this section). This perspective brings together two elements (categories of effects): Collateral Damage and Military Advantage, as later defined in this section.
- The second perspective is of *military-operational nature (*phases I, III-V) and is based on considering further preparations for supporting developing different CoAs for engaging military targets. This perspective brings together a broader perspective by embedding both intended and unintended effects under three categories of effects named: Collateral Damage, Military

Advantage, and Military Disadvantage, as later defined in this section.

The Laws of Armed Conflict

The scientific and practitioner communities consider that targeting must be conducted and targeting decisions must be taken in accordance with the correspondent legal framework applicable in the specific warfare context at stake: the laws of war (NATO, 2016; U.S. Army, 2013; Joint Targeting School, 2014; ICRC, 2004) which as (Malcolm, 2008) argues were "originally termed the laws of war and then the laws of armed conflict [LOAC]. More recently, it has been called international humanitarian law [IHL]". This shift of terms was done "in order to reflect the growing influence of the humanitarian aims of the law" (Hernandez, 2019). Luban (2013) argues that "military lawyers refer to the laws of war as 'LOAC' – Laws of Armed Conflict – while civilians from the world of non-governmental organizations call the laws 'IHL' – International Humanitarian Law". For the purpose of this dissertation, we will adopt the military perspective: LOAC. These laws are part of the international law (ICRC, 2004) and find their roots in the "pioneering work of Henry Dunant" from 1864 (Malcolm, 2008) who was horrified by the Battle of Solferino. This battle was a conflict between the French and Austrian forces that took place in 1859 in the north of Italy (Malcolm, 2008; Bauvier, 2012). Since then, these laws continue to develop (Boothby, 2012) based on lessons learned from different wars and new technologies that were developed, integrated, and used in different military operations.

More concretely, the following two guidelines should be considered based on the experiences gathered from a long human history of war and legal dimensions further elaborated in this section. First, that "the right of belligerents to adopt means of injuring the enemy is not unlimited" (Boothby, 2012), which means that actors should not fight to achieve their goals without a legal limit. Second, that "the progress of civilization should have the effect of alleviating as much as possible the calamities of war" (ICRC, 1868), which signifies that the more we advance as humankind we should try to minimize the unintended or negative impact of war by all means. The abovementioned guidelines reflect restrictions and limits further contained in the principles of the laws of war (also referred as principles of targeting law by Boothby (2012)) below resumed. These principles are embedded in the Rules of Engagement (RoE), and these rules are defined for each military operation (NATO, 2016; U.S. Army, 2013). The RoE are directives defined by competent military authority in order to establish the circumstances and limitations under which military forces "initiate or continue combat engagement with other forces encountered" (U.S. DoD,

2019). Aligned with this, in (CLAMO, 2000; Hosang, 2016), the RoE are depicted as the intersection of legal, policy, and military operational aspects involved in the conduct of military operations, as illustrated in Figure 1.2. Moreover, RoE have to be effective and need to be respected during the whole process in order to assure the accomplishment of military operations (CLAMO, 2000).

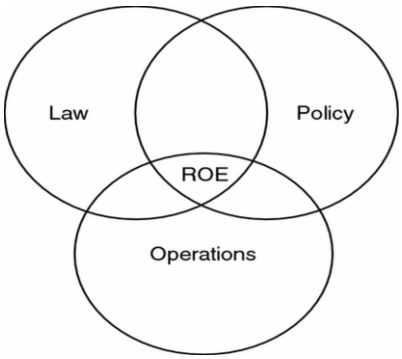


Figure 1.2. Rules of Engagement (as in Hosang, 2016)

A common understanding-through education, exercise, and practice-should exist among the armed forces in regard to which tasks should be performed based on which laws of war (U.S. Army, 2013). Accordingly, we further address the principles of the laws of war (AP I Art.52(2), 1977; AP I Art.51(5)(b), 1977; Downey, 1953; Malcolm, 2008; Hayashi, 2010; Whittemore, 2010; Dill, 2010; Noll, 2012; U.S. Army, 2016; Boothby, 2012; Dinstein, 2016; Gill & Fleck, 2011; U.K. MOD, 2010; Schmitt, 2011; Gillard, 2018; Hernandez, 2019):

- Military necessity: actors are justified to use efficiently and quickly all means and methods to attain military advantage in front of the enemy and achieve their aims. However, this should not result in a diversion from the LOAC or should not be in contradiction with other aspects or principles of the LOAC. In order words, "military necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of war, and which are lawful according to the modern law and usages of war" (Downey, 1953). Aligned with this, Whittemore (2015) considers that "if an action is not necessary under this definition, then it should not be conducted". This makes the difference between competent war-making versus incompetent war-making, in the eyes of Hayashi (2010).
- Humanity: actions that produce unnecessary suffering, injury or destruction are forbidden and should be avoided. Boothby (2012)

argues that the principle of military necessity is linked with the one of humanity, Schmitt (2011) considers that the principle of military necessity "exists in equipoise with the principle of humanity", and Boothby (2012) scrutinizes that the principle of humanity represents the basis "for the requirement of proportionality". Moreover, (Fast, 2015) goes further considering that "humanity as a principle must also be defined legally and morally by what it is not: inhuman treatment, the denial of human rights or the degradation of the person, all of which imply the absence of respect and dignity."

Distinction: Boothby (2012) considers that the roots of the LOAC are in the principle of distinction which implies "that a distinction must be made between those who may be lawfully attacked and those who must be respected and protected". This means, that the participating actors need to make a distinction between military targets (combatants and military objects), and civilians (non-combatants) and civilian objects. In practice, this depends "on the quality of the information available to the military Commander when he/she makes the decision. So he/she should make reasonable efforts to gather intelligence, review the available intelligence, and conclude in good faith that he/she is attacking a legitimate military target" (UK MOD, 2010). In this way, force should be directed only against military targets and all feasible precautions need to be taken when choosing means and methods to engage the military targets, while avoiding collateral damage on civilians and civilian objects. In regard to military targets, the "attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" (AP I Art.52(2), 1977). This principle is divided into multiple parts and requires multiple decisions from the Commander, as follows (Whittemore, 2015): i) deciding if the intended target is a human or an object, ii) taking into consideration different criteria, deciding if the human or object is a lawful target that contributes to the achievement of military aims. In this way, the author illustrates in (Whittemore, 2015) the basic decision matrix for the principle of distinction, as depicted in Figure 1.3. In this dissertation the military term 'military target' is used as the military equivalent to the military-legal term 'military objective'. This is done in order to prevent confusion with the military objective that means the objective, goal, or aim in an operation.

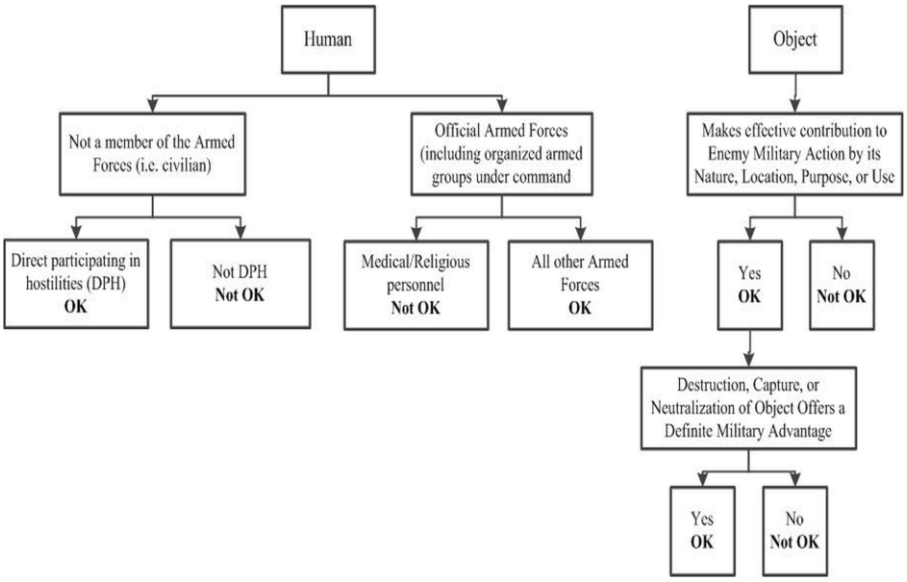


Figure 1.3. Principle of Distiction (as in Whittemore, 2015)

- Proportionality: an attack that can "cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" is disproportional, thus forbidden (AP I Art.51(5)(b), 1977). (Cannizzaro, 2006) scrutinizes that "proportionality is not a rule of conduct but a rule which requires a balancing of antagonistic values, such as the interest of the belligerent in carrying out a military action on the one hand, and the interest of civilians who, although extraneous in the conduct of hostilities, might be victimized by that action". At the same time, proportionality assessment is "done on a target-by-target basis" by Commanders "at the time the target is vetted/approved during the target development process and just prior to the planned attack on the target" (U.S. Army, 2003) based on "timely, accurate, and reliable information" available at that time (U.S. Army, 2013). Commanders are the responsible authority and decision makers (NATO, 2016; Jachec-Neale, 2014) having the ability "to see in real time the position and status of his assets-as well as his enemy's-and the ability of a war fighter to know with assurance what's around the next corner or behind the next mountain is simply invaluable".

  The two components participating in assessing proportionality are Collateral Damage and Military Advantage. For both terms, the working definitions in this research are provided below. While the

Collateral Damage component is provided by an existing methodology (referred as one of the following: CDM-Collateral Damage Methodology/CDE-Collateral Damage Estimation/CDEM-Collateral Damage Estimation Methodology) done by the military intelligence (NATO, 2011; NATO, 2016; U.S. Army, 2012; U.S. Army, 2013; U.S. Army, 2015), the Military Advantage component does not rely on a specific methodology and is conducted by the Commander who takes into consideration the information available at the time together with the anticipation of intended effects that contribute to the achievement of military goals. Moreover, the components of the principle of proportionality are considered by (Oxford Institute for Ethics, Law, and Armed Conflict, 2009) as Military Advantage being the positive part and Collateral Damage being the negative part in this assessment. At the same time, (Oxford Institute for Ethics, Law, and Armed Conflict, 2009) argues that the application of this principle "involves the accommodation of two potentially contradictory aims: the protection of civilian life [Collateral Damage] and obtaining a concrete military advantage [Military Advantage]". Thus, the principle of proportionality seeks to reflect the balance (Gillard, 2018) between its two antagonist components trying to not allow that the expected Collateral Damage is excessive (i.e. disproportional) in relation to the anticipated Military Advantage.

For defining the scope of our research in terms of relevant military targeting principles, we consider two principles of the laws of war, namely, the principle of distinction and the principle of proportionality. Additionally, to narrow down even more the scope of our research, we are not analysing RoE as they require a different type of research that implies focusing on military, legal, and political dimensions, and they are defined in the field for each military operation. These choices are based on the following considerations:

- The main classification criteria considered for the effects of Cyber Operations are their intention and nature. That means that the effects were first of all classified as intentional and unintentional considering the intention criterion, and were classified as military and civilian considering the nature criterion. This classification, and implicitly, separation, relates to the principle of distinction in the sense of making a clear difference or separation between what could be considered a military target which means possibly targetable versus what could be considered a civilian or civilian asset which means un-targetable. As Noll (2012) scrutinizes, the separated parts (military part and civilian part) from the principle of distinction are

jointed or brought together through the principle of proportionality as the results of military action (engagement of military targets). It is then the principle of proportionality the one that tries to make sure that the damage produced on the civilian side by the military action (e.g. Collateral Damage) is proportional to the expected military advantage of the military action (Dill, 2010) on the military side.

- Since the principle of military necessity implies "that the armed forces can do whatever is necessary-provided always that it is not otherwise unlawful under humanitarian law-to achieve their legitimate military objectives in warfare" (Turns, 2012), the discussion regarding investigating if an actor or object is a military target (i.e. legitimate military objective) and the question if LOAC is applicable are outside the scope of this research since we only address military Cyber Operations conducted in the context of war and we only consider the actors or objects attacked in the military Cyber Operations scenarios used as being military targets.
- Since we do not focus on what will be the right military action to be taken and which would be the proper cyber weapon to be used to avoid or forbid unnecessary suffering, injury, or destruction, the principle of humanity is not further directly addressed in this research. In this research we position ourselves in the moment when specific military action could to be taken with a specific cyber weapon that was chosen to be used on a specific military target.

By combining the two major military perspectives or contexts of use (military-legal and military-operational) described above with the relevant principles of the laws of war, we can define the effects for each context of use and depict the relation between them in Figure 1.4 below.

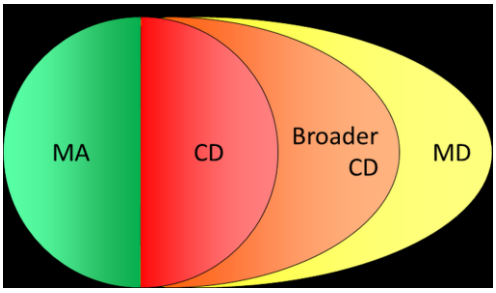


Figure 1.4. Effects of Cyber Operations and military perspectives in this research

The difference between the chosen military perspectives can be expressed from how the investigated effects are defined:

- For the military-legal perspective:

    - Collateral Damage (CD in Figure 1.4.) is defined as unintended effects that do not contribute to the achievement of military objectives in Cyber Operations, but impact civilian assets in the form of civilian (i.e. physical) injury or loss of life and/or damage or destruction to civilian objects and/or environment.
    - Military Advantage (MA in Figure 1.4.) is defined as intended effects that contribute to the achievement of military objectives in Cyber Operations.

- For the military-operational perspective which includes the legal perspective, but has some additional points which have been captured from the interviews and Focus Groups conducted in this research:

    - Collateral Damage (broader CD in Figure 1.4.) is defined as unintended effects that do not contribute to the achievement of military objectives in Cyber Operations, but impact civilian assets in the form of civilian (i.e. physical and psychological/mental) injury or loss of life and/or damage or destruction to civilian objects and/or environment.
    - Military Advantage (MA in Figure 1.4.) is defined as intended effects that contribute to the achievement of military objectives in Cyber Operations.
    - Military Disadvantage (MD in Figure 1.4.) is defined as unintended effects that do not contribute to achieving military objectives in Cyber Operations, but impact allies, friendly, neutral, even the target or conducting actors.

In Section 1.3.2. it is explained how both perspectives are considered in relation to and embedded in the artefacts proposed in this research, and in Section 7.1. it is explained how both perspectives can be further of use.

To summarize the present section (1.2.), we can say having brought together the two main dimensions of the research background of this research: i) the cyber security dimension in Section 1.2.1. where we have discussed the structure of cyberspace as well as the cyber activities i.e. Cyber Operations together with their effects, and ii) the military targeting dimension in Section 1.2.2 where we have discussed the military targeting process, the principles of the laws of war and reflected in the ones most relevant in this research, and defined the two perspectives of use considered

in this research: military operational and military legal. In this way we can say that we have established the cyber military background of this research to enable us to further model the effects of Cyber Operations in the described war context based on which further support can be provided to targeting decisions.

1.3. Research Aim, Research Questions, and Modelling Framework

Having described the background and motivation of our research, we now present the precise aim (Section 1.3.1.) as well as the main research question together with its (Section 1.3.2.).

1.3.1. Research Objective

The previous sections of this chapter settled the ground through its cyber security dimensions in Section 1.2.1. and military dimensions and the two perspectives or contexts of use in Section 1.2.2., as well as the motivation of this dissertation. Thus, the research objective of this dissertation is built and is defined as follows:

To design a series of models, methodologies, and frameworks that assess the effects of Cyber Operations in order to support military targeting decisions in Cyber Warfare.

To be able to achieve this objective, a multidisciplinary research in the fields of Cyber Security, Artificial Intelligence, and Military Operations is conducted from a technical-military perspective. To be able to build the artefacts 1, 3 and 5 needed to provide the information for supporting military targeting decisions (to be discussed in further detail below), research is conducted in the field of AI as it contains techniques to build intelligent systems for problem solving and decision making.

From the field of Cyber Security methods from incident analysis, vulnerability and impact assessment are used; from the field of Artificial Intelligence techniques from the sub-fields Knowledge Representation & Reasoning, and Fuzzy Logic are used; and from the field of Military Operations theory and doctrine regarding targeting, and military law are used.

The research objective of this research cannot be achieved in one single step due to its complexity and multidisciplinary nature. In order to be

able to tackle it properly and achieve it, a logical decomposition in five sub-objective is executed.

As such, the stated research objective is decomposed into five sub-objectives each with a corresponding research sub-question, all embedded in a conceptualization framework that will be introduced later in this section. The logic behind the decision to split into five sub-questions relies on the fact that in order to understand the phenomenon itself (Cyber Operations) and assess its effects, one needs first to comprehend it as a whole together with its means (cyber weapons) to produce effects. After doing that, it is possible to investigate what are the effects and on what are they impacting or applied to, and by that further assessing them in order to support targeting decisions in Cyber Warfare. Moreover, each research question was answered sequentially in a separate chapter (II to VI) and implied the design of an artefact using the Design Science Research approach (Hevner & Chatterjee, 2010; Peffers et al., 2008) as this research methodology allows designing artefacts with societal relevance. In this way, the following sub-section introduces each research sub-question together with its correspondent artefact.

1.3.2. Research Questions

The main research question is formulated as follows:

How to assess the effects of Cyber Operations in order to support military targeting decisions in Cyber Warfare?

The main research question has been decomposed into the following sub-research questions shown in Figure 1.5.:

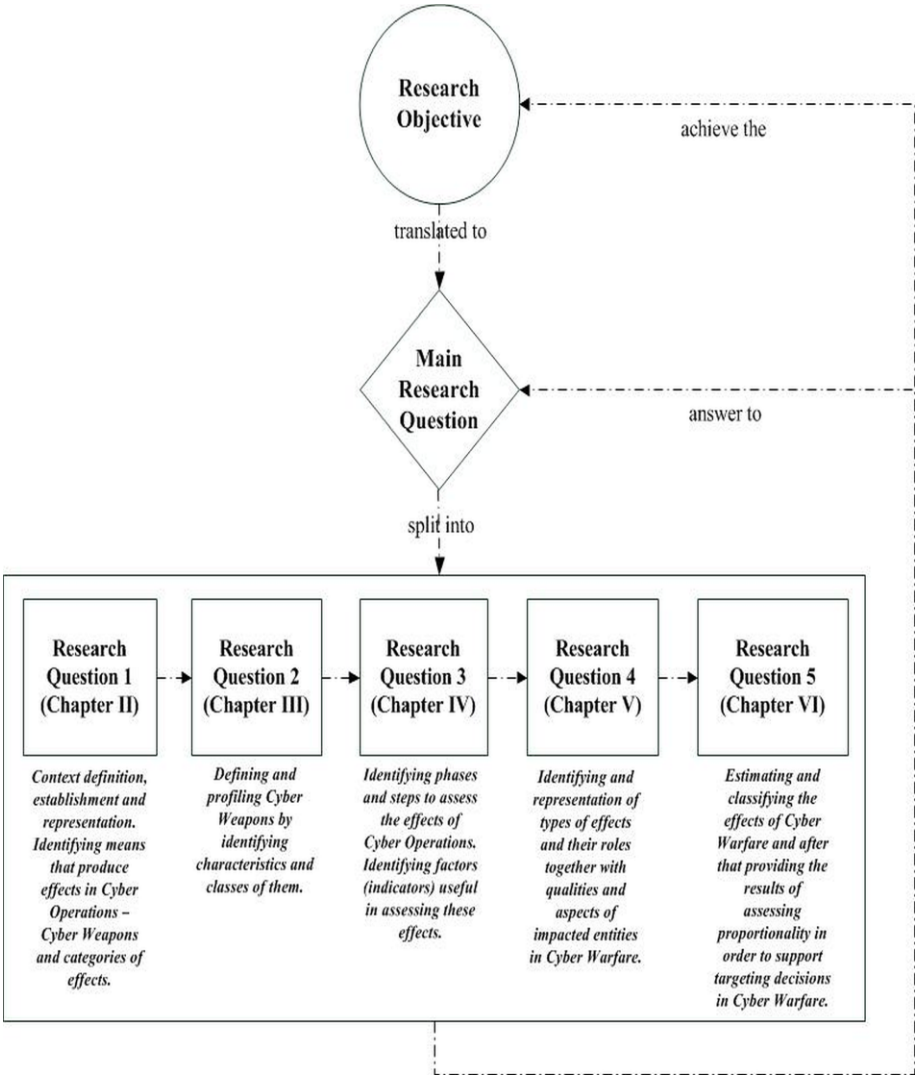


Figure 1.5. Relation between Research Objective, Main Research Question, Research Questions together with artefacts' description, and Dissertation Chapters

Research Question 1: How to represent the entities involved in Cyber Operations?

The first research question aims at establishing the context of the research by providing understanding for the concept of Cyber Operations as well as its component entities (e.g. actor, target, cyber weapon), and a way of modelling them based on technical-military knowledge and expertise. The resulting knowledge/data model is a computational ontology in the form

of a knowledge graph/base of Cyber Operations which has been exemplified on Cyber Operations case studies conducted on incidents from Georgia during the Russian-Georgian war (in 2008), Stuxnet/Operation Olympic Games (discovered in Iran in 2010), and Black Energy 3 (in Ukraine in 2015). For both considered perspectives (military-legal and military-operational as introduced in Section 1.2.2.), the proposed model is applicable in the same way. That is possible since this model provides an modelling approach to Cyber Operations and their entities which could be further defined as one intends in both perspectives/contexts of use.

Research Question 2: What should a profiling framework for Cyber Weapons look like?

The second research question provides understanding of the concept of cyber weapons by advancing their definition, structure, and life cycle. Based on these, a profiling framework is proposed as a way to reflect main characteristics and classification criteria of cyber weapons.

As this research is positioned in the context of war, additional control measures have to be considered from the *design* phase of a cyber weapon (third phase in the cyber weapon's life cycle) considering ways to avoid, limit, or control collateral damage that could possibly impact other collateral assets outside the intended target. These measures are related to the accuracy of the intelligence information provided about the target which has to be properly integrated in the *development* phase of a cyber weapon (fourth phase in the cyber weapon's life cycle) through target's specificity at all functional levels: network and communication, hardware, software, and data. Such measures have to be further tested through different checks based on specific test cases in the *testing* phase of a cyber weapon (fifth phase in the cyber weapon's life cycle) and validated in the validation phase of a cyber weapon (sixth phase in the cyber weapon's life cycle) if its designers and corresponding decision makers want to avoid or minimize collateral damage in the field when it is deployed on its target. The introduced profiling framework has been exemplified on Cyber Operations case studies such as Operation Orchard, Stuxnet, and Black Energy 3. For both considered perspectives (military-legal and military-operational as introduced in Section 1.2.2.), the proposed framework is applicable in the same way as the main focus of this framework is to identify features of cyber weapons that could be further of use when assessing their effects in Cyber Operations.

Research Question 3: What methodology is adequate to assess the effects of Cyber Operations?

The third research question advances an assessment methodology for the intended and unintended effects of Cyber Operations (i.e. Military Advantage, Collateral Damage, and Military Disadvantage) in order to support targeting decisions in Cyber Warfare. Hence, the introduced assessment methodology considers multidimensional factors, phases, and steps, and was evaluated in a focus group on a virtual, but realistic Cyber Operation case study conducted on Ballistic Missile Defense Systems. For the military-operational perspective or context of use (as introduced in Section 1.2.2. and depicted in Figure 1.4.), the proposed methodology could be of use as it is, and for the military-legal perspective or context of use (as introduced in Section 1.2.2. and depicted in Figure 1.4.), the proposed methodology could be of use as it is by ignoring the Military Disadvantage assessment component.

Research Question 4: How to assess the effects of Cyber Operations?

The fourth research question introduces a knowledge-based model to assess the effects of Cyber Operations which represents and reasons about types and classes of effects, as well as human and non-human aspects and qualities impacted by these effects. The introduced model was exemplified on Cyber Operations case studies conducted on the incidents in Georgia, and Black Energy and NotPetya from 2017 in Ukraine. For both considered military targeting perspectives (military-legal and military-operational as described in Section 1.2.2. and depicted in Figure 1.4), the proposed model is applicable in the same way since both perspectives are embedded.

Research Question 5: How to estimate the effects of Cyber Operations in order to support targeting decisions in Cyber Warfare?

The fifth research question, designs, develops, and proposes a multi-layered model that i) estimates and classifies the effects of Cyber Operations, and ii) advises targeting decisions concerning the proportionality assessment/test in Cyber Warfare. The advanced model was evaluated on two virtual, but realistic Cyber Operations case studies on a suicide drone and a cargo ship. For both considered military targeting perspectives (military-legal and military-operational as described in Section 1.2.2. and depicted in Figure 1.4), the proposed model is applicable, and implies that the further researcher/user is able to select what kind of effects and decisions wants to assess by considering less effects and variables for the military-legal perspective or by directly considering the model as it is for the military-operational perspective. More explanations are provided in Chapters 6 and 7 of this dissertation.

Now going back to the roots of this research: cyberspace is difficult to be grasped intuitively (Bryant, 2011) since it cannot be always directly experienced through human senses. However, human factors and aspects are the ones that surround all the decisions taken in Cyber Operations, since no matter the nature of war, war is a "nasty, violent, [and] brutal affair" (Boothby, 2012).

In (Boothby, 2012), the author argues that there is a broad spectrum of conflict (e.g.. armed or unarmed, criminal acts of violence) with different intensities carried out by different types of actors at international or national level. Considering these findings, these conflicts actually call for applying different specific laws. This research refers to Cyber Operations as independent or with a supportive role to other military operations when the military have an approved mandate to conduct operations in time of war where the laws of targeting apply (jus in bello) (ICRC, 2015; Tallinn Manual Rule 20, 2013).

As already mentioned, we introduce a conceptual modelling framework for targeting decisions in Cyber Warfare where we capture the main components of this research based on i) the research background presented in Section 1.2.1. and 1.2.2., and ii) the design and empirical research that we have conducted. We discuss its components in order to comprehend and reflect how targeting decisions with regard to assessing the effects of Cyber Operations and proportionality assessment in Cyber Operations are made.

Before introducing the modelling framework and artefacts proposed, a series of requirements/prerequisites were given at the beginning of this research for scoping the purpose of this research:

- The context of this research is war, and more specific Cyber Warfare, thus remaining in the arena of targeting in military Cyber Operations.

- The real incidents (Cyber Operation based on real historical data(sets)) or the ones designed (Cyber Operations based on synthetic data(sets)) are in a war context or in a hidden conflict context as considered by the scientific and practitioner communities (e.g. Stuxnet).

- The means used in these Cyber Operations are cyber weapons, and their effects were assessed (analysed and estimated) to support

targeting decisions concerning proportionality assessment in Cyber Operations.

- The limited number of data(sets) of real Cyber Operations data(sets) publicly available led to the following two measures:

    - Firstly, designing and constructing synthetic/virtual, but realistic Cyber Operations by consulting technical-military experts recommended by research partners in regards to evaluating their design, realism, and applicability in Cyber Operations. The real Cyber Operations used are presented in Chapters 2, 3, 5, and 6, and the virtual/synthetic Cyber Operations are presented in Chapter 4 and 6.
    - Secondly, using an approach that uses data gathered from merging case studies on (real and synthetic) Cyber Operations combined with interviews and Focus Groups with experts that were suggested to the researcher, and are presented in Chapters 3-6.

As we previously discussed in this chapter, a series of aspects and factors (e.g. human) contribute and influence military Commanders when they have to decide if engaging a specific target with a specific cyber weapon/capability/means is not-disproportional or disproportional. These military operational, social, and legal aspects and factors are depicted in the further introduced modelling framework depicted in Figure 1.6. and structured on four blocks.

Block 1.

Cyber Operations are more and more recognized as feasible options and sometimes preferred to achieving political and/or military goals (U. S. Army, 2018). Additionally, taking into consideration the context or background where a Cyber Operation needs to be planned and executed, once an "entity" (U.S. Army, 2013) which can be an "area, structure, object, person or group of people" (NATO, 2016)-has been considered legally targetable (principle of distinction), further considerations regarding the possibility of achieving intended/desired effects (Military Advantage) that would contribute to the achievement of military objectives as well as the possibility of impacting collateral actors and/or systems (Collateral Damage) have to be made, fact depicted in Block 2. Examples of possible military targets are C4I systems, military and criminal forces, adversary leadership (including political), weapons of mass destruction assets or critical infrastructure (NATO 2016, Theohary & Harrington, 2015).

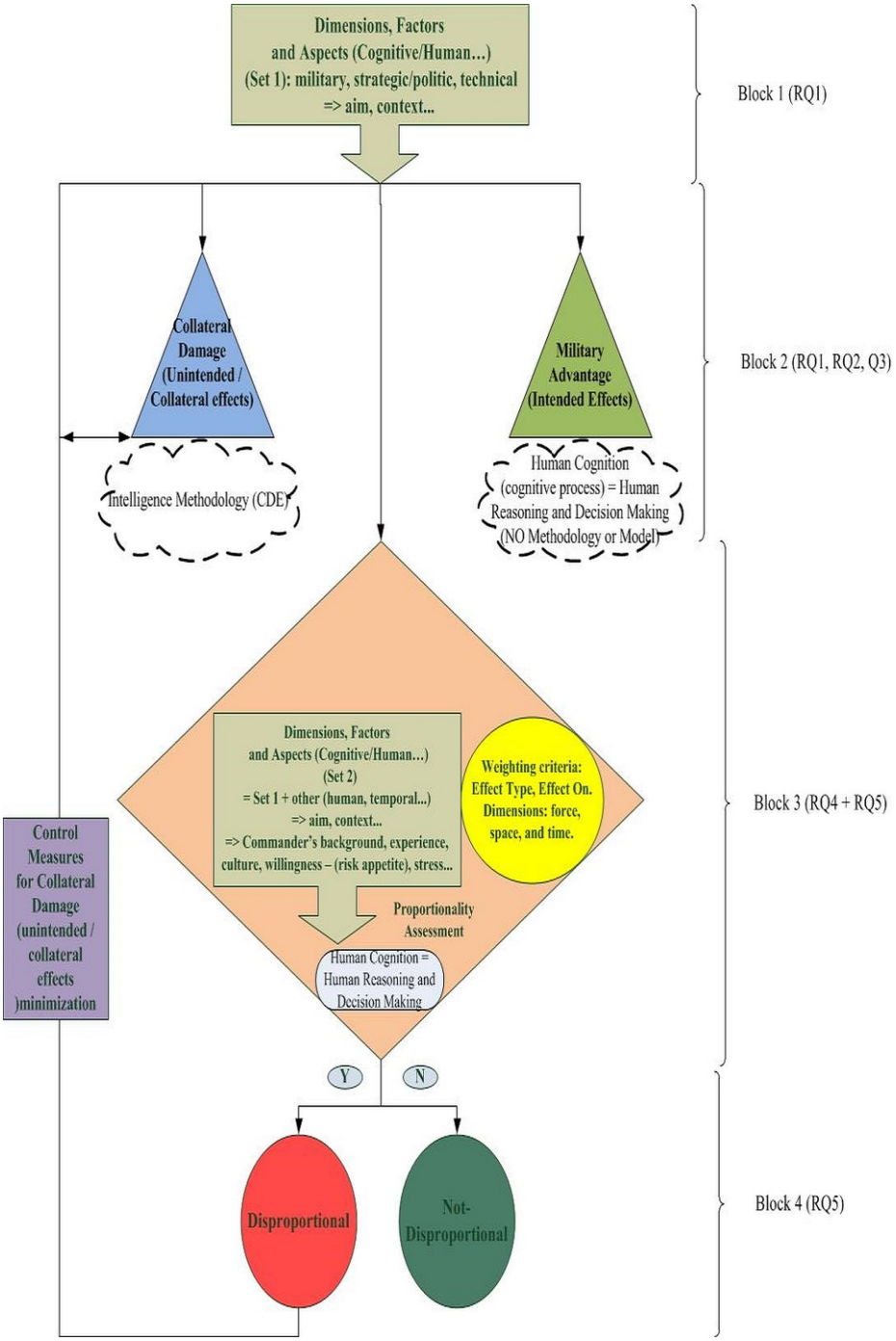


Figure 1.6. Targeting Decisions Modelling Framework in Cyber Warfare/Operations and corresponding research sub-questions

Block 2.

The modelling framework intends to conceptualize the aspects and factors contributing to targeting decisions based on proportionality assessment in Cyber Operations, and considers Cyber Operations as (part of) Military Operations (Maathuis et al., 2018). From the field work conducted (e.g. interviews and Workshops with military experts as well as direct participation and observation in joint military exercises) along with the consulted scientific literature, we conclude that an appropriate methodology or model that assesses proportionality in Military Operations or both of its components separate (Collateral Damage and Military Advantage as addressed in Section 1.2.2.) is missing with the exception of Collateral Damage (i.e. CDE). Hence, CDE is a methodology executed by military intelligence (U.S. Army, 2018) and is opposed to Military Advantage which is not based on a methodology or model, but is mainly a cognitive process based on Human Reasoning and decision making, or as one of the military experts consulted pointed, is based on "the feeling of knowing the opponent" at the given time with the given information.

In addition, control measures for avoiding or limiting Collateral Damage should be considered from the first moment that it is expected. In addition, the interviewed military Commanders have a different perspective in regards to the meaning of Collateral Damage and proportionality: they see these terms broader than the military legal perspective. In this sense, while the legal perspective interprets Collateral Damage (and implicitly, proportionality) as damage or destruction applied to civilian objects and/or injury or loss of life to civilians, military Commanders extend this notion by embedding the unintended effects that impact military actors and systems (e.g. own military forces and systems or the target itself); these effects are termed in this research Military Disadvantage (as defined in Sections 1.2.2.). This could be explained as a normal phenomenon based on the difference of perspective between different experts from different fields or different experts from the same field. To cope with this difference in perspective we have considered in this research both legal and operational perspectives, and to be able to cope with the legal requirements we have considered for assessing the principle of proportionality (artefact five) only Collateral Damage. Additionally, control measures for avoiding and/or minimizing Collateral Damage should be considered in two moments before target's engagement in a Cyber Operation: i) when Collateral Damage is expected, and ii) when it is expected to be disproportional to engage a target in a Cyber Operation (Collateral Damage is excessive).

Block 3.

Moving to the proportionality assessment (military-legal perspective) signifies not only bringing two different entities surrounded by uncertainty together in a complex environment (Collateral Damage and Military Advantage), but also dealing (as the consulted experts have assessed) with other human aspects and factors. These include military Commander's background, experience, culture, (exposure and resistance to) stress, willingness to take risks (risk appetite), and even religion. To cope with these facts, military Commanders need to be "flexible, quick, resilient, adaptive, risk taking, and accurate" (Cannon-Bowers & Bell, 1997), responsible, and legally compliant. The same factors are present also in the assessment conducted from the operational perspective.

Block 4.

As a result of the proportionality assessment (military-legal perspective), the following two options can be considered. First, in case the Cyber Operation is not-disproportional, then the considered target could be engaged using the assessed cyber weapon. Second, in case the Cyber Operation is disproportional (thus unlawful), then the Cyber Operation should be aborted/stopped in the sense of not being executed, and control measures for avoiding or minimizing Collateral Damage should be examined. In a worst case scenario i.e. in case of intentionally conducting an unlawful Cyber Operation, then this act is punishable since it is a war crime (Boothby, 2012; Schmitt, 2013). Considering the operational assessment, the final decision supports the development process of CoAs.

The introduced modelling framework and aims to structure and conceptualize the material researched in this dissertation. This implies that the modelling framework has *just* a conceptual role and should not be considered an artefact in this research. The framework is drawn based on the military-legal perspective or context of use considered in this research and provides a global overview of the entities, aspects, and factors that participate in key moments during targeting in Cyber Operations such as assessing the effects of and proportionality in Cyber Operations. Additionally, the modelling framework was designed due to the fact that at the moment of speaking, tools or artefacts that assess the effects of Cyber Operations and support targeting decisions in Cyber Operations do not exist although they are critical for military Commanders and their advisors for targeting in Cyber Operations. Moreover, a direct relation between the components of this modelling framework and the research questions of this dissertation is provided in section 1.4.2.

1.4. Research Approach

In this section we discuss the approach followed when conducting this research. We begin by discussing different aspects about the followed research philosophy and strategy (Section 1.4.1.), we continue by addressing the main research methodology used (Section 1.4.2.), after that we discuss all the research instruments used in order to design the proposed artefacts (Section 1.4.3.), and we end by presenting the further outline of this dissertation (Section 1.5.).

1.4.1. Research Philosophy and Strategy

When conducting research, "a general orientation about the world" (Creswell, 2009) is constructed. This is done through what is called a research paradigm or research philosophy that guides the researcher to select a proper research strategy and choose convenient and useful research methods. A research philosophy contains all the ontological, epistemological, and axiological assumptions done by the researcher (Gregg, 2001). At the same time, a research philosophy implies a system of beliefs, assumptions, and limits regarding the process of knowledge development (Saunders et al., 2009). In other words, a research philosophy sets the boundaries and limits to the (new) knowledge that can be produced. (Creswell, 2009) identifies four main types of research philosophies: postpositivism, constructivism, advocacy/participatory, and pragmatism. The postpositivism research paradigm implies a deterministic philosophy where "causes probably determine effects or outcomes" (Creswell, 2009) in the sense of identifying and assessing the causes that produce outcomes through measurement and experiments. The constructivism research paradigm entails understanding the world through varied and multiple meanings regarding "certain objects or things" (Creswell, 2009) and generate new theories. The advocacy/participatory research paradigm suggest the involvement of a political agenda in the sense of implying reforms "that may change the lives" (Creswell, 2009) of participants, institutions, and even the ones of researchers. The pragmatism research paradigm denotes a worldview based on "actions, situations, and consequences" (Creswell, 2009) shifting the focus from the methods to using all available approaches to understanding the problem.

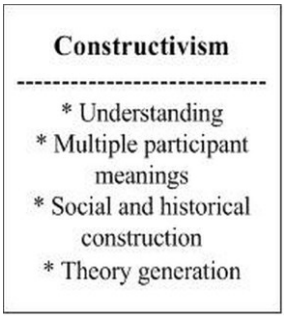


Figure 1.7. Constructivism research paradigm (captured from (Creswell, 2009 at page 39))

The present research is conducted according to the constructivism paradigm based on the considerations illustrated in Figure 1.7. and are here further resumed:

- Understanding: the researcher is looking for meaning and constructs understanding even if the information is scarcely defined or is incomplete (Watzlawick, 1980). In this research, the one conducting it tries to understand i) Cyber Warfare or military Cyber Operations from a military-technical perspective and as a socio-technical phenomenon, ii) cyber weapons as the means to produce effects in Cyber Operations, and iii) effects of cyber weapons' action in Cyber Operations as well as the qualities and aspects of the impacted entities (target and collateral).
- Multiple participant meanings: the researcher integrates multiple views on the problem that needs to be tackled i.e. as a multidisciplinary research conducted as the union between Cyber Security, Artificial Intelligence, and Military Operations domains, where several military-technical experts have been consulted either as input data or as new theory (e.g. artefact) evaluation.
- Social and historical construction: the researcher considers historical data regarding five real Cyber Operations incidents as well as a historical and structured description for three virtual, but realistic Cyber Operations case scenarios/use cases considered for evaluating new generated artefacts (e.g. models, methodology) and which were evaluated from the design phase by military-technical experts. The experts consulted have in average 20 years of experience gathered through technical and military education and practice in military exercises and field operations, as well as scientific research.
- Theory generation: the researcher contributes theoretically by proposing a series of artefacts useful in the fields of Cyber Security and Military Operations (e.g. three models, one methodology, and one framework)

that are sequentially designed, developed, and evaluated to achieve the aim of the present research.

Accordingly, as this research aims to produce new useful artefacts, the way to do that is by considering a Design Science Research approach. This approach is further described in the following section.

1.4.2. Research Methodology: Design Science Research

A research methodology is the mechanism of systematically achieving a research aim and solving a scientific or societal problem. That demands a "logic and objective procedure" (Pearson, 1965). As already stated in the previous section, this research considers as a research strategy the Design Science Research approach (Offermann, 2009; Peffers et al., 2008; Hevner & Chatterjee, 2010; March & Smith, 1995) because of the following reasons:

- It allows the construction and evaluation of new and innovative artefacts in a systematic and logic way through a set of steps or activities.
- It involves researcher's direct participation to be able to build artefacts and construct knowledge.
- It implies that the artefacts are built for human/societal purposes.

In a Design Science Research approach, an artefact is built through technological or engineering lenses, is something 'artificial' (Simon, 1996) which denotes something that is human made i.e. antithetical to something that is natural or exists in nature (Vaishnavi & Kuechler Jr., 2008). Artefacts exist in the form of models, methodologies, algorithms, frameworks etc. Hence, the present research produces the following list of artefacts, as depicted in Table 1.1.:

Artefact no.	Name Artefact	Type Artefact	Artefact described in
1	Cyber Operations Computational Ontology	Model	Chapter II (answer to RQ1)
2	Cyber Weapons Profiling Framework	Framework	Chapter III (answer to RQ2)
3	Effects of Cyber Operations Assessment Methodology	Methodology	Chapter IV (answer to RQ3)
4	Effects of Cyber	Model	Chapter V

	Warfare Knowledge-Based Model		(answer to RQ4)
5	Effects estimation and targeting decisions in Cyber Warfare	Model	Chapter VI (answer to RQ5)

Table 1.1. Relation between artefacts, type of artefacts, and chapters that describe the artefacts

The proposed artefacts have been designed based on multidisciplinary research (NATO, 2016) that integrates theories, methods, and techniques from the fields of Cyber Security, Artificial Intelligence, and Military Operations, as follows. From the field of Cyber Security, incident analysis as well as vulnerability and impact assessment was used in order to analyse the real Cyber Operations incidents/scenarios for Artefacts 1-5, and incident analysis was used in order to build virtual/synthetic and realistic Cyber Operations incidents for Artefacts 3 and 5. From the field of Artificial Intelligence, AI sub-fields named Knowledge Representation & Reasoning and Fuzzy Logic were used in order to develop the Artefacts 2, 4 and 5. From the field of Military Operations, military targeting knowledge and methods as well as legal aspects (i.e. distinction and proportionality) were used.

Moreover, the role of the proposed artefacts in the global picture reflected in the proposed modelling framework in this research is depicted in Fig. 1.4., as already introduced in Section 1.3.2.

Thereupon, a Design Science Research approach is adopted in the present dissertation because it starts with understanding the context and identifying the problem for which artefacts are built in order to solve it and produce new knowledge that can be of use to different scientific communities and practitioners from domains such as: Cyber Security, Artificial Intelligence, Computer Science, Military Operations, Military Law, Conflict Studies, and Political Science.

For building the five proposed artefacts using a Design Science Research methodology, the following activities have been considered and discussed in each correspondent chapter (Peffers et al., 2008):

- Activity I – Problem identification: the problem is identified either as a societal problem that needs to be solved or as a research gap that needs to be tackled in order to build the artefact. Additionally, the underlying relevance and motivation are established and/or clarified.
- Activity II – Defining objectives of a solution: the overall aim/objective is established, and if necessary is decomposed into smaller objectives that should be accomplished in order to attain the overall aim/objective.

- Activity III – Design and Development: the artefact is created and designed starting with establishing its functionality and architecture, and going to its implementation based on all the gathered requirements and resources.
- Activity IV – Demonstration: the artefact is demonstrated through case study or experimentation which intends to reflect how it can solve one or more instances of the problem.
- Activity V – Evaluation: the artefact is evaluated in regards with its functionality through demonstration and by that how it supports the achievement of the objective(s) for the identified problem.
- Activity VI – Communication: the importance, utility, and novelty of the proposed artefact are communicated to relevant audiences such as scientific communities (e.g. conferences and journals) and professionals.
- Activity VII – Contribution: the contribution and relevance to the existing body of knowledge and space of artefacts from one or more scientific domains as well as to society in regards to solving existing (societal, socio-technical or technical) problems, are refined.

Conclusively, the methodological approach is further elaborated for each proposed artefact in each chapter of this dissertation, as reflected in Table 1.1.

1.4.3. Research Instruments

In order to construct theories and enrich knowledge using a research strategy, research instruments are used to be able i) to collect and analyse data, and ii) to evaluate proposed theories or artefacts. Galliers (1992) considers the following research instruments: case studies, literature studies, experiments (e.g. field, laboratory), surveys etc. The use of these instruments depends on factors such as research's aim, objectives, questions, and existing knowledge or artefacts (Vaishnavi & Kuechler, 2008). In the present research, the following research instruments were used: literature review, case studies, interviews, Focus Groups, and field work. These research instruments have been merged in order to design the proposed artefacts as follows. Literature review was done in order to understand the field of research, state of the art, and to identify existing knowledge gaps that this research can tackle. Case studies were conducted on both real and virtual/synthetic Cyber Operations in order to understand these types of cyber activities and assess their effects. Interviews were carried out in this research for the purpose of identifying necessary requirements and information (Stefik, 2014) for designing the proposed artefacts. Focus Groups were conducted in the sense of evaluating two of the proposed

artefacts as well as providing necessary input for another one. Field work was carried out in military exercises in order to get familiar with the military targeting process and contribute to the integration of Cyber Operations into military planning and by that seeing Cyber Operations as a realistic option for achieving military goals. Each of these instruments is elaborated in the next sub-sections.

1.4.3.1. Literature review

This dissertation is the result of a multidisciplinary research as a union between domains like Cyber Security, Artificial Intelligence, and Military Operations. This implies that different schools of thought were used from the abovementioned domains, based on resources such as scientific articles and books, technical, strategical, and policy reports, and media news, together with military doctrine (NATO and the U.S.), strategies, and reports, in order to assess what it is known and what could be tackled in this research (Jesson et al., 2011). To find the scientific resources, we have searched in online databases such as Web of Science, Scopus, IEEE Explore Digital Library, ACM Digital Library, DBLP Library, and Google Scholar. The search was built and conducted using the following keywords: 'cyber', 'security', 'operation', 'attack', 'conflict', 'war', 'military operations', 'targeting', 'proportionality', 'effect', 'impact', 'consequence', 'damage', 'collateral damage', 'assessment', 'estimation', 'analysis', 'AI', 'Artificial Intelligence', 'intelligent', 'computational', 'ontology', and 'fuzzy', and 'neuro-fuzzy'. To find the doctrines, strategies, and reports, we have searched using the online database Google Scholar and Google searching engine using the keywords: 'cyber', 'security', 'operation', 'war', 'military', 'doctrine', 'strategy', 'policy', 'report', 'United States', 'US', and 'NATO'. To find descriptive resources for the Cyber Operations case studies conducted (both real and synthetic incidents), we have searched using the online database Google Scholar and Google searching engine using the keywords: 'cyber', 'security', 'operation', 'attack', 'incident', 'Orchard', 'Georgia', 'Stuxnet', 'Operation Olympic Games', 'Ukraine', 'Black Energy', 'NotPetya', 'source code', 'Russia', 'Israel', 'ISIS', 'ISIL', 'Al-Qaeda' 'ballistic missile', 'ballistic missile defense system', 'suicide drone', 'Unmanned Aerial Vehicle', 'Unmanned Aerial Systems', and 'cargo ship'.

This ample search process resulted in a series of peer-reviewed conferences and journals articles as well as reports, military doctrine, and strategies. To further filter these resources, we conducted an initial analysis by reading their Abstract, keywords, Introduction, and Conclusions sections, and scanning the rest of their sections. The selection criterion was the

relevance to the topic of this research. In case that this criterion was not fulfilled, resources were further dropped from this process. In case that this criterion was fulfilled, resources were further completely read. Furthermore, for each resource, its references were analysed and when possible relevant resources were found (based on the title), they were further analysed in the same way as described above. Moreover, the results of the literature review is presented in each chapter of this dissertation in order to accompany the proposed artefact, and to integrate it into the existent body of knowledge and space of artefacts.

1.4.3.2. Case Studies

In this research, five case studies on real Cyber Operations incidents and three case studies (Yin & Campbell, 2008) on virtual realistic Cyber Operations were conducted aiming at i) identifying the necessary design requirements and constituents to designing the aimed artefacts, and ii) evaluating some of the built artefacts.

For the case studies conducted on real Cyber Operations incidents, data were collected from publicly available data(sets), reports, and (manual and static) source code analysis of pre-compiled code or parts of the reversed engineered code for incidents like the ones in Georgia, Stuxnet, and Ukraine. For the case studies conducted on virtual, but realistic (as assessed by the consulted experts) Cyber Operations incidents, the data was gathered from publicly available sources such as reports and requirements documents (i.e. technical, functional, operational), and have been inspired in order to establish the context, objective, target, and weapon in such an operation, as follow: first, by real or plausible terrorism and counter-terrorism incidents, for instance, related to (para)military groups such as ISIS/Daesh and Al-Qaeda, second, by possible (e.g. nuclear) threats such as North Korea, and third, by previous or ongoing crises and conflicts in Syria, Iraq, and Afghanistan. Henceforth, an overview with the case studies on Cyber Operations incidents conducted in this dissertation is presented in Table 1.2.

Due to the limited number of data(sets) of real Cyber Operations data(sets) publicly available, the following two measures have been considered in this research:

- Firstly, designing and constructing synthetic/virtual, but realistic Cyber Operations as analytic war-games (Jensen & Banks, 2018) that describe concrete activities and have a well-defined aim (Carroll, 1995) by consulting technical-military experts. These

experts have been consulted in regards to evaluating their design, realism, and applicability. The real Cyber Operations used are presented in Chapters 2, 3, 5, and 6, and the virtual/synthetic Cyber Operations are presented in Chapter 4 and 6.

- Secondly, considering an approach that uses data gathered from merging case studies on (real and synthetic) Cyber Operations combined with interviews (in Appendices, Annex A-C) and Focus Groups (in Appendices, Annex D-E) with experts that were suggested to the researcher, and are presented in Chapters 3-6.

Case Study No.	Case Study Name (Incident Year)	Case Study Conducted on Year	Case Study Status
1	Operation Orchard (2007) used for Artefact 2, 4, and 5 presented in Chapters 3, 5 and 6.	2016 – 2017	Real
2	Georgia (2008) used for Artefact 1, 4, and 5 presented in Chapters 2, 5, and 6.	2016 – 2017	Real
3	Operation Olympic Games / Stuxnet (2010) used for Artefact 1, 2, 4, and 5 presented in Chapter 2, 3, 5, and 6.	2016 – 2017	Real
4	Black Energy 3 (2015) used for Artefact 1, 2, 4, and 5 presented in Chapters 2, 3, 5, and 6.	2016 – 2017	Real
5	NotPetya (2017) used for Artefact 4 and 5 presented in Chapter 5 and 6.	2017 – 2018	Real
6	Ballistic Missile Defense System used for Artefact 3 and 4 presented in Chapter 4 and 5.	2017	Virtual, but realistic
7	Suicide drone used for Artefact 5 presented in Chapter 6.	2019	Virtual, but realistic
8	Cargo ship used for Artefact 5 presented in Chapter 6.	2019	Virtual, but realistic

Table 1.2. Cyber Operations Case Studies details

1.4.3.3. Interviews

To further be able to identify the necessary design and functional requirements as well as to evaluate some of its constituents (e.g. concepts such as Collateral Damage) of this research, three series of semi-structured interviews (Yin & Campbell, 2008) were conducted with forty military experts from NATO member countries considered due to their background and significant international experience (Greenwell, 1988; Negnevitsky, 2005; Mach, 2017; Ericsson, 2018). Initially, a list with the names of military experts was provided by the partners of this research as they are representative in this field considering their background and experience in the cyber and military domains. Furthermore, from these experts other relevant military experts were also interviewed as suggested.

The experience of these experts ranges between 15 to 35 years in military planning, targeting, and the experts were holding positions in the field of Cyber Operations. The experts were from the following countries (alphabetical order): France, Germany, the Netherlands, and U.S., and the interviews were conducted in the Netherlands and Germany in 2016 and 2017 as reflected in Table 1.3. Moreover, we present below the process of collecting and analysing the data as well as the results for each set of interviews and we continue with this in each chapter by reflecting the role of the interviews to designing the artefacts proposed in this research.

The first set of interviews tried to answer the question: "What does Collateral Damage in Cyber Operations mean, and how can this be assessed in the context of military Cyber Operations?" (see Appendices-Annex A). The military experts were asked to elaborate on their understanding of Collateral Damage in Cyber Operations, and to further express their requirements and considerations concerning the assessment of Collateral Damage in Cyber Operations. When analysing the transcript, categories and classes were defined for structuring purposes considering the aim of the interview, and marked using different colours. In this sense, three categories were defined: 'Collateral Damage understanding', 'Collateral Damage assessment requirements', and 'Collateral Damage features/indicators'. Further, for analysis we have used the following categories:

- The first category was labelled as 'Collateral Damage understanding' and corresponds to the answers received from the second question (Q2) of the interview. This category contains two classes classified by their own information provided: definition/meaning (concept meaning) and context (of assessment).
- The second category was labelled as 'Collateral Damage assessment requirements' and corresponds to the answers received from the

third, fourth, sixth, and seventh questions (Q3, Q4, Q6, and Q7) of the interview. This category contains four classes defined by their own information provided: functionality, relation to existing methodologies/models, evaluation, and challenges.

- The third category was labelled as 'Collateral Damage features/indicators' and corresponds to the answers received from the fifth question (Q5) of the interview. This category contains four classes defined by their own information provided: physical (embodies hardware and communications), software, data, and human.

The results of the first set of interviews contributed together with the results of the third set of interviews to: i) establishing a definition for Collateral Damage in Cyber Operations, ii) establishing requirements for designing Artefacts 3, 4 and 5 (Chapters 4-6), iii) developing the mentioned artefacts in the sense of defining and addressing phases and steps of assessment (Artefact 3-Chapter 4), iv) defining the types of effects as well as aspects or values that are being impacted (Artefact 4-Chapter 5, see Appendix), and v) to grasping the variables used for estimating the effects (Artefact 5-Chapter 6, see Appendix).

The second set of interviews tried to answer the question: "How to conduct proportionality assessment for targeting decision support in Cyber Operations?" (see Appendices-Annex B). The military experts were asked to elaborate on their on their requirements and considerations in regards to targeting decisions in Cyber Operations through proportionality assessment in Cyber Operations, the meaning of the word 'excessive'. After that, the experts were asked to elaborate on proposing control measures for avoiding and limiting Collateral Damage in Cyber Operations. When analysing the transcript, categories and classes were defined for structuring purposes considering the aim of the interview, and marked using different colours. Then, four categories were defined: 'Factors and aspect influencing targeting decisions', 'Targeting decisions concerning proportionality', 'Understanding the meaning of 'excessive'', and 'Avoiding and limiting Collateral Damage'. Further, for analysis we used the following categories:

- The first category was labelled as 'Factors and aspect influencing targeting decisions' and corresponds to the answers received from the third question (Q3) of the interview. This category contains two classes classified by their own information provided: definition/meaning (concept meaning) and context (of assessment). This category contains third classes defined by their own information provided: technical, context, and human.

- The second category was labelled as 'Targeting decisions concerning proportionality' and corresponds to the answers received from the fourth question (Q4) of the interview. This category contains four classes classified by their own information provided: requirements functionality, relation to existing methodologies/models, evaluation, and challenges.
- The third category was labelled as 'Understanding the meaning of 'excessive'' and corresponds to the answers received from the fifth question (Q5) of the interview. This category contains one classes defined from the information provided: excessive.
- The fourth category was labelled as 'Avoiding and limiting Collateral Damage' and corresponds to the answers received from the sixth and seventh questions (Q6 and Q7) of the interview. This category contains three classes classified by their own information provided: target, cyber weapon, and context.

The results of the second of interviews contributed to: i) identifying factors and aspects that play a role while proportionality assessment is conducted, and were integrated in the modelling framework that this research proposes and Artefact 5 (Chapter 6), ii) understanding that there are different perspectives on grasping the meaning of the word 'excessive' as illustrated in Artefact 5-Chapter 6, iii) establishing requirements for designing Artefacts 4 and 5 (Chapters 5 and 6), and iv) defining control measures for avoiding and limiting Collateral Damage in Cyber Operations (Artefact 5-Chapter 6).

The third set of interviews tried to answer the question: "What does Military Advantage in Cyber Operations mean and how can this be assessed in the context of military Cyber Operations?" (see Appendices-Annex C). The military experts were asked to elaborate on their understanding about Military Advantage in Cyber Operations, and to further express their requirements and considerations concerning the assessment of Military Advantage in Cyber Operations. When analysing the transcript, categories and classes were defined for structuring purposes considering the aim of the interview, and marked using different colours. In this sense, three categories were defined: 'Military Advantage understanding', 'Military Advantage assessment requirements', and 'Military Advantage features/indicators'. Further, for analysis we have used the following categories:

- The first category was labelled as 'Military Advantage understanding' and corresponds to the answers received from the second question (Q2) of the interview. This category contains two classes classified by their own information provided: definition/meaning (concept meaning) and context (of assessment).

- The second category was labelled as 'Military Advantage assessment requirements' and corresponds to the answers received from the third, fourth, and seventh questions (Q3, Q4, and Q7) of the interview. This category contains four classes defined by their own information provided: functionality, relation to existing methodologies/models, evaluation, and challenges.
- The third category was labelled as 'Military Advantage features/indicators' and corresponds to the answers received from the fifth and sixth questions (Q5 and Q6) of the interview. This category contains four classes defined by their own information provided: strategic, operational, and tactical.

The results of the third set of interviews contributed together with the results of the third set of interviews to: i) establishing a definition for Military Advantage in Cyber Operations, ii) establishing requirements for designing Artefacts 3, 4 and 5 (Chapters 4-6), and ii) developing the mentioned artefacts in the sense of defining and addressing phases and steps of assessment (Artefact 3-Chapter 4), defining the types of effects as well as aspects or values that are being impacted (Artefact 4-Chapter 5, see Appendix), and to grasping the variables used for estimating the effects (Artefact 5-Chapter 6, see Appendix).

Consequently, these sets of interviews helped the researcher to identify required requirements together with identifying key concepts, understand their meaning, and design ways to assess them in Cyber Operations. Thereupon, an overview with the sets of interviews conducted with military experts is depicted in Table 1.3.

Interview Set no.	**Number of participants**	**Participants countries (NATO members)**	**Interview period and use**
1	8	The Netherlands, Germany	April 2016 used for Artefacts 3, 4, and 5 presented in Chapters 4, 5, and 6.
2	22	The Netherlands, Germany, the U.S., France	May – December 2017 used for Artefacts 4, and 5 presented in Chapters 5, and 6.
3	10	The Netherlands, the U.S.	August – December 2017 used for Artefacts 3, 4, and 5 presented in Chapters 4, 5, and 6.

Table 1.3. Set of Interviews details

1.4.3.4. Field Work

The role of a participant observer and reflective practitioner (Iacono et al., 2009) implies that a researcher needs to travel outside his/her regular working place(s) in order to study different customs and practices. This means participating in specific situations and collecting data for own research purposes. Although it can be a challenging process, it represents an essential chance to "obtain unique insights" (Iacono et al., 2009). Accordingly, while conducting the present research, field work was done in two joint military operations in 2016 and 2017, as reflected in Table 1.4. This facilitated the following considerations:

- achieving a comprehensive vision on Cyber Operations and broader on Military Operations;
- getting familiar in a practical sense with processes such as targeting, operational planning, assessment of effects, Collateral Damage Estimation Methodology (CDE) etc.
- allowed the researcher to conduct the first set of interviews and establish new connections for further interviews, as already resumed in Table 1.3.

Field work (Joint Military Exercise) Set no.	Participant countries	Field work period and use
1	NATO members	April 2016 used for Artefacts 2 –5 presented in Chapters 3 – 6.
2	NATO members	June 2017 used for Artefacts 2 –5 presented in Chapters 3 – 6.

Table 1.4. Field Work details

1.4.3.5. Focus Groups and Expert Meetings

For almost a century Focus Groups have been used in science as a mechanism of data collection and evaluation in a form of group discussions "focused on a particular topic or set of issues" (Onwuegbuzie, 2009) constituted by a group of experts and a moderator (Baumgartner, 2005; Krueger & Casey, 2002; Remenyi, 2012). When using the Design Science Research approach, Focus Groups are of great use in designing and

evaluating artefacts (Peffers et al., 2006; Tremblay et al., 2010) that have a human and societal purpose (Brandtner et al., 2015) as the ones built and proposed by this research. In a Focus Group, the researcher comes "into direct contact with the potential users of the artefact and with the domain experts" (Tremblay, 2010). In this way, Focus Groups gather experts' opinions (Krueger & Casey, 2014) to "clarifying artefact design questions and probing respondents on key design issues" (Tremblay et al., 2010b) based on the background, experience, and judgements of experts (Greenwell, 1988; Negnevitsky, 2005; Mach, 2017; Ericsson, 2018). In other words, as Remenyi (2012) considers, "a focus group uses a number of knowledgeable informants with different views about which they will debate and this debate should lead to revised or new ideas for the researcher." In the present research three Focus Groups with military experts were organized in the Netherlands and Spain between June 2017-April 2019 with experts from the Netherlands, the U.S., and Canada. These experts are military officers that have significant technical and military experience (e.g. cyber, ICT) and medical experience (i.e. military medical doctors that are able to properly assess the meaning of physical and mental injury/damage). The experience of the consulted experts is above 15 years, with senior officers having 30-35 years of experience.

The first Focus Group (see Appendices-Annex D) aimed at evaluating Artefact 3 regarding the effects assessment methodology in Cyber Operations. This evaluation was carried out using structured questions and was based on a virtual Cyber Operation case scenario conducted on a Ballistic Missile Defence Command and Control system (see Chapter 4 in Section 4.5. for description), and was successful. When analysing the transcript, have been defined categories, classes, and tables for structuring purposes considering the aim of the Focus Group, and they have been marked using different colours. In this sense, five categories were defined: 'Effects meaning', 'Effects assessment', 'Factors and aspects influencing targeting decisions', 'Targeting decisions concerning proportionality assessment', and 'Avoiding and limiting Collateral Damage'. Further, these categories are addressed:

- The first category was labelled as 'Effects meaning' and corresponds to the answers received from the third and sixth questions (Q3 and Q6) of the Focus Group. This category contains two classes defined by their own information provided: understanding and indicators.
- The second category was labelled as 'Effects assessment' and corresponds to the answers received from the fourth, fifth, seventh, eight, and nine questions (Q4, Q5, Q7, Q8, and Q9) of the Focus Group. This category contains three classes defined by their own

information provided: Collateral Damage, Military Advantage, and Military Disadvantage.

- The third category was labelled as 'Factors and aspects influencing targeting decisions' and corresponds to the answers received from the eleventh question (Q11) of the Focus Group. This category contains three classes defined by their own information provided: technical, context, and human.
- The fourth category was labelled as 'Targeting decisions concerning proportionality assessment' and corresponds to the answers received from the tenth question (Q10) of the Focus Group. This category contains two classes defined by their own information provided: yes and no.
- The fifth category was labelled as 'Avoiding and limiting Collateral Damage' and corresponds to the answers received from the tenth question (Q10) of the Focus Group. This category contains three classes defined by their own information provided: target, cyber weapon, and context.

The results of the first focus group contributed to the evaluation of the third artefact and are presented in Tables 4.8.-4.11. in Chapter 4.

The second Focus Group (see Appendices-Annex E) aimed at providing input for Artefact 4 (in Chapter 5) regarding understanding the meaning of injury and how to assess it in Cyber Operation. This Focus Group was carried out using a series of semi-structured questions. When analysing the transcript, have been defined categories and classes for structuring purposes considering the aim of the Focus Group, and they have been marked using different colours. In this sense, three categories were defined: 'Injury understanding, 'Injury assessment requirements', and 'Injury features/indicators'. Further, these categories are addressed:

- The first category was labelled as 'Injury understanding' and corresponds to the answer received from the third, fourth, and fifth questions (Q3, Q4, and Q5) of the Focus Group. This category contains three classes defined by their own information provided: definition/meaning, types, and context.
- The second category was labelled as 'Injury assessment requirements' and corresponds to the answer received from the sixth question (Q6) of the Focus Group. This category contains four classes defined by their own information provided: functionality, relation to existing methodologies/models, evaluation, and challenges.
- The third category was labelled as 'Injury features/indicators' and corresponds to the answer received from the seventh and eight

questions (Q7 and Q8) of the Focus Group. This category contains two classes defined by their own information provided: physical and mental/psychological.

The results of the second Focus Group contributed to: i) establishing a definition for injury as Collateral Damage that includes both physical and mental/psychological injury, ii) establishing requirements for designing Artefacts 4 and 5 (Chapters 5 and 6), and to iii) grasping variables used for estimating injury as effects in Cyber Operations (Artefact 5-Chapter 6, see Appendix).

The third Focus Group (see Appendices-Annex F) aimed at evaluating Artefact 5 meaning effects estimation model and proposing targeting decisions concerning proportionality assessment in Cyber Operations. The evaluation was conducted using structured questions and was done on two virtual Cyber Operations case scenarios on a suicide drone and a cargo ship (see Chapter 6 in Sections 6.6.1. and 6.6.2. for description), and was successful. The data collected was used for evaluating the last artefact and structured in the tables presented in Tables 6.5. and 6.6. using the variables provided in Section 6.8. and Appendix.

Hence, in Table 1.5. are illustrated details for each conducted Focus Group together with their involvement in building the proposed artefacts in this research.

Focus Group no.	**Number of participants**	**Participant countries (NATO members)**	**Focus Group date**	**Used for**
1	9	The Netherlands	21.06.2017	Evaluation of Artefact 3 presented in Chapter 4.
2	3	The Netherlands, the U.S., Canada	18.05.2018	Input for Artefact 4 presented in Chapter 5.
3	4	The Netherlands	26.04.2019	Evaluation of Artefact 5 presented in Chapter 6.

Table 1.5. Focus Groups/Workshops details and relation to Artefacts' building

Additionally, a series of individual face-to-face meetings with military-technical experts with significant technical (e.g. cyber, ICT) experience and military (i.e. military officers) with significant international experience from the Netherlands were organized between May 2017 and August 2019. These experts have in average 20 years of experience gathered through technical and military education and practice in military exercises and field operations. For the design of the virtual Cyber Operation case studies used for Artefact 3 and 5, the experts were consulted in order to build realistic Cyber Operation scenarios and they have provided useful technical materials for understanding the background and used technology. The same experts were the ones that suggested to choosing these specific three Cyber Operations and their choice was based on the realism in the sense if these Cyber Operations could actually happen in reality and their vast experience in military exercises (scenarios based) and missions. The experts consulted in order to evaluate Artefacts 1, 3 and 4 (see Chapters 2, 3 and 4) have considered evaluation criteria (see Appendices-Annex G) such as accuracy, clarity, conciseness, applicability and adaptability.

In Table 1.6. are depicted details for each conducted meeting together with their role in building the proposed artefacts in this research. The results of the expert-based evaluation-sense interviews, Focus Groups, expert meetings in this research-are presented in each chapter in a special dedicated section, and when necessary (i.e. Artefact 1 and 4 discussed in Chapters 2 and 5) changes were made as the experts suggested.

Expert meeting no.	**Interview period**	**Used for**
1 – 2	October – November 2017	Evaluation of Artefact 1 presented in Chapter 2.
3 – 4	January – May 2017	Design case study for Artefact 3 presented in Chapter 4.
5 – 6	May – October 2017	Evaluation of Artefact 3 presented in Chapter 4.
7 – 9	July – August 2018	Evaluation of Artefact 4 presented in Chapter 5.
10 – 11	March – April 2019	Design case studies for Artefact 5 presented in Chapter 6.

Table 1.6. Expert Meetings details and relation to Artefacts' building

1.4.4. Research Modelling Techniques: Artificial Intelligence

The main concepts and directions that surround Artificial Intelligence are intelligence, humans, and artefacts built as intelligent systems (Barr & Feigenbaum, 2014). Artificial Intelligence implies building artefacts that are not human by nature, thus are artificial (based on software), but are capable to capture and comprehend characteristics and functions of humans through understanding and miming the nature and actions of human intelligence i.e. reasoning, problem-solving, and learning. As it will be later explained, the core of this dissertation relies on AI techniques from the first two categories: reasoning and problem solving. Although our intention was from the beginning to fully integrate the learning function as well (e.g. deep learning), the lack of data(sets) did not allow us to do so. Thus a full learning approach represents an extension of this dissertation as it will be explained in the last chapter of this dissertation. Taking into consideration that the ability to generally perform as good as or overcome human intelligence is still yet to come (going from AI to AGI-Artificial General Intelligence and hybrid intelligence), the use of different AI techniques is beneficial to humanity even from its incipient times in the 40's with roots in the antiquity.

Among systems that have integrated from an early stage AI– initially named machine intelligence – solutions developed by computer scientists based on AI techniques we recall gaming (i.e. chess playing), military technologies developed by DARPA-Defense Advanced Research Project Agency for UAVs (Unmanned Aerial Vehicle), pattern recognition, language understanding and processing, and robots (McCorduck, 1977; Buchanan, 2005). As time passed, different AI techniques such as Artificial Neural Networks and Fuzzy Logic encountered dark times, and the systems developed using them were seen as un-trustable or competitive to humans (Ferber, 1999). These AI techniques needed to be rediscovered decades later, fact which conducted to a significant development and utilization in almost all human domains and corresponding services. By that, among day to day modern solutions or systems that integrate AI techniques we can think of ones ranging from military planning tools (BryanSpear), military surveillance and targeting for Autonomous Weapons (Roth, 2019), national and Homeland security use of IBM Watson's natural language super-computer (IBM, 2019), planning and delay avoidance in aviation (MindTitan), diagnosis, gene editing, and diagnostic personalization in medicine as well as robotic surgery (Datarevenue; Martin, 2018), and going to Tesla as well as smart home hubs and personal assistants such as Alexa, Siri, and Google assistant. Additionally, in the cyber/information security domain, AI-based solutions are proposed for instance in intrusion detection, malware classification, cyber defense, and threat assessment (Tyugu, 2011).

Given our short introduction in Artificial Intelligence, we will continue discussing about its use in this research. Hence, in order to model the first, fourth, and fifth proposed artefacts, the model-driven AI approach was considered (Geffener, 2018) in combination with the data-driven AI approach (Ashri, 2018). This implies using different AI techniques from the AI sub-fields named Knowledge Representation and Reasoning (Levesque, 1986; Randall et al., 1993; Zadeh, 1989; Efraim et al., 2005) and Fuzzy Logic (Lucas & Van Der Gaag, 1991; Grosan & Abraham, 2011; Mishra & Jha, 2014; Mitchell et al, 1975; Elliott, 2005; Efraim et al., 2005; Ericsson el al., 2018) as they allow pursuing a AI hybrid approach (limited data combined with knowledge), as follows:

- Computational Ontologies/Knowledge Graphs (Knowledge Representation and Reasoning) for building and modelling the first and fourth artefact, and
- Fuzzy Logic (Knowledge Representation and Reasoning, and Expert Systems) for building and modelling the fifth artefact.

Moreover, the following two sub-sections discuss each technique as well as the reasons for choosing each specific technique in this research.

1.4.4.1. Computational Ontologies

Ontologies are used in this research as in a Computer Science interpretation, not a philosophical one, and that is why they are not used with the simple term of 'ontology', but 'computational or computer ontologies'. Since they represent models that conceptualize and formalize the world of interest or the context in a studied domain, they are implemented using an Ontology Engineering methodology, and is defined as a quadruple (Russell & Norvig, 2016; Fernández-López et al., 1997; Roussey et al., 2011; d'Aquin et al., 2012):

Definition 1 $O = \{E, P, R, I\}$

that contains the following elements:

- E as the set of entities (i.e. classes or nodes) as main concepts that define the context.
- P as the set of properties or attributes that characterize the entities (i.e. data properties).

- *R* as the set of relationships between entities through their instantiations (i.e. object properties).
- *I* as the set of instances/objects/data values of entities.

A simple exemplification for such a model is illustrated in the figure below.

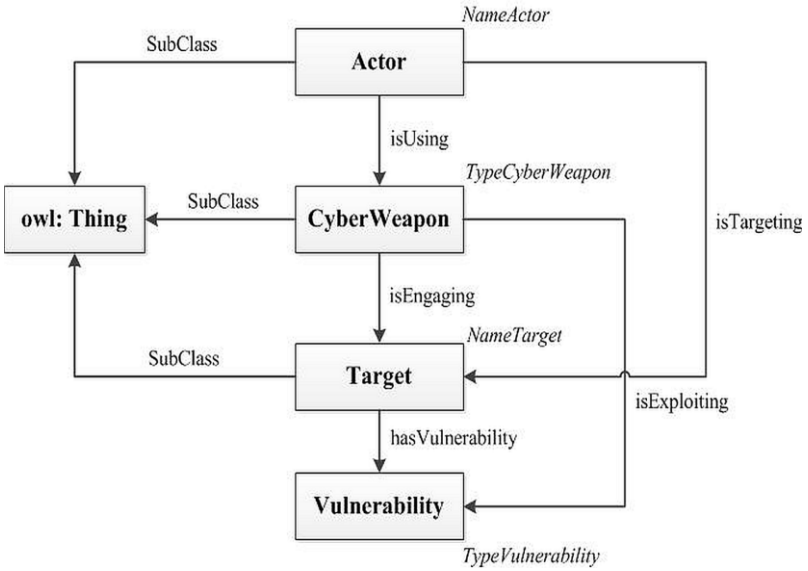


Figure 1.8. Computational ontology exemplification

When considering *Definition 1* for the exemplified model, we can see that:

- The set *E* contains the following classes/entities: *Thing* (i.e. the root class which means mother of all classes), *Actor, Cyber Weapon, Target,* and *Vulnerability.*
- The set *P* contains the following data properties/attributes: *NameActor, TypeCyberWeapon, NameTarget, and TypeVulnerability.*
- The set *R* contains the following object properties/relations: *SubClass, isUsing, isEngaging, hasVulnerability,* and *isTargeting.*
- The set *I* could contain the following instances/data values: *Russia* (for class Actor), *DDoS* (for class CyberWeapon), *GeorgianCommunications* (for class Target), *and ConfigVulnerability* (for class Vulnerability).

Among the application domains where computational ontologies or knowledge graphs have been built as knowledge/data models, we can think

of medical experimentation (Cvjetkovic, 2014), traffic light control (Balushi, 2016), autonomous robots (Paull et al., 2012), cyber threat intelligence (Mavroeidis & Bromander, 2017), and intrusion detection in SCADA systems (Balushi et al., 2016).

However, the underlying question would be why we have used this technique in order to implement two of the five artefacts: i) the first artefact meaning the Cyber Operations computational ontology, and ii) a part of the fourth artefact meaning the Knowledge-based model for assessing the effects of Cyber Warfare, respectively. The motivation behind choosing this technique is decomposed in the following parts (Sanzogni, 2017; Owen, 1988; De Spiegeleire, 2017; Uschold & Gruninger, 1996; Staab & Studer, 2010):

- The existing gap regarding understanding and representing Cyber Operations as a (socio-technical) phenomenon through both technical and military lenses, together with the existing gap concerning understanding, representing, and classifying their effects. In other words, this facilitates having an adequate view on Cyber Operations' reality as well as towards comprehending what kind of effects they have on certain aspects and qualities of the impacted entities (i.e. actors, targets, and/collateral assets).
- (Owen, 1988) considers that "good representations are the key to good problem solving". We interpret this quote as seeing these two artefacts existing both stand-alone as well as fundament or support for building the fifth artefact which aims at estimating and classifying the effects of Cyber Operations together with advising targeting decisions based on proportionality assessment in Cyber Warfare. This implies that the way these artefacts are structured and built are done through a classical and pure computer scientist/AI perspective.
- These models allow to refine and update different concepts by embedding operations such as modification, addition or deletion.
- These models are exchangeable and support interoperability between different domains, systems, applications, and experts.
- And these models are easy to explain to and understand by experts from different (congruent or not) domains and communities.

1.4.4.2. Fuzzy Logic

The roots of the Fuzzy Logic techniques which are based on fuzzy sets are found in the multiple-valued logic introduced by Lukasiewicz in

1920 (Łukasiewicz, 2011). He considered that the dual values of true and false are not enough to represent human reasoning and real events, so a third value should be introduced to define the intermediary space between true and false. In this way, the father of Fuzzy Logic technique – which extends the multiple-valued logic 45 years later – Zadeh, considered in his fundamental work presented in (Zadeh, 1965; Zadeh, 1975a; Zadeh, 1975b; Zadeh, 1975c; Zadeh, 1989) that a gradual transition should be done between true and false, in the way that intermediary states such as maybe true or maybe false could also exist, in other words: a transition of values (Munakata, 2008). This is possible by attributing a grade or function of membership μ which takes values between 0 and 1 and expresses how an element x belongs (as a grade) to a universe of discourse U (i.e. the set of elements that come into consideration in a specific context).

Moreover, this technique has a diverse pallet of options or classes of Fuzzy Inference Systems (FIS) such as Mamdani, Sugeno, and Tsukamoto (Singhal & Banati, 2013) which allow to design and implement different intelligent systems (e.g. expert systems) providing the main advantage of mathematically dealing with the vagueness, impreciseness and uncertainty of information (Negnevitsky, 2005) that is "gray" by nature (Smith, 1995). In this research we implement our last artefact using the Mandani inference system type due to its suitability to our needs and the fact that it is most commonly used alone or in conjunction with other AI/Machine Learning techniques such as Artificial Neural Networks or Genetic (Evolutionary) Algorithms. Moreover, a more detailed technical discussion is presented in Chapter VI of the present dissertation.

A simple exemplification for such a model is further presented in Figure 9. In this case, a MISO (Multi Input Single Output) architecture was considered in order to estimate the level of exposure for a software application considering the state of a software vulnerability and the capacity/nature of the defense mechanism that the software application contains using triangular functions.

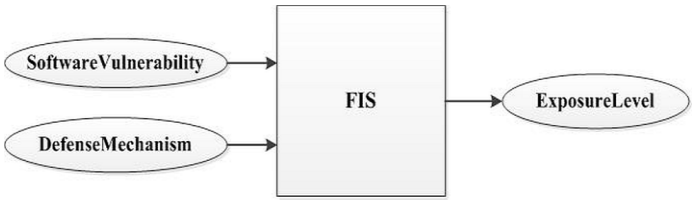


Figure 1.9. Fuzzy Inference System (FIS) exemplification

Input variables: *SoftwareVulnerability*

DefenseMechanism

Output variables: *ExposureLevel*

These variables are defined using the following fuzzy values (linguistic terms):

SotwareVulnerability = {Unpatched, Patched, Unknown}
DefenseMechanism = {Low, Medium, High}
ExposureLevel = {Low, Medium, High}

For this exemplification, further computations are left behind, the focus being pointed to explicitly defining a possible rule, further defined:

IF SoftwareVulnerability is Unpatched AND DefenseMechanism is Low THEN ExposureLevel is High

which represents a conditional sentence where the part directly following *IF* is called *antecedent*, and the part directly following *THEN* is called *consequent.*

Among the applications which are built using the Fuzzy Logic technique (e.g. for assessment, evaluation, estimation, prediction, diagnose, decision support purposes) we can think of a very diverse range contained in several domains, such as: military tracking (Smith, 1995), agriculture (Cornelissen et al., 2003), chemical attacks severity (Samad-Soltani & Langarizadeh, 2015), battlefield situational awareness (Hanratty et al., 2013), earthquake prediction (Arash et al., 2016), IoT based healthcare (Ali et al., 2018), cryptography for the substitution cipher algorithm (Kulkarni et al., 2012), terrorist event classification (Inyaem et al. 2010), threat assessment (Yun et al., 2012), ICS security (Pricop et al., 2016), fault detection in cyber-physical systems (Sargolzaei et al, 2016), intrusion detection in Wireless Sensor Networks (Singh, 2017), alert systems for controlling cyber bullying (Kumar & Kathiresan, 2016), and cyber situation awareness (Huang et al., 2016).

In Decision Support Systems, Fuzzy Logic models are used in order to support different decision making processes, activities, or phases of a domain (Laskey, 2006; Turban et al., 2007). In a nutshell, three phases are considered in supporting decision making processes (Rospocher & Serafini, 2012):

- Formulating the decision making problem.
- Collecting and analysing relevant data for the given problem.

- Reasoning on the data to provide decision making support.

A Decision Support System (Burstein & Holsapple, 2008; Rospocher & Serafini, 2012; Druzdzel & Flynn, 2017) is a tool composed by three modules:

- Model module: is represented by the designed model that contains the mechanism used for the investigated decision making process.
- Database/Data module: is represented by the knowledge/data used for designing and evaluating the investigated decision making process.
- User interface module: is represented by the Graphical User Interface (GUI) developed for using the model.

Just as in the case of using computational ontologies to build the first and the fourth artefacts, the underlying question that we are going to answer now is why we have chosen this technique (Fuzzy Logic as elaborated in Chapter 6) inspired by and used in a deep learning approach in order to build the fifth artefact. From a Decision Support System perspective, the fifth artefact proposed in this research contains the model and data modules, while leaving for further implementation the user interface module as it is outside the scope of this research. The motivation behind choosing the Fuzzy Logic technique relies on the coming arguments (Negnevitsky, 2005; Turban et al., 2007; Russell & Norvig, 2016; Rabunal, 2009; Grosan & Abraham, 2011):

- Due to the already illustrated struggle in dealing with the lack of data(sets) for Cyber Operations incidents, as well as the uncertainty that surrounds the entities involved in this phenomenon, expert knowledge was used being collected from different sets of interviews, meetings, and Focus Groups.
- Considering the use of natural language in order to express information which facilitates a proper communication with the participating experts.
- Benefiting from its interpretability power in the sense that fuzzy rules and reasoning are explicit and understandable.
- Granting its adaptability in the sense of being able to adapt and refine the initial model.
- Useful for decision making having a history of decades of being used as or representing the fundament for Decision Support Systems in different domains and applications.
- And because this techniques can be easily extended when more data(sets) will be available into a more hybrid approach i.e.

combining with Artificial Neural Networks or Evolutionary Algorithms (e.g. Genetic) that would result in a neuro-fuzzy or evolutionary fuzzy approach, respectively.

Until now, the context of this research was introduced together with the aim of this research and the research approach followed. From now, the outline of this dissertation is addressed, followed by the chapters of this dissertation that present in-depth the research conducted for the purpose of writing this dissertation.

1.5. Dissertation Outline

Figure 1.10. depicts the outline of the present dissertation. Chapter II addresses *RQ1* by recommending a definition for Cyber Operations and proposing a knowledge/data model as a computational ontology (knowledge graph/base) for Cyber Operations in order to represent and reason about its essential entities. Chapter III deals with *RQ2* and proposes a definition for Cyber Weapons, analyses their life cycle, their structure and advances a profiling framework to analyse their characteristics and classification criteria. Hence, Chapter II and Chapter III set the scene for the following chapter. Chapter IV tackles *RQ3* by introducing an assessment methodology for Military Advantage, Collateral Damage, and Military Disadvantage in Cyber Operations which considers multidimensional factors and comprises several phases and steps. Chapter V addresses *RQ4* and advances a knowledge/data-based model for assessing the effects of Cyber Warfare. Accordingly, Chapter IV and Chapter V set the scene for the following chapter. Chapter VI tackles *RQ5* by proposing a multi-layered model that estimates and classifies the effects of Cyber Operations, and further advises targeting decisions in Cyber Warfare. Chapter VII reflects on the results, limitations, and applicability of this research, provides a direct extension in a parallel domain (Modelling and Simulation), and discusses further extensions (AI based), and future lines of research.

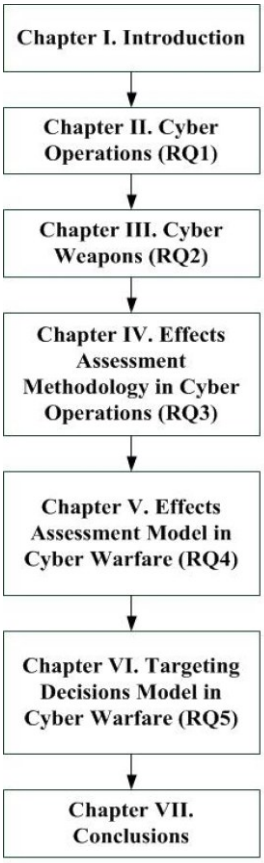


Figure 1.10. Outline of this dissertation

Consequently, in Chapter II to VI the results of this research are presented, and they have been blindly reviewed, published, and presented to the peer-review scientific venues of this field and to the international scientific community of this field (e.g. journals, conferences, and workshops), as follows:

Chapter no.	Publication reference
II	Maathuis, C., Pieters, W. & van den Berg, J. 2018, "Developing a Computational Ontology for Cyber Operations", 2018, *Journal of Information Warfare*, vol. 17, issue 3, , pp. 33-52. Maathuis, C., Pieters, W. & van den Berg, J. 2018, 'A Computational Ontology for Cyber Operations', *Proceedings of the 17th European Conference on Cyber Warfare and Security,*

	pp. 278-288.
III	Maathuis, C., Pieters, W. & van den Berg, J. 2016, 'Cyber Weapons: a Profiling Framework', *Proceedings of the 1st International Conference on Cyber Conflict (CyCon U.S.),* IEEE Computer Society, pp. 1-8.
IV	Maathuis, C., Pieters, W. & van den Berg, J. 2018, 'Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations', *Proceedings of the IEEE Military Communications Conference 2018,* pp. 1-6.
V	Maathuis, C., Pieters, W. & van den Berg, J. 2018, "A Knowledge-Based Model for Assessing the Effects of Cyber Warfare", *Proceedings of the 12th NATO Conference on Operations Research & Analysis,* , pp. 1-7.
VI	Maathuis, C., Pieters, W. & van den Berg, J. 2020, 'Decision Support Model for Effects Estimation and Proportionality Assessment for Targeting in Cyber Operations', *Journal of Defence Technology,* 2019(1), DOI: https://doi.org/10.1016/j.dt.2020.04.007, Elsevier.
VII	Boltjes, B., Maathuis, C., van den Berg, T. & Gouweleeuw, R. 2019, "Developing Standards for Including the Cyber Domain in Military Training and Exercises", *SISO, Proceedings of the Simulation Innovation Workshop 2019*, , pp. 1-17.

Table 1.7. Dissertation chapters and publications overview

1.6. References

Additional Protocol I (1977). Art 52(2) – General protection of civilian objects.

Additional Protocol I (1977). Art 51(5)(b) – Protection of the civilian population.

Additional Protocol I (1977). Art 57(2) – Precautions in attack.

Albright, D, Brannan, P, Stricker, A, Walrond, C & Wood, S 2012, *Preventing Iran from getting nuclear weapons: Constraining its future nuclear options*, ISIS.

Ali, F., Islam, S. R., Kwak, D., Khan, P., Ullah, N., Yoo, S. J., & Kwak, K. S. (2018). Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare. *Computer Communications*, *119*, pp. 138-155.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. *Comparative Strategy*, 12(2), pp. 141-165.

Arash, A., Zare, M. & Atry, F. (2016). A fuzzy expert system for earthquake prediction, case study: the Zagros range. *arXiv preprint arXiv:1610.04028*.

Ashri, R. (2018). Building AI software: Data-driven vs model-driven AI and why we need an AI-specific software. https://hackernoon.com/building-ai-software-data-driven-vs-model-driven-ai-and-why-we-need-an-ai-specific-software-640f74aaf78f: Accessed December 25, 2019.

Balushi, A.A., McLaughlin, K., & Sezer, S. (2016). OSCIDS: An Ontology based SCADA Intrusion Detection Framework. In Proceedings of the 13th International Joint Conference on e-Business and Telecommunications. SCITEPRESS-Science and Technology Publications, pp. 327-335.

Barr, A., & Feigenbaum, E. A. (Ed). (2014). *The handbook of artificial intelligence* (2). Butterworth-Heinemann.

Baumgartner, T. A., Clinton H. S. & Hensley, L.D. (2005). *Conducting and reading research in health and human performance*. McGraw-Hill Humanities/Social Sciences/Languages.

Bauvier, A.A. (2012). International Humanitarian Law and the Law of Armed Conflict. Peace Operations Training Institute. https://cdn.peaceopstraining.org/course_promos/international_humanitarian_law/international_humanitarian_law_english.pdf: Accessed December 20, 2019.

Berg, van den, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., van de Koppen, L., ... & De Bos, T. (2014). On (the emergence of) cyber security science and its challenges for cyber security education. In *The NATO IST-122 Cyber Security Science and Engineering Symposium*.

Berg, van den, J., (2019). A Basic Set of Mental Models for Understanding and Dealing with the Cyber Security Challenges of Today, Journal of Information Warfare, 19(1):26-47.

Brenner, S. W. (2006). At light speed: Attribution and response to cybercrime/terrorism/warfare. *J. Crim. L. & Criminology*, *97*, 379.

Bryant, W.D. (2016). *International conflict and cyberspace superiority*. Routledge.

Brown, G. D. & Owen W. T. (2012). On the Spectrum of Cyberspace Operations. Journal Article.

Brandtner, P., Helfert, M., Auinger, A., & Gaubinger, K. (2015). Conducting focus group research in a design science project: Application in developing a process model for the front end of innovation. *Systems, Signs & Actions*, *9*(1), pp. 26-55.

BryanSpear. Military use of artificial intelligence. https://www.techwalla.com/articles/military-use-artificial-intelligence: Accessed July, 05, 2019.

Bryant, W. D. (2015) *International conflict and cyberspace superiority: theory and practice*. Routledge, pp. 2.

Buchanan, B. G. (2005). A (very) brief history of artificial intelligence. *Ai Magazine*, *26*(4), 53-53.

Burstein, F., & Holsapple, C. W. (Eds.). (2008). *Handbook on decision support systems 2: variations*. Springer Science & Business Media.

Cannizzaro, E. (2006). Contextualizing proportionality: jus ad bellum and jus in bello in the Lebanese war. *International Review of the Red Cross*, *88*(864), 779-792.

Cannon-Bowers, J.A. & Bell, H.H. (1997). Training decision makers for complex environments: implications of the naturalistic decision making perspective, In: *Naturalistic decision making*, 99-110.

Carroll, J. M. (Ed.). (1995). *Scenario-based design: envisioning work and technology in system development*. John Wiley & Sons, Inc..

CLAMO (2000). *Rules of Engagement Handbook for Judge Advocates*. Center for Law and Military Operations.

Clausewitz, C. & Maude, F.N. (1982). *On war*. Penguin U.K., pp. 6, 73.

Cornelissen, A. M. G., van den Berg, J., Koops, W. J., & Kaymak, U. (2003). Elicitation of expert knowledge for fuzzy evaluation of agricultural production systems. *Agriculture, ecosystems & environment*, *95*(1), 1-18.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On cyber warfare*. London: Chatham House, pp. 21-22.

Creswell (2009). *Research Design*. Sage Publications Inc, pp. 39, 40, 41, 43.

Cvjetković, V., Đokić, M., Arsić, B., & Ćurčić, M. (2014). The ontology supported intelligent system for experiment search in the scientific research center. *Kragujevac Journal of Science*, (36), 95-110.

Datarevenue. Artificial Intelligence in Medicine. https://www.datarevenue.com/en/usecases/artificial-intelligence-in-medicine: Accessed July, 05, 2019.

d'Aquin, M, Kronberger, G & Suarez-Figueroa, M.C. (2012). Combining data mining and ontology engineering to enrich ontologies and linked data. In Proceedings of the first international workshop on Knowledge Discovery and Data Mining Meets Linked Open Data. CEUR Workshop Proceedings, 868, pp. 19-24.

De Spiegeleire, S., Maas, M. & Sweijs, T. (2017). Artificial intelligence and the future of defence. *The Hague Centre for Strategic Studies*.

Department of the Army (1978). *U.S. Defense Perspectives*. USGPO, pp. 10.

Dill, J. (2010). *Applying the principle of proportionality in combat operations*. Oxford Institute for Ethics, Law, and Armed Conflict.

Dinstein, Y. (2016). The conduct of hostilities under the law of international armed conflict. Cambridge University Press.

Dipert, R. (2013). The essential features of an ontology for cyberwarfare. In P. Yannakogeorgos & A. Lowther (Eds.), *Conflict and cooperation in cyberspace,* Taylor & Francis (pp.35-48).

Downey, William Gerald. (1953). "The law of war and military necessity." *American Journal of International Law* 47.2: 251-262.

Ducheine, Paul & Gill, Terry. (2018). From Cyber Operations to Effects: some Targeting Issues. The Netherlands Ministry of Defense.

Efraim, T., Jay, E. A., Liang, T. P., & McCarthy, R. V. (2005). Decision support systems and intelligent systems. *Yogyakarta: Andi.*

Elliott, T. (2005). Expert decision-making in naturalistic environments: A summary of research. Defence Science and Technology Organisation Salisbury Systems Sciences Lab.

Ericsson, K. A., Hoffman, R. R., Kozbelt, A., & Williams, A. M. (Eds.) (2018). *The Cambridge handbook of expertise and expert performance*. Cambridge University Press.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6), pp. 29.

Fast, L. (2015). Unpacking the principle of humanity: Tensions and implications. *International Review of the Red Cross*, *97*: 897-898, 111-131.

Ferber, J., & Weiss, G. (1999). *Multi-agent systems: an introduction to distributed artificial intelligence* (Vol. 1). Reading: Addison-Wesley.

Fernández-López, M, Gómez-Pérez, A & Juristo, N. (1997). 'Methontology: From ontological art towards ontological engineering', Proceedings of the fourteenth national conference on Artificial Intelligence, AAAI-97, Spring Symposium Series, pp. 33-40.

Fitton, O. (2016). Cyber operations and gray zones: challenges for NATO. *Connections*, *15*(2), 109-119.

Foltz, A. C. (2012). "Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate". Air War College Maxwell Air Force Base United States.

Galliers, R. (1992). *Information systems research: Issues, methods and practical guidelines*. Blackwell Scientific.

Geffner, H. (2018). Model-free, model-based, and General Intelligence. Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI 2018), pp. 10-17.

Gill, T.D. & Fleck. D. (Eds.) (2011). *The handbook of the international law of military operations*. Oxford University Press, pp. 246.

Gillard, E. C. (2018). *Proportionality in the conduct of hostilities: the incidental harm side of proportionality assessments*. Chatman House the Royal Institute of International Affairs.

Gioe, D. V. (2018). Cyber operations and useful fools: the approach of Russian hybrid intelligence. *Intelligence and National Security*, *33*(7), 954-973.

Gray, C.S. War, peace and international relations: an introduction to strategic history. Routledge, pp. 12.

Greenwell, M. (1988). Knowledge Engineering for Expert Systems. Ellis Horwood.

Gregg, D., Kulkarni, U. & Vinze, A. 2001, Understanding the philosophical underpinnings of software engineering research in information systems, *Information Systems Frontiers*, 3(2), pp. 169-183.

Grosan, C. & Abraham, A. (2011). *Intelligent Systems*. Springer.

Hanratty, T. P., Hammell II, R. J., Bodt, B. A., Heilman, E. G., & Dumer, J. C. (2013). Enhancing battlefield situational awareness through fuzzy-based value of information. In *2013 46th Hawaii International Conference on System Sciences*, pp. 1402-1411.

Hayashi, N. (2010). Requirements of military necessity in international humanitarian law and international criminal law. *BU Int'l LJ*, *28*, 39.

Headquarters Department of the Army. (1991). *Field Manual 100-1*. Pentagon Library.

Hernandez, G. (2019). *International Law*. Oxford University Press, 377.

Hevner, A. & Chatterjee, A. (2010). Design Science Research in Information Systems, Design research in information systems. Springer, pp. 9-22.

Hillson, R. (2009). *The DIME/PMESII model suite requirements project*. Naval Research Lab Washington DC Information Technology Div.

Hopkins, N. (2011). U.K. developing cyber weapons programme to counter attack cyber war threat. https://www.theguardian.com/uk/2011/may/30/military-cyberwar-offensive: Accessed July, 05, 2019.

Hosang, H. B. (2016). Rules of Engagement and Targeting. In *Targeting: The challenges of modern warfare*: 159-174. TMC Asser Press, The Hague.

Huang, Z., Shen, C.C., Doshi, S., Thomas, N. & Duong, H. (2016). Fuzzy sets based team decision-making for Cyber Situation Awareness, In: IEEE 33th International Conference on Military Communications, pp. 1077-1082.

Iacono, J., Brown, A. & Holtham, C. (2009). Research Methods--a Case Example of Participant Observation. *Electronic journal of business research methods* 7,1.

IBM (2019). *National security and intelligence*. https://www.ibm.com/industries/federal/national-security: Accessed July, 05, 2019.

International Committee of the Red Cross (1868). Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November / 11 December 1868. *IHL Database.*

International Committee of the Red Cross (2004). *What is International Humanitarian Law?* ICRC Report.

International Committee of the Red Cross (2011). *International Humanitarian Law and the challenges of contemporary armed conflicts*. ICRC Report.

International Committee of the Red Cross (2013). *Decision-making process in military combat operations*. ICRC Reference.

International Committee of the Red Cross (2015). *What are jus ad bellum and jus in bello?*. ICRC Report.

INTEL.GOV. Clear and present danger: cyber-crime, cyber-espionage, cyber-terror, cyber-war. https://www.intelligence.gov/index.php/ic-on-the-record-database/results/40-clear-and-present-danger-cyber-crime-cyber-espionage-cyber-terror-and-cyber-war-video: Accessed June, 12, 2019.

International Telecommunication Union (2011). *ITU National Cyber Security Strategy*.

ISO (2012). ISO/IEC 27032: 2012 Information technology – Security technologies – Guidelines for cybersecurity.

Jachec-Neale, A. (2014). *The concept of military objectives in international law and targeting practice;* Routledge, 204.

Jansen, M. (2006). The Phantom Agony. Epica. https://www.youtube.com/watch?v=UAlRf9qf9d0&list=RDEMUhaj5LvG1RbRiTEA7Rp0kQ&index=2: Accessed July, 11, 2019.

Jensen, B. & Banks, D. (2018). *Cyber Operations in conflict: lessons learned from analytic wargames*. Center for long term Cyber Security.
Krueger, R. A., & Casey, M.A. (2002). Designing and conducting focus group interviews.

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. Sage.

Joint Targeting School (2014). *Joint Fires and Targeting Student Guide*.

Krueger, R.A. & Casey, M.A. (2014). *Focus groups: a practical guide for applied research,* Sage Publications.

Kulkarni, S.S., Rai, H.M. & Singla, S. (2012). Design of an effective substitution cipher algorithm for information security using Fuzzy Logic, *International Journal of Innovations in Engineering and Technology*, 1(2).

Kumar, S.S. & Kathiresan, V. (2016). Alert system for controlling cyberbullying words using Fuzzy Logic and Fuzzy Inference Engine. *Asian Journal of Computer Science and Technology*, 5(2), pp. 29-31.

Langner, R. (2013). To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve, *The Langner Group*.

Lehto, M. (2016). Theoretical examination of the Cyber Warfare environment. Proceedings of the International Conference on Cyber Warfare and Security (pp. 223-230).

Levesque, H. J. (1986). Knowledge representation and reasoning. *Annual review of computer science*, 1(1), pp. 255-287.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation.

Lucas, P., & Van Der Gaag, L. (1991). *Principles of expert systems*. Wokingham: Addison-Wesley.

Luban, D. (2013). Military necessity and the cultures of military law. *Leiden Journal of International Law*, *26*.2: 315-349.

Łukasiewicz, D. (2011). On Jan Łukasiewicz's many-valued logic and his criticism of determinism. *Philosophia Scientiæ. Travaux d'histoire et de philosophie des sciences*, (15-2), pp. 7-20.

Maathuis, C., Pieters, W. & Berg, v.d. J. (2016). Cyber Weapons: a Profiling Framework. In Proceedings of the 1st International Conference on Cyber Conflict U.S. (pp. 1-8). IEEE.

Maathuis, C., Pieters, W. & v.d. Berg, J. (2018). Developing a computational ontology for Cyber Operations, Journal of Information Warfare, 17(3):32-51.

Mach, K. J., Mastrandrea, M. D., Freeman, P. T., & Field, C. B. (2017). Unleashing expert judgment in assessment. Global environmental change, 44, 1-14.

Malcolm, S.N. (2008). *International Law*. Cambridge University Press, 1167.

March, S., & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*, pp. 251–266.

Martin, R. (2018). 10 ways Artificial Intelligence is transforming healthcare. Ignite. https://igniteoutsourcing.com/healthcare/artificial-intelligence-in-healthcare/: Accessed July, 05, 2019.

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98). IEEE.

McCorduck, P., Minsky, M., Selfridge, O. G., & Simon, H. A. (1977). History of Artificial Intelligence. In *IJCAI* (pp. 951-954).

McDonald, G, Murchu, LO, Doherty, S & Chien, E. (2013). *Stuxnet 0.5: The missing link*, Symantec Security Response, Cupertino, CA, US.

McNeal, G. S. (2013). Targeted killing and accountability. *Geo. lj*, *102*, 681, pp. 8.

Melzer, N. (2008). *Targeted killing in international law*. Oxford.

MindTitan. Artificial Intelligence in aviation/travel. https://www.mindtitan.com/case/artificial-intelligence-in-aviation-and-travel/: Accessed July, 05, 2019.

Mishra, N., & Jha, P. (2014). Fuzzy expert system and its utility in various field. *Recent Research in Science and Technology*, *6*(1).

Mitchell, A., Dodge, B. H., Kruzic, P. G., Miller, D. C., & Schwartz, P. (1975). *Handbook of forecasting techniques*. Stanford Research Inst Menlo Park Ca Center For The Study Of Social Policy.

Munakata, T. (2008). *Fundamentals of the new artificial intelligence: neural, evolutionary, fuzzy and more*. Springer Science & Business Media.

NATO (2011). *Collateral Damage Estimation*.

NATO (2016). *NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting*. NATO Standardization Office.

NATO (2013). *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim 2.0*.

NATO (2016b). Cyber defence. http://www.nato.int/cps/en/natohq/topics_78170.htm: Accessed June 15, 2019.

Negnevitsky, M. (2005). *Artificial intelligence: a guide to intelligent systems*. Pearson education.

NLTimes. (2019). https://nltimes.nl/2019/09/03/netherlands-played-crucial-role-sabotaging-irans-nuclear-program-report: Accessed September 10, 2019.

Noll, G. (2012). Analogy at war: proportionality, equality and the law of targeting. *Netherlands yearbook of international law*, *43*, 205-230.

Odobleja, S. (1938). *Psychologie consonantiste*. Librairie Maloine, 1.

Odobleja, S. (1939). *Psychologie consonantiste*. Librairie Maloine, 2.

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. In Proceedings of the 4th International

Conference on Design Science Research in Information Systems and Technology. ACM, p. 7.

Oliveira, A. (2010). Using the Military Instrument in Conflict Resolution: A Changing Paradigm. *JANUS. NET, e-journal of International Relations,* 1, 1, 45-58.

Onwuegbuzie, A. J., Dickinson, W. B., Leech, N. L., & Zoran, A. G. (2009). A qualitative framework for collecting and analyzing data in focus group research. *International journal of qualitative methods*, *8*(3), 1-21.

Owen, T. (1988). Artificial Intelligence. *Robotica.* Patrick Henry Winston Addison-Wesley Publishing Company, 6(2), pp. 165-165.

Oxford Institute for Ethics, Law, and Armed Conflict. (2009). Proportionality in War. Workshop Report. Symposium Conveyed by the Oxford Institute for Ethics, Law, and Armed Conflict.

Paull, L., Severac, G., Raffo, G. V., Angel, J. M., Boley, H., Durst, P. J., ... & Saeedi, S. (2012). Towards an ontology for autonomous robots. In 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (pp. 1359-1364). IEEE.

Pfeffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The design science research process: A model for producing and presenting information systems research. In Proceedings of the First International Conference on Design Science Research in Information Systems and Technology,pp. 83-106.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chaterrjee, A. (2008). A Design Science Research Methodology for Information Systems Research, *Journal of Management of Information Systems*. 2008, 24(3), pp. 45-78.

Pohoata, G. (2016). Consonantist psychology and cybernetics from T. Odobleja to N. Wiener. *Euromentor Journal* 7, 3, pp. 17.

Pricop, E., Mihalache, S.F. & Fattahi, J. (2016). Innovative fuzzy approach on analyzing industrial control systems security. *Recent Advances in Systems Safety and Security*. Springer, 223-239.

Raboin, B. (2011). Corresponding evolution: international law and the emergence of Cyber Warfare. https://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5/: Accessed July, 05, 2019.

Rabunal, J. R., Dorado, J. & Alejandro, P. S. (Eds.) (2009). *Encyclopedia of artificial intelligence*. IGI Global Snippet.

Randall, D., Shrobe, H. & Szolovits, P. (1993). What is a knowledge representation? *AI magazine,* 14(1), pp. 17-17.

Remenyi, D. (2012). Field methods for academic research: Interviews, focus groups and questionnaires. The business and management series. *Reading, UK: Academic Publishing International*.

Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies* 35.1, pp. 5-32.

Roth, M. (2019). Artificial Intelligence in the Military – An overview of capabilities. https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/: Accessed July, 05, 2019.

Romanosky, Z. & Goldman, Z. (2017). Understanding cyber collateral damage. Journal of National Security Law and Policy, 9, 233.

Rospocher, M., & Serafini, L. (2012). An ontological framework for decision support. *Proceedings of Joint International Semantic Technology Conference*, Springer, pp. 239-254.

Roussey, C, Pinet F, Kang, MA & Corcho O (2011). An introduction to ontologies and ontology engineering', G Falquet, C Métral, J Teller & C Tweed (Eds.), *Ontologies in urban development projects*. Springer, 1, pp. 9-38.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson Education Limited.

Samad-Soltani, T., Ghanei, M., & Langarizadeh, M. (2015). Development of a fuzzy decision support system to determine the severity of obstructive pulmonary in chemical injured victims. *Acta Informatica Medica*, *23*(3), 138.

Sanzogni, L., Guzman, G. & Busch, P. (2017). Artificial intelligence and knowledge management: questioning the tacit dimension. *Prometheus* 35(1), pp. 37-56.

Sander, B. (2019). The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-21). IEEE.

Sargolzaei, A., Crane, C. D., Abbaspour, A., & Noei, S. (2016). A machine learning approach for fault detection in vehicular cyber-physical systems. In 2016 15th IEEE International Conference on Machine Learning and Applications (pp. 636-640). IEEE.

Saunders, M., Lewis, P. & Thornhill, T. (2009). Understanding research philosophies and approaches. *Research methods for business students,* 4(1), pp.106-135.

Schmitt, M. N. (2011). Military necessity and humanity in international humanitarian law: preserving the delicate balance. In *Essays on Law and War at the Fault Lines:*89-129. TMC Asser Press.

Schmitt, M.N. (Ed.). (2013). *Tallinn Manual on the international law applicable to cyber warfare.* Cambridge University Press, pp. 68, 80.

Schmitt, M.N. (Ed.). (2017). *Tallinn Manual 2.0. on the international law applicable to cyber operations*. Cambridge University Press, pp. 451.

Schreier, F. (2015). *On cyberwarfare*. Geneva Centre for the Democratic Control of Armed Forces.

Simon, H. (1996). *The sciences of the artificial* (3rd ed.). MIT Press.

Singh, R., Singh, J., & Singh, R. (2017). Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. *Wireless Communications and Mobile Computing*.

Singhal, A. & Hema, B. (2013). Fuzzy logic approach for threat prioritization in Agile security framework using DREAD model, arXiv preprint arXiv: 1312.6836(2013).

Smart, S.J. (2010). Joint Targeting in Cyberspace. Headquarters U.S. Air Force.

Smith, E.S. (1995). *An application of fuzzy logic control to a classical military tracking problem*. United States Naval Academy.

Solce, N. (2008). The battlefield of cyberspace: The inevitable new military branch-the cyber force. *Alb. LJ Sci. & Tech.*, *18*.

Staab, S., and Studer, R. (Eds.) (2010). *Handbook on ontologies*. Springer Science & Business Media.

Stefik, M. (2014). *Introduction to knowledge systems*. Elsevier.

Stevens, C. (2019) "Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet." *Contemporary Security Policy*, 41.1: 129-152.

Stone, J. (2013). Cyber war will take place!. *Journal of Strategic Studies*, *36*(1), pp. 101-108.

Theohary, C. A., & Harrington, A. I. (2015). *Cyber Operations in DOD Policy and Plans: Issues for Congress*. Congressional Research Service.

Tremblay, M. C., Hevner, A. R., & Berndt, D. J. (2010). The use of focus groups in design science research. In *Design Research in Information Systems*. Springer, pp. 121-143.

Tremblay, M. C., Hevner, A. R., & Berndt, D. J. (2010b). Focus groups for artifact refinement and evaluation in design research. *Cais*, *26*(27), pp. 599-618.

Turns, D. (2012). *Military Necessity*. Oxford University Press.

Turban, E., Aronson, J.E., Liang, T.-P. (2007). *Decision Support System and Intelligent System.* Prentice Hall, Upper Saddle River.

Tyugu, E. (2011). Artificial intelligence in cyber defense. In *Proceedings of the 3rd International Conference on Cyber Conflict* (pp. 1-11). IEEE.

U.K. Ministry of Defense (2010). UK Manual of the Law of Armed Conflict.

U.K. Ministry of Defense (2016). Cyber Primer. Development, Concepts and Doctrine Center.

United States Army (2003). *Joint Publication 2-01.1 Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting*. United States Army.

United States Army (2010). The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028. TRADOC Pamphlet 525-7-8.

United States Army (2012). *No – strike and Collateral Damage Estimation Methodology.* United States Army.

United States Army (2013). *Joint Publication 3-60 Joint Targeting*. United States Army.

United States Army (2013). Joint Publication 3-12 (R). *Cyberspace Operations*. United States Army.

United States Army (2015). *ATP 3 – 60. Targeting*. United States Army.

United States Army (2016). *Joint Publication 1-04 Legal Support to Military Operations.* United States Army.

United States Army (2016b). *Cyberspace Operations Concept Capability Plan 2016-2018.* United States Army.

United States Army (2018). Joint Publication 3-12. *Cyberspace Operations*. United States Army.

United States Department of Defense (2019). *Dictionary of Military and Associated Terms*, 69.

Uschold, M. & Gruninger, M. (1996). Ontologies: principles, methods and applications. *The Knowledge Engineering Review*, 11(2), 93-136.

Vaishnavi, V. K., & Kuechler Jr, W. (2008). *Design science research methods and patterns. Innovating information and communication technology*. Boca Raton: Auerbach Publications, Taylor & Francis Group.

Vinik, D. (2015). America's secret arsenal. https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331: Accessed July, 05, 2019.

Vlada, M., & Adascalitei, A. (2017). Stefan Odobleja: A scientific visionary, precursor of Cybernetics and Artificial Intelligence. *On Virtual Learning*, 44.

Warner, M. (2012). Cybersecurity: a pre-history." *Intelligence and National Security,* 27, 5, pp. 781-799.

Watzlawick, P. (Ed.). (1980). *The Invented Reality: How Do We Know What We Believe We Know?* W. W. Norton & Company.

Weissbrodt, D. (2013) Cyber-conflict, Cyber-crime, and Cyber-espionage." *Minnesota Journal of International Law*, *22*, 347.

Whittemore, L. A. (2015). Proportionality Decision Making in Targeting: Heuristics, Cognitive Biases, and the Law. *Harvard National Security Journal*, *7*, 577.

Worley, R. (2012). *A Critical Examination of the U.S. National Security System*. Center for Advanced Governmental Studies. John Hopkins University.

Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine*. Technology Press.

Yin, R.K. & Campbell, D.T. (2008). *Case Study Research*. Sage Publications Inc.

Yun, J., Hong, S. S., & Han, M. M. (2012). A dynamic neuro fuzzy knowledge based system in threat evaluation. In The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems (pp. 1601-1605). IEEE.

Zadeh, L. A. (1965). Fuzzy sets. *Information and control*, 8(3), pp. 338-353.

Zadeh, L. A. (1975a). The concept of a linguistic variable and its application to approximate reasoning I. *Information sciences,* 8(3), pp. 199-249.

Zadeh, L. A. (1975b). The concept of a linguistic variable and its application to approximate reasoning II. *Information sciences.* 8(4), pp. 301-357.

Zadeh, L. A. (1975c). The concept of a linguistic variable and its application to approximate reasoning-III. *Information sciences*, *9*(1), pp. 43-80.

Zadeh, L. A. (1989). Knowledge representation in fuzzy logic. *IEEE Transactions on knowledge and data engineering*, *1*(1), pp. 89-100.

Zetter, K 2015, *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*, Crown Publishing Group, New York, NY, US.

Chapter 2. Cyber Operations

"We're the day birds
Deciding to fly against the sky
Within our dreams, we all wake up
To kiss the ones who are born to die."
*(*Serj Tankian – Harakiri)

Based on Maathuis, C., Pieters, W. & van den Berg, J. 2018, "Developing a Computational Ontology for Cyber Operations", 2018, *Journal of Information Warfare*, vol. 17, issue 3.

Based on Maathuis, C., Pieters, W. & van den Berg, J. 2018, 'A Computational Ontology for Cyber Operations', *Proceedings of the 17th European Conference on Cyber Warfare and Security,* pp. 278-288.

Cyber Operations lack models, methodologies, and mechanisms to describe relevant data and knowledge. This problem is directly reflected when Cyber Operations are conducted and their effects assessed, and it can produce dissonance and disturbance in corresponding decision-making processes and communication between different military actors. To tackle these issues, this chapter proposes a knowledge model for cyber operations implemented as a computational ontology following a design science approach grounded on extensive technical-military research. This model classifies the essential entities of cyber operations and was exemplified on three case studies; validation results show that this model can be used to describe cyber operations clearly and concisely.

Keywords: Cyber Operations, Cyber Warfare, Cyber Weapons, Cyber Security, Artificial Intelligence, Data Science, Ontology.

2.1. Introduction

Frederick the Great considered that for war "a great deal of knowledge, study and meditation is necessary to conduct it well" (Luvaas, 2001). However, interpreting this quote nowadays can be challenging since societies deal with data, information, and knowledge that empower and revoke participant actors in (un)foreseeable ways. Considering the innovations and advancements in the ICT domain, military actors are able to fight their adversaries in traditional warfare domains, as well as in cyberspace. This is reflected in how they understand, conduct, and deal with Cyber Operations. A decade ago – shortly before, during, and shortly after the Russo-Georgian war (August 2008) – a series of Cyber Operations were conducted against Georgia by undermining its governmental communication capabilities at national and international levels. It was a war planned and conducted on multiple battlefields which impacted Georgia's national security (Beidleman, 2009) and caused significant psychological effects (Shakarian et al., 2013). Cyber Operations acted as a force multiplier in active combat (Willems, 2011) and since then opened long academic debates focused on analysing the incident itself or different aspects through technical, military, or military-legal lenses (Schmitt, 2012; Schmitt, 2013; Ottis, 2015; Barrett, 2015).

A decade after, although other Cyber Operations were conducted, such as the ones in Ukraine, there is still no international consensus regarding their meaning, their definition, or a way to represent them. Currently, different countries are integrating Cyber Operations into traditional warfare surfaces (Lewis, 2015), and these countries acquire or invest in cyber warriors to get the necessary knowledge, skills, and abilities

(Li & Daugherty, 2015; Arimatsu, 2012). Since different actors may be involved in different Cyber Operations phases, lacking an agreed-upon meaning can directly impact their ability to achieve military objectives.

Addressing both a scientific and societal gap regarding understanding Cyber Operations, this chapter began as a piece presented at the 2018 ECCWS conference (Maathuis et al., 2018) by providing a supplementary way of using the model as well as a third case study (conducted in Ukraine) for exemplification.

Hence, this chapter proposes a knowledge/data model for Cyber Operations that elaborates and supports the proposed Cyber Operations definition; provides and shares a common understanding of entities and relations involved in Cyber Operations by illustrating them in different case studies and in practical use; and raises the level of awareness and responsibility of decision makers, security experts, and academics when reasoning about the effects of Cyber Operations that could be contributing to (the process of) designing doctrines, strategies, and methodologies for Cyber Operations.

The remainder of this chapter is structured as follows. The second section discusses related research. The third section presents a multidisciplinary definition for Cyber Operations and stresses the necessity of introducing a model that offers a knowledge/data-based representation for Cyber Operations to enable simulation of them in any life-cycle phase. The fourth section discusses the methodology used to design, develop, and evaluate the proposed model-a Cyber Operations computational ontology. The fifth section describes the model's design and correspondent decisions for implementation. The sixth section presents the model's implementation in Protégé and illustrates a way to use it. The seventh section presents the validation mechanism, in terms of both technical and expert validation. The eighth section analyses how the model is exemplified in three case studies to reflect its functionality and applicability in real-world settings. The last section discusses possible extensions, reflections, and future research.

2.2. Related Research

In recent years, a growing number of studies on ontologies were proposed in the cyber security domain which aimed to describe notions such as vulnerability, threat, and attack vector (Obrst et al., 2012; National Institute of Standards and Technology, 2014; Syed et al., 2016), defense technologies (NIST, 2014; Ben-Asher et al., 2015), digital forensics (Ćosić & Ćosić, 2012), intrusion detection (Undercoffer et al., 2003), cyber-

physical systems (Smirnov et al., 2018; Sun et al., 2016) and human factors (Oltramari et al., 2015). These studies can also be used to understand some of the entities participating in Cyber Warfare, for instance, the vulnerabilities embedded by targets exploited in Cyber Operations. However, only a limited number of studies aimed at designing ontologies for Cyber Warfare or conflict exist. Applegate & Stavrou (2013) already identified participant entities in cyberspace conflicts, such as actors and types of impact, but did not formalise them. On modelling network operations, Oltramari et al. (2015) propose a theoretical ontology that contributes to predicting and preventing cyberattacks but needs further reflection and extension in real case scenarios in the cyber realm. Furthermore, the initial stage of a cyber-network attack-planning ontology aiming at supporting the planning of Cyber Operations was introduced by Chan et al. (2015).

As this research interprets and embeds ontology in a Computer Science/Artificial Intelligence way, a series of prerequisites must be fulfilled to enable the design, development, and evaluation of the ontology. Since both cyber security and military reasoning are considered by Dipert (2013), his proposed requirements, which are both universal and widely applicable, were adopted in this research. Dipert (2013) scrutinised these requirements in order to support the development of a fundamental ontology for Cyber Warfare for standardisation purposes.

2.3. Methodology

To be able to formalise Cyber Operations by means of a computational ontology, this research relies on different multidisciplinary resources in a triangulating manner (Yin, 2003). Ontology Engineering translates the philosophical understanding of ontology to the Computer Science and Artificial Intelligence domains by using different methodologies to implement a computational ontology. The 'methontology' methodology (Fernández-López et al., 1997) was selected for use because it is grounded in an extensive survey of literature, reports, and military doctrine, combined with direct participation and observation in joint military exercises. At the same time, the necessary features of a Cyber Warfare ontology proposed by Dipert (2013) were followed. Additionally, one of the authors' experience in planning and conducting Cyber Operations as (cyber) war games resonates in the mechanism of conducting in-depth case studies on Georgia, Iran (Stuxnet), and Ukraine as exemplifying cases for the proposed model.

Ontology Engineering methodologies are used to design formal models of different domains and aspects of reality by constructing a

knowledge/data model, conceptualising the world of interest, and proposing definitions of entities and relationships, which not only allows knowledge to be accumulated, computed, and accessed, but also shared among different audiences and communities (Fernández-López et al., 1997; Mizoguchi & Ikeda, 1998; Roussey et al., 2011; d'Aquin et al., 2012).

The methodology in this research was selected because it is also one of the most comprehensive and used Ontology Engineering methodologies (Paquette, 2010). This methodology presupposes implementing computational ontologies from scratch or using existing ones, is fully compatible with *IEEE 1074-2006 Standard for Developing Software Project Life Cycle Process*, and is aligned with the requirements of Dipert (2013). In this sense, each phase of the followed methodology is elaborated as follows (Fernández-López et al., 1997; Sawsaa & Lu, 2012):

- Specification: the purpose, requirements, and knowledge are established to represent Cyber Operations as military operations.
- Knowledge acquisition: the necessary information for building the model is collected from the abovementioned resources.
- Conceptualisation: the knowledge gathered is structured as a formal model in the formof a taxonomy with concepts, meanings, and attributes that describe Cyber Operations.
- Formalisation: the knowledge model is formalised and has the following classes: Context, Actor, Type, MilitaryObjective, Phase, Target, CyberWeapon, Asset,Geolocation, Action, and Effect.
- Integration: other ontologies were reviewed and are presented in the Related Worksection. However, the proposed ontology was designed from scratch.
- Implementation: the knowledge engineering environment for building intelligent systems – Protégé – is prepared to develop the model using Ontology Web Language(OWL) and describe the knowledge about entities, groups of entities, and relations between entities.
- Maintenance: the model is refined and updated so that actions such as modifying, adding, and removing concepts and definitions are possible.
- Evaluation: the structure/consistency evaluation and the military experts' evaluation (see Appendices-Annex G) are carried out together with exemplification on three real cases of cyber operations performed in Georgia, Iran (Stuxnet), and Ukraine.
- Documentation: this phase occurs during the entire process of design and development of the new model and requires a detailed description of contained concepts and relations between these concepts. Such a description is presented in the following section.

2.4. Defining Cyber Operations

Most wars do not involve just state-on-state military confrontations (Brown, 2017). Non-state actors can also conduct Cyber Operations, which can lead to global (and even devastating) implications and consequences impacting not only the targeted adversaries, but also other actors such as the neutral or friendly ones, and even the attackers themselves. Caton (2015) argues that Cyber Operations "have been ongoing since before the advent of the Internet, and their influence on traditional Military Operations continues to increase". Indeed, they can be found now globally integrated into military commanders' toolboxes as means and methods to achieve political goals and military objectives by synchronising activities and actions in all warfare domains.

This research is aligned with the vision of Herr & Herrick (2016), which stresses the need for understanding Cyber Operations and describes them as "the acquisition and use of cyber capabilities at the strategic, operational, and tactical levels of conflict". To that end, this research calls for a unified definition for Cyber Operations before engaging in designing and developing a model that represents its surrounding knowledge and serves as a knowledge-based simulation environment useful in all its life cycle phases. At the same time, this definition is necessary because the level of awareness and reasoning of the participating communities (cyber, military, military-legal) needs to be raised to insure the unification of effort between the different experts who compose them. Therefore, the following multidisciplinary definition of 'Cyber Operation' is essential and is proposed based on extensive review of scientific literature, reports, and military doctrine:

A Cyber Operation is a type of or a part of a military operation in which cyber weapons/capabilities are used to achieve military objectives in front of adversaries inside and/or outside cyberspace.

The following apply to the proposed definition:

- As 'a type of or a part of a military operation'**,** a Cyber Operation can be either an independent military operation or a part of a broader military operation in a supporting role.
- 'Cyber weapons/capabilities' are programs or scripts employed to achieve military objectives (Maathuis et al., 2016).
- 'To achieve military objectives' implies to accomplish military goals by engaging targets in cyber operations.
- 'In front of adversaries' refers to the opponents participating in the Cyber Operation.

– ‘Inside and/or outside cyberspace’ recognises that although Cyber Operations act on different cyberspace entities, their effects are borderless since they cross geographical and virtual borders. They impact targets as well as collateral assets which are distinct from the engaged targets.

2.5. Model Design

Section 2.3. presented the approach followed in this research. Hence, to be able to understand the rationale behind the design of the proposed model, the design requirements and the followed design decisions are described here. This research follows the requirements for a Cyber Warfare ontology established by Dipert (2013) along with experience writing Cyber Operations scenarios, and direct participation and observation in joint military operations exercises, facts also reflected in other lines of research. To the best of the authors’ knowledge, this set of requirements is the only one proposed in the existing scientific literature, and we have introduced a computational ontology for Cyber Operations for the first time in 2018.

The design requirements considered by Dipert (2013) are:

– to be humanly understandable by using controlled vocabularies;
– to be an ontology that uses widely known and accepted concepts;
– to be represented in one of the best available languages for formalising ontologies, suchas OWL or Common Logic; and,
– to be able to apply methodologies for building ontologies and for illustrating instance-level data.

At the end of these phases, the taxonomical representation of the proposed model contains the following upper classes: Context, Actor, Type, MilitaryObjective, Phase, Target, CyberWeapon, Asset, Geolocation, Action, and Effect. These classes map the components of the proposed definition for Cyber Operations and are depicted in Table 2.1, below.

Elements of the cyber operations definition	Mapping on cyber operations upper classes
A type of a part of a military operation	Context, MilitaryObjective
Cyber weapons/capabilities	CyberWeapon
To achieve military objectives	Context, MilitaryObjective, Type,

	Phase
In front of adversaries	Actor, Type, Phase, Target, Geolocation
Inside and/or outside cyberspace	Target, Geolocation, Asset, Effect

Table 2.1: Mapping between the components of the proposed Cyber Operations definition and the upper classes of the proposed model

The first four phases of the methodological approach – specification, knowledge acquisition, conceptualisation and formalisation – are the steps followed to design the artefact (computational ontology model) in a design science approach (Hevner et al., 2004).

Based on (Russell & Norvig, 2016; Fernández-López et al., 1997; Roussey et al., 2011; d'Aquin et al., 2012), we can define the proposed model as a quadruple (i.e. group of four sets or elements):

Definition 1

$$CO\_ONT = \{E, P, R, I\}$$

that contains the following elements:

- *E* as the set of entities (i.e. classes or nodes) as main concepts that define the context.
- *P* as the set of properties or attributes that characterize the entities (i.e. data properties).
- *R* as the set of relationships between entities through their instantiations (i.e. object properties).
- *I* as the set of instances/objects/data values of entities.

Furthermore, each upper class was elaborated to consider concepts and relations (subclasses and properties) between them in the way of representing its knowledge using known and accepted concepts from cyber, military, and military-legal domains. Consequently, the initial design of the proposed ontology was established and proposed for evaluation.

2.6. Model Implementation and Use

Once the initial design was established, the ontology was further developed in the knowledge engineering environment named Protégé as a set of structured concepts together with relationships between these concepts organised in a logical way. Afterwards, the double process of evaluation (technical and expert based) was carried out, and small changes

were applied to the Actor and Target classes. These changes are presented in the Validation section. Hence, the final form of the proposed model was accordingly implemented; contains 140 classes, 53 individuals (instances), and 96 (55 data and 41 object) properties; and is depicted in Figure 2.1., where classes marked with + are further extended.

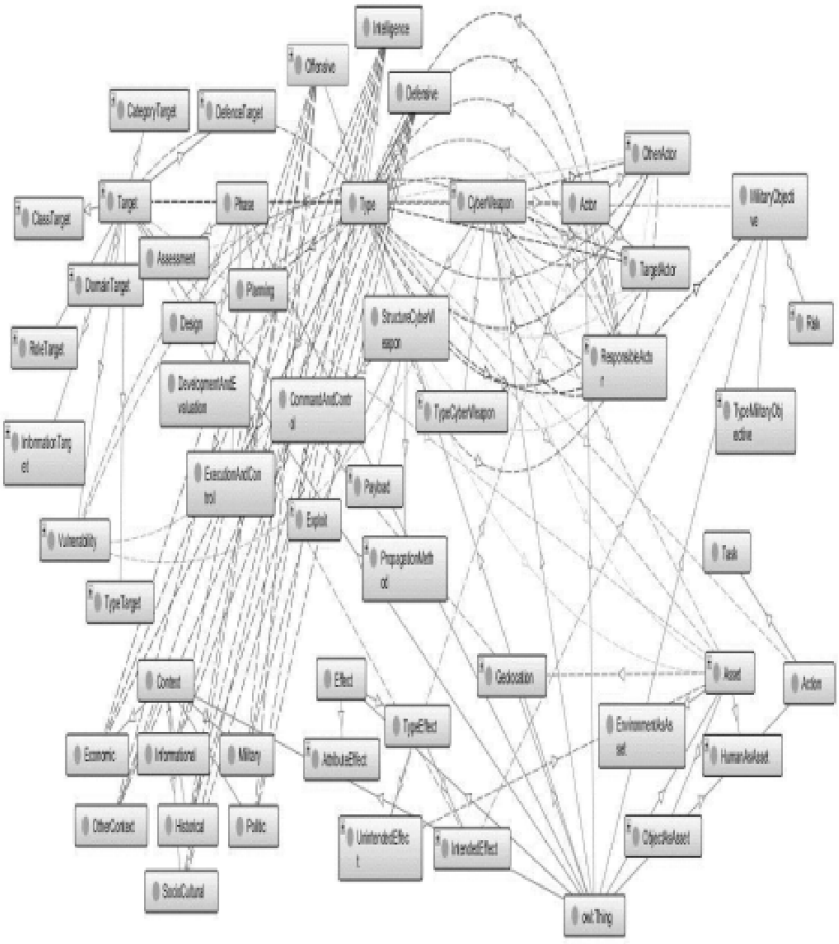


Figure 2.1. Cyber operations ontology classes hierarchy

Ontologies represent a context-dependent projection of a reality. In this way, the proposed ontology is organised as a collection of entities that describe the universe of Cyber Operations structured on four levels, as discussed below.

Level 1 contains the upper classes that can be found in set E and that are shown in Figure 2.2., below. They are mapped based upon the concept of Cyber Operations, specifically the use of cyber weapons as

described by United States Army (2013), Williams (2014), and by Maathuis et al. (2016). In the figure below, the entity owl:Thing represents the mother of all classes (e.g. the highest upper-class also named as the root class), it defines the fundamental or basic state or behaviour of all classes and corresponding objects, and is the equivalent of the class Object from Java programming language.

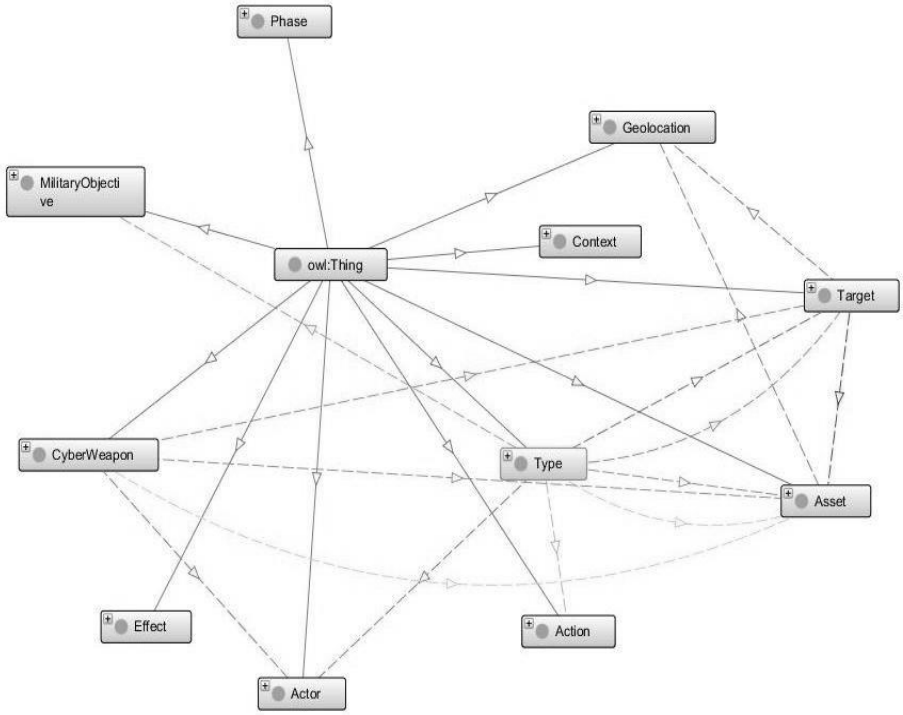


Figure 2.2. Cyber Operations ontology upper classes

The classes are described as follows:

- Context: the following dimensions: Political, Military, Economic, Informational, Historical, Sociocultural, and Other Context (keeping the argument of Arimatsu's (2012) that a broader context needs to be considered for Cyber Operations).
- Actor: distinct types of actors who are either responsible for planning, executing, or assessing Cyber Operations are the targeted ones or the ones unintentionally impacted by cyber operations.
- Type: distinct types of Cyber Operations, specifically offensive, defensive, and intelligence (United States Army, 2013; Williams, 2014).

- MilitaryObjective: the military goal or aim that actors want to achieve in Cyber Operations(Theonary & Harrington, 2015).
- Phase: the phases of Cyber Operations from planning to assessment.
- Target: a military entity (person or object) legally targetable in Cyber Operations (Liles et al., 2012).
- CyberWeapon: the means employed in Cyber Operations to achieve military objectives.
- Asset: either humans or objects unintentionally impacted in Cyber Operations.
- Geolocation: incorporated geolocation information about targets or assets.
- Action: the actions and tasks involved or performed in Cyber Operations.
- Effect: the implications and consequences of Cyber Operations. The intention criterion is decisive when classifying the effects of Cyber Operations: intended effects that support the achievement of military objectives (Military Advantage) by targets' engagement; and unintended effects that do not contribute to the achievement of military objectives, but do still unintentionally impact other assets (for instance, Collateral Damage).

Level 2 contains the sub-classes that can be found in set E and further extend and describe the upper classes, such as Offensive, Vulnerability, Exploit, and UnintendedEffect.

Level 3 contains the individual (instances) of classes that compose the ontology and that can be found in set I. This ontology, applied to cyber operations conducted in Georgia, Iran (Stuxnet) and Ukraine, is depicted in Figure 2.3., below.

Level 4 contains the relationships between classes and individuals, are found in sets P and R. They characterise classes (as attributes or data properties which are found in set P) as well as links between individuals (as relations or object properties which are found in set R), as depicted in Figure 2.4. below and further in the Appendix of this chapter.

Figure 2.3. Cyber operations ontology individuals

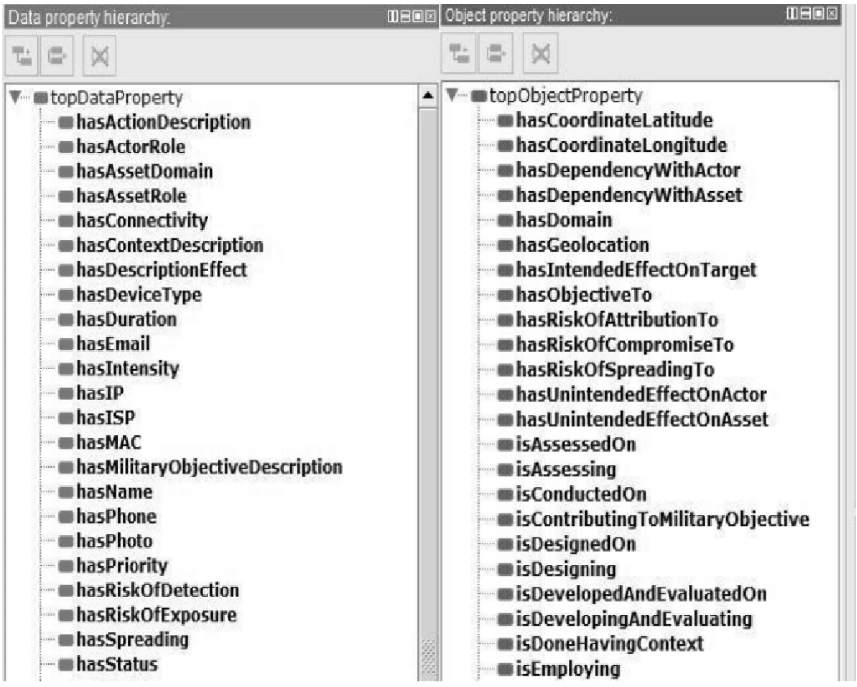


Figure 2.4. Cyber Operations ontology data and object properties

For instance, four data and object properties are described as follows:

- ‘hasMilitaryObjectiveDescription’ represents the military objective that needs to be achieved.
- ‘isExploiting’ reflects which vulnerability is exploited.
- ‘isDeliveringMilitaryAdvantage’ verifies whether or not a target delivers a military advantage.
- **‘**isProducingCollateralDamage’ checks if collateral damage is produced by engaging a target.

Therefore, a section of the universe of Cyber Operations is depicted as a complete picture, as shown in Figure 2.5., below. In this figure, contained classes, sub-classes as well as data and object properties can be identified.

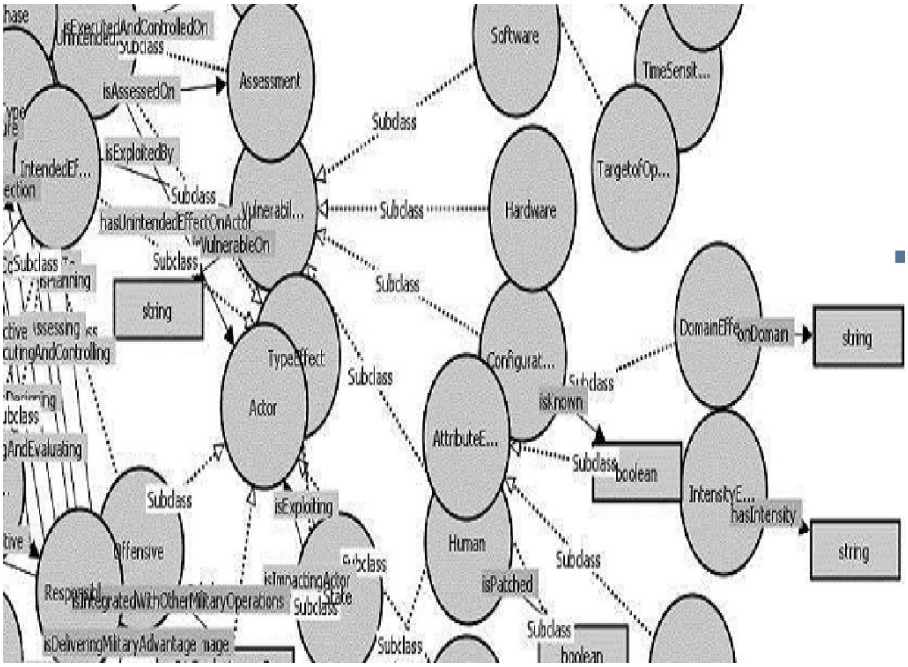


Figure 2.5. Cyber Operations universe containing classes and sub-classes, plus data and object properties

Computational ontologies are used effectively to model knowledge and deal with its representation and retrieval (Munir & Anjum, 2017). OWL has the highest level of expressivity compared to similar standards or languages, and allows great machine interpretability. It is also the AI-based ontology implementation language considered as a requirement by Dipert (2013). However, no matter which syntax is used to design and develop an

ontology (OWL, JSON [Java Script Object Notation], Turtle, for example), there are several ways of using it to allow automated extraction and visualisation. Furthermore, a way is presented using the SPARQL (Sparql Protocol and RDF Query Language) in Protégé. To illustrate, a query for extracting all classes, their subclasses, and individuals is depicted below in Figure 2.6.

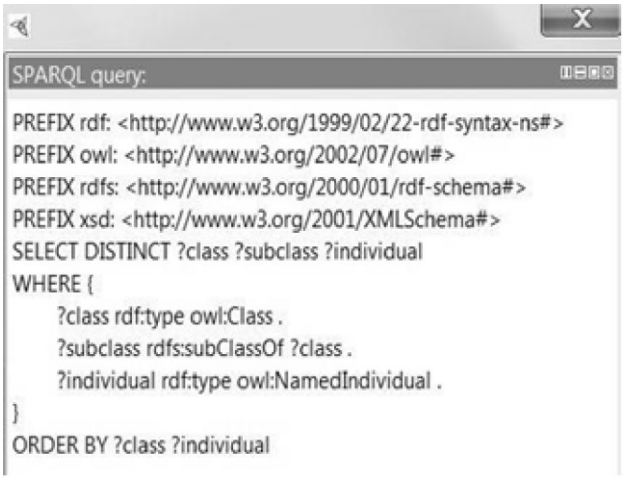


Figure 2.6. Example of SPARQL query for cyber operations ontology

This query can also be adapted to extract the exploitable vulnerabilities for considered targets using clauses such as *OPTIONAL* and *FILTER*.

2.7. Model Validation

There are two ways of evaluating and validating a developed computational ontology: technically based or expert based (Sawsaa & Lu, 2012). To make sure that the proposed model represents Cyber Operations in an accurate, clear, and concise way, both evaluation mechanisms were applied. This model is also exemplified by instantiation based on three case studies of Cyber Operations conducted in Georgia, Iran (Stuxnet), and Ukraine.

The technical evaluation applied considered indicators such as consistency and reusability (Sawsaa & Lu, 2012; Esposito et al., 2011), and was successful using the Hermit reasoner. The expert evaluation was conducted in a few rounds of meetings and reviews with two military-technical experts who had in average 20 years of international experience in

missions and operations. For the expert evaluation, indicators such as accuracy, clarity, conciseness, and adaptability (Vrandečić, 2009; Sawsaa & Lu, 2012) were considered as in Appendices-Annex G. Applying these criteria and stressing again the necessity of representing the knowledge that would assist and simulate Cyber Operations, the experts welcomed and agreed with the proposed model. After consideration, the experts recommended making minor changes, and the model was updated accordingly in the following three ways:

- Introducing 'target's role' in the sense of intended targets that can be attacked directly or through intermediary targets (Target class).
- Introducing 'targets of opportunity' as well as other possible targets (Target class).
- Introducing 'unknown actor' in recognition of the fact that limited to no information might be available to help attribute a Cyber Operation to an actor (Actor class).

After these updates were incorporated, the model reached its final state and met all the requirements of a Cyber Warfare ontology as proposed by Dipert (2013).

2.8. Case Studies of Cyber Operations

To exemplify the proposed model, three use cases were created based on extensive case study research (Yin, 2003) on Cyber Operations conducted in Georgia, Iran (Stuxnet), and Ukraine. Furthermore, each case study was briefly described. The case study regarding Georgia focused on the Cyber Operations conducted in 2008 surrounding the war between Russia and Georgia, that aimed at isolating or limiting Georgian communications of political and public assets at national and international levels. The case study focusing on Iran addressed the series of Cyber Operations or what can be seen as a long-term Cyber Operation discovered in 2010 (Operation Olympic Games/Stuxnet) conducted on Iranian nuclear facilities with the purpose of reducing the nuclear enrichment productivity as part of Iran's nuclear program. The case study with regard to Ukraine focused on the Cyber Operation (Black Energy 3) carried out in 2015 in Ukraine that targeted the Ukrainian power grid through different electricity distributors in Ivano-Frankivsk. Hence, Table 2.2, below, summarises all three case studies in order to exemplify both the proposed model and definition for Cyber Operations.

The goal of these case studies is to provide guidance and support to military and policy decision-makers when they encounter difficulties in

understanding and comprehending Cyber Operations. As this model explicitly reveals its main characteristics, it also plays an important role in clarifying the Cyber Operations phenomenon. Its use on these three case studies proves its effectiveness and applicability to real-world situations. Additionally, it exposes the strong relationships between entities such as Context, MilitaryObjective, and Effect since a MilitaryObjective finds its roots and motivations in the Context of a Cyber Operation, and the intended effects contribute to achieving the MilitaryObjective. Hence, these aspects are depicted for all three cases in Table 2.2. and demonstrate above all that the context of a Cyber Operation cannot be separated from the Cyber Operation itself if one wants to comprehend the effects. In other words, the implications and consequences of Cyber Operations.

Class	**Georgia**	**Iran (Stuxnet/Operation Olympic Games)**	**Ukraine (Black Energy 3)**
	(Grigolia, 2008; Swanson, 2010; Tikk et al., 2008; Nazario, 2009; Hollis, 2011; Mshvidobadze, 2015)	(Albright, 2003; Avramovic, 2007; Albright et al., 2008; Langner, 2013; Falliere et al., 2011; McDonald et al., 2013; Albright et al., 2012; Zetter, 2015)	(SANS, 2016; Fire Eye, 2016; GReAT, 2016; Liang et al., 2017; Damsky, 2016; Shamir, 2016; Sun et al., 2016; Department of Homeland Security, 2016)
Context	Political: tensions grounded on the independence aim of two Georgian regions, Abkhazia and South Ossetia supported by Russia. Military: Russo-Georgian war.	Political: tensions regarding the development of Iran's nuclear program. Military: the possibility of Iran investing in its nuclear program for military purposes.	Political: tensions grounded on the Russian annexation of Crimea and further resistance and protests. Military: a possible proof or demonstration of 'show of force', reply to previous Ukrainian activities, all backed by revealing and exploiting

			civilian/societal vulnerabilities.
Actor	Russia vs Georgia	U.S. and Israel vs Iran	SandWorm (Russia) vs Ukraine
Type	Offensive	Offensive	Offensive
MilitaryObjective	To (digitally) isolate Georgia and disrupt its ICT communications through governmental, media and financial websites.	To delay Iran's nuclear program.	To disrupt the information systems of three electricity distributors in order to produce service outages, a societal discomfort and influence public opinion.
Phase	Assessment	Assessment	Assessment
Target	Georgia's communication systems of governmental, media and financial institutions by exploiting software and configuration vulnerabilities.	Iran's nuclear facilities/program by exploiting software and human vulnerabilities.	Ukrainian power grip and electricity distribution companies in the Ivano-Frankivsk region.
CyberWeapon	Georgia	Stuxnet – Operation Olympic Games	Black Energy 3
Asset	Other systems and people/society.	Other facilities, systems and people/society.	Other facilities, systems and people/society.
Geolocation	Target: in Georgia. Asset: global (for example Georgia, Russia, Azerbaijan, U.S.).	Target: in Iran. Asset: global (for instance Indonesia, India, U.S.).	Target: in Ukraine. Asset: local and national (in Ukraine).
Action	(Part of) A Military Operation that took place around the war between the involved parties.	(Possible part of) A Military Operation that did not take place during war.	(Possible part of) A Military Operation that took place during the conflict in Eastern Ukraine

			and extended influential areas.
Effect	Intended: isolation, confusion and inconvenience in Georgia, as well as limiting communications access and use. Unintended: communications denial in supportive countries.	Intended: damage or destroy nuclear enrichment centrifuges by sabotaging them. Unintended: infecting other facilities and systems.	Intended: disruption or damage of power grid information systems. Unintended: future escalation and global exposure.

Table 2.2: Case studies exemplifying the proposed ontology for Cyber Operations

2.9. Conclusions

As different actors are integrating Cyber Operations in their military theatre of operations, it is necessary to understand what these new types of operations are to be able to represent and simulate, and it is necessary to understand how to use them properly to further deal with the effects of their actions. A way to do this was presented in this chapter as a joint venture of theoretical, empirical, and practical efforts. Hence, a knowledge/data model for Cyber Operations was proposed as a computational ontology in a Design Science Research approach implemented in Protégé. In this way, understanding, flexibility, and reusability (Tolk & Smith, 2011; Sawsaa & Lu, 2012) for composing entities and parties involved are ensured.

This research overcomes the current limits of the state of the art and contributes to the body of knowledge of cyber and military domains, and to the efforts of decision makers, security experts, and academic researchers when understanding what these operations mean and how to plan them or assess their effects. The results of this research accomplished the Cyber Warfare ontology requirements considered by Dipert (2013), were successfully evaluated technically and by military experts, and were exemplified on three Cyber Operations case studies on Georgia, Iran (Stuxnet), and Ukraine.

This research also contributes to the existing body of knowledge of Artificial Intelligence and Computer Science domains, and calls for their involvement when conducting research in Knowledge Modelling and Data Science useful in emerging or complex assessments and decision-making

processes. Possible extensions of this work can be considered by elaborating the classes Context and Effect to define more context dimensions and domains, attributes, and metrics of effects. Other extensions are also possible in the sense of representing Hybrid Warfare/Operations or Multi-Domain Operations possibly using (at least) the same upper classes structure to be able to (better) understand and represent different types of threats, ends, ways, and means.

An intrinsic limitation is that, when representing knowledge in the form of an ontology, there is not just one form that it can take since the knowledge representation formalism consists of different kinds of representations, depending on the perspective(s) and vision(s) that one has. An extrinsic limitation is that this model was instantiated using just three use cases due to the limited number of incidents publicly known and, implicitly, available empirical data(sets).

The proposed model represents a *machete* that can be further elaborated to understand, represent, and simulate current and new types of operations in all phases of their life cycles. The authors will be using these findings in their future research concerning the design of models and methodologies for assessing the effects of Cyber Operations.

2.10. Appendix

Attribute No	Attribute name	Attribute Definition	Characterizing class	Attribute Type
1	hasActionDescription	represents the action that should be taken to achieve the military objective.	Action	String
2	hasActorRole	represents the role of an actor.	Actor	String
3	hasAssetDomain	represents the domain or field where the asset belongs to.	Asset	String
4	hasAssetRole	represents the role or function of an asset.	Asset	String
5	hasConnectivity	represents a check mechanism to see if	Target	Boolean

		connectivity is up (value = 1 or TRUE) or down (value = 0 or FALSE).		
6	hasContext Description	represents the description of the context of a particular Cyber Operation.	Context	String
7	hasDescriptionEffect	represents the description of a particular effect of a Cyber Operation.	Effect	String
8	hasDeviceName	represents the name of the device.	Target	String
9	hasDuration	represent the duration of a particular effect of a Cyber Operation.	Effect	String
10	hasEmail	represents the e-mail of the target.	Target	String
11	hasIntensity	represents the (assessment of) intensity of a particular effect.	Effect	String
12	hasIP	represents the IP (Internet Protocol) address that could be represented using both ipv4 and ipv6 standards.	Target	String
13	hasISP	represents the name of the ISP (Internet Service Provider) of the target.	Target	String
14	hasMAC	represents the name of the MAC address (Media Access Control) of the target.	Target	String
15	hasMilitaryObjectiveDescription	represents the military objective that needs to be achieved in a particular Cyber Operation.	Actor	String
16	hasName	represents the name of an actor, target, and asset.	Actor, Target, Asset	String
17	hasPhone	represents the mobile / fix phone number of the target.	Target	String
18	hasPhoto	represents a reference to the photo of the target.	Target	String

19	hasPriority	represents the property assigned to the target.	Target	positiveInteger
20	hasRiskOfDetection	represents the assigned / assessed risk of detection for a particular cyber weapon.	CyberWeapon	String
21	hasSpreading	represents the scale / level of spreading of a particular effect.	Effect	String
22	hasStatus	represents the current status of a cyber weapon.	CyberWeapon	String

Table 2.3: Attributes / data properties for the proposed model

Relation No	Relation name	Relation Definition	Relation source class	Relation source destination
1	hasCoordinateLatitude	reflects the latitude coordinate of the target.	Target, Asset	Geolocation -> Latitude
2	hasCoordinateLongitude	reflects the longitude coordinate of the target.	Target, Asset	Geolocation -> Longitude
3	hasDependencyWithActor	shows dependencies between the actor conducting the Cyber Operation and other actor(s).	Responsible Actor	Actor -> OtherActor
4	hasDependencyWithAsset	shows dependencies between the target engaged in the Cyber Operation and other asset(s).	Target	Asset
5	hasDomain	depicts the network domain of the target and / or asset.	Target, Asset	Geolocation -> Domain
6	hasGeolocation	depicts the complete geolocation position for the target and / or asset.	Target, Asset	Geolocation
7	hasIntendedEffectOnTarget	illustrates the intended effects that impact the target.	IntendedEffect	Target
8	hasObjectiveTo	shows the military objective(s) of the Cyber Operation.	Type	MilitaryObjective

9	hasRiskOfAttributionTo	reflects the risk of attributing an effect of the Cyber Operation / cyber weapon to specific actor(s).	Type, CyberWeapon	Actor -> ResponsibleActor, Actor -> OtherActor
10	hasRiskOfCompromiseTo	reflects the risk of compromising other actors and / or even the one(s) responsible to conducting the Cyber Operation.	Type, CyberWeapon	Actor -> ResponsibleActor, Actor -> OtherActor, Actor -> TargetActor
11	hasRiskOfSpreadingTo	reflects the risk of spreading to other actors and / or even the one(s) responsible to conducting the Cyber Operation.	Type, CyberWeapon	Actor -> ResponsibleActor, Actor -> OtherActor, Actor -> TargetActor, Asset
12	hasUnintendedEffectOnActor	illustrates the unintended effects that impact an actor.	Unintended Effect	Actor
13	hasUnintendedEffectOnAsset	illustrates the intended effects that impact an asset.	Unintended Effect	Asset
14	isAssessedOn	shows when the Cyber Operation is assessed.	Type	Phase -> Assessment
15	isAssessing	shows that the responsible actor is assessing the executed Cyber Operation.	Actor -> Responsible Actor	Type
16	isConductedOn	reflects on what (i.e. actor and / or system) is the Cyber Operation conducted on.	Type	Target, Actor -> TargetActor
17	isConductingToMilitaryObjective	shows the contribution of intended effects to the achievement of military objectives.	IntendedEffect	MilitaryObjective
18	isDesignedOn	shows when the Cyber Operation is designed.	Type	Phase -> Design
19	isDesigning	shows that the responsible actor is	Actor -> Responsible	Type

		designing the executed Cyber Operation.	Actor	
20	isDevelopedAndEvaluatedOn	shows when the Cyber Operation is developed and evaluated.	Type	Phase -> DevelopmentAndEvaluation
21	isDevelopingAndEvaluating	shows that the responsible actor is developing and evaluating the executed Cyber Operation / or to be executed Cyber Operation.	Actor -> Responsible Actor	Type
22	isDoneHavingContext	reflects the multiple dimensions of the context that surrounding the Cyber Operation.	Type	Context
23	isEmploying	Shows the direct relation of employing the cyber weapon by one or more responsible actor(s).	Actor -> Responsible Actor	CyberWeapon

Table 2.4: Relations / object properties for the proposed model

2.11. References

Albright, D. Institute for Science and International Security (2003). “Iran at a nuclear crossroads”. http://isis-online.org/publications/iran/crossroads.html: Accessed November 12, 2017.

Albright, D., Brannan, P. & Shire, J. Institute for Science and International Security (2008). Can military strikes destroy centrifuge program? Probably not. Retrieved November 12, 2017, from https://www.isis-online.org/publications/iran/Centrifuge_Manufacturing_7August2008.pdf.

Albright, D., Brannan, P., Stricker, A., Walrond, C. & Wood, S.. Institute for Science and International Security (2012). Preventing Iran from getting nuclear weapons: Constraining its future nuclear options. Retrieved November 12, 2017, from https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf.

Avramovic, J. Institute for Science and International Security (2007). Iran’s nuclear program: What the 2008 presidential candidates are saying. Retrieved November 13, 2017, from http://www.isis-online.org/publications/iran/PresidentialCandidates.pdf.

Applegate, S.D. & Stavrou, A. (2013). Towards a cyber conflict taxonomy. Proceedings of the 5th IEEE International Conference on Cyber Conflict (pp. 1-8). IEEE.

Arimatsu, L. (2012). A treaty for governing cyber weapons: potential benefits and practical limitations. Proceedings of the 4th IEEE International Conference on Cyber Conflict (pp. 1-19). IEEE.

Barrett, E.T. (2015). Reliable old wineskins: The applicability of the just war tradition to military cyber operations. *Philosophy and Technology*, 28, 3, 387-405.

Beidleman, S.W. Defense Technical Information Center (2009). "Defining and deterring cyber war". http://www.dtic.mil/docs/citations/ADA500795: Accessed October 10, 2017.

Ben-Asher, N., Oltramari, A., Erbacher, R.F. & Gonzales, C. (2015). Ontology-based Adaptive Systems of Cyber Defense. *STIDS*, 34-41.

Brown, J. Over the horizon: Multi-Domain operations & Strategies (2017). "Making sense of irregular war". https://overthehorizonmdos.com/2017/04/19/making-sense-of-irregular-war/: Accessed April 19, 2017.

Caton, J.L. Strategic Studies Institute (2015). "Army support of military operations: Joint contexts and global escalation implications". http://www.strategicstudiesinstitute.army.mil/pubs/download. cfm?q=1246: Accessed November 6, 2017.

Chan, P., Theron, J., van Heerden, R. & Leenen, L. (2015). An ontological knowledge base for cyber network attack planning. Proceedings of the 10th International Conference on Cyber Warfare and Security (pp. 69).

Ćosić, J., & Ćosić, Z. (2012). The necessity of developing a digital evidence ontology. Proceedings of the Central European Conference on Information and Intelligent Systems (pp. 325-30).

Damsky, I. ThreatSTOP (2016). Black Energy Security Report. Retrieved February 3, 2016, from https://threatstop.com/sites/default/files/ThreatSTOP_BlackEnergy.pdf.

Department of Homeland Security (2016). “Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian critical infrastructure”. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-0: Accessed February 5, 2016.

Dipert, R. (2013). The essential features of an ontology for cyberwarfare. In P. Yannakogeorgos & A. Lowther (Eds.), *Conflict and cooperation in cyberspace,* Taylor & Francis (pp.35-48).

D’Aquin, M., Kronberger, G. & Suarez-Figueroa, M.C. (2012). Combining data mining and ontology engineering to enrich ontologies and linked data. Proceedings of the first international workshop on Knowledge Discovery and Data Mining Meets Linked Open Data (pp. 19-24).

Druzdzel, M. J., & Flynn, R. R. (2017). Decision support systems. In *Encyclopedia of Library and Information Sciences* (pp. 1200-1208). CRC Press.

Esposito, A., Zappatore, M. & Tarricone, L. (2011). Evaluating scientific domain ontologies for the electromagnetic knowledge domain: A general methodology. *Journal of Web & Semantic Technology*, 2, 2, 1-19.

Falliere, N., Murchu, L. & Chien, E. Symantec Security Response (2011). W32.Stuxnet dossier, version 1.4. Retrieved September 11, 2016, from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Fernández-López, M., Gómez-Pérez, A. & Juristo, N. (1997). Methontology: From ontological art towards ontological engineering. Proceedings of the 14th National Conference on Artificial Intelligence, Spring Symposium Series (pp. 33-40).

Fire Eye (2016). Cyber attacks on the Ukrainian grid: what you should know. Retrieved December 3, 2017, from https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

GReAT Securelist (2016). “Black Energy APT attacks in Ukraine employ spearphishing with Word documents”. https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/: Accessed September 17, 2018.

Grigolia, G. Cyber Security Bureau Georgia (2008). Georgia 2008: Legal evaluation according to Georgian and International law. Retrieved

November 15, 2017, from http://csbd.gov.ge/doc/labour/Georgia-2008-Legal-Evaluation-According-To-Georgian-And-International-Law.pdf.

Herr, T. & Herrick, D. (2016). Military cyber operations: A primer. Retrieved September 17, 2018, from https://ssrn.com/abstract=2725275.

Hevner, A.R., March, S.T. & Park, J. (2004). Design research in information systems research. *MIS Quarterly,* 28, 1, 75-105.

Hollis, D. (2011). Cyberwar case study: Georgia 2008. Retrieved December 03, 2017, from http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Langner, R. (2013). To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve, *The Langner Group*.

Lewis, J. (2015). The role of offensive cyber operations in NATO's collective defence. *The Tallinn Papers*, *no. 8*, NATO Cooperative Cyber Defence Centre of Excellence.

Li, J. & Daugherty, L. (2015). Training cyber warriors: What can be learned from defense language training? RAND.

Liang, G., Weller, S.R., Zhao, J., Luo, F. & Dong, Z.Y. (2017). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32, 4, 3317-8.

Liles, S., Dietz, J.E., Rogers, M. & Larson, D. (2012). Applying traditional military principles to cyber warfare. Proceedings of the 4th IEEE International Conference on Cyber Conflict (pp. 1-12). IEEE.

Luvaas, J. (2001). *Napoleon on the Art of War*. Simon and Schuster, pp. 21.

Maathuis, C., Pieters, W. & van den Berg, J. 2016. Cyber weapons: A profiling framework. Proceedings of the 1st international conference on Cyber Conflict U.S. (pp. 1-8). IEEE.

Maathuis, C., Pieters, W. & van den Berg, J. 2018. A computational ontology for cyber operations. Proceedings of the 17th European Conference on Cyber Warfare and Security (pp. 278-88).

McDonald, G., Murchu, L.O., Doherty, S. & Chien, E. Symantec Security Response (2013). Stuxnet 0.5: The missing link. Symantec Security Response. Retrieved September 11, 2016, from

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/stuxnet-missing-link-13-en.pdf.

Mizoguchi R. & Ikeda, M. (1998,). Towards ontology engineering. *Journal of the Japanese Society for Artificial Intelligence,* 13, 9-10.

Mshvidobadze, K. Rondeli Foundation (2015). Georgia cyber barometer report. Retrieved November 15, 2017, from https://www.gfsis.org/files/library/pdf/2423.pdf

Munir, K. & Anjum, M.S. (2017). The use of ontologies for effective knowledge modelling and information retrieval. *Applied Computing and Informatics*, 14, 2, 116-26.

Nazario, J. (2009). Political motivated Denial of Service attacks. In C. Czosseck & K. Geers (Eds.), *The virtual battlespace: Perspectives on cyber warfare'*, IOS Press (pp 163-181).

National Institute of Standards and Technology (2014). Framework for improving critical infrastructure cybersecurity, version 1.0. Retrieved October 14, 2017, from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Obrst, L., Chase, P. & Markeloff, R. (2012). Developing an ontology of the cyber security domain. *STIDS*, 49-56.

Oltramari, A., Cranor, L.F., Walls, R.J. & McDaniel, P. (2015). Computational ontology of network operations. Proceedings of the Military Communications Conference (pp. 318-23). IEEE.

Ottis, R. 2015. Cyber warfare. In M Lehto & P Neittaanmäki (Eds.), C*yber security: Analytics, technology and automation*, Springer, eBook (pp. 89-96).

Paquette, G. (Ed.) 2010. *Visual knowledge modeling for semanting web technologies: Models and ontologies*, IGI Global.

Roussey, C., Pinet F., Kang, M.A. & Corcho O. (2011). An introduction to ontologies and ontology engineering. In G. Falquet, C. Métral, J. Teller & C. Tweed (Eds.), *Ontologies in urban development projects*, 1, Springer (pp. 9-38).

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson Education Limited.

SANS Industrial Control Systems (2016*)*. Analysis of the cyber attack on the Ukranian power grid: Defense use case. Retrieved October 15, 2017, from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Sawsaa, A.F. & Lu, J. (2012). Building information science ontology (OIS) with Methontology and Protégé. *Journal of Internet Technology and Secured Transactions*, 1, 3/4.

Schmitt, M. (2012). "Attack" as a term of art in international law: The cyber operations context. Proceedings of the 4th International Conference on Cyber Conflict (pp.1-11). IEEE.

Schmitt, M. (Ed.) (2013). *Tallinn manual on the international law applicable to cyber warfare,* Cambridge University Press.

Shakarian, P., Shakarian, J. & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*, Elsevier.

Shamir, U. (2016). Analyzing a new variant of Black Energy 3: Likely insider-based execution. Retrieved October 15, 2017, from https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf.

Smirnov, A., Levashova, T. & Kashevnik, A. (2018). Ontology-Based resource interoperability in socio-cyber-physical systems. *IT in Industry*, 6, 2, 19-24.

Sun, Y., Yang, G., & Zhou, X. (2016). A novel ontology-based service model for cyber physical system. Proceedings of the 5th international conference on Computer Science and Network Technology (pp. 125-131). IEEE.

Sun, C.C., Liu, C.C. & Xie, J. (2016). Cyber-Physical system security of a power grid: State-of-the-art. *Electronics*, 5, 3, 40.

Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loyola of Los Angeles International and Comparative Law Review*, 303-33.

Syed, Z., Padia, A., Finin, T., Mathews, L. & Joshi, A. (2016). UCO: A Unified Cybersecurity Ontology'. Proceedings of the 13th AAAI Conference on Artificial Intelligence.

Theonary, C.A. & Harrington, A.I. (2015). Cyber operations in DoD policy and plans: Issues for Congress. Retrieved October 12, 2017, from https://fas.org/sgp/crs/natsec/R43848.pdf.

Tikk, E., Kasha, K., Runnimeri, K., Kert M., Taliharm A.M. & Vihul, L. (2008). Cyber attacks against Georgia: Legal lessons identified, *NATO CCD COE.*

Tolk, A. & Smith, B. (Eds.) (2011). Command and Control ontology. *International Journal of Intelligent Defence Support Systems*, 4, 3, 209-14.

Undercoffer, J., Joshi, A. & Pinkston, J. (2003). Modeling computer attacks: An ontology for intrusion detection. In G. Vigna, C. Kruegel & E. Jonsson (Eds.), *Recent Advances in Intrusion Detection,* 2820, Springer (pp.113-35).

United States Army (2013). "Joint publication 3-12 (R): Cyberspace operations. https://nsarchive2.gwu.edu/dc.html?doc=2692126-Document-18: Accessed September 17, 2018.

Vrandečić, D. (2009). Ontology evaluation. In S. Staab, & R. Studer (Eds.), *Handbook of ontologies, 2nd ed,* Springer-Verlag (pp. 293-313).

Willems, E. (2011). Cyber-terrorism in the process industry. *Journal of Computer Fraud & Security*, 3, 16-9.

Williams, B.T. 2014. The joint force commander's guide to cyberspace operations. *Joint Force Quarterly*, 73, 2, 12-19.

Yin, R.K. (2003). *Case study research: Design and methods*, Applied Social Research Methods Series, 5, Sage Publications.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*, Crown Publishing Group.

Chapter 3. Cyber Weapons

"This is the slowest dance
The dance of a thousand years
The dance of the frozen statues
Clinging together in tears
This is the darkest fight
The fight of a thousand years
The pounding of blood
Through our veins
In our veins
In our eyes
The circles of fear
(Tristania – Equilibrium)

Based on Maathuis, C., Pieters, W. & van den Berg, J. 2016, "Cyber Weapons: a Profiling Framework", *Proceedings of the 1st International Conference on Cyber Conflict (CyCon U.S.),* IEEE Computer Society, pp. 1-8.

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. In this chapter an answer to the question "How to define cyber weapons?" is investigated and further proposed a conceptual framework that defines and profiles cyber weapons from a multidisciplinary perspective: cyber security and Military Operations, considering military-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 research 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 exemplified on three case studies conducted on Stuxnet, Operation Orchard and Black Energy and we detail Stuxnet's profiling based on the existing literature and reports. We conclude by presenting our future research.

Keywords: Cyberspace, Cyber Weapon, Cyber Warfare, Impact.

3.1. 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 (Internet Live Stats, 2016)**.** 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" (Singer & Friedman, 2014), an environment resulting from the interaction between technology, services and people (ISO/IEC, 2012; Cornish et al., 2010; U.S. Army 3-12(R), 2013) "the space of cyber activities" (vd Berg et al., 2014). By being officially recognized as a new battlefield and domain of warfare next to the land, sea, air and space (Lynn III, 2010), 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 further realizing 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

(Jennings, 2015). More than 30 countries have integrated cyber capabilities in their armed forces (Berlk & Noyes, 2012) and more than 140 countries invest in new ones (Suciu, 2014).

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 (U.S. Air Force 3-12, 2011; Hare, 2009) by investing in their strategies, policies and programs (Geers, 2014) and preparing for possible conflict situations by creating new plans of cyber weapons implementation and use. We are now trying to understand what cyber weapons 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 which is a necessary requirement in having a clear and proper understanding and picture about them, the context where they are deployed and their effects. Additionally, is a lack of research concerning their profile, action and impact from a multidisciplinary or interdisciplinary perspective which would support the design and development of different solutions for deploying them and dealing with them. 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 and profiling cyber weapons.

This chapter 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.

3.2. 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" (Tzu). 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 (Shakarian et al., 2013) which makes it a real threat to the national security (Geers, 2011) that needs international cooperation in providing optimal solutions (Geers, 2014). In this settlement, we illustrate in the following figure a conceptual design model that represents at a high level of abstraction the context of use of cyber weapons in war context. Below we continue with explaining each component of it.

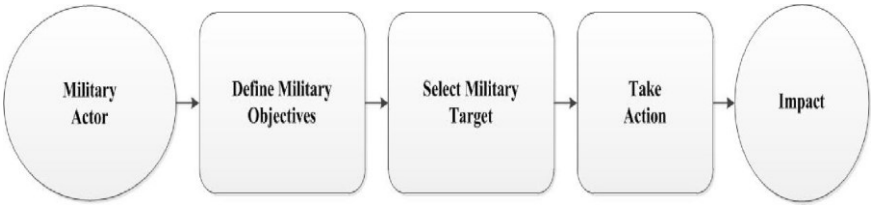


Fig. 3.1. Conceptual design model of context of use of cyber weapons.

- Actor: is responsible for conducting Cyber Operations having a purpose in achieving military objectives (U.S. DoD, 2015).
  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 (Herr & Armbrust, 2015). The available evidence seems to suggest that Stuxnet had a "sophisticated design, which a state could afford" (Shaheen, 2014).
  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, terrorists or criminals (National Cyber

Security Centre, 2015; Andress & Winterfeld, 2011). 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 (Nye, 2011).

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 (Wirtz, 2015) by creating and employing different tools and techniques as means and methods to gain advantage on their adversaries (Lin, 2012; Starr, 2009) 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/she/they 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 (principle of distinction). 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, known in current Military Operations as CDE-Collateral Damage Estimation) and assessment (after the employment of a cyber weapon, known in current Military Operations as BDA-Battle Damage Assessment) of collateral damage is done by remaining in the military targeting boundaries. The available literature on Stuxnet suggests that its intention was to limit the estimated collateral damage, thus before Stuxnet's deployment (Turner, 2013).

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 was not intended from the beginning.
b) Unexpected effects: this category of impact describes the unexpected results that can have multiple consequences (i.e. side effects) 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 (Dougherty, 2015; Schreier, 2015; Demier, 2009; Iasiello, 2015; Tyugu, 2012; Broad et al., 2011; Falliere et al., 2011; Zetter, 2016), 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 (Dougherty, 2015).
- 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 (Schreier, 2015).
- 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 (Demir, 2009; Iasiello, 2015). Additionally, in this phase the necessary information related to avoiding, limiting and controlling expected Collateral Damage of the cyber weapon should be considered based on the intelligence information gathered and analysed in Phase II.

- 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. Furthermore, in order to make sure that the cyber weapon to be deployed is able to avoid. or at least control or limit the expected Collateral Damage that it might produce on civilian objects and civilians, corresponding measures have to be embedded in the cyber weapon, such as: i) target specificity directly contained in the program(s)/script(s) that compose the cyber weapon, ii) target specificity indirectly through links (calls-operations) to corresponding software/network/database configuration files, iii) target specificity through time and space as scheduling the moment of engagement and mobility considerations, and iv) target isolation through ending/breaking target's connections. Additionally, from a software security perspective, for a proper and efficient discovery of target's vulnerability(ies) that the cyber weapon exploits and from there assessing which one could produce less Collateral Damage, the following two lines of attack should be considered: first, static code analysis that facilitates (manually or automated) the discovery of different types of software or connection vulnerability(ies) before the code to be exploited is compiled, and second, penetration testing (with the help of hacking tools or manually done) based on exploiting known existing vulnerabilities or trial-and-error techniques for finding other unknown vulnerabilities on software that is already compiled and runs on different systems.
- 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 essential 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 (Tyugu, 2012). Accordingly, taking into consideration different control measures that could be considered to avoid or at least control or limit unintended effects of cyber weapons, in this phase the ones applied should be tested considering different test cases (in relation to the considered use cases in Phase IV as well as other new ones)

in settings such as cyber ranges where the effects of the cyber weapons could be directly monitored based on their behaviour that they have or based on the reports written to their log files and/or communication to a C2 centre, or just indirectly be deduced through other changes in the environment of the target or the target itself. Some 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" (Broad et al., 2011).

- 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 (Falliere, 2011).
- 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 fulfil 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:* in this phase of 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 (U.S. Air Force 3-12, 2011). In the third case, the attackers do not 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 succeeded on pointing the attack to the Russian government (Zetter, 2016).

In case of procuring a cyber weapon (i.e. not built in-house) from another actor that has developed it, additional concerns about the circumstances and legality of its use and its effects have to be raised. If the actor that built the cyber weapon followed a plan that was previously together established with the actor that will deploy the cyber weapon, that means that the expected effects of the cyber weapon should be known (to some degree). However, if the cyber weapon was procured as a tool and limited details about its expected effects are known (besides the intended ones), then the actor that will deploy it has to make sure that will test and validate it properly. These concerns find their fundament in the Rule 43 of (Tallinn Manual, 2013) and (API Art. 51(4)) that consider the following aspects: "is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means and methods of cyber warfare are indiscriminate by nature when they cannot be: a) directed at a specific military objective, b) limited in their effects as required by the LOAC and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction. It prohibits the use of any means or methods of warfare that cannot be directed against a specific lawful target."

3.3. 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. For the concept *cyber* there is no globally accepted definitions. In this regard, 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" (Oxford Dictionary). Along these lines, the "Tallinn Manual on the

International Law Applicable to Cyber Warfare" (Schmitt, 2013) 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, (Herr, 2014) argues that "Weaponry is not a tool of espionage."

For the purpose of this research, 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 ractically the enabler and the gate into the system for a cyber weapon in order to achieve the attacker's goals (U.S. Air Force 3-12, 2011; Andress & Winterfeld, 2011). 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) 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 (Singer & Friedman, 2014).

There is support for the claim that vulnerabilities and cyber weapons are for sale on the black market (Baer, 2015; Stockton & Golabek-Goldman, 2013; Shane, 2014).

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 (Wikileaks, 2011). One of its biggest customers was NSA (Schwartz, 2013). 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" (Fisher, 2015).

- 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. (Herr & Armbrust,

2015) 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, (Herr & Rosenzweig, 2015) 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.

3.4. Profiling Cyber Weapons

In the previous sections of this chapter we have seen that the reason behind the creation and utilization of cyber weapons is the idea of achieving ones objectives in a war situation. In this section we continue by creating a multidimensional profile of cyber weapons that contains characteristics and classification criteria for them. 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 can represent a cheaper alternative to conventional weapons having "minimal expenses in lives and resources" (Rustici, 2011; Mele, 2013; Denning, 2000). However, depending on the context, objective, as

well as the targets itself, the development and deployment of a cyber weapon can still be an expensive process.

- 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 (Turner, 2013). However, if countermeasures are not taken, it is possible to use the same cyber weapon again, and this implies less investment in the process of development and deployment of a cyber weapon.
- Violent nature: in (Turner, 2013) 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 (Mele, 2013), the author considers that it is another class of cyber weapons that can be used for both offense and defense.

- Use:

a) Single: the case where only one cyber weapon is used.
b) System: while (U.S. DoD, 2010; U.S. Strategic Command, 2009) consider a cyber weapon system as "a combination of one of more offensive cyber capabilities ", (U.S. 1-02, 2016; U.S. 1-02, 2009) and the older version (U.S. 1-02, 1994) 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 selfsufficiency" (U.S. DoD, 2010; U.S. Strategic Command, 2009; U.S. 1-02, 2016; U.S. 1-02, 2009; U.S. 1-02, 1994). For the purpose of this research 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 contained in cyber toolboxes 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.

In the above depicted context of use of cyber weapons, the question that raises is if cyber weapons are worth to be used. A single and direct answer to this question is hard to be provided as it is dependent on factors such as aim, sophistication, unexpected collateral damage, achievement of military objective, financial costs, exposure, and re-use. These aspects should be considered and analysed for each cyber weapon on an individual base as well as when compared to other options in the Courses of Action development phase.

3.5. Profiling Matrix for three Cyber Weapons

In this section we will analyse and profile three cyber weapons, Stuxnet, Operation Orchard and Black Energy based on the case studies that we have conducted on them. 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 based on the three case studies conducted that helps decision makers and academia better understand what cyber weapons mean and what the impact scale is.

Name Parameter	**Stuxnet / Operation Olympic Games**	**Operation Orchard**	**Black Energy 3**
Purpose	Offensive	Offensive	Offensive
Sophistication	Highly sophisticated. Some experts have concluded that it was created and orchestrated by US and Israel (Thabet, 2011).	Highly sophisticated. Some experts have concluded that it was created and orchestrated by Israel (Clements, 2014).	Highly sophisticated. Some experts have concluded that it was created and orchestrated by the Russian hacking group Sandworm Team (SANS 2016; Fire Eye, 2016; Stone, 2016).
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 (Writers,	Single	According to Kaspersky it's one of the Black Energy APT cyber attack family that goes back to 2014 (Great Kaspersky Lab, 2016).

	2010).		
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 (Turner, 2013; Falliere et al., 2011, Langner, 2013).	Strong technical skills: advanced and specific knowledge of electronic warfare and air defense (Clements, 2014).	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 (Fire Eye, 2016).
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 (Zetter, 2009).	Used on December 23, 2015. Was fast discovered and analysed.
Area of action	Global: Indonesia, India, U.S. and other countries (Shearer, 2010).	Local: Al Kabir complex in Syria (Clements, 2014).	Regional: affected half of the people from Ivano-Frankivsk region, Ukraine (Fire Eye, 2016).
Violent nature	Yes	Yes	Yes

Table 3.1.: Profiling matrix for three cases of Cyber Weapons use

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.

3.6. 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" (Foltz, 2012) or the first cyber weapon that was designed, implemented and used against a specific target (Dougherty, 2015) – a critical infrastructure system of a state actor (Herr & Armbrust, 2015; Shaheen, 20) – Stuxnet was a computer program written in multiple programming languages, a combination of high level and low level programming languages such as C/C++ and Assembler, it was compiled in Microsoft Visual Studio 2005 and Microsoft Visual Studio 2008 by a professional team of Software and Control Engineers who probably worked at its development and testing somewhere between six months and one year. This proves 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 (Falliere, 2011; Matrosov et al., 2011). 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 (Falliere et al., 2011; Herr & Rosenzweig, 2015).

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 expert opinions suggest the involvement and collaboration between state nations like U.S. and Israel (Shaheen, 2014; Thabet, 2011), others suggest state nations like India and Russia (Porteous, 2010). There is an ample amount of literature and reports on Stuxnet's objective: to sabotage the nuclear facility from Natanz (Nye, 2011; Shane, 2014) that targeted the nuclear program of Iran (Thabet, 2011; Kaspersky Lab, 2011). This was possible by intruding the network with an infected USB stick and by successfully exploiting four existing vulnerabilities (Nye, 2011) 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 which are 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 (Falliere et al., 2010). 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 (Thabet, 2011). 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 (Matrosov, 2011).

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.

3.7. Conclusions

In 2011 the U.S. Department of Defense 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 chapter 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 security, 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 three case studies 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 (Kanuck, 2012), both a military and a civilian domain (Mueller, 2014) 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.

3.8. References

Andress, J. & Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Elsevier.

Additional Protocol I (1977). *Art 51(4) – Protection of the civilian population.*

Baer, M. (2015). Toward Criteria for International Cyber Weapons Bans. In *2013 World Cyberspace Cooperation Summit IV (pp. 1-3). IEEE.*

Berlk, R. & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities*. The Office of Naval Research.

Broad, W.J., Markoff, J. & Sanger, D.E. (2011). "Israeli test on worm called crucial in Iran nuclear delay". http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0 : Accessed April 20, 2016.

Clements. R. (2014). "How a Syrian nuclear facility was destroyed by the Israeli Air Force 7 years ago today". https://theaviationist.com/2014/09/06/operation-orchard-anniversary/: Accessed January 21, 2016.

Cornish, P., Livingstone, D., Clemente, D. & Yorke, C. (2010). *On cyber warfare*, London: Chatham House.

Demir, D.A. (2009). Challenges of weapon systems software development, *Journal of Naval Science and Engineering*, 5, 3, 104-116.

Denning, D. (2000). Reflection on Cyberweapons Controls. *Computer Security Journal*, 16, 4. 43-53.

Dougherty, J. (2015). "The Pentagon is developing cyber weapons that are extremely lethal". http://www.cyberwar.news/2015-11-09-the-pentagon-is-

developingcyber-weapons-that-are-extremely-lethal.html: Accessed June 11, 2016.

Falliere, N., Murchu, L. & Chien, E. Symantec Security Response (2011). W32.Stuxnet dossier, version 1.4. Retrieved March 21, 2016, from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Fire Eye Industry Intelligence Report (2016). *Cyber Attacks on the Ukranian grid: what you should know*. Fire Eye.

Fisher, D. (2015). "Vupen Founder Launches New Zero – Day Acquisition Firm Zerodium". https://threatpost.com/vupen-launches-new-zero-day-acquisition-firmzerodium/113933/: Accessed November 24, 2015.

Foltz, A.C. (2012). *Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate*. Air War College Maxwell Air Force Base United States.

Herr, T. & Rosenzweig, P. (2015). Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP model. *The Journal of National Security, Law & Policy*, 8, 2.

Herr, T. & Armbrust, E. (2015). Milware: Identification and Implication of State Authored Malicious Software. In Proceedings of the 2015 New Security Paradigms Workshop (pp. 29-43).

Geers, K. (2011). Sun Tzu and Cyber War, *NATO CCD COE.*

Geers, K. (2014). Cyberspace as Battlespace, *Black Hat Webcast.*

Geers, K. (2014). Pandemonium: Nation States, National Security, and the Internet, *NATO CCD COE.*

GReAT - SECURELIST Kaspersky Lab. (2016). *Black Energy APT Attacks in Ukraine employ spear phishing with Word documents*. Kaspersky Lab.

Herr, T. (2014). PrEP: A Framework for Malware & Cyber Weapons. *The Journal of Information Warfare*, 13, 1, 87-106.

Hare, F. (2009). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?, *NATO CCD COE.*

Iasiello, E. (2015). Are cyber weapons military effective tools? *Journal of Military and Strategic Affairs*, 7, 1.

Internet Live Stats (2016). "Internet Users". http://www.internetlivestats.com/internet-users/: Accessed July 07, 2016.

ISO/IEC 27032:2012. (2012). *Information technology - Security techniques - Guidelines for Cybersecurity*, International Organization for Standardization.

Jennings, D. (2015). "Homeland Security Preparing for 'Cyber Pearl Harbor'". http://www.offthegridnews.com/current-events/homeland-securitypreparing-for-cyber-pearl-harbor/: Accessed June 11, 2016.

Kanuck, S. (2012). *Sovereign Discourse on Cyber Conflict Under International Law*. University of Pennsylvania Law School.

Kaspersky Lab (2011). *Stuxnet Spotlight*. Kaspersky Lab.

Langner, R. (2013). *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. The Langner Group.

Lin, H. (2012). Cyber Conflict and International Humanitarian Law. *International Review of the Red Cross*, 94, 886.

Lynn, W., J. III. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy". https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain: Accessed June 11, 2016.

Matrosov, A., Rodionov, E., Harley, D. & Malcho, J. (2010). *Stuxnet under the microscope*. Esset LLC.

Mele, S. (2011). *Cyber-weapons: legal and strategic aspects*. Istituto Italiano di Studi Strategici.

Mueller, B. (2014). *On the need for a treaty concerning cyber conflict*. The London School of Economics and Political Science.

National Cyber Security Centre (2015). *Cyber Security Assessment Netherlands 2015*, National Cyber Security Centre.

Nye, J.S. (2011). Power and National Security in Cyberspace. *America's Cyber Future: Security and Prosperity in the Information Age*, 2, 1, 5-24.

Oxford Dictionary, Oxford University Press.

Porteous, H. (2010). *The Stuxnet Worm: Just Another Computer Attack or a Game Changer*. Canada Library of Parliament.

Rustici, R.M. (2011). *Cyberweapons: Leveling the International Playing Field.* The U.S. Strategic Studies Institute.

SANS Institute (2004). *Information warfare: cyber warfare is the future warfare.* Global Information Assurance Certification Paper.

SANS Institute (2016*). Analysts of the Cyber Attack on the Ukranian Power Grid: Defense Use case*. ICS SANS.

Schmitt, M. (Ed.) (2013). *Tallinn manual on the international law applicable to cyber warfare,* Cambridge University Press.

Schreier, F. (2015). *On cyberwarfare*, DCAF Working paper.

Schwartz, M.Z. (2013). "NSA Contracted With Zero – Day Vendor Vupen". http://www.darkreading.com/riskmanagement/nsa-contracted-with-zero-day-vendor-vupen/d/did/1111564: Accessed November 24, 2015.

Shaheen, S. (2014). Offence - Defence balance in Cyber Warfare. In *Cyberspace and International Relations*, Springer, (pp. 77-93).

Shane, H. (2014). "Black Market for Malware and Cyber Weapons is Thriving". http://foreignpolicy.com/2014/03/25/black-market-for-malware-andcyber-weapons-is-thriving/: Accessed May 21, 2016.

Shakarian, P., Shakarian, J. & Ruef, A. (2013). *Introduction to Cyber Warfare: a Multidisciplinary Approach*, Elsevier.

Singer, P.S. & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*, Oxford University Press.

Starr, S. H. (2009). Towards an Evolving Theory of Cyberpower. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare, 3, 18.*

Stockton, P.N. & Golabek-Goldman, M. (2013). Curbing the Market for Cyber Weapons. *Yale Law & Policy Review*, 32, 1.

Stone, J. (2016). "Russian Hacking Group Sandworm Targeted U.S. Before Knocking Out Power In Ukraine*"*. http://www.ibtimes.com/russian-

hacking-group-sandwormtargeted-us-knocking-out-power-ukraine-2257194: Accessed March 18, 2016.

Suciu, P. (2014). "Why cyberwarfare is so attractive to small nations". http://fortune.com/2014/12/21/whycyber-warfare-is-so-attractive-to-small-nations/: Accessed May 15, 2016.

Symantec Security Center (2010). "W32.Stuxnet". https://www.symantec.com/security-center/writeup/2010-071400-3123-99: Accessed October 14, 2015.

Thabet, A. (2011). "Stuxnet Malware Analysis Paper". Code Project. https://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper: Accessed October 12, 2015.

Turner, M. (2013). Is there such a thing as violent act in cyberspace?. *International Security and Intelligence Summer School*, University of Cambridge.

Tyugu, E. (2012). Command and control of cyber weapons. In Proceedings of the 4th International Conference on Cyber Conflict (pp. 1-11). IEEE.

Tzu, S. *The art of war.*

United States Department of Defense. (2010*) Joint Terminology for Cyberspace Operations*.

United States Department of Defense. (2015). *The DoD Cyber Strategy*, United States Army Department of Defense.

United States Air Force 3-12. (2011). *Cyberspace Operations*, United States Army.

United States Army Joint Publication 3-12 (R) (2013). *Cyberspace Operations*, United States Army.

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

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

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

United States Strategic Command. (2009) *The Cyber Warfare lexicon*. United States Army Department of Defense.

Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, N., Boeke, S., Van de Koppen, L…. & De Bos, T. (2014). On (the emergency of) Cyber Security science and its challenges for Cyber Security education. In *The NATO IST-122 Cyber Security Science and Engineering Symposium*.

WikiLeaks (2011). "Vupen: Threat Protection Program". https://wikileaks.org/spyfiles/docs/vupen-security/279_threat-protection-program-exploits-for-law-enforcement.html: Accessed November 24, 2015.

Wirtz, J.S. Cyber War and Strategic Culture: the Russian Integration of Cyber Power into Grand Strategy. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*, 3, NATO CCD COE (29 – 37).

Writers, S. (2010). Stuxnet worm rampaging through Iran: IT official. http://www.spacedaily.com/reports/Stuxnet_mutating_rampaging_through_Iran_IT_official_999.html: Accessed January 03, 2016.

Zetter, K. (2016). "Everything we know about the Ukrainian power plant hack". https://www.wired.com/2016/01/everything-we-know-about-ukrainespower-plant-hack/: Accessed May 14, 2016.

Zetter, K. (2009). "Mossad Hacked Syrian Official's Computer Before Bombing Mysterious Facility". https://www.wired.com/2009/11/mossad-hack/: Accessed March 12, 2016.

Chapter 4. Effects Assessment Methodology in Cyber Operations

”Sors immanis
Et inanis,
Rota tu volubilis,
Status malus,
Vana salus
Semper dissolubilis,
Obumbrata
Et velata.”
/
“Monstrous fate
And empty,
You whirling wheel,
You are malevolent,
Well-being is vain
And always fades to nothing,
Shadowed
And veiled.”
(Carl Orff – O Fortuna)

Based on Maathuis, C., Pieters, W. & van den Berg, J. 2018, “Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations”, *Proceedings of the 37th International Conference on Military Communications (MILCOM),*IEEE Computer Society, pp. 1-6.

Cyber Operations stopped being utopia or Sci-Fi based scenarios: they became reality. When planning and conducting them, military actors encounter difficulties since they lack methodologies and models that support their actions and assess their effects. To address these issues by tackling the underlying scientific and practical gap, this chapter proposes an assessment methodology for the intended and unintended effects of Cyber Operations, labelled as Military Advantage, Collateral Damage, and Military Disadvantage, and aims at supporting the targeting process when engaging targets in Cyber Operations. To arrive at this methodology, an extensive review on literature, military doctrine and methodologies was conducted combined with two series of interviews with military commanders and field work in joint military exercises. The assessment methodology is proposed considering multidimensional factors, phases and steps in a technical-military approach. For validation, one realistic Cyber Operation case study was conducted in a focus group with nine military experts plus four face-to-face meetings with another four military experts.

Keywords: Cyber Operations, Cyber Warfare, Cyber Weapons, Targeting, Collateral Damage, Military Advantage, Effects Assessment.

4.1. Introduction

"War is never an isolated act…in war the result is never final." (Clausewitz, On war)

Compared with other warfare domains, cyberspace is geographically less constrained (MoD Shrivenham, 2015) as it is a dynamic and fast changing environment where "new nodes are discovered and a kaleidoscope of network patterns occurs and disappears" (Kallberg & Thuraisingham, 2013). Since Cyber Operations can amplify or support other Military Operations (Maathuis et al., 2016), they embed the power to influence or threaten to influence enemies (Schreier, 2015) by efficiently and effectively engaging targets with proper cyber weapons/capabilities. When assessing, predicting, or estimating the effects of Cyber Operations, one needs to "think the unthinkable" (Samaan, 2010) since this is very difficult (Schreier, 2016; Goldsmith, 2013) considering data reliability and accuracy. Different methodologies and mechanisms are used to (partially) solve these issues in kinetic Military Operations, but for Cyber Operations they are inexistent in the field and scarcely tackled in the academic literature.

Addressing these issues combined with the growing number of Cyber Operations globally conducted (e.g. Georgia, Stuxnet, Ukraine), this

research aims at designing an assessment methodology for the intended and unintended effects (Military Advantage, Collateral Damage and Military Disadvantage) that supports military commanders and their staff (e.g. intelligence and execution) when targeting in Cyber Operations. We should mention here that this research is not aimed at tackling other implications and consequences of Cyber Operations such as economic and political as they go behind the purpose of this research. However, from a strategic point of view, we do acknowledge that these aspects play a role and should be further investigated, but are out of the scope of this research. Accordingly, in this research, the following definitions were considered (Maathuis et al., 2018):

a) Military Advantage as intended effects that contribute to achieving military objectives.
b) Collateral Damage as unintended effects that do not contribute to achieving military objectives, but impact civilian assets, in the form of civilian injury or loss of life and/or damage or destruction to civilian objects and/or environment.
c) Military Disadvantage as unintended effects that do not contribute to achieving military objectives and impact allies, friendly, neutral, even the target or conducting actors.

A multidisciplinary research was carried based on reviewing academic literature and military doctrine, military methodologies and mechanisms. Additionally, two sets of semi-structured interviews with eighteen military commanders with an average of 20 years of experience in military operations and exercises were conducted plus field work in joint military exercises (see Appendices-Annex A and C). Since traditional approaches are less applicable to Cyber Operations (e.g. collateral damage estimation) (Romanosky & Goldman, 2016) the abovementioned resources allowed the design of this methodology. To validate, one virtual but realistic Cyber Operations case scenario/use case was conducted in this chapter. The validation was done in two steps: first, in a focus group organized with nine military experts, and second, in four face-to-face meetings with another four military experts.

The remainder of this chapter is structured as follows. The second section summarises relevant research. The third section presents the research approach pursued by this chapter. The fourth section introduces the assessment methodology. The fifth section presents the Cyber Operation case study on which this methodology was validated and the validation results. The last section discusses contributions and future work.

4.2. Related Work

(EU Council, 2016) provides guidance to conducting Military Operations by EU forces and discusses necessary requirements and steps for avoiding or at least minimizing Collateral Damage. This view is aligned with the one enclosed in the methodology used by NATO and US (NATO, 2011; Joint Chief of Staff, 2012) and implies the following levels of assessment: i) target validation and initial CDE (Collateral Damage Estimation) analysis, ii) general and target size analysis overview, iii) weaponeering analysis overview, iv) refined analysis overview, and v) casualty analysis overview. Control measures for avoiding or minimizing the unintended effects in Cyber Operations and a multi-level/phase perspective are likewise incorporated in this research.

A methodology for assessing collateral damage for nonfragmenting Precision-Guided Weapons was designed by (Joint Chief of Staff, 2012) considering as lethality scale: lethal, severe, moderate, light and no injury. The severity scale used by U.S. DoD is: deceased (lethal), very serious, serious, incapacitated and not serious injured (Humphrey, 2008). Both scales are integrated in this research.

(Gordon & Douglas, 2005) analyses tools used to assess Collateral Damage in Operations Allied Force, Enduring Freedom and Iraqi Freedom, and argues that collateral damage estimation methodologies need to be accurate, responsive and human-factored by providing graphics that facilitate decisions. Aligned with (EU Council, 2016; NATO, 2011), this research uses different tables to support the assessment process and decision making.

(Grimaila et al., 2009) proposes the following design considerations when assessing the impact of a cyber incident: focus on information, information asset valuation, knowledge retention, mission representation and mission impact estimation, and secure notification. Due to their generality and applicability, these considerations were presumed when designing the assessment methodology that this research introduces. Additionally, an effective cyber damage assessment is based on identifying and valuating assets considering how they are vulnerable, presented in a structured and documented way. Accordingly, each phase of the assessment methodology proposed in this research is structured, documented and sequentially introduced.

(Dogan & Kosaner, 2015) conducts a cyber security assessment for tactical C2 evaluated on case studies, in a similar way that the evaluation is done in the present research.

4.3. Research Methodology

This research aims at designing an effects assessment methodology for targeting in Cyber Operations. This requires a multidisciplinary perspective by combining multiple methods of research from cyber and military domains. Accordingly, a Design Science Research approach (Peffers, 2008) is considered since it allows artefacts (i.e. frameworks, methods, models) to be designed and evaluated systematically based on the following activities:

Activity I: Problem Identification and Motivation

The motivation underlying this research is twofold. First, Cyber Operations have the potential to becoming a key component of military operations, however they lack dedicated methodologies for planning and execution, and this impacts military and civilian actors, and society itself. On this ground, two sets of semi-structured and focused interviews (Peffers, 2008) with eighteen military commanders (eight in the first set and ten in the second) with significant international experience gathered through several years of military-technical education and practice in military exercises and field operations (see Appendices-Annex A and C). The experts were from Netherlands, Germany and U.S. were held in 2016 and 2017. The military experts were asked to elaborate on their requirements and expectations regarding assessing Collateral Damage and Military Advantage in Cyber Operations. Moreover, they were questioned regarding the possibility of not receiving the expected information and asked how they would react in such a case. Furthermore, field work was carried out in 2016 and 2017 by direct participating and observing in two joint military exercises (Iacono, 2009) that contributed to achieving a comprehensive vision on Cyber Operations and considerations for assessing their effects. Secondly, from an extensive review of scientific literature, military doctrine, and reports, general approaches for effects or impact assessment have been considered (in Related Work section) or focused on limiting or controlling Collateral Damage (Raymond et al., 2013), but lack methodologies for assessing Collateral Damage, Military Advantage, and Military Disadvantage in Cyber Operations.

From the abovementioned resources, as the interviewed experts considered, the following requirements were established for designing the effects assessment methodology in Cyber Operations:

a) To be structured, adaptable, and illustrative.
b) To be compatible, familiar or designed in a similar way as the methodologies used in kinetic Military Operations.

c) To consider time, space and force dimensions.
d) To be evaluated on realistic Cyber Operations scenarios.

Activity II: Solutions Objectives

Furthermore, the objectives of this research are:

- To identify the dimensions and factors that can be used to assess Collateral Damage, Military Advantage, and Military Disadvantage when targeting in Cyber Operations.
- To design an assessment methodology for Collateral Damage, Military Advantage, and Military Disadvantage when targeting in Cyber Operations.

Activity III: Design and Development

The functionality and architecture of the assessment methodology (artefact) are determined, and based on all gathered resources, the design is executed following the requirements defined in *Activity I.*

Activity IV: Demonstration

To demonstrate through experimentation or case study, two face-to-face meetings with two military experts were individually organized in 2017. The first meeting was a brainstorming session regarding the development of virtual and realistic case studies that would be suitable to evaluate the proposed methodology. In the second meeting, two alternatives were proposed to the experts, and they advised to choose one.

Activity V: Evaluation

The assessment methodology designed in *Activity III* is evaluated on a case developed in *Activity IV* in two phases. In the first phase, in a focus group (Tremblay, 2010) organized by TNO (the Netherlands Organization for Applied Scientific Research) and the Netherlands MoD in one day in June 2017 under the name "Effects Assessment and Targeting Decisions in Cyber Warfare" (see Appendices-Annex D). Nine experts were selected and invited to participate based on their background and experience. In the second phase, in four face-to-face meetings organized between June-October 2017 with another four military experts (see Appendices-Annex D) to refine this methodology. Finally, the methodology is proposed.

Activity VI: Communication

The results of this research are communicated through meetings, e-mails and the present chapter.

4.4. Design of Assessment Methodology

The effects assessment in Cyber Operations methodology was designed based on the requirements and considerations previously presented, and aims at assessing effects prior to engaging targets in Cyber Operations. However, it could also be used after engaging targets as guidance when analysing effects. The military experts interviewed and (Maathuis et al., 2018; Maathuis et al., 2016; Gallina, 2002) argue that an integration of spatial (spreading), temporal (duration) and force (severity) factors, together with probabilities needs to be considered. Force is expressed by the type of effects. Hence, these factors are presented in Table 4.1-3. and further used:

Target (T)	Network of Target (T)	National (N)	Regional (R)	Global (G)

Table 4.1. Spatial scale factors (spreading)

Short Term (ST)	Medium Term (MT)	Long Term (LT)
0 – 1h 1h – 1 day	1 day – 1 week 1 week – 1 month	1 month – 6 months 6 months – 1 year 1 year – 3 years

Table 4.2.Temporal scale factors (duration)

Probability	Value
No	0%
Low	0 – 25%
Moderate	25 – 50%
High	50 – 75%
Very High	75 – 100%

Table 4.3. Probability

The proposed methodology is structured in five phases compatible with the current methodologies used in kinetic Military Operations (NATO, 2011; Joint Chief of Staff, 2012), as follows: Phase I. Target Identification and Validation, Phase II. Target Analysis, Phase III. Target Effects Assessment, Phase IV. Collateral Effects Assessment and Phase V. Minimization of Unintended Effects. Furthermore, each phase is elaborated:
Phase I: Target Identification and Validation

In this phase, entities that allow to (threaten to) influence adversaries and achieve military objectives are identified and validated as targets. This phase is similar to the first level of assessment applicable to kinetic Military Operations (NATO, 2011; Joint Chief of Staff, 2012]. Therefore, the necessary information needs to be considered as illustrated in the next two steps.

Step I: Target Identification

To identify targets the next information is needed: name, category, set, type, description, function, geolocation, surroundings, environment, defense mechanism, vulnerability, sensitivity, priority, engagement timestamp, and status (Gallina, 2002; NATO AJP 3.9., 2016; U.S. JP 3-12(R), 2013; U.S. JP 2-01.1, 2013).

Step II: Target Validation

To be validated as a target, an entity should be a lawful military target considering the criteria provided by LOAC (Fischerkeller, 2016), and further explained by (AP I-Art 52): "attacks shall be limited to military objectives [i.e. military targets as persons or objects]. In so far as objects are concerned, military objectives [i.e. military targets] are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" (principle of distinction). Accordingly, if this entity is not positive identified (PID), then it cannot be engaged (Red Cross Rule 8, 1977) and other options should be considered for engagement or the operation should be suspended or cancelled.

Phase II: Target Analysis

In this phase, sufficient information about the target should be acquired to be engageable in a Cyber Operation. From this phase, the assessment is tailored to the cyber context. Hence, necessary information useful to analyse it should be considered regarding its system, hardware, and software architectures and elements included, as illustrated in the layered model depicted in Fig. 4.1. and described in the next steps:

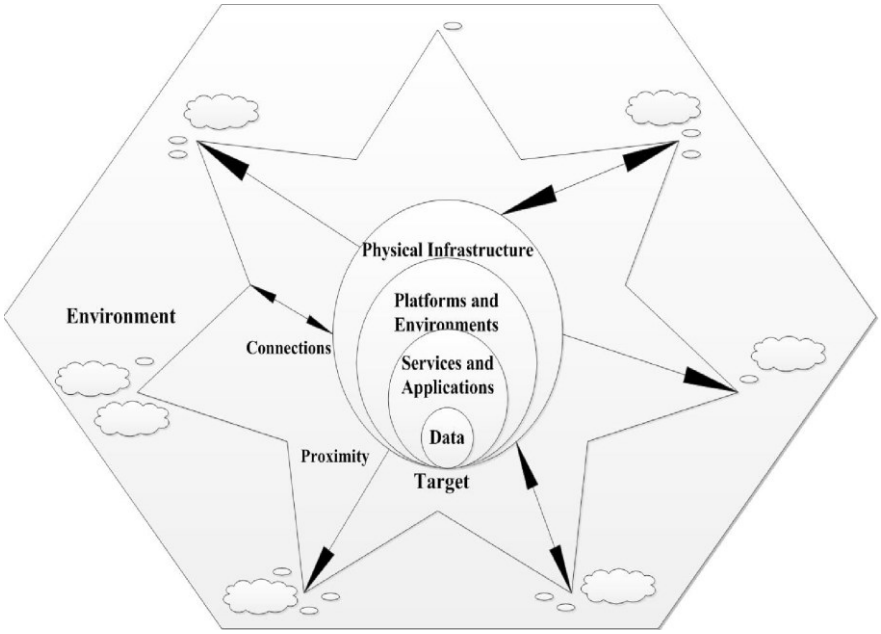


Fig. 4.1. Target Analysis Model

Step II.I: System Architecture

Step II.I.I: Structure, components, functions and behaviour

Information about the system structure, components, their functions and behaviour is required (Gallina, 2002; NATO, 2016; U.S. JP 3-12(R), 2013).

Step II.I.II: Connections, dependencies and connectivity

Information about the network topology, traffic, connections and dependencies (McNeal, 2011; Fischerkeller, 2016; Holsopple, 2014) as well as type, status and operator/provider of connectivity have to be known.

Step II.II: Hardware Architecture

Information about the physical infrastructure, devices (e.g network devices like routers or switches, different sensors), their functionality, status, defense mechanisms (e.g. locks, encryption), protocols, and vulnerabilities (hardware or configuration) should be acquired.

Step II.III: Software Architecture

Information about the software infrastructure, applications (e.g. firmware, middleware, desktop, web, or mobile), protocols and data together with their functionality, status, defense mechanisms (e.g. encryption, firewalls, IDS/IES, VPN) and vulnerabilities (software or configuration) should be gained.

Phase III: Target Effects Assessment

The intended and unintended effects of Cyber Operations are assessed using of the factors introduced by Table 4.1.-3.

Step III.I: Military Advantage Assessment

The interviewed military experts stressed that currently Military Advantage is assessed by military Commanders and their staff based on feeling, background, experience, common sense using the information about the target, without relying on a specific assessment methodology. Furthermore, Military Advantage should be assessed on all warfare levels as well as in other warfare domains since cyberspace is a cross-domain of warfare (Gallina, 2002), as Tables 4.4. and 4.5. portray:

Battlefield/Level	Strategic	Operational	Tactical
Land/Sea/Air/Space/Cyber			

Table 4.4. Military Advantage on each level of warfare

Type	**On Target**	**Duration**	**Spreading**	**Severity**	**Probability**

Table 4.5. Military (Dis)Advantage in Cyber Operations

In Table 4.5., '*Type'* represents the type of Military Advantage, such as communication delay or target neutralization. '*On Target'* means combatants, military logic/virtual objects and military physical objects as military targets.

Step III.II: Efficiency, effectiveness and performance

Indicators regarding the efficiency, effectiveness (MoE) and performance (MoP) (NATO, 2016) in achieving military objectives in Cyber Operations are useful since the effects assessment process is a continuous and adaptive process. This is indicated in Table 4.6..

Name Indicator	**Level Of**
Efficiency	Low
Effectiveness	Medium
Performance	High

Table 4.6. Efficiency, effectiveness and Performance in Cyber Operations

Phase IV: Collateral Effects Assessment

Cyber Operations have a wide range of effects (McNeal, 2011) that can impact the target as well as other actors, military or civilian in the sense of allies, friendly, neutral, or even conducting actors. Moreover, each category of collateral effects is elaborated.

Step IV.I: Collateral Damage Assessment

In Table VII, '*Type'* means the type of Collateral Damage, such as injury of people or communications delay. '*On Asset'* represents non-combatants, civilian logic/virtual objects and civilian physical objects that are forbidden to target.

Type	On Asset	Duration	Spreading	Severity	Probability

Table 4.7.: Collateral Damage in Cyber Operations

A significant role in deciding if a target can be engaged in a Cyber Operation is played by the proportionality assessment, which stresses that Collateral Damage should not be excessive in relation to Military Advantage (Red Cross Rule 14, 1977). That being said, Collateral Damage is considered either: i) Not Accepted, ii) Tolerated, iii) Accepted. However, further in this research we will only consider the i) and ii) categories since ii) category is not compliant with the military-legal constraints of this research.

Step IV.II: Military Disadvantage Assessment

Table V applies also for assessing Military Disadvantage. Military Disadvantage impacts allies, friendly, neutral actors, and could also impact even the target or conducting actors when unintended effects are impacting the target or conducting actors. For instance, altering the functionality of a software application running on a server produces Military Advantage but indirectly implies disturbing or closing connections to other applications or processes or performance issues to other applications or processes that are used for communication purposes with the C2 of the attacker, fact that could be seen as Military Disadvantage. '*Type'* can be for example communications perturbation or operational instability.

Phase V: Minimization of Unintended Effects (Collateral Damage and Military Disadvantage)

In this phase, control measures for avoiding or minimizing Collateral Damage and Military Disadvantage are proposed:

Step V.I: Minimization of Collateral Damage

Step V.II: Minimization of Military Disadvantage

To avoid or minimize Collateral Damage and Military Disadvantage, control measures regarding a better situational awareness, correct, accurate, multi-source, and last minute (up to date) intelligence are necessary. Furthermore, high accuracy and precision regarding engaging the right target in the most specific way by using efficient, effective, and desirably adaptive and intelligent cyber weapons/capabilities are decisive. These measures should be considered from the design phase to be optimal. Moreover, control measures regarding engaging the target with a different cyber weapon or a different engagement method should also be included. Additionally, if all control measures are considered ineffective, another target should be nominated or the operation should be suspended or cancelled.

4.5. Validation Case Study: Ballistic Missile Defense Cyber Operation

A case study was designed from scratch and prepared between January to May 2017 respecting the last requirement concerning the design of an assessment methodology, the advices that military Commanders provided, and current global security issues. This case study was virtually conducted, is depicted in Fig. 4.2., and was used to validate the proposed methodology with military-technical experts, in a double process: first, in a focus group, and second, in four face-to-face meetings. The experts were asked 13 questions structured in five groups (Appendices-Annex D): opening, introductory, transition, key, and ending questions.

Hence, following the context description proposed by (Maathuis et al., 2018) for representing and simulating Cyber Operations, the following information was used to evaluate Phases I and II of the methodology: Context, Actor, Type, Military Objective, Target, Cyber Weapon, and Geolocation, as follows:

Context: A crisis in Risian evolved into an international armed conflict due to humanitarian concerns, terrorist groups support that impacted Risian's population, neighbour countries and escalated internationally. Amdasia

supported by other states decided to launch a ballistic missile attack on Risian's military land HQ in Risian's capital. Recently, Risian invested in its missile program. Its Ballistic Missile Defense System which is a land-based system that can detect, track, engage, and destroy short and medium range ballistic missiles, is procured from Limia (a neutral country and ally to Amdasia).

Actor: Risian, Amdasia, Limia.

Type: Offensive Cyber Operation.

Military Objective (for Amdasia): to prevent the surface-to-air anti-ballistic missile of Risian to reach its target-the surface-to-surface ballistic missile launched by Amdasia against the military land HQ located in Risian's capital.

Target: the anti-ballistic missile of Risian (see 4 in Fig. 4.2.) fired from the missile squadron located at the military base at 100 km distance to the capital of Risian that is a part of Risian's Ballistic Missile Defense System.

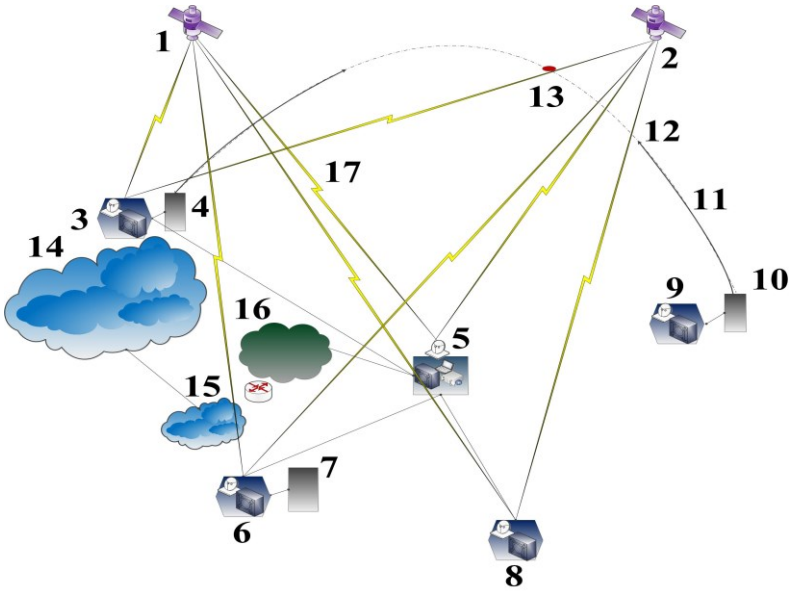


Figure 4.2. Ballistic Missile Defense Cyber Operation

Legend Figure 4.2.
1. Communications satellite, 2. Surveillance satellite (early warning), 3. Ballistic Missile Defense System (BMDS) Ground Base, 4. BMD Interceptor/Launcher, 5. BMDS Command and Control (C2), 6. Another BMDS Ground Base, 7. Another BMD Interceptor/Launcher, 8. BMDS radar, 9. BMDS Ground Base, 10. BM

launcher, 11. BM at the beginning of the mid-course phase, 12. BM trajectory, 13. Calculated collision point between the BM and the anti-BM, 14. Capital of Risian, 15. Civilian airport, and 16. Air Force military base.

Cyber Weapon: Risian subcontracted a software development company from Limia to develop the software that its Ballistic Missile Defense Command and Control uses. Amdasia is a step ahead of Risian considering possible counterattacks in case of launching ballistic missiles against Risian. That is why a Senior Software Engineer (insider) was infiltrated in the design and development phases of Risian's software at the software company. This allowed the introduction of a software vulnerability of which exploit will automatically be activated in special geostrategic conditions when a ballistic missile from Amdasia is detected. If Amdasia launches its ballistic missile, preparations are made by Risian to launch an anti-ballistic missile against it. As this happens, the anti-ballistic missile self-destroys in the boost phase and explodes in the neighbourhood, probably at the periphery of Risian's capital. Therefore, Amdasia's ballistic missile follows its ballistic flight to deliver its warhead and impact its target.

Tables 4.8. and 4.9. present the results from evaluating Phase III of the proposed methodology. Regarding efficiency, effectiveness, and performance in achieving the military objective, this Cyber Operation was considered by the military experts as being High or between Medium to High.

Battlefield/Level	**Strategic**	**Operational**	**Tactical**
Land	Limit Risian's ability to C2 Military objective is achieved.	Damage or destruction of Risian's land HQ. Disruption of Risian BMDS.	Limit Risian's means to receive orders and C2.
Sea	No / Possible option.	NAK	NAK
Air	Influence or limit Risian's response. Limit Risian's defensive reaction in air & space.	Limit Risian's ability to C2 operations and to use anti-BM in near-future air&space operations. Limit or alter the order to process information.	Limit Risian's means and ability to receive orders and information through the C2.
Space			
Cyber	Attribution. Cyber	Influence /	Reducing the

	as a real offensive option and general awareness. Limit / Influence Risian's cyber defense capability. Risian's systems and C2 exposure, compromise.	Allowing future exploitation of Risian's sytems and operations. Limit or destroy Risian's ability Risian to C2 operations.	BMD functionality and capability. Control of Risian's C2 systems.

Table 4.8.: Military Advantage in Case Study on War Levels

Type	On Target	Duration	Spreading	Severity	Probability
Limit effectivity	BMD C2	ST- MT	T,NT or N	Disruption and Control	H–VH
			R or G		L
	anti-BM	ST	T	Destruction	VH
Influence	Risian	MT- LT	N or R	Influence power balance	H
Limit	Combatants	ST- MT	N or R	Limit physical force	H
Disruption and Control	BMD C2	ST- MT	T,NT and N	Disruption and Control	H

Table 4.9.: Military Advantage in Case Study

Tables 4.10. and 4.11. present the results from evaluating Phase IV. Kinetic effects are produced by the fired missiles. Experts considered Collateral Damage as being Accepted or Tolerated.

Type	On Target	Duration	Spreading	Severity	Probability
Injury or Loss of life	Civilians	ST-MT	Capital area	Injury or Death	L-M
Mental / Psychologic	Civilians	MT-LT	Capital area or N	Mental injury	M
Damage or destruction	Civilian Critical Infrastructure	ST	N	Damage or destruction	L-M
Infection	Civilian systems and services	ST-MT	N or G	Infection	L
Alteration or destruction	Civilian data	ST-MT	N, R or G	Alteration or destruction	L

Damage or destruction	Environment	ST- MT	or R	Damage or destruction	L-M

Table 4.10.: Collateral Damage in Case Study

Type	On Target	Duration	Spreading	Severity	Probability
Risian and Limia (if attributed)	Between Risian and Limia	NAK	R or G	Tenstions / Conflict	M- H
Distrust BMD C2	Limia or Risian	ST- MT	T	Distrust	M- H
Failure (if C2 is updated)	Cyber Operation on Risian's BMD C2	ST	T or NT	Failure	H-VH
Detection	Cyber Weapon	ST	T	Detection	L
Spreading and Infection	Limia, allies, friendly or neutral actors	ST- MT	R or G	Infection or disruption	L-M
Instability	Amdasia,allies, friendly or neutral actors	ST- MT	G	Instability	L
Re-use	BMD C2	All	T	Re-use	L

Table 4.11.: Military Disadvantage in Case Study

When evaluating phase V, the experts advised to engage this target since Collateral Damage was not expected excessive in relation to Military Advantage. In unanimity, they decided that if insufficient information is given, the target should not be considered for engagement, and stressed that "civilian lives are the most precious and most important". Aligned with (Dogan & Kosaner, 2015; Nusinov et al., 2009), this research gradually assesses the effects of Cyber Operations to anticipate possible futures and validates it by bringing "the researcher into direct contact with the potential users of the artefact" (Tremblay et al., 2010) and with domain experts by considering suitability, feasibility, acceptability and completeness as evaluation criteria (Tremblay et al., 2010). Based on these results, the methodology fulfilled the requirements, reflects its effectiveness and applicability, and provided meaningful insight into the dynamics of targeting in Cyber Operations.

4.6. Conclusions

Since the dawn of history wars were a part of the human existence and experience (Tabansky, 2011). By expanding the theatre of operations in the cyber domain, we deal with a "radical shift in the nature of the wartime battlefield" (Solce, 2008). This is also reflected when planning, conducting, and assessing Cyber Operations. Lacking methodologies that support these actions, significant implications and consequences can be triggered and propagated in unexpected ways: they can impact collateral (military and civilian) actors such as allies, friendly, neutral, or even the target or conducting actors. Addressing these issues, this chapter contributes to the existing body of knowledge from cyber and military domains by proposing an assessment methodology for Military Advantage, Collateral Damage, and Military Disadvantage to support military decision makers and their staff when targeting in Cyber Operations. The methodology is primarily useful before the engagement of military targets in Cyber Operations referring to assessing their effects in the sense of estimating them only by considering the values of being Accepted and Not Accepted, thus excluding Tolerated due to the fact that it is not in concordance with the applicable legal framework. Secondarily useful after their engagement when assessing their effects in the sense of analysing them. The methodology was validated by military-technical experts on a case study and is the basis for future work on modelling the effects of Cyber Operations.

4.7. References

Additional Protocol I (1977). Art 52(2) – General protection of civilian objects.

Council of the European Union (2016). *Avoiding and Minimizing Collateral Damage in EU-led Military Operations Concept*.

Dogan, O. & Kosaner, K.M. (2015). A Case Study for Cyber Security Assessment on Tactical Command and Control Systems. In Proceedings of the International Conference on Military and Security Studies, pp. 26-31.

Fischerkeller, M. P. (2016). *Incorporating Cyber Offensive Operations into Conventional and Strategic Deterrence Strategies.* Institute for Defense Analyses.

Gallina, D., Gorman, P., Herman, P., MacDonald, J. & Ryer, R. (2002). *Military Advantage in History*. Information Assurance Technology Analysis Center.

Goldsmith, J. (2013). How cyber changes the laws of war. *European Journal of International Law*, 24.1, 129-138.

Gordon, S.C. & Douglas, D. (2005). *Modelling and simulation for collateral damage estimation in combat.* Enabling Technologies for Simulation Science IX, pp. 309-318.

Grimaila, M., R., Fortson, L.W. & Sutton, J.L. (2009). Design Considerations for a Cyber Incident Mission Impact Assessment. International Conference on Security and Management.

Holsopple, J., Sudit, M. & Yang, S.J. (2014). Impact Assessment. *Advances in Information Security,* 62, pp. 219.

Hughes, J. & Cybenko, G. (2014). Three tenets for secure cyber-physical system design and assessment. *Cyber Sensing, International Society for Optics and Photonics*, 9097, 90970A.

Humphrey, A., See, S. & Faulkner, D. (2008). A Methodology to Assess Lethality and Collateral Damage for Nonfragmenting Precision-Guided Weapons. *ITEA Journal,* 29, pp.411-419.

Iacono, J., Brown, A. & Holtman, C. (2009). Research Methods-a Case Example of Participant Observation. *Electronic Journal of Business Research Methods*, 7, pp. 39-46.

International Committee of the Red Cross (1977). Rule 8. Definition of Military Objectives. *IHL Database*.

International Committee of the Red Cross (1977). Practice Relating to Rule 14. Proportionality in Attack. *IHL Database*.

Joint Chief of Staff (2012). *No-Strike and Collateral Damage Estimation Methodology*. United States Army.

Kallberg, J. & Thuraisingham, B. (2013). Cyber operations: Bridging from concepts to cyber superiority. *Joint Forces Quarterly*, 68.1, 53-58.

Maathuis, C., Pieters, W. & van den Berg, J. (2016) Cyber Weapons: a Profiling Framework. In Proceedings of the 1st International Conference on Cyber Conflict, pp.1-8. IEEE.

Maathuis, C., Pieters, W. and van den Berg, J. (2018). A Computational Ontology for Cyber Operations. Proceedings of the 17th European Conference on Cyber Warfare and Security, pp. 278-288.

McNeal, G. (2011). The US Practice of Collateral Damage Estimation and Mitigation. *Social Science Research Network*.

Ministry of Defence Shrivenham (2015). *Cyber Primer*. The Development, Concepts and Doctrine Centre.

NATO (2011). *Collateral Damage Estimation*.

NATO (2016). *AJP 3.9 Allied Doctrine for Joint Targeting*.

Nusinov, M., Yang, S.J., Holsopple, J. & Sudit, M. (2009). ViSaw: Visualizing threat and impact assessment for enhanced situation awareness. In Proceedings of the International Conference on Military Communications, p.1-7. IEEE.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chaterrjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management of Information Systems*, 24, 3, 45-78.

Powell, W.S. (2010). Methodology for Cyber Effects Prediction. Black Hat Technical Security Conference.

Raymond, D., Conti, G., Cross, T. & Fanelli, R. (2013). A control measure framework to limit collateral damage and propagation of cyber weapons. In Proceedings of the 5th International Conference on Cyber Conflict, pp.1-16. IEEE.

Romanosky, S. & Goldman, Z. (2016). Cyber Collateral Damage. Procedia Computer Science, 95, pp. 10-17.

Samaan, J.L. (2010). Cyber command: The rift in US military cyber-strategy. *The RUSI Journal*, 155.6, 16-21.

Schreier, F. (2015). *On cyberwarfare*, DCAF Working paper.

Solce, N. (2008). The battlefield of cyberspace: the inevitable new military

branch-the cyber force. *Alb. LJ Sci. & Tech*, 18, 293.

Tabansky, T. (2011). Basic concepts in cyber warfare. *Military and Strategic Affairs*, 3.1, pp. 75-92.

Tremblay, T., C., Hevner, A., R. &. Berndt, D., J. (2010). Focus groups for artefact refinement and evaluation in Design Research. *Communications of the Association for Information Systems*, 26, 27.

United States Army Joint Publications 2-01.1 (2013). Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting.

United States Army Joint Publications 3-12 (R). (2013). *Cyberspace Operations*.

Chapter 5. Effects Assessment Model in Cyber Warfare

"Același viitor prins în trecut
Pierdute idei pe care vreau
Să le aduc în prezent
Iluzii smulse din imensul inert
Balansul ce-l caut în suflete străine
Departe de tot ce mă înalță, susține
Ferit de răspunsuri
Ascunse în mine."
/
"The same future caught in the past
Lost ideas that I want
To bring in the present
Pulled out illusions from the immense inert
The balance I look for in strange souls
Far from everything that exalts me, supports
Protected by answers
Hidden in me."
(Implant pentru refuz feat. Adrian Despot - Ajar)

Based on Maathuis, C., Pieters, W. & van den Berg, J. 2018, "A Knowledge Based Model for Assessing the Effects of Cyber Warfare", *Proceedings of the 12th NATO Conference on Operations Research and Analysis,* NATO.

Cyber Operations such as the ones in Georgia, Ukraine or Stuxnet demonstrated their ability to disrupt, sabotage, or destroy (ICT) systems or (ICT) components of systems and opened long global debates. These incidents show that their effects cross geographic and digital borders, prove to be multi-domain, and affect both military and civilian actors and systems. Although these incidents contributed to a global awareness and development of different (cyber) security programs and strategies, limited attention is paid to understanding and classifying the effects of Cyber Warfare. This is particularly important when planning, executing, and/or assessing the effects of Cyber Operations. To cope with the dynamics, interconnectedness, and evolving nature of cyberspace together with missing or incomplete data(sets) about targets and their environments, embedded under the umbrella of uncertainty and vagueness, we propose a new Operations Analysis model as a knowledge-based model for assessing the effects of Cyber Warfare, nominated as Collateral Damage and Military (Dis)Advantage. The proposed model was implemented in Protégé using OWL to develop the knowledge base, SWRL to write the rules that apply to the knowledge base, and SPARQL to extract data from the knowledge base. This model can serve as a (knowledge-based) simulation environment for decision support in Cyber Operations. It is grounded on empirical and design research in the cyber and military domains, and was evaluated by military-technical experts, the results of which are also presented.

Keywords: Cyber Operations, Cyber Warfare, Cyber Weapons, Cyber Security, Artificial Intelligence, Data Science, Ontology.

5.1. Introduction

"I hear and I forget. I see and I remember. I do and I understand." (Confucius)

Lessons from history show that the Romans were innovative and focused on destroying an enemy's centre of gravity to achieve strategic (military) advantage and win their battles (Gallina et al., 2002). Transposing this ability into cyberspace is difficult since to find the key point that weakens the enemy and achieve the military objective(s) in a Cyber Operation is challenging because of the following two reasons. First, due to the dynamics and uncertainty that surrounds cyberspace, and second because of the fact that information is stored, processed, and transmitted through military and civilian systems since cyberspace is a global shared domain. Cyber Operations like Stuxnet or the ones aimed at Georgia and Ukraine demonstrate that unintended and unforeseeable effects can be

encountered locally, regionally, and even globally (Maathuis et al., 2016; Maathuis et al., 2018a). Although these incidents contributed to global awareness and development of different programs and strategies which mainly focus on detection, incident response, and defense mechanisms, less attention was shown to defining, classifying, or assessing their effects. To address these issues, this research proposes a new Operations Analysis which concerns an Artificial Intelligence knowledge-based model to represent the knowledge around the (un)intended effects of Cyber Operations. The model embeds technical-military knowledge in a comprehensive empirical and design research, and aims at serving as a (knowledge-based) simulation environment for targeting when planning and assessing the effects of Cyber Operations.

In the cyber warfare literature, knowledge-based models are increasingly used. For instance, Chan et al. (2015) proposed a cyber network attack planning knowledge base for supporting planning cyber operations, but it demands further development to become operational. Ormrod et al. (2015) developed a series of ontologies to federating them and simulate the effects of cyber attacks on military units. However, a more detailed approach for each ontology and types of effects needs to be considered. Bodeau & Graubart (2013), Bernier (2013), Marinos (2016), and Simmons et al. (2009) proposed inspirational taxonomies for cyber effects, but without formalizing them. Though, the present chapter builds up on the same logic followed when developing a knowledge graph/base for Cyber Operations in Maathuis et al. (2018a), and supports the assessment methodology for the effects of Cyber Operations by Maathuis et al. (2018b).

The remainder of this chapter is organized as follows. Section 2 describes the followed research approach. Section 3 presents the followed modelling approach and the validation mechanism together with its results. Concluding remarks, limitations, and future research are discussed in Section 4.

5.2. Research Approach

The overarching question underlying this research is: “How to classify and assess the effects of Cyber Warfare?”. To answer this question, an AI approach named Knowledge Representation and Reasoning is taken using the Knowledge Engineering methodology (Schreiber, 2000) followed in a Design Science Research approach (Hevner et al., 2004) because it concerns the design, implementation, and validation of knowledge-based models for different domains and aspects of reality. The resulting model contains a knowledge graph/base implemented as a computational ontology

that represents the effects of Cyber Warfare, a set of rules that reflects the (un)intended effects of Cyber Warfare, and an inference engine that applies the rules to the implemented knowledge graph/ base. Below, each phase of this research approach is elaborated (Schreiber, 2000):

- Requirements and Knowledge acquisition: the necessary information and requirements for building the model are gathered. This is done based on empirical research on five case studies on real incidents (Operation Orchard 2007, Georgia 2008, Stuxnet 2010, Ukraine Black Energy 3 2015, and NotPetya 2017), one case study of a virtual incident (2017) (described in Chapter 4, Section 4.5.), review of scientific literature and military doctrine, combined with field work in joint military exercises, three rounds of interviews with forty military Commanders (see in Appendices-Annex A to C), and a Workshop with three military medical doctors.
- Design: the knowledge collected is prepared to describe and represent the effects.
- Implementation: the knowledge model is implemented in Protégé (a knowledge engineering environment for intelligent systems) using OWL (Ontology Web Language) to develop the knowledge base, SWRL (Semantic Web Rule Language) to write the rules that apply to the knowledge base, and SPARQL Query Language to extract data from the knowledge base.
- Validation: is based on technical and expert evaluation with results presented in Section 3.3.

5.3. Modelling Approach

To develop the proposed model, four (architectural) layers were considered for an (ICT-based) entity (military target/collateral asset, either human or object): physical, software, data, and human, aligned with the information architectures proposed by United States Army (2013), van den Berg et al. (2014), Riley (2016), and Tagarev et al. (2017). Furthermore, on each architectural layer different aspects and qualities of an (ICT-based) entity can be considered, such as performance, functionality, or stability. Accordingly, different types of effects that impact aspects and qualities of a target/asset were identified and depicted: see Annex I and II.

5.3.1. Model Design and Implementation

A Knowledge Representation and Reasoning is an AI-subfield where knowledge is part of a computational process that results into an

intelligent system which emulates existing facts (knowledge) into symbols using semantics (representation) and creates representations for new facts (reasoning) (Brachman & Levesque, 2003). This approach is suitable to assessing effects of Cyber Warfare since it firstly deals with knowledge (technical and expert based) and secondly with data considering the significant lack of available data(sets) of Cyber Warfare incidents which would support working with actionable data in an AI feedback learning-based approach for decision making. Therefore, three points surrounding the model are further discussed: i) knowledge base, ii) rules, and iii) extraction.

The knowledge base is a computational ontology that embeds the architectural layers previously described, is represented in Figure 5.1. and 5.2., and is implemented in Protégé using OWL and Hermit reasoner. Based on (Russell & Norvig, 2016; Fernández-López et al., 1997; Roussey et al., 2011; d'Aquin et al., 2012) we define it as a quintuple (i.e. group of five sets or elements:

Definition 1

$$CWREFF\_KS = \{E, P, C, I, R\}$$

that contains the following elements:

- *E* as the set of entities (i.e. classes or nodes) as main concepts that define the context.
- *P* as the set of properties or attributes that characterize the entities (i.e. data properties).
- *C* as the set of relationships between entities through their instantiations (i.e. object properties).
- *I* as the set of instances/objects/data values of entities.
- R as a set of rules associated with the model.

The knowledge base/graph (proposed model) contains 426 classes, 51 individuals, 358 data properties, and 85 object properties, and is structured on four levels. On the first level are the upper classes which can be found in set E and represent the entities (*TargetOrAsset* class) that are (un)intentionally impacted (*EffectCategory*, *EffectType*, *EffectRole*, and *EffectOn* classes) in a Cyber Operation conducted by an actor (*Actor* class) using a Cyber Weapon (*CyberWeapon* class) measured using a set of socio-technical metrics (*Metric* class). On the second level, the upper classes are extended for a more detailed representation, defining sub-classes which are also found in set E, such as *ResponsibleActor*, *Ransomware*, *CollateralDamage*, *Availability*, *Disturb*, and *SoftwareComplexity*. On the third level are the individuals/objects/data that encapsulate the data collected

from the exemplification case studies, and can be foundin set I. On the fourth level are the data and object properties that describe relations between classes and individuals, as in Figure 5.2, and which can be found in set C. Here *hasJurisdictionOver* establishes which actor has jurisdiction on an object (military target or civilian asset), *hasPrivacyPolicy* shows that an object has implemented a privacy policy, and *hasVendor* establishes which actor is the vendor of an object (either software or hardware).

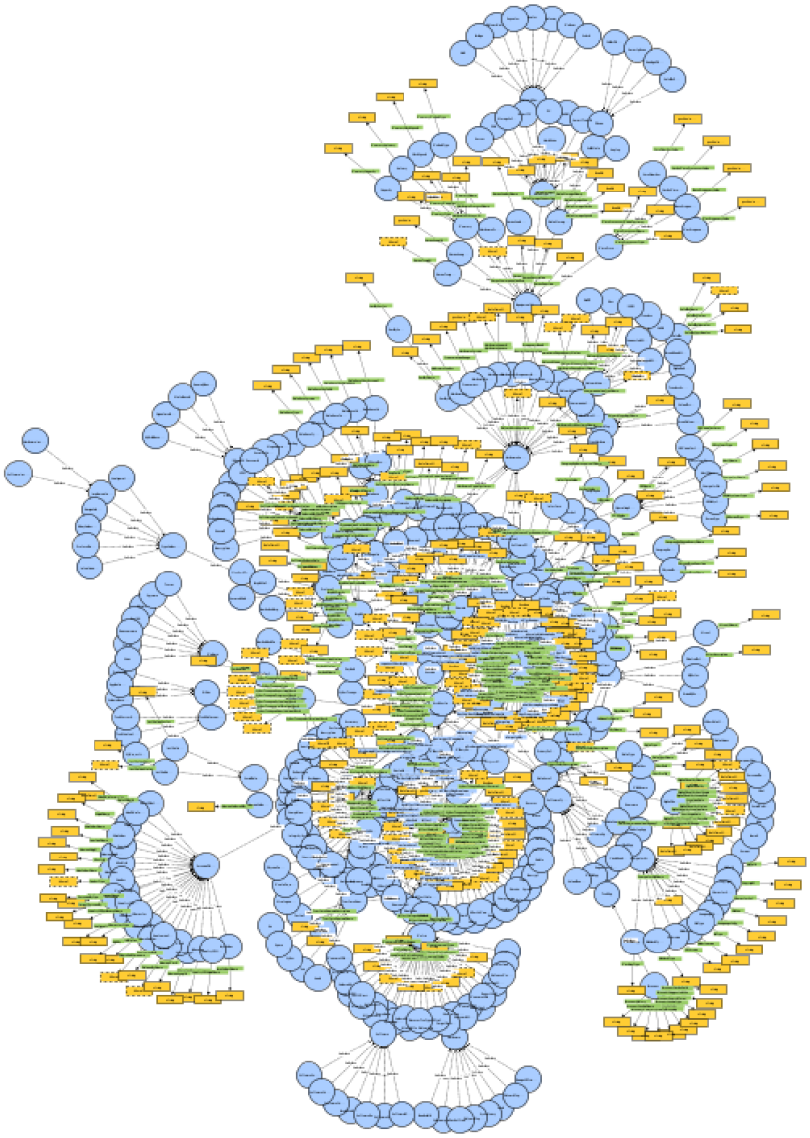


Figure 5.1.a. Cyber Warfare effects knowledge base universe

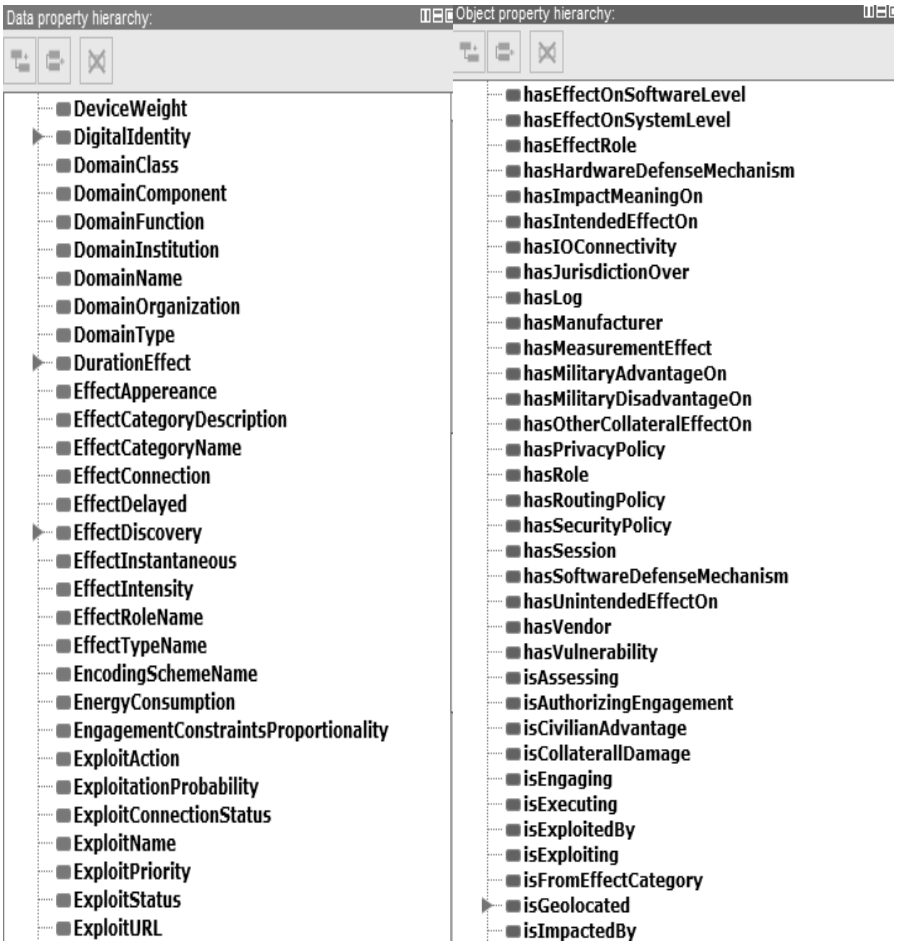


Figure 5.1.b. Cyber Warfare effects data (left) and object (right) properties

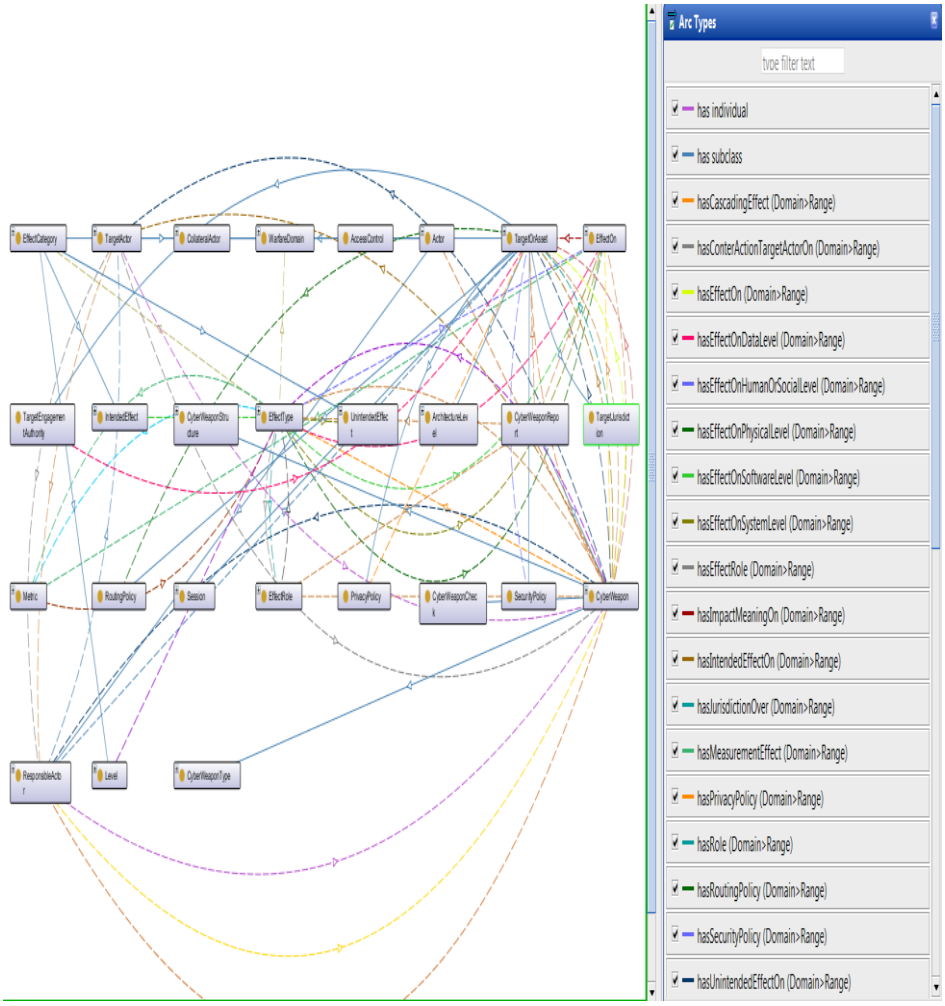
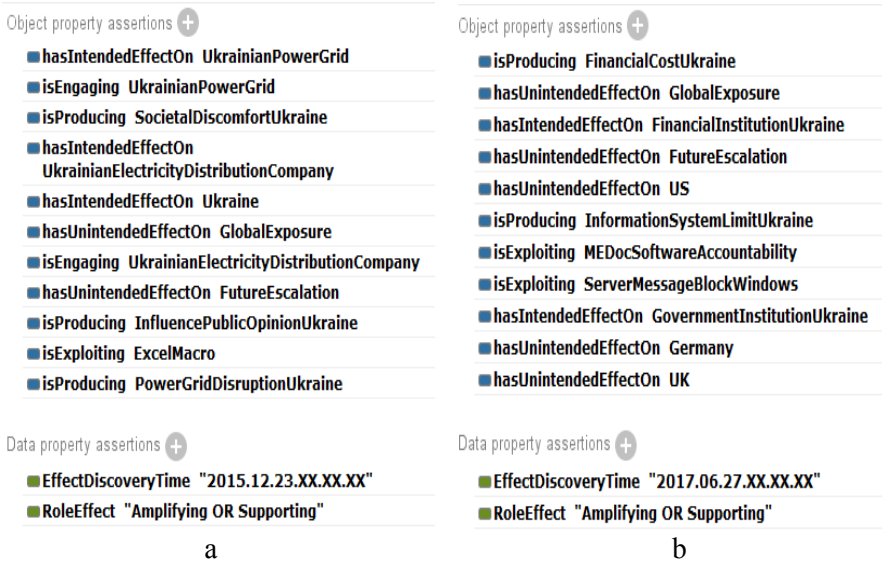


Figure 5.2. Cyber Warfare effects model properties selection

To illustrate the use of this model, the knowledge base was populated with data collected in case studies conducted on Georgia and Ukraine. Furthermore, in Figure 5.3.a and b are depicted values associated with the Cyber Weapons used in Ukraine based on the case studies conducted on them . For each element in the left side the name of a property has a value associated in the right side: for instance, BlackEnergy 3 (individual of class Trojan->Malware- >CyberWeapon) isEngaging (object property) UkrainianPowerGrid (individual of class TargetOrAsset).



class	instance
Availability	TelecomLineAvailabilityUkraine
CollateralDamage	CommunicationStabilityGeorgia

Figure 5.3. Knowledge base data selection on both Ukraine case studies (a, b) and data extraction (c).

Furthermore, 10 rules were designed for further classifying the effects considering the intention and nature criteria (Maathuis et al., 2016; Maathuis et al., 2018b): Military Advantage, Civilian Advantage, Collateral Damage, and Military Disadvantage. These rules apply to the knowledge base and were written in SWRL using forward chaining/reasoning, which means that if the elements in the antecedent are true (IF clause), then the system can infer/conclude the consequent (THEN clause or ->). If we would like to conclude that the *ResponsibleActor* is the *Actor* that *isExecuting* a *CyberWeapon* on a specific legitimate *TargetOrAsset,* the following rule (part of set R) could be considered:

Actor(?x), CyberWeapon(?y), isExecuting(?x, ?y), TargetOrAsset(?z) -> ResponsibleActor(?x)

Furthermore, if we would like to conclude that Collateral Damage is the *EffectType* produced on civilian *TargetOrAssetCheckMilitaryStatus* from the use of a CyberWeapon, then the following rule (part of set R) could be considered:

CyberWeapon(?x), isProducing(?x, ?y), EffectType(?y), TargetOrAssetCheckMilitaryStatus(?z, "civilian"^^xsd:string) -> CollateralDamage(?y)

Moreover, to extract data from the knowledge base a few queries were written in SPARQL. For instance, to extract specific (information about) types of effects using regular expressions, the following can be used:

FILTER regex(?class, "IntendedEffect") .
FILTER regex(?class, "Collateral Damage") .
FILTER (?date > "2015-12-23T14:09:15+06:30"^^xsd:dateTime) . , which returns the items reflected in Fig. 5.3c.

Given the fact that this model allows different operations at both knowledge and data level (e.g. insert, alter or select for extraction), this can be done not just as already described in the implementation languages that were used, but also by using a user interface (e.g. web or desktop) to communicate with this model. Two directions of further practical use within other Military Operations are considered. First, generate a FOM (Federated Object Model) for HLA (High Level Architecture) distributed simulations that implies an alignment between this model and other ones. Second, develop a MAS (multi-agent system) or Multi-Agent Reinforcement Learning based model where multiple intelligent agents interact with each other based on the entities (e.g. classes) and relations between them.

5.3.2. Model Validation

To validate the model and make sure that can reflect real Cyber Warfare incidents, a double approach was considered: technical and expert based (Preece, 2001; Sawsaa & Lu, 2012). The technical based validation implied verifying aspects such as consistency and reusability using the Hermit reasoner in Protégé, and ended being successful. The expert based validation (Appendices-Annex G) involved evaluation aspects like accuracy, clarity, conciseness, and adaptability (Vrandecic, 2009; Sawsaa & Lu 2012), and was conducted in a few meetings organized in July-August 2018 with three military-technical experts with considerable international experience- in average 20 years of experience in military targeting and occupying functions in the field of Cyber Operations (see in Appendices-Annex G). The experts' suggestions were integrated in this model and show that it reflects a realistic representation which can be used to illustrate and assess the effects of Cyber Operations. The experts have considered that the model is accurate and clear, considered that each entity in the model is unique and concise, and due to the fact that the model can be easily extended or

components contained could be deleted, that it is adaptable. Additionally, this model was exemplified on three different case studies of real Cyber Warfare incidents to contemplate its applicability and realism.

5.4. Conclusions

Galileo Galilei advised to "measure what is measurable and make measurable what is not so" (Galileo Galilei). Applied to Cyber Operations, this implies awareness, practice, and a multidisciplinary approach to deal with the challenges and uncertainty that surrounds them, as well as in regards to their effects. Cyber Operations "have moved from a theoretical construct to a realistic option" (Boothby & Schmitt, 2012), imply multiple orders of effects (Boothby & Schmitt, 2012) that can impact both military or civilian actors, allies, friendly, neutral, the target, or even the attackers themselves. When dealing with assessments pre- or post-engagement of (military) targets, (military) decision makers, and their advisers need to have a comprehensive picture of what kind of effects can occur or have occurred on the engaged targets and collateral assets. As these aspects were just scarcely dealt with in the academic literature from a technical-military perspective, in this research a knowledge-based model for assessing the effects of Cyber Warfare in both moments (pre- as in CDE and after- as in BDA) is proposed having in mind to "don't tell the [computer] program what to do, tell it what to know" (Reid Smith).

The proposed model contains an extensive knowledge base and a set of rules that can be easily modified, deleted or shared between different or intersecting fields and experts. The model was evaluated by three military experts, and was exemplified on three real Cyber Warfare incidents to reflect its potential in real events. However, although this model embeds multi-domain types of effects, it mainly focusses on the military-technical (ICT) based ones and just on a high level on the human based ones. This happens due to the level of complexity and significant amount of expertise necessary to represent the knowledge surrounding the effects for all domains which implies a joint multi-domain effort between experts from multiple fields to tackle Cyber Operations conducted in hybrid conflicts. To tackle this point, the Authors suggest to map the list of effects to a shorter list (5 - 10) that could be easier comprehended by other experts, and based on that to consider additional dimensions for the impacted entities. Nonetheless, this model is useful when targeting in Cyber Operations before or post targets' engagement. Conclusively, the results of this research will be used in our future work on limiting the unintended effects and targeting decisions in Cyber Operations.

5.5. Appendix

No	Effect Type Name	Understanding
1	Alter/Manipulate	Refers to modifying information, system's aspects (e.g. functionality, performance), human behaviour or operations' aspects.
2	Attribute	Refers to tracking and identifying the conducting/ executing actor of a cyber weapon/Cyber Operation.
3	Capture/Contain	Refers to detaining an entity having the possibility of commanding, controlling, and restraining it.
4	Compromise	Refers to propagating and infecting other systems.
5	Control	Refers to managing and influencing a human, system, or operation.
6	Deceive	Refers to misleading a system or human by building an unreal or false representation or appearance of entities.
7	Delete/Erase/Wipe	Refers to putting away resources while still being possible to be accessed by using different recovering means (delete) or permanently becoming inaccessible and unrecoverable (erase / wipe).
8	Physical damage	Refers to harming an entity by restraining its access, function or use.
9	Degrade	Refers to depriving or reducing functional, behavioural, or quality aspects of an entity.
10	Delay	Refers to holding on an entity by producing discontinuity in its actions or activities.
11	Demonstrate	Refers to having the ability and means to manifest as a proof of showing force.
12	Deny	Refers to limiting the access or use of systems or information.
13	Destroy	Refers to completely and permanently damage an entity so that it becomes useless and irreparable.
14	Detect	Refers to discovering the conducting/executing actor of a cyber weapon/Cyber Operation.
15	Disrupt	Refers to breaking or altering the functionality of an entity.
16	Disturb	Refers to interfering or perturbing an entity.
17	Encrypt (Decrypt)	Refers to encoding (decoding) information in such a way that is only accessible to the authorised entity (human or system) which has the means to decode it.

18	Expose (Disclose)	Refers to extracting and revealing information about humans, systems, or operations.
19	Fail	Refers to unsuccessfully performing systems, operations, or humans.
20	Injury	Refers to both physical and mental human injury.
21	Isolate	Refers to closing or breaking external connections (including C2) of humans, systems, or operations.
22	Kill/Loss of life	Refers to human fatality.
23	Limit	Refers to applying control measures that infringe the capability of a human, system, or operation to conduct future actions or activities.
24	Monitor	Refers to observing and tracking a human, system, or activity.
25	Neutralize	Refers to applying control measures that infringe the capability of a human, system, or operation to conduct future actions or activities.
26	Overload	Refers to overwhelming or overreaching the capacity or load of a system to impact for instance its functionality, performance, or stability.
27	Recover	Refers to extracting entities from an uncontrolled area or reverting a system to a previous state in which unintended or unforeseeable effects did not occur.
28	Secure	Refers to infringing/protecting the confidentiality, integrity, and availability of humans, systems, or operations.
29	Spread	Refers to propagating to other systems.
30	(De)Stabilize	Refers to equilibrating or making a situation, system, human, or operation (un)stable, (un)balanced, or (in)variable.

Table 5.1. Cyber Warfare Effects types

No	Effect on	Physical Layer	Software Layer	Data Layer	Human Layer	Understanding
1	Access (control)	X	X	X		Refers to controlling the access or actions of a user to a system by granting or limiting its rights.
2	Accuracy			X		Refers to the correctness of data values.

3	Authentication	X	X	X		Refers to verifying a user in order to gain access to a system.
4	Availability	X	X	X		Refers to the availability (in the sense of accessibility and usability) of resources and information to the authorized users or systems.
5	Completeness			X		Refers to the expected fullness and comprehensiveness of data.
6	Confidentiality		X	X		Refers to requiring protecting measures and controls of resources and information to prevent access or disclosure of unauthorized users or systems.
7	Communication Interoperability	X	X			Refers to the ability of communicating and exchanging information between different systems.
8	Connectivity	X				Refers to the ability of a system to be linked to other systems.
9	Consistency		X	X		Refers to the quality of a system or information of being invariable or variable as expecting considering its usability.
10	Encryption	X	X	X		Refers to the mechanism of encoding resources or information to be

						accessible only to the authorized users.
11	Environmental damage or destruction	X				Refers to the partial, temporal or total damage or destruction of geographical (natural) environment.
12	Functionality	X	X			Refers to the ability of a system of executing the expected and designated purpose or function.
13	Integrity	X	X	X		Refers to the correctness and trustfulness of resources and information.
14	Loss of Life				X	Refers to human fatalities.
15	Mental injury				X	Refers to human mental injuries such as: anxiety, depression, stress (PTST), and trauma.
16	Non-repudiation	X	X	X		Refers to reassuring the authenticity (un-deniability) of resources of information.
17	Ownership			X		Refers to the state of legally owning specific data being able of doing different operations e.g. alteration or sharing.
18	Performance	X	X		X	Refers to the ability of a system to fulfil its expected activities or actions.
19	Physical injury				X	Refers to human

						physical injuries such as eye or arm injuries.
20	Privacy			X	X	Refers to the ability or state in which information is selectively expressed/exposed by its owner and is free of intrusion or interference.
21	Robustness	X	X			Refers to the ability of a system to deal with different perturbations by tolerating them.
22	Redundancy	X	X	X		Refers to the existence of other/duplicate resources (backup solutions) that assure the proper functionality of a system.
23	Relevance			X		Refers to the proper meaning of data to different resources/systems.
24	Reliability	X	X	X		Refers to the ability of a system or information to constantly perform its expected function for a specific period of time.
25	Resilience	X	X			Refers to the capacity of a system to recover and adapt from an event and fulfil its expected functionality.
26	Reputation				X	Refers to the (general) opinion or standing regarding a

						person or organization.
27	Scalability	X	X			Refers to the capability of a system to grow and adapt according to its needs.
28	Sensitivity			X		Refers to recommended protecting measures and controls of resources and information to prevent the access of unauthorized users.
29	Stability	X	X			Refers to the quality or state of a system in which its functionality and performance / functional and performance parameters do not variate in an unexpected way.
30	Trust				X	Refers to the capability of being confident in someone or something.
31	Understandability			X	X	Refers to the capability of being comprehended (with reasonable knowledge) in given circumstances.
32	Validity			X		Refers to the correctness and usefulness of information.
33	Vizualization			X		Refers to the visual representation of information.

Table 5.2. Cyber Warfare effects on different layers considering aspects and qualities of (ICT-based) systems

Attribute No	Attribute name	Attribute Definition	Characterizing class	Attribute Type
1	DeviceWeight	represents the weight of the target.	TargetOrAsset -> DeviceWeight	Long
2	DigitalIdentity	contains information about the digital identity of the target.	TargetOrAsset	String
3	DomainClass	contains the domain of the target.	TargetOrAsset -> Domain	String
4	DomainComponent	contains the component of a specific domain of the target.	TargetOrAsset -> Domain	String
5	DomainFunction	contains the function of the target's domain.	TargetOrAsset -> Domain	String
6	DomainInstitution	contains information about the target's domain institution.	TargetOrAsset -> Domain	String
7	DomainName	contains the name of target's domain.	TargetOrAsset -> Domain	String
8	DomainOrganization	contains the name of target's organization where it belongs to.	TargetOrAsset -> Domain	String
9	DomainType	shows the type of domain.	TargetOrAsset -> Domain	String
10	DurationEffect	captures the duration of the effect.	EffectOn, EffectType	String
11	EffectAppearence	captures information about effect's appereance.	EffectOn, EffectType	String
12	EffectCategoryDescription	contains information about effect categories.	EffectCategory	String
13	EffectCategoryName	contains the name for effect categories.	EffectCategory	String
14	EffectConnection	contains information about the moment when an effect appears or relations between different types of effects from a temporal	EffectOn, EffectType	{"Before", "After" , "During"}

		perspective.		
15	EffectDelayed	shows the way the effects are delayed.	EffectType	{"Distributed" , "Localized"}
16	EffectDiscovery	contains information about the moment when the effects are discovered.	EffectOn, EffectType	String
17	EffectInstantaneous	shows how the instantaneous effects where perceived.	EffectType	{"Distributed" , "Localized"}
18	EffectIntensity	shows the intensity of effects.	EffectOn, EffectType	{“Weak”, “Mild”, “Moderate”, “Severe”, “Fatal”}
19	EffectRoleName	captures details about the role of effects.	EffectRole	String
20	EffectTypeName	captures the name of effect types.	EffectType	String
21	EncodingSchemeName	contains the encoding scheme name.	TargetOrAsset	String
23	EnergyConsumption	contains information about the target’s energy consumption.	TargetOrAsset	String
24	EngagementConstraintsProportionality	contains information about proportionality constrains in Cyber Operations.	TargetOrAsset	String
25	ExploitAction	depicts the action of used or planned to be used exploits.	CyberWeapon -> Exploit	String
26	ExploitationProbability	shows the probability of exploitation for a specific cyber weapon.	CyberWeapon -> Exploit	positiveInteger
27	ExploitConnectionStatus	shows the status of connection for a specific cyber weapon.	CyberWeapon -> Exploit	{"Active" , "Inactive"}
28	ExploitName	contains the name of exploit(s).	CyberWeapon -> Exploit	String

29	ExploitPriority	contains the (pre)defined priority for a specific exploit.	CyberWeapon -> Exploit	positiveInteger
30	ExploitStatus	contains the status for a specific exploit.	CyberWeapon -> Exploit	{"Active", "Inactive", "Ready"}
31	ExploitURL	contains the URL (Uniform Resource Locator) of an exploit.	CyberWeapon -> Exploit	String

Table 5.3: Attributes / data properties for the proposed model

Relation No	Relation name	Relation Definition	Relation source class	Relation source destination
1	hasEffectOnSoftwareLevel	shows that effects are perceived at software level.	EffectType	EffectOn, Target -> SoftwareLevel
2	hasEffectOnSystemLevel	shows that effects are perceived at system level.	EffectType	EffectOn, Target -> SystemLevel
3	hasEffectRole	shows the role of specfici types of effects.	EffectType	EffectRole
4	hasHardwareDefenseMechanism	shows the defense mechanism applied at hardware level.	TargetOrAsset	TargetOrAsset -> TargetDefenseMechanism
5	hasImpactMeaningOn	show which effects are perceived by targets and / or assets.	EffectOn	TargetOrAsset
6	hasIntendedEffectOn	shows that a specific cyber weapon has desired effects on a specific target.	CyberWeapon	TargetActor TargetOrAsset
7	hasIOConnectivity	illustrates the level of IO connectivity at software level.	SotwareLevel	TargetOrAsset -> IOConnectivity
8	hasJurisdictionOver	shows who has jurisdiction on a specific target.	Domain -> TargetJurisdiction	TargetOrAsset
9	hasLog	shows that log exists at software / hardware	TargetOrAsset	SoftwareLevel, HarddwareLev

		level.		el
10	hasManufacturer	shows who is the manufacturer for specific software / hardware.	TargetOrAsset	Software / HarddwareLevel -> Software / HadrwareManufacturer
11	hasMeasurementEffect	shows how or in which way the effect could be measured.	EffectType, EffectOn	Metric
12	hasMilitaryAdvantageOn	shows that there is Military Advantage on specific targets or assets.	EffectCategory -> MilitaryAdvantage	TargetOrAsset, TargetOrActor
13	hasMilitaryDiasdvantageOn	shows that there is Military Disadvantage on specific targets or assets.	EffectCategory -> MilitaryDisadvantage	TargetOrAsset, TargetOrActor
14	hasCollateralDamageOn	shows that there is Collateral Damage on specific collateral civilian assets.	EffectCategory -> MilitaryDisadvantage	TargetOrAsset, TargetOrActor
15	hasPrivacyPolicy	shows that specific targets or assets have implemented a privacy policy.	TargetOrAsset	Domain -> PrivacyPolicy
16	hasRole	reflects the role of a specific effect type.	EffectType	EffectRole
17	hasRoutingPolicy	shows that specific targets or assets have implemented a routing policy.	TargetOrAsset	Domain -> RoutingPolicy
18	hasSecurityPolicy	shows that specific targets or assets have implemented a security policy.	TargetOrAsset	Domain -> SecurityPolicy
19	hasSession	reflects opened sessions from both hardware and software levels.	HardwareLevel, SoftwareLevel	Domain -> Session
20	hasSoftwareDefenseMechanism	shows the defense mechanism applied at software level.	TargetOrAsset	TargetOrAsset -> TargetDefenseMechanism
21	hasUnintend	shows that a specific	CyberWeap	Actor,

	edEffectOn	cyber weapon has undesired effects on a specific target.	on	TargetOrAsset
22	hasVendor	shows the manufacturer of the target or a specific component of the target.	TargetOrAsset	Software / HarddwareLevel -> Software / HadrwareVendor
23	hasVulnerability	reflects a software or hardware vulnerability of a specific target.	TargetOrAsset	SoftwareLevel -> SoftwareVulnerability, HardwareLevel -> HardwareVulnerability
24	isAssessing	shows that an actor is assessing the effects of a cyber weapon.	Actor	CyberWeapon
25	isAuthorizingEngagement	shows who is the authorizing engagement authority in order to engage a specific target.	Domain -> TargetEngagementAuthority	TargetOrAsset
26	isCivilianAdvantage	shows that specific effects types can be categorized as Civilian Advantage (i.e. effects that bring a positive impact to civilian actors and systems).	EffectType	EffectCategory -> CivilianAdvantage
27	isCollateralDamage	shows that specific effects types can be categorized as Civilian Advantage.	EffectType	EffectCategory -> CollateralDamage
28	isEngaging	shows which target is engaged by a cyber weapon.	CyberWeapon	TargetOrAsset
29	isExecuting	shows what actor is executing a particular cyber weapon.	ResponsibleActor	CyberWeapon
30	isExploitedBy	shows which vulnerability(ies) is (are) exploited by particular exploit(s).	SoftwareVulnerability, HardwareVulnerability	Exploit

31	isExploiting	shows who is exploiting particular vulnerability(ies).	Exploit	SoftwareVulnerability, HardwareVulnerability
32	isFromEffectCategory	reflects from which effects category belong specific effect types.	EffectType	EffectCategory
33	isGeolocated	captures the geolocation for a specific target or asset.	TargetOrAsset	Geolocation
34	isImpactedBy	captures which mean (cyber weapon) is impacting a specific target, asset, and / or actor.	TargetOrAsset, Actor	CyberWeapon

Table 5.4: Relations / object properties for the proposed model

5.6. References

Bernier, M. (2013). *Military activities and cyber effects (MACE) taxonomy.* Defence Research and Development Canada, Centre for Operational Research and Analysis.

Bodeau, D. & Graubart, R. (2013). *Characterizing effects on the cyber adversary: A vocabulary for analysis and assessment*. The MITRE Corporation.

Boothby, W., H. & Schmitt, M., N. (2012). *The law of targeting*. Oxford University Press.

Brachman, R., J. & Levesque, H., J. (2003). *Knowledge Representation and Reasoning*.

Chan, P., Theron, J., van Heerden, R. & Leenen, L. (2015). An ontological knowledge base for cyber network attack planning. In Proceedings of the 10th International Conference on Cyber Warfare and Security (pp. 69).

D'Aquin, M., Kronberger, G. & Suarez-Figueroa, M.C. (2012). Combining data mining and ontology engineering to enrich ontologies and linked data. Proceedings of the first international workshop on Knowledge Discovery and Data Mining Meets Linked Open Data (pp. 19-24).

Fernández-López, M, Gómez-Pérez, A & Juristo, N. (1997). 'Methontology: From ontological art towards ontological engineering', Proceedings of the fourteenth national conference on Artificial Intelligence, AAAI-97, Spring Symposium Series, pp. 33-40.

Gallina, D., Gorman, P., Herman, M., MacDonald, J. & Ryer, R. (2002). *Military Advantage in History*. Office of the Secretary of Defense for Net Assessment, Pentagon.

Hevner, A., R., March, S., T. & Park, J. (2004). Design Research in Information Systems Research. *MIS Quarterly.* 28, 1, 75 – 105.

Maathuis, C., Pieters, W. and van den Berg, J. (2016). Cyber weapons: a profiling framework. In Proceedings of the 1st International Conflict on Cyber Conflict U.S. (pp. 1-8). IEEE.

Maathuis, C., Pieters, W. and van den Berg, J. (2018a). A Computational Ontology for Cyber Operations. In Proceedings of the 17th European Conference on Cyber Warfare and Security (pp. 278-288).

Maathuis, C., Pieters, W. and van den Berg, J. (2018b). Assessment methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations. In Proceedings of the 35th IEEE International Conference on Military Communications Conference. IEEE.

Marinos, L. (2016). *ENISA Threat Taxonomy: A tool for structuring threat information.* ENISA, Heraklion.

Ormrod, D., Turnbull, B. & O'Sullivan, K. (2015). System of systems cyber effects simulation ontology. In Proceedings of the Winter Simulation Conference (pp.2475-2486). IEEE.

Preece, A. (2001). Evaluating verification and validation methods in knowledge engineering. *Industrial Knowledge Management*, 91-104.

Riley, S. (2016). A model for increased understanding of cyber activity. Centre for Strategic Cyberspace and Security Science. Retrieved March 3rd, 2017, from http://cscss.org/CS/2016/08/20/cyber-terrain-a-model-for-increased-understanding-of-cyber-activity.

Roussey, C, Pinet F, Kang, MA & Corcho O (2011). An introduction to ontologies and ontology engineering', G Falquet, C Métral, J Teller & C

Tweed (Eds.), *Ontologies in urban development projects*. Springer, 1, pp. 9-38.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson Education Limited.

Sawsaa, A.F. & Lu, J. (2012). Building Information Science ontology (OIS) with Methontology and Protégé. *Journal of Internet Technology and Secured Transactions*, 1, 3/4.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A cyber attack taxonomy. Proceedings of 9th Annual Symposium On Information Assurance (pp. 2-12).

Schreiber, A. T., Schreiber, G., Akkermans, H., Anjewierden, A., Shadbolt, N., de Hoog, R. & Wielinga, B. (2000). *Knowledge engineering and management: the CommonKADS methodology*. MIT press.

Tagarev, T., Sharkov, G. & Stoianov, N. (2017). Cyber security and resilience of modern societies: a research management architecture. *Information & Security*, 28, 93-108.

United States Army Joint Publications 3-12 (R). (2013). *Cyberspace Operations*.

Van den Berg, J. (2018). Cybersecurity for Everyone. Cyber Security Best Practices. M. Bartsch. & S. Frey (Eds.), Springer.

Vrandecic, D. (2009). Ontology Evaluation. S. Staab. & R. Studer (Eds.). *Handbook of Ontologies* (pp. 293-313). Springer.

Chapter 6. Effects estimation and targeting decisions in Cyber Warfare

"Now that the war
is through with me
I'm waking up, I
cannot see
That there is not
much left of me
Nothing is real but
pain now
….
Back to the world
that's much too
real,
In pumps life that I
must feel
But can't look
forward to reveal
Look to the time
when I'll live."
(Metallica - One)

Based on Maathuis, C., Pieters, W. & van den Berg, J. 2020, "Decision Support Model for Effects Estimation and Proportionality Assessment for Targeting in Cyber Operations", Journal of Defence Technology, 2019(1), DOI: https://doi.org/10.1016/j.dt.2020.04.007, Elsevier.

Cyber Operations are relatively a new phenomenon of the last two decades. During that period, they have increased in number, complexity, and agility, while their design and development have been processes well kept under secrecy. As a consequence, limited data(sets) regarding these incidents are available. Although various academic and practitioner public communities addressed some of the key points and dilemmas that surround Cyber Operations (such as attack, target identification and selection, and collateral damage), still methodologies and models are needed in order to plan, execute, and assess them in a responsibly and legally compliant way. Based on these facts, it is the aim of this article to propose a model that i)) estimates and classifies the effects of Cyber Operations, and ii) assesses proportionality in order to support targeting decisions in Cyber Operations. In order to do that, a multi-layered fuzzy model was designed and implemented by analysing real and virtual realistic Cyber Operations combined with interviews and focus groups with technical-military experts. The proposed model was evaluated on two Cyber Operations use cases in a focus group with four technical-military experts. Both the design and the results of the evaluation are revealed in this article.

Keywords: Cyber Operations, Cyber Warfare, Cyber Weapons, Artificial Intelligence, Intelligent Systems, Fuzzy Logic, Targeting.

6.1. Introduction

motto:
"I can calculate the motion of heavenly bodies, but not the madness of people." (Isaac Newton)

Listening to an 8D audio song (Malham & Myatt, 1995; Baalman, 2010) is a unique experience as sound comes from multiple directions *travelling through the human brain*. Applying this surround sound technique to a song it is currently perceived as one of the last revolutions in the musical industry, although it was developed and played with by rock bands since the 70's. The technique itself uses multiple audio channels from a listener's setup (e.g. headphones or speakers) implying enriching the fidelity and depth of sound reproduction. The way how sound *travels through the human brain* is consonant to the way how information travels at incredibly fast speeds through rapid changing, dynamic, and interconnected networks of cyberspace. In cyberspace, information is surrounded by its uncertain interpretation and use in distinct activities (e.g. Cyber Operations) by different actors and systems. Although cyberspace is currently sensed as the fifth and latest warfare domain (NATO, 2018), it relies on ICT, which exists

for decades. As cyberspace represents "a critical feature of modern society" (Kanuck, 2009), its usage through Cyber Operations as a common landscape and battlefield for everyone and everything raises significant amount of questions, doubt, and poses great challenges and threats. Among these challenges, when conducting military Cyber Operations in order to transit from a current state that needs to be changed to a desired end state (Center for Army Lessons Learned, 2015), military forces need to act responsibly and be legally compliant. But how is this possible when there are no commonly agreed definitions, methodologies, models, techniques or frameworks that would facilitate their planning, execution, and/or assessment?

As in the last two decades incidents labelled as Cyber Warfare or military Cyber Operations have increased in number, complexity, and agility, they represent a wake-up call to what it is possible to happen in the future. This signifies being aware what kind of implications and consequences they have or can have, in other words knowing or being able to predict or estimate what the effects of their actions are. The aforementioned statement points into two main directions. First, the effects of Cyber Operations need to be (as much as it is possible with the given information at the time) known before their execution as basis for judgement in regards with the proportionality principle (Additional Protocol I 1977 Art. 48; Additional Protocol I 1977, Art. 57(2)(a)(iii); Additional Protocol I 1977, Art. 57(2)(b)). Based on this principle, is established if a specific target can be proposed for engagement with an explicit cyber weapon. And second, the effects of Cyber Operations need to be (as much as it is possible with the given information at the time) known after their execution in order be able to further proceed in their assessment, assess the effectivity of Cyber Operations, and to learn lessons for future operations. This is aligned with the aim of this research that aims at assessing the effects of Cyber Operations and advising targeting concerning the proportionality assessment before targets' engagement in Cyber Operations.

For Cyber Operations such as the ones conducted in Georgia in 2008 (Hollis, 2011), Stuxnet conducted on a larger timescale but discovered in 2010 (Falliere et al., 2011; McDonald et al., 2013) or the ones conducted in Ukraine between 2015 and 2017 (Case, 2016; Fayi, 2018), significant amount of analysis was conducted by both academic researchers and practitioners in regards to their effects. This represents the second direction as it was abovementioned described, where the effects of these Cyber Operations were analysed based on historical revealed data(sets) from sources such as reports or observations. However, in order to address the first direction previously outlined, and to be more specific in regards to planning and execution of Cyber Operations as key moments during

targeting in Cyber Operations, the rationale for conducting this is research is as follows.

This research addresses key points and dilemmas regarding targeting in Cyber Warfare (e.g. related to the meaning of a target and collateral damage, as well as the applicability of the proportionality principle) which have been pointed in studies such as (Boothby, 2012; Gill & Fleck, 2011; Romanosky, 2017; Schmitt, 2013; Schmitt, 2017). These key points and dilemmas have also been tackled by practitioners from participating and intersecting domains (military, technical-military, technical, military-legal, political), which have been put forward in various occasions like congresses, conferences, and workshops. At the same time, this study deals with the availability of empirical data, empirical studies, and a significant gap in the identified space of artefacts (e.g. models, methodologies, and techniques) developed for or applied in Cyber Operations. Thus, more research needs to be done in this field for assessing in both senses of analysing (e.g. types, classes, and metrics) and estimating or predicting the effects of Cyber Operations while taking into consideration the fact that some notions (might) need per definition a re-interpretation or extension.

On this subject, this research builds on previous work that concerned understanding Cyber Operations and building models and methodologies to assess their effects (Maathuis et al, 2018b; Maathuis et al., 2018c; Maathuis et al., 2018d; Maathuis et al., 2016) by proposing a novel AI-based multi-layered model with the following objectives:

- To estimate and classify the effects of Cyber Operations as the core of the proportionality assessment in Cyber Operations.
- To conduct the proportionality assessment in order to support targeting decisions in Cyber Operations.

Furthermore, this chapter contributes with two embedded Cyber Operations use cases to designing realistic cyber war-games as Cyber Operations case scenarios useful for implementing other artefacts such as models and methodologies, and further doctrines, strategies, and policies for Cyber Operations.

The remainder of this chapter is organized as follows. The second section summarizes important and relevant research from both technical and military angles. The third section describes the research approach pursued in order to design, develop, and evaluate the model proposed in this chapter. The fourth section provides an overview of the AI technique used in this chapter to implement the model: Fuzzy Logic. The fifth section discusses the considered design and implementation requirements and decisions

followed for the proposed model and its components. The sixth section discusses the evaluation mechanism using both experts and use cases, presents the use cases that have been selected for evaluation purposes, and illustrates simulation results of the proposed model for the considered use cases together with experts' evaluation remarks. The last section deliberates concluding reflections, possible extensions as well as future lines of research.

6.2. Background and Related Research

In order to achieve the aim of this chapter, a literature review was conducted crossing domains such as Cyber Security, Military Operations/Defense Studies, and Artificial Intelligence. The aim of this literature review was not to get a complete overview of all existing dilemmas and possibilities in these domains, but to gather the necessary background information from a technical-military perspective, and to identify the existing gaps in the body of knowledge aligned with the objectives of this chapter. The results of the review are discussed in the two sub-sections below.

6.2.1. Military Operations: military and legal dimensions

Military targeting denotes conducting military operations against opposing parties in conflict in order to achieve established political and/or military aims or goals (*ends* through *effects*), implies establishing operational approaches (*ways*) where targets (*nodes*) should be engaged (*action*) using available *resources* (*means*) as illustrated in Figure 6.1. (NATO , 2016; NATO, 2013; U.S. Army, 2013).

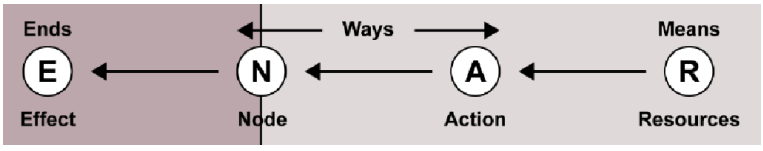


Figure 6.1. Military Targeting: ends, ways, and means (capture from NATO, 2016 at page 21)

Targeting is considered to link strategic-level direction and guidance to tactical-level activities through an operational-level targeting cycle in order to create effects that support the achievement of military objectives and the end state of the mission. Furthermore, the targeting

cycle contains the following six phases (NATO, 2016; Boothby, 2012; Melzer, 2008):

- Phase I – Commander's intent, objectives, and guidance: political and strategic direction and guidance is provided in order to identify clear and well-defined objectives together with under what circumstances and parameters these objectives can be achieved.
- Phase II – Target development: centres of gravity of the enemy are established and through their associated vulnerabilities, eligible targets are identified in order to affect them and achieve the objectives. Furthermore, the identified targets are analysed, vetted, validated, and prioritized producing a prioritized target list that also considers the estimation and minimization of Collateral Damage-Collateral Damage Estimation (CDE). CDE is a methodology that is being applied from Phase II, is continued in Phase III and is also relevant in Phase V by providing an estimation of collateral damage.
- Phase III – Capabilities analysis (sometimes also referred as Weaponeering): once the prioritized list of targets has been developed, these potential targets are further analysed and matched with appropriate lethal and non-lethal capabilities in order to generate intended effects and achieve the objectives defined while minimizing unintended effects by considering CDE. Furthermore, the proportionality assessment is conducted by the Commander in order to analyse if collateral damage (based on CDE) is excessive in relation to the concrete and direct military advantage anticipated. This corresponds with the military-legal targeting perspective as defined in Chapter I, Section 1.2.2 Additionally, different are consider for engaging military targets by considering the development of multiple Courses of Action (CoAs). This implies developing, analysing, and comparing different ways to achieving military aims by incorporating and weighting the both expected intended and unintended effects, and correspond with the military-operational targeting perspective as defined in Chapter I, Section 1.2.2.
- Phase IV – options Commander's decision, force planning, and assignment: the results obtained in the previous phase are assigned to specific forces/units for further planning and execution while taking into consideration any relevant constraints and restraints.
- Phase V – Mission planning and force execution: the mission is further planned at tactical level and prepared for execution while a final target positive identification (PID) is controlled together with other information checks and collateral damage avoidance or

minimization. Furthermore, force execution consists of six steps (Find, Fix, Track, Target, Engage, Exploit).

- Phase VI – Assessment (sometimes also referred as Battle Damage Assessment): evaluation regarding produced effects and the achievement of objectives is conducted based on collected information and it further contributes to wider assessments, lessons learned or input for other missions.

As it can be concluded from the above description, targeting concerns a complex and challenging process. Both consulted technical-military experts and military scientific literature describe the conduct of military operations as both "science and art" since movement or weapon effects calculations are quantifiable, thus they are perceived as "the science of war", while other aspects such as leadership or predicting enemy's intentions are seen as "the art of war" (HQ Department of the Army, 1997). These mainly human aspects add and sometimes amplify technical aspects (e.g. changing and uncertain environment, identification, attribution) of conducting military operations inside or outside cyberspace by using cyber weapons/capabilities/means as acts of Cyber War or military Cyber Operations (Maathuis et al., 2018d). As (Schreier, 2015) argues that "warfare of the 21st century involving opponents possessing even a modicum of modern technology is not possible without access to cyberspace", this implies the following processes. Firstly, to be first aware of the role cyberspace and Cyber Operations play or can play since "newly employed technologies provide unprecedented platforms" (Couretas, 2019) when achieving military and/or political goals. Secondly, to prepare properly for their planning, execution, and assessment together with anticipated synergies for achieving military and/or political goals (e.g. Cyber Operations conducted against Georgia in 2008, Ukraine in 2015-2017 or years later in the counter-terrorism fight).

The "sluggish nature of the law's responses to new developments in the very nature of warfare" (Boothby, 2012) led to different debates and positions among military-legal, military, and military-technical scholars and practitioners towards the applicability of the Law of Armed Conflict (LOAC) or the laws of war to cyber weapons/Operations/Warfare. The key stays not only in the possible advances and developments of technology and the body of law, but in the hands and in the eyes that interpret these advances and developments, or contrarily, their lack thereof. It is important to acknowledge NATO's position regarding the applicability of the LOAC in cyberspace, expressed at the NATO Wales Summit in 2014: "our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace" (NATO, 2014). This vision

is aligned with the one provided by the Tallinn Manual (Schmitt, 2013; Schmitt, 2017).

Furthermore, the core of LOAC/IHL (International Humanitarian Law) is represented by Geneva Conventions and their Additional Protocols that intend to "regulate the conduct of armed conflict and seek to limit its effects" (ICRC, 2010). Of particular interest, the Additional Protocol I argues that there it should be a clear distinction between civilian population and civilians objects on one side and lawful targets on the other side, and stretches the fact that the operations should only be directed to lawful targets (Additional Protocol I 1977 Art. 48; ICRC, 2005). Moreover, when a lawful/legitimate target is considered to be engaged in attack, military commanders and their staff have to do "everything feasible to verify" (Additional Protocol I 1977, Art. 57(2)(a)(i)) that it is a real legitimate target. Accordingly, attacks shall be limited to military objectives [i.e. military targets as persons or objects]. In so far as objects are concerned, military objectives [i.e. military targets] are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" (Additional Protocol I 1977, Art. 52(2)). Furthermore, they should not allow, avoid or limit an attack that would (Additional Protocol I 1977, Art. 57(2)(a)(ii)) "cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (Additional Protocol I 1977, Art. 57(2)(a)(iii); Additional Protocol I 1977, Art. 57(2)(b)).

The "excessive" term is interpreted by some military-legal advisors as "shock to the conscience", "clearly unreasonable", "unreasonable" or "significant imbalance" (Wright, 2012). To be able to conduct the proportionality assessment/principle in Cyber Operations (just as in any other type of Military Operations, in phases III-V), "timely, accurate, and reliable information" needs to be collected, processed, analysed, disseminated, and further used (Joint Staff, 2003) together with Commander's – as responsible authority and decision maker (NATO, 2016a; Jachec-Neale) – ability "to see in real time the position and status of his assets – as well as his enemy's – and the ability of a war fighter to know with assurance what's around the next corner or behind the next mountain is simply invaluable". To do that, the (cyber war) fighting team (Franz, 2011) guided under the responsibility of a Commander relies on their "creative application of knowledge, practice, cognition, imagination, and intuition" (Tuija et al., 2016]. Granting these facts that cross the technical realm and go into the human realm (e.g. human cognition capacities such as reasoning,

evaluation, and judgement together with human mental states and feelings such as stress or anger), it is obvious that the need for further research regarding applying traditional approaches to new technologies exists.

Grounded on the abovementioned observations, targeting decision making and in particular, proportionality assessment, can be seen as a Naturalistic Decision Making (NDM) process since the decisions that must be taken are "based on experience, pattern, situation awareness, and story constructions" (Stone, 2015) and are by definition surrounded by uncertainty in dynamic environments in ill-defined or ill-structured problems (Lipshitz et al., 2001; Orasanu, 2005). Among the domains where NDM is applicable, are next to the military domain (e.g. command and control, aviation), domains such as management, business and industry (e.g. manufacturing), health care (e.g. anaesthesiology), nuclear plant operations, software design, and jury deliberations (Lipshitz et al., 2001; Orasanu, 2005; Zsambok & Klein, 1996). Furthermore, as the aim of the present chapter is to propose an AI model that estimates, classifies, and advices targeting decisions based on proportionality assessment, it basically attempts to quantify the effects and propose the advising decision as a Rational Choice decision aid system (Zsambok & Klein, 1996), in other words a Decision Support System (Burstein & Holsapple, 2008; Rospocher & Serafini, 2012; Druzdzel & Flynn, 2017) in Cyber Operations. In other words, the proposed multi-layered fuzzy model uses a combination of data(sets) and expertise gathered from translating mental processes (e.g. cognition-reasoning and judgement) to action.

6.2.2. Fuzzy Logic used in Cyber Warfare and Security

The use of Artificial Intelligence techniques in the cyber or information domain has significantly increased in the last years as it enables designing automatic computing solutions to solve different relevant societal problems (Dilek et al., 2015). In particular, Fuzzy Logic is an AI technique "heavily used" in cyber defence (Newcomb & Hammel, 2016) and military decision tools (Prelipcean et al., 2010). Relevant research to this chapter is further outlines.

(Tavana et al., 2014) advances a fuzzy logic model for military C2 systems that estimates financial impact of an attack on the availability and integrity of assets.

In (Alali et al., 2018), a cyber security risk assessment fuzzy model is proposed to assess the risk of different entities to cyber crime incidents. In

this regard, the risk factors that were utilized are as follows: vulnerability, threat, likelihood, and impact.

Sallam (2015) introduces a multi-layered fuzzy system to assess the risk scale to cyber threats considering the following contributing risk factors: overall capabilities of an attacker, overall likelihood of an attack success, and the impact of an attack.

In (Azimirad & Haddaria, 2015) a target threat fuzzy based assessment model is presented to support weapon assignment and intelligence sensor support systems.

In (Yang, 2016) a grey-based clustering algorithm for vulnerability assessment for electric cyber-physical systems is introduced integrating confidentiality, integrity, availability, and collateral damage potential as defining variables.

(Graf et al., 2016) introduces a fuzzy model as a decision support system for Situational Awareness in national Cyber Operations Centres by combining anomaly data with expert (user) knowledge.

In (Zheng et al., 2009), a fuzzy model for evaluating the harm of computer viruses is advanced considering the following levels of harm: slight, ordinary, serious, great, and devastating.

Hence, the review presented in this sub-section reflects a broader range of applications in the cyber and information domains including military or warfare applications. However, to the best of the authors' knowledge, the present chapter introduces for the first time a novel multi-layered model that classifies and estimates the effects of Cyber Operations, and advances targeting decisions concerning proportionality in Cyber Warfare.

6.3. Research Approach

The present chapter is based on empirical and design technical-military research aiming at introducing a multi-layered model that estimates the effects of Cyber Operations and advices targeting decisions based on proportionality of target's engagement. To be able to do that, research was conducted as the combination of Cyber Security, Artificial Intelligence, and Military Operations expertise, techniques, and methods. Accordingly, a Design Science Research (Peffers et al., 2008; Hevner & Chatterjee, 2010) approach was followed as it facilitates the design, development, and

evaluation of artefacts such as models, methods, and frameworks considering the following scientific activities:

Activity I: Problem Identification and Motivation

This research intends to support targeting in Cyber Operations/ Warfare, and its underlying motivation is threefold.

Firstly, is grounded on the increasing number of Cyber Operations globally integrated more and more in political and military vision (e.g. strategies and policies) and toolboxes together with the acknowledgement of their use on different moments and in different countries. Henceforward, for the present research the following Cyber Operations case studies were conducted on: Operation Orchard (Syria, 2007), in Georgia during the Russian-Georgian war (Georgia, 2008), Stuxnet (Iran, 2010), Black Energy 3 (Ukraine, 2015), and NotPetya (Ukraine, 2017).

Secondly, the practical need for decision support when targeting in Cyber Warfare was clearly emphasized in:

- three sets of semi-structured interviews held in 2016 and 2017 with forty military Commanders with significant international military and technical experience (above 15 years in military operations and exercises), from Netherlands, Germany, and U.S. (see Appendices-Annex A to C). The interviewed military experts were asked to present and discuss their requirements and expectations regarding the assessment of Collateral Damage and Military Advantage together with targeting decisions in Cyber Operations. Additionally, they were asked to elaborate on how they would deal with excessive Collateral Damage or not receiving customary information.
- direct participation and observation in two joint military exercises in 2016 and 2017 as field work which facilitated the achievement of a comprehensive vision on Cyber Operations in regards with their role, use, assessment of effects, and targeting decisions.

Thirdly, is based on the identified gap in the space of scientific artefacts in the field of Cyber Warfare reflected by the (already mentioned) real need for targeting decision support in Cyber Operations. Hence, from an extensive review of scientific literature in all the research domains considered in this research (Cyber Warfare and Security, Military Operations, and Artificial Intelligence), military doctrine, strategies, and reports, it can be concluded that military Cyber Operations lack models and methodologies for planning, execution, and assessment although the effects of their use can impact not only the engaged targets, but also other

collateral civilian and military actors and systems (Maathuis et al. 2018a). Accordingly, related research that tackles tangent points to this research is presented in the Related Work section of this chapter and Activity III.

Activity II: Definitions of the Objectives for a Solution

Based on Activity I, the aim of this research is to support targeting decision making in Cyber Warfare by designing a fuzzy-based multi-layered model that has the following objectives:

- To estimate and classify the effects of Cyber Operations, and
- To advice targeting decisions in the sense of concluding if engaging a specific target in a specific Cyber Operation is not-disproportional or disproportional (proportionality principle).

Activity III: Design and Development

The functionality, architecture, and design of the artefact proposed in this research (multi-layered model) are determined based on the resources gathered and presented in Activity I and Section 6.5. Moreover, based on these resources, the following design requirements were established:

- To be structured, adaptable, and illustrative.
- To be compatible, familiar or designed in a similar way as the methodologies and models used in conventional Military Operations.
- To consider space and force dimensions.
- To be evaluated on realistic Cyber Operations scenarios.

Additionally, previous work regarding the assessment of effects (Maathuis et al., 2018b) and targeting decisions in Cyber Operations (Maathuis et al., 2018c) was used as guidance and input in the present research.

Activity IV: Demonstration

To be able to demonstrate the proposed artefact as a proof-of-concept, two-face-to-face meetings with a military technical expert with significant international experience were organized in March-April 2019. In the first meeting, a brainstorming session was carried out about the development of virtual and realistic use cases/case studies that would be suitable to evaluate the proposed model. In the second meeting, some alternatives for two use cases were discussed with the military expert, and for each use case was selected the best one advised by the military expert.

Conclusively, the proposed model in this research was evaluated using two Counter-terrorism Cyber Operations on a suicide drone and a cargo ship, further elaborated in the Evaluation and Results sections.

Activity V: Evaluation

The model designed and developed in Activity III was proposed for demonstration in Activity IV and evaluation in the present activity, based on two virtual use cases conducted in a Focus Group (Tremblay et al. 2010) organized by TNO (the Netherlands Organization for Applied Scientific Research) and the Netherlands MoD in one day in April 2019 with the name "From Effects Estimation to Targeting Decisions in Cyber Warfare" (see Appendices-Annex F). In this regard, four military-technical experts were selected based on their background and experience (in military operations, training, and exercises) which can provide reliable and credible information and findings. The selected experts were invited to participate in this Focus Group. Consequently, the model was evaluated and simulated with the collected data (see variables in the Appendix) from the consulted military-technical experts, and the results of this process are presented in the Evaluation and Results section of this chapter.

Activity VI: Communication

The results of the present research were communicated and presented through presentations, meetings, e-mails, the present chapter, and double-blind reviewed article (Maathuis et al., 2020).

6.4. Fuzzy Logic

This chapter proposes an AI model based on Fuzzy Logic in order to estimate and classify the effects of Cyber Operations, and propose targeting decisions based on proportionality assessment in Cyber Operations. In this research, this modelling technique was used to design the proposed solution inspired by the deep learning (Goodfellow et al., 2016) approach (multi-layers that refine the information and predict the final advising decision). This was chosen due to the fact that it facilitates modelling problems that need to be solved "in an environment of imprecision, uncertainty, incompleteness of information, conflicting information, partiality of truth and partiality of possibility-in short, in an environment of imperfect information" (Zadeh, 2008) reflected by the lack of available data(sets) together with the uncertainty and dynamism that governs Cyber Operations as well as other human and operational aspects and factors discussed in Section II of this chapter. To cope with these concerns, a mix between

limited datasets (e.g. case studies on real and virtual incidents) and expertise from military-technical experts (e.g. interviews and Workshops) was used (Prelipcean et al., 2010).

To describe human reasoning and real live events, a logic based on duality (true/false, good/bad) is not enough or not always adequate. In this sense, Lotfi A. Zadeh – the pioneer or the creator of fuzzy sets and based on that, fuzzy logic (1965) as the redesign of the multivalued logic advanced by Lukasiewicz (Shanmugavadivu & Nagarajan, 2011) – extended in his work the classical two valued logic which is defined by the binary values 0 and 1, to the whole continuous interval between these two values, [0,1]. Hence, a gradual transition between *false* and *true* is realized due to the existence of a grade or membership function noted by μ, that is a real number between 0 and 1. The membership function $\mu_U(x)$ denotes how an element x belongs (as a grade) to a *universe of discourse* U (i.e. all elements that come into consideration in a specific context).

A membership function can be represented in a continuous or a discrete way. In a continuous way, the membership function is a mathematical function such as the most used ones in different fuzzy logic applications: triangular, trapezoidal or Gaussian. In a discrete way, the membership function is represented by values in a vector (list). To be able to completely describe the fuzzy variable x, *linguistic variables* are used. The linguistic variables take as values words or sentences, and have associated different membership functions. For an example, see Fig. 3.

Due to its major use in decision making applications, this chapter uses triangular membership functions (Mandami & Assillian, 1975; Klir & Yuan, 1995; Goztepe, 2012). These functions are described by the three parameters in the universe of discourse U, as such: ll represents the low limit or bound which is the smallest possible value, m represents the mean, and hl represents the high limit or bound which is the biggest possible value. These functions are further defined in (1) and illustrated in Fig. 6.2.

$$\mu_U(x) = \begin{cases} 0, x < ll \\ \frac{x-ll}{m-ll}, ll < x < m \\ \frac{hl-x}{hl-m}, m < x < hl \\ 0, x > hl \end{cases} \quad (1)$$

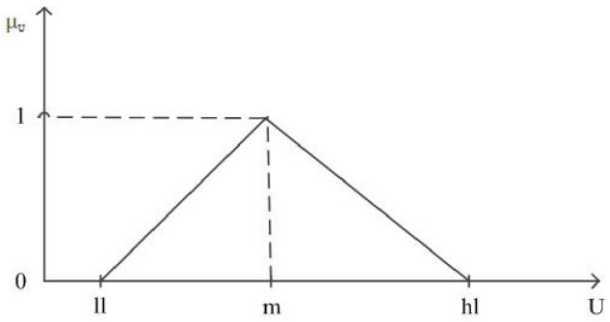


Figure. 6.2. Triangular membership functions

Direct exemplifications of how these functions are used in this research are provided in the following section. Furthermore, taking into consideration that human reasoning can interpret and use imprecise, vague or ambiguous terms and logic in different contexts and problems, logical statements are constructed as sentences using *connectives (*correspondent to *logical operations)* just as in a natural language used by the human brain, such as AND, OR, NOT, and IF-THEN. For exemplification, IF-THEN means a *conditional* sentence where the sentence following IF is called *antecedent*, and the sentence after THEN is called *consequent*.

For instance, the mechanism of defense of a target is computed in the proposed model in this chapter using a linguistic variable named TargetDefenseMechanism that is computed using triangular membership functions and has Weak and Strong as defined fuzzy sets. This variable is depicted in Figure 6.3.

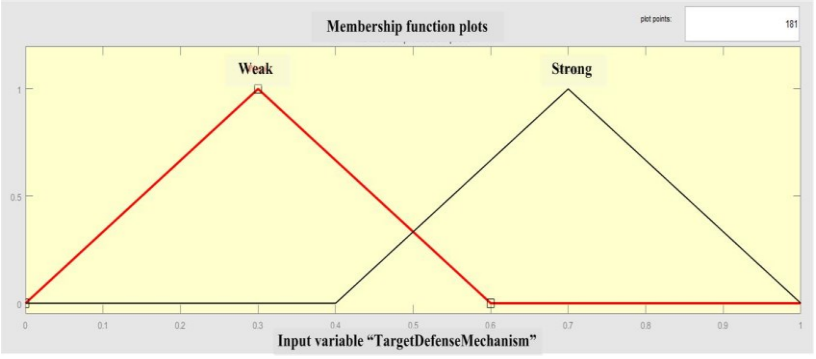


Figure. 6.3. TargetDefenseMechanism linguistic variable computed using triangular membership functions

Moreover, a Fuzzy Inference System is able to extract conclusions from approximations of data using these linguistic variables and their

membership functions (Baturone et al., 2000). Accordingly, the Fuzzy Inference System mechanism is presented and illustrated in Figure 6.4. At the beginning, a crisp set of input value is gathered and converted into a fuzzy set using the input fuzzy linguistic variables and input membership functions through the Fuzzification Interface. Furthermore, based on the established fuzzy rule base consisting of a set of fuzzy if-then rules and by using an inference mechanism, the fuzzy inference is made in the Decision-making unit. At the end, in the Defuzzification Interface, the resulting output is defuzzified and mapped into a crisp output value using a weighted averaging approach of the calculated fuzzy output values.

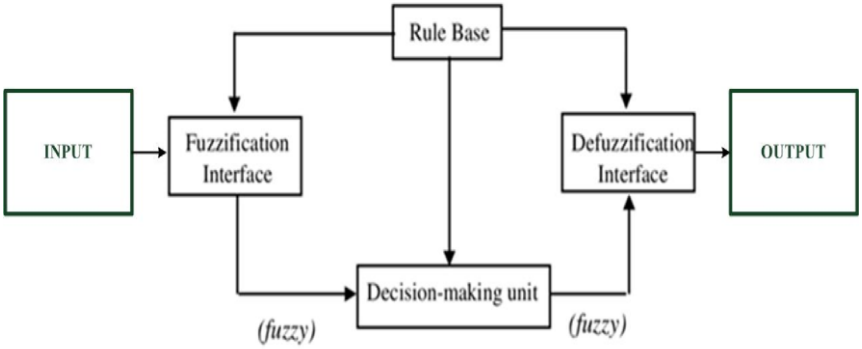


Figure. 6.4. Fuzzy Inference System

There are three common inference systems known. These are Mamdani Fuzzy models, Sugeno Fuzzy Models, Tsukamoto Fuzzy models (Singhal & Banati, 2013). In our approach, we are using the Mamdani Fuzzy inference system as it is best suitable to adapt our approach and is most commonly used alone or in conjunction with other AI/Machine Learning techniques based on Artificial Neural Networks or Genetic (Evolutionary) Algorithms. Hereby a short list of applications: intrusion detection (Lu et al., 2018), Internet of Things performance evaluation (Wibowo & Grandhi, 2018), alert systems for controlling cyber bullying (Kumar & Kathiresan, 2016), cyber situation awareness (Huang et al., 2016), in information hiding with stenography (Kumar et al., 2019), in cryptography for the substitution cipher algorithm (Kulkarni et al., 2012), navigation of humanoid robot (Rath et al., 2018), terrorist event classification (Inyaem et al., 2010), and pilot's behaviour assessment in warfare simulations (Rao & Balas-Timar, 2014).

Hence, the illustrated technique has a diverse pallet of applications in different domains by representing a way to design and implement intelligent systems (e.g. expert systems) providing the main advantage of mathematically dealing with the uncertainty of information that is "gray"

(i.e. vague, ambiguous, imprecise) by nature (Smith, 1994). Accordingly, in the coming section of this chapter, the design and implementation of the model are further presented.

6.5. Design and Implementation

To be able to introduce the design and the way the proposed model was implemented (see Activity III in Section 6.3.), a reflection on the underlying mechanism is necessary. This mechanism is depicted in Figure 6.5. and embedded in Figure 6.6., and contains the following key points:

- First, Military Advantage and Collateral Damage (A in Figure 6.5.) are two separate types of effects (intended and unintended) of Cyber Operations and their estimation is done at different moments, circumstances, and by different actors. From the field work conducted in the present research (e.g. interviews and Workshops with military experts as well as direct participation and observation in joint military exercises) along with the scientific literature consulted and resumed in Section 2 of this chapter, the coming remarks can be made. On one side, in past and current Military Operations, the estimation of Military Advantage is based on the human reasoning and decision making as important functions of human cognition of military Commanders advised by their team. Aligned with this, one of the military experts interviewed pointed that is based on "the feeling of knowing the opponent" at the given time with the given information, thus not relying on specific models or methodologies. On the other side, in past and current Military Operations, the estimation of Collateral Damage is based on the CDE (Collateral Damage Estimation) methodology which is an estimation methodology done by the intelligence forces (U.S. Army, 2018) in order to advise military Commanders.
- Second, from the abovementioned resources, as suggested by the military Commanders consulted in this research, a broader perspective was considered in order to model both Military Advantage and unintended effects represented by Collateral Damage and Military Disadvantage in Cyber Operations. Both perspectives are below elaborated when the architecture of the proposed artefact is introduced (see Figure 6.6). That implies also including unintended effects on military actors and systems (e.g. own military forces and systems or the target itself) which are named in this research as Military Disadvantage in further decisions. The proportionality assessment/principle signifies not only bringing two different entities surrounded by uncertainty together in a complex environment (Collateral Damage and Military Advantage), but also dealing (as the consulted military experts

assessed) with other human aspects and factors such as military Commander's background, experience, culture, (exposure and resistance to) stress, willingness to take risks (risk appetite), and even religion. To cope with these facts, military Commanders need to be "flexible, quick, resilient, adaptive, risk taking, and accurate" (Cannon-Bowers & Bell, 1997), responsible and legally compliant.

- Third, as a result of the proportionality assessment, the following two options can be considered. First, in case the Cyber Operation is not-disproportional, then the considered target could be engaged using the specific cyber weapon. Second, in case the Cyber Operation is disproportional (thus unlawful), then the Cyber Operation should be aborted/stopped and control measures (C in Figure 6.5.) for avoiding or minimizing Collateral Damage should be examined. Additionally, these control measures should be considered from the beginning when Collateral Damage is expected (C with an arrow in both senses in Figure 6.5.). In case of a worst case scenario i.e. in case of intentionally conducting an unlawful Cyber Operation, then this is punishable as it is a war crime (Boothby, 2012; Schmitt, 2013).

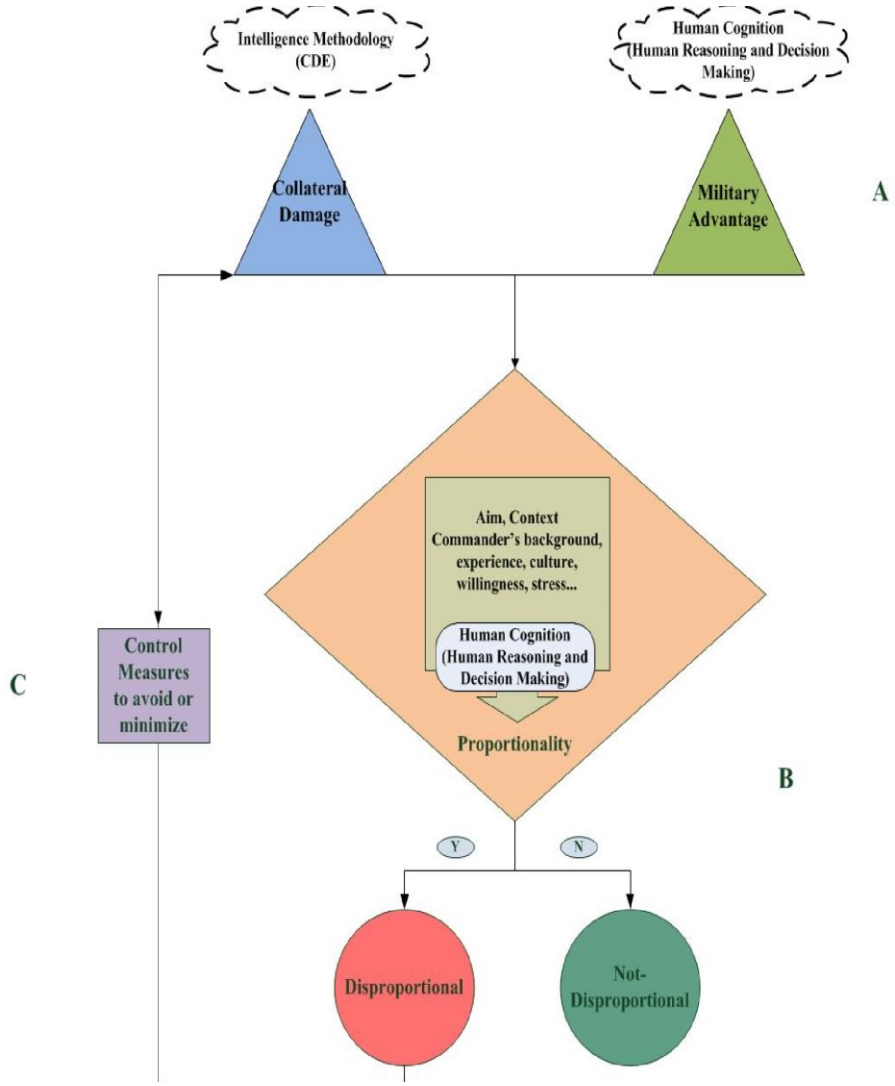


Figure 6.5. Effects estimation and targeting decisions in Cyber Operations

Based on the underlying mechanism described, a multi-layered fuzzy model has been designed as an intelligent system (Grosan & Abraham, 2011) with its architecture illustrated in Figure 6.6. The first and second layer/model depicted in Figure 6.6. correspond to the blocks before the decision depicted in Figure 6.5., and the third layer/model illustrated in Figure 6.6. corresponds to the decision block illustrated in Figure 6.5. The model was implemented using the Mandani fuzzy inference system in MATLAB, and contains three layers of fuzzy models aiming at first, estimating the effects of Cyber Operations, second, classifying the effects of Cyber Operations considering as main classification criteria intention and

nature (Maathuis et al., 2016), and third, deciding if the act of engaging a specific target with a specific cyber weapon in a Cyber Operation is not-disproportional or disproportional. The proposed multi-layered model is based on a deep learning approach, and uses limited data and expertise (Shang & Zakir, 2013) and previous work (Maathuis et al., 2016; Maathuis et al., 2018a; Maathuis et al., 2018b; Maathuis et al., 2018c; Maathuis et al., 2018d) in regards to assessing Cyber Operations and their effects, while aiming at (prescriptively) supporting targeting decision making in Cyber Operations. This represents a hybrid approach (combination of data and knowledge) used since it allows embedding both data (from the incidents) and expertise (from the consulted experts) in the designed model. Moreover, each component is discussed considering design and implementation decisions.

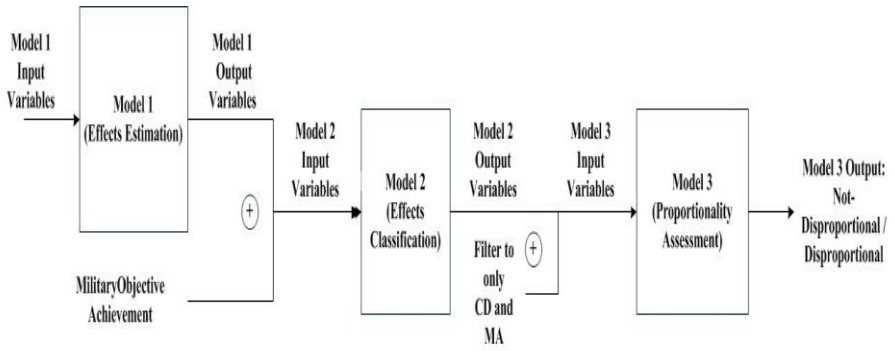


Figure. 6.6.. Multi-layered model for effects estimation and targeting decisions in Cyber Warfare

Based on the abovementioned aspects and design decisions, two perspectives or contexts of use were firstly introduced in Chapter I in Section 1.2.2. and are further considered for the proposed multi-layered model:

- The first perspective is of *military-legal nature* and is based on the legal interpretation of the proportionality assessment (as already introduced and further elaborated in this section). This perspective brings together two categories of effects: Collateral Damage and Military Advantage.
- The second perspective *military-operational nature* and is based on considering preparations for developing different CoAs for engaging military targets. This perspective brings together a broader perspective by embedding both intended and unintended effects under three categories of effects named: Collateral Damage, Military Advantage, and Military Disadvantage.

The first model is illustrated in Figure 6.7.-9. clearly separates military targets from civilian objects (based on the principle of distinction), as follows: in Figure 6.7. are depicted the input and output variables, in Figure 6.8. is illustrated a membership function for one of the input variables, and in Figure 6.9. are captured a part of the rules. The model embeds the military-operational perspective or context of use as defined in Section 1.2.2. which means that includes all the effects considered in Figure 1.4. The model contains 11 input variables and 7 output variables identified in (Maathuis et al., 2018b; Maathuis et al., 2018c) and are based on information given before the execution of a Cyber Operation. These variables are characterized by triangular membership functions.

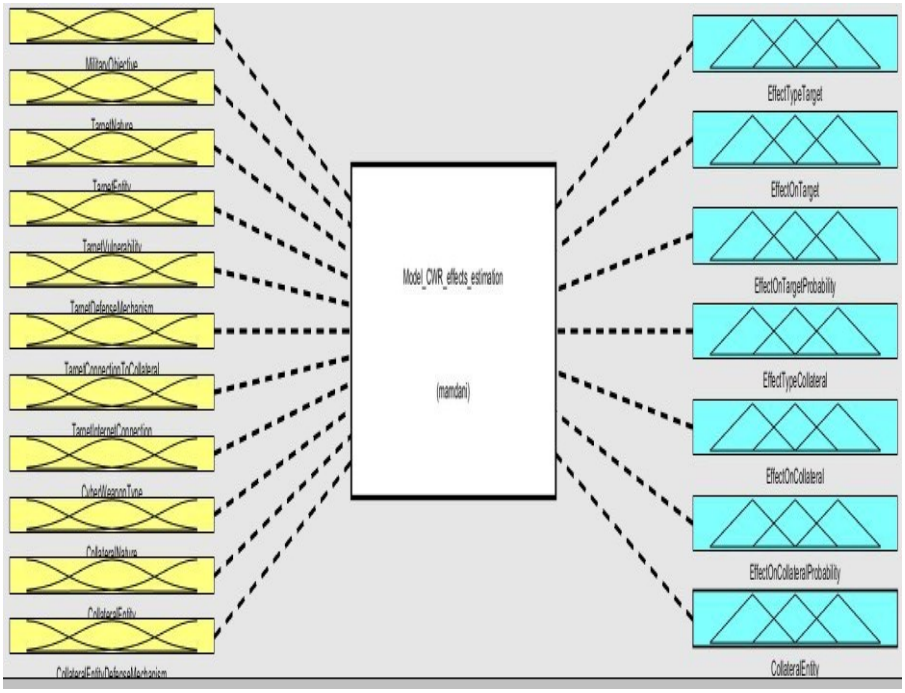


Figure. 6.7. Effects Estimation Model in Cyber Operations

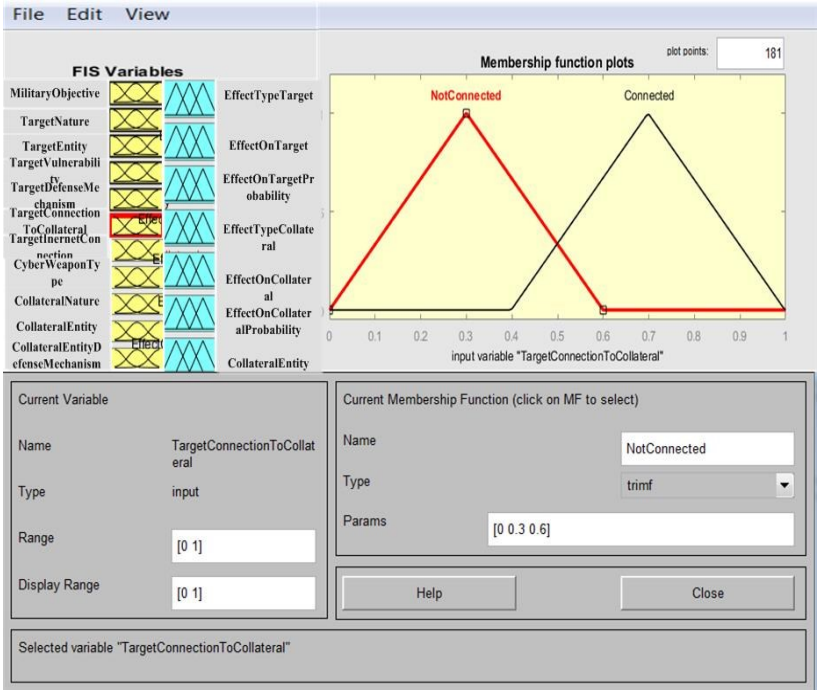


Figure. 6.8. TargetConnectionToCollateral input variable membership functions

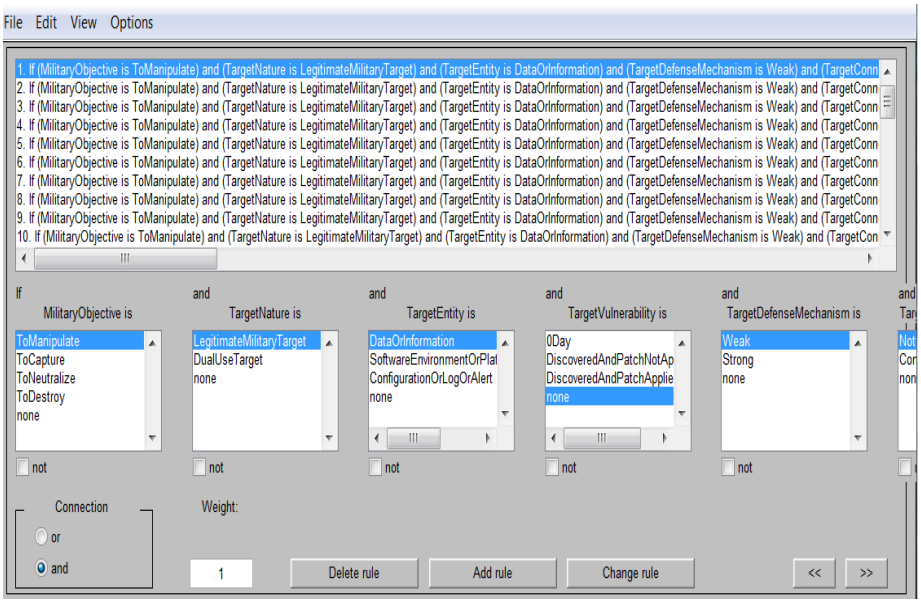


Figure. 6.9. Effects Estimation Model rules in Cyber Operations

A detailed description for calculating the membership functions of the variables *MilitaryObjective* and *TargetVulnerability* are further provided using equation (2) in equations (3) and (4) below. Further, in the Appendix section of this chapter are defined all the variables used.

$$\mu_{MilitaryObjective}(x) = \begin{Bmatrix} \left(\max\left(min\left(\frac{x}{0.15}, \frac{0.3-x}{0.15}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.23}{0.15}, \frac{0.53-x}{0.15}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.463}{0.15}, \frac{0.763-x}{0.15}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.7}{0.15}, \frac{1-x}{0.15}\right), 0\right)\right) \end{Bmatrix} \quad (3)$$

$$\mu_{TargetVulnerability}(x) = \begin{Bmatrix} \left(\max\left(min\left(\frac{x}{0.19}, \frac{0.38-x}{0.19}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.31}{0.19}, \frac{0.69-x}{0.19}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.62}{0.19}, \frac{1-x}{0.19}\right), 0\right)\right) \end{Bmatrix} \quad (4)$$

A rule which concludes that there is a Very High probability to achieving the intended effects on a software-based target with a weak defense mechanism based on an exploited 0-day vulnerability and that there are no collateral effects on other collateral civilian systems when the target has no collateral connections and no Internet connection, is defined in such a way:

IF (MilitaryObjective IS ToManipulate) AND (TargetNature IS LegitimateMilitaryTarget) AND (TargetEntity IS) AND (TargetEntity IS SoftwareEnvironmentOrPlatformOrApplication) AND (TargetVulnerability IS 0Day) AND (TargetDefenseMechanism is Weak) AND (TargetConnectionToCollateral IS NotConnected) AND (TargetInternetConnection IS NotConnected) AND (CyberWeapon IS Malware) AND (CollateralNature IS CollateralCivilian) AND (CollateralEntity IS DataOrInformation) AND (CollateralEntityDefenseMechanism IS Strong) THEN (EffectTypeTarget IS Alter) AND (EffectOnTarget IS Integrity) AND (EffectOnTargetProbability IS VeryHigh) AND (EffectTypeCollateral IS No) AND (EffectOnCollateral IS No) AND (EffectOnCollateralProbability IS No) AND (CollateralEntity IS OnCollateralCivilian)

Above an example of just one single rule was introduced. In practice, depending on the input provided, multiple rules get activated (fired) and their output is aggregated and defuzzyfied to a crisp value using the centroid weighted averaging algorithm (Chen et al. 2001; Siler & Buckley, 2005)

Moreover, a selection of the input and output variables are depicted in Table 1 with complete definitions for all the variables presented in the Annex of this chapter.

Input / Output Variable and Definition	Value Variable (Fuzzy Set)
MilitaryObjective = The aim / goal of a Cyber Operation.	ToManipulate / ToCapture / ToNeutralize / ToDestroy
TargetDefenseMechanism = The assessment of a target's defense mechanism(s).	Weak / Strong
CyberWeaponType = The type of cyber weapon.	Malware / DDoS
CollateralNature = The status of a collateral entity in the sense of being civilian, allied, friendly or neutral to this Cyber Operation.	CollateralAlliedOrFriendlyOrNeutralMilitary / CollateralCivilian
EffectOnTarget = The aspect or quality of the target that is impacted.	No/MentalOrPhysicalHealthOrLossOfLife / Trust / Reputation / Privacy / Confidentiality / Integrity / Availability / Authenticity / Accountability
EffectOnTargetProbability = The probability of impacting the target.	No / Low / Medium / High / VeryHigh
EffectTypeCollateral = The type of effect that impacts a collateral entity.	No / MentalOrPhysicalInjuryOrLossOfLife / Alter / Disclose / Degrade / Control / Isolate / Delete / Destroy / Accountability

Table 6.1. Effects Estimation Model variables in Cyber Operations

The second model is illustrated in Figure 6.10.-6.11., as follows. In Figure 6.10. are depicted the input and output variables and in Figure 6.11 are captured a part of the rules. The model embeds the military-operational perspective or context of use as defined in Section 1.2.2. which means that includes all the effects considered in Figure 1.4. The model contains 8 input variables and 6 output variables based on the effects classification presented in (Maathuis et al., 2016; Maathuis et al., 2018c) characterized by triangular membership functions.

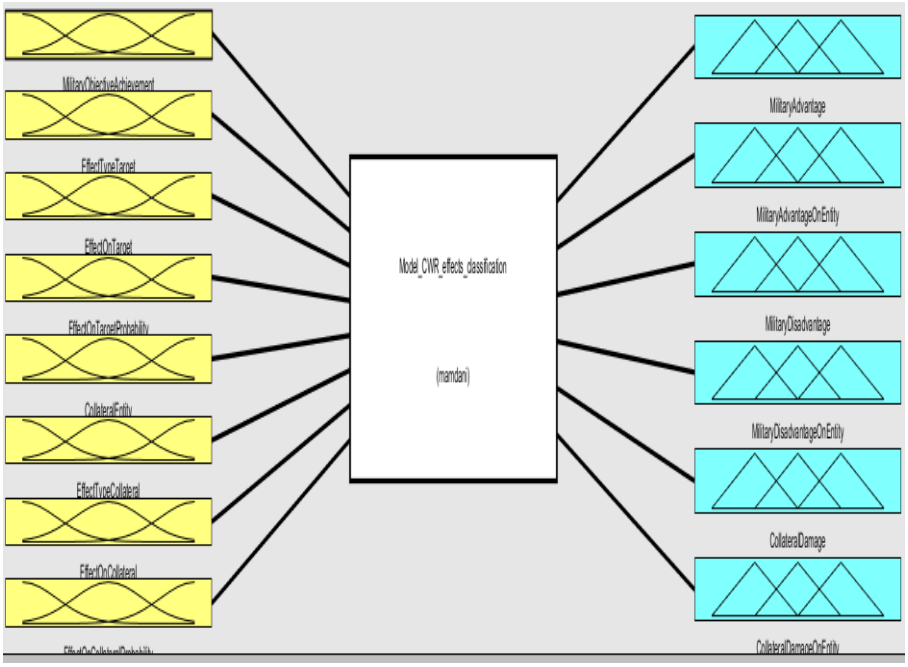


Figure 6.10. Effects Classification Model in Cyber Operations

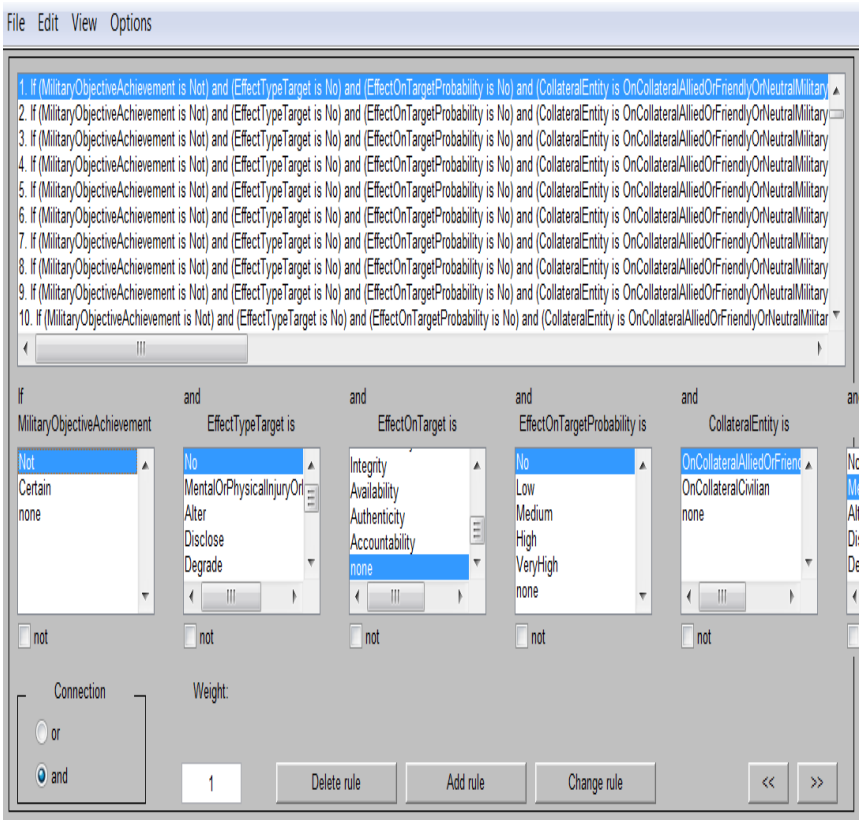


Figure 6.11. Effects Classification Model rules in Cyber Operations

A detailed description for calculating the membership functions of the variable *EffectTypeTarget* is further provided using equation (2) in equations (5) below. Further, in the Appendix section of this chapter are defined all the variables used.

$$\mu_{EffectTypeTarget}(x) = \left\{ \begin{array}{l} \left(\max\left(min\left(\frac{x}{0.0555}, \frac{0.111 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.111}{0.555}, \frac{0.222 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.222}{0.555}, \frac{0.333 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.333}{0.555}, \frac{0.444 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.444}{0.555}, \frac{0.555 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.555}{0.555}, \frac{0.666 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.666}{0.555}, \frac{0.777 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.777}{0.555}, \frac{0.888 - x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x - 0.888}{0.555}, \frac{1 - x}{0.0555}\right), 0\right)\right) \end{array} \right\} \quad (5)$$

A rule which concludes that the there is a high Military Advantage while Collateral Damage is low is further defined:

IF (MilitaryObjectiveAchievement IS Certain) AND (EffectTypeTarget IS Degrade) AND (EffectOnTarget IS Availability) AND (EffectOnTargetProbability IS High) AND (CollateralEntity IS CollateralCivilian) AND (EffectOnCollateralProbability IS Low) THEN (MilitaryAdvantage IS High) AND (MilitaryAdvantageOnEntity IS NonHuman) AND (MilitaryDisadvantage IS No) AND (MilitaryDisadvantageOnEntity IS No) AND (CollateralDamage IS Low) AND (CollateralDamageOnEntity IS NonHuman)

Furthermore, a selection of the input and output variables are defined in Table 2 with complete definitions for all the variables presented in the Annex of this chapter.

Input / Output Variable and Definition	Value Variable (Fuzzy Set)
MilitaryObjectiveAchievement = The achievement of the already defined Military Objective.	No / Certain
MilitaryAdvantage = Intended effects that contribute to the achievement of military objectives.	No / Low / Medium / High / VeryHigh
MilitaryAdvantageOnEntity = The type of	Human / NonHuman

entity which is impacted by Military Advantage.	
MilitaryDisadvantage = Unintended effects that do not contribute to achieving military objective(s), but impact allies, friendly, neutral, even the target or conducting actors.	No / Low / Medium / High / VeryHigh
CollateralDamage = Unintended effects that do not contribute to achieving military objectives, but impact civilian assets, in the form of civilian injury or loss of life and/or damage or destruction to civilian objects and/or environment.	No / Low / Medium / High / VeryHigh
CollateralDamageOnEntity = The type of entity which is impacted by Collateral Damage.	Human / NonHuman

Table 6.2. Effects Classification Model variables in Cyber Operations

The third model is illustrated in Figure 6.12.-14. is based on the proportionality test, as follows. In Figure 6.12. are depicted the input and output variables, in Figure 6.13. is illustrated a membership function for one of the input variables, and in Figure 6.14. are captured a part of the rules. The model embeds only the military-legal perspective or context of use as defined in Section 1.2.2. which means that includes only Collateral Damage and Military Advantage depicted with green and red in Figure 1.4. The model contains 4 input variables and 1 output variables characterized by triangular membership functions.

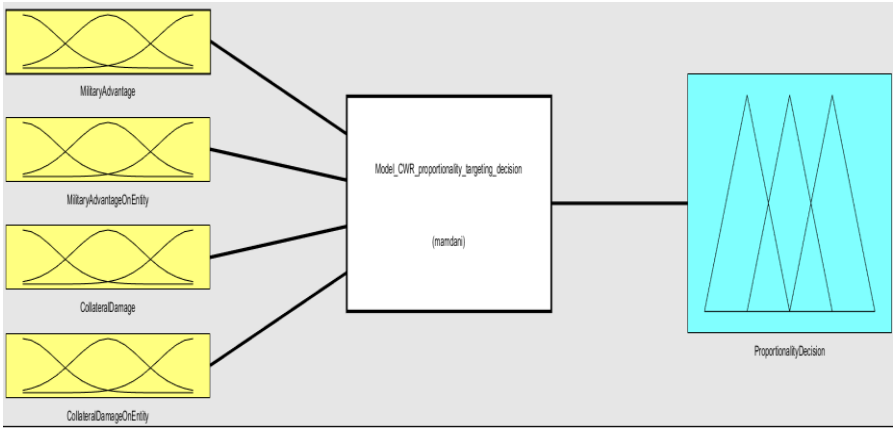


Figure 6.12. Targeting Decision Model based on Proportionality Assessment in Cyber Operations

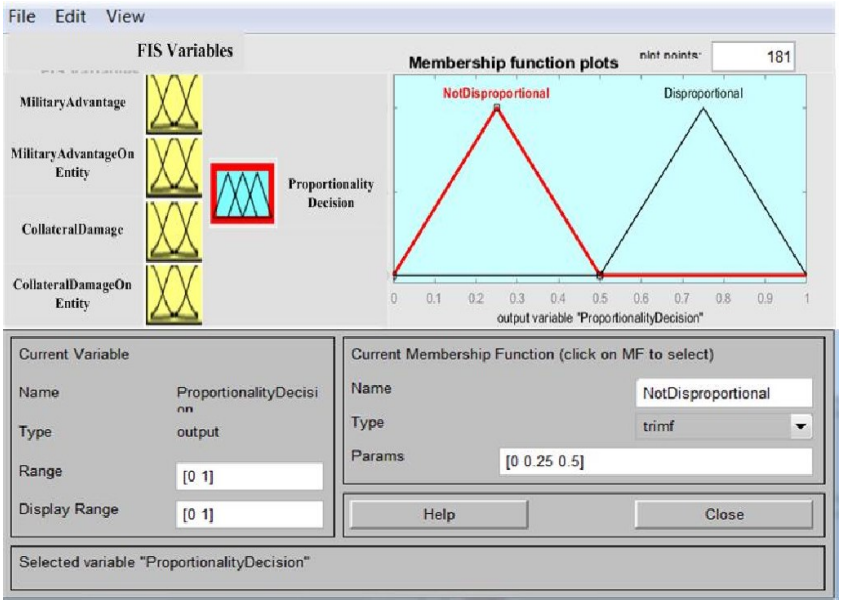


Figure 6.13. ProportionalityDecision output variable membership functions

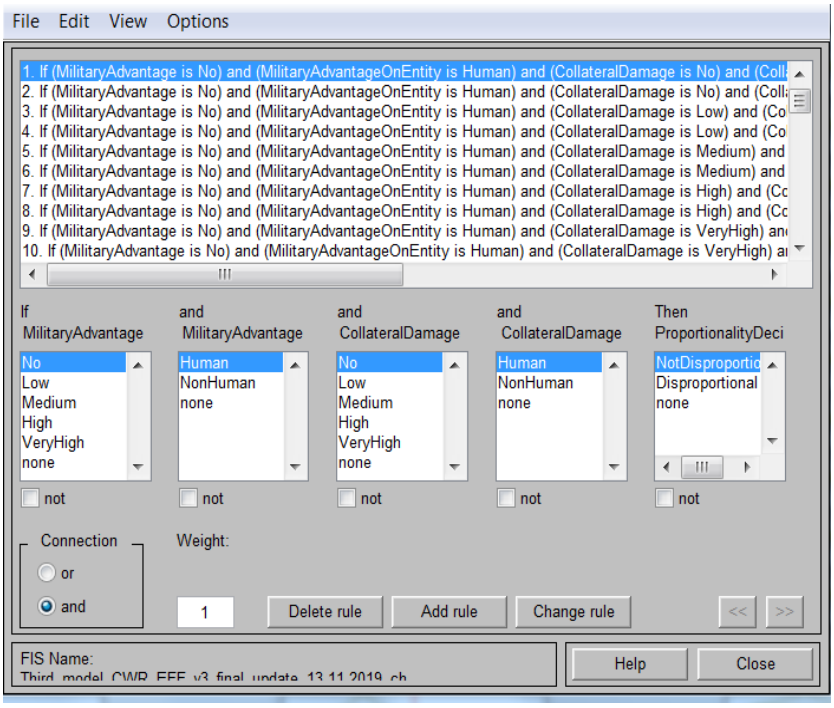


Figure 6.14. Targeting Decision Model rules based on Proportionality Assessment in Cyber Operations

A detailed description for calculating the membership functions of the variable *CollateralDamage* and *ProportionalityDecision* further provided using equation (2) in equations (6) and (7) below. Further, in the Appendix section of this chapter are defined all the variables used.

$$\mu_{CollateralDamage}(x) = \left\{ \begin{array}{l} \left(\max\left(min\left(\frac{x}{0.12}, \frac{0.24-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.19}{0.12}, \frac{0.43-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.37}{0.12}, \frac{0.61-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.56}{0.12}, \frac{0.8-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.7}{0.12}, \frac{1-x}{0.13}\right), 0\right)\right) \end{array} \right\} \quad (6)$$

$$\mu_{ProportionalityDecision}(x) = \left\{ \begin{array}{l} \left(\max\left(min\left(\frac{x}{0.25}, \frac{0.5-x}{0.25}\right), 0\right)\right), \\ \left(\max\left(min\left(\frac{x-0.5}{0.25}, \frac{1-x}{0.25}\right), 0\right)\right) \end{array} \right\} \quad (7)$$

For instance, a rule which advises that is disproportional to engage a target with a specific cyber weapon in a particular Cyber Operation is defined as follows:

IF (MilitaryAdvantage IS Low) AND (MilitaryAdvantageOnEntity IS NonHuman) AND (CollateralDamage IS High) AND (CollateralDamageOnEntity IS NonHuman) THEN ProportionalityDecision IS DisProportional.

Moreover, the output variable is defined in Table 6.3. with complete definitions for all variables presented in the Annex of this chapter.

Input / Output Variable and Definition	Value Variable (Fuzzy Set)	Definition Value Variable
ProportionalityDecision = Proportionality assessment that considers as Not-Disproportional if	Not-Disproportional	Engaging this specific target with this specific cyber weapon is not-disproportional (not excessive), in other words

Collateral Damage is not excessive in relation to Military Advantage.		engaging this target in this Cyber Operation is allowed.
	Disproportional	Engaging this specific target with this specific cyber weapon is disproportional (excessive), in other words engaging this target in this Cyber Operation is prohibited.

Table 6.3. Targeting Decision Model variables in Cyber Operations

The above described model is structured in three layers that estimate and classify the effects of Cyber Operations in the first two layers, and based on that advise targeting decisions in Cyber Operations. The complex layered structure of the model implies solving the problem by moving through its layers from the first to the third layer, and at the end advising a single decision: it is not-disproportional or disproportional to engage a specific target using a specific cyber weapon in a specific Cyber Operation.

For the identified perspectives or contexts of use presented in Section 6.5. and presented in more detail in Section 1.2.2, the proposed model can be used:

- In the *military-operational* context, multiple degrees of (dis)proportionality could be considered if an analogue approach is desired. That means that instead of using a digital/boolean approach where two values are defined i.e. NotDisproportional and Disproportional, an analogue approach could be considered. Such an analogue approach implies using multiple values of (dis)proportionality such as NotDisproportional, LowDisproportional, MediumDisproportional, HighDisproportional, and VeryHighDisproportional. These values only apply in the last layer (sub-model) of the proposed model.
- In the *military-legal* context, considering only the integration of physical effects directed to civilians and civilian assets as Collateral Damage which means excluding psychological/mental effects and other effects that have an impact on different aspects or values such as privacy, trust, and reputation. These considerations contain actions such as deleting and renaming, and are further depicted in Table 6.4. Strictly for exclusion purposes the necessary action is deleting and for naming compatibility the necessary action is renaming. The delete action means that in the estimation process the additional variables used in the operational context would not be

present in the legal context. For instance, by deleting from the second layer (sub-model) the variable MilitaryDisadvantage signifies that Military Disadvantage is excluded from this process. That implies that only Collateral Damage and Military Advantage are considered. The rename action means that the renamed variables are used in the same way according to their definition. For instance, by renaming in the first and second layers (sub-models) the variable from EffectTypeTarget to MilitaryAdvantage implies limiting the effects on the engaged target only to Military Advantage.

Layer/Model No.	Action	Action on variable
First	Rename	From MentalOrPhysicalHealthOrLossOfLife to PhysicalInjuryOrLossOfLife
First	Delete	Trust, Reputation, Privacy for EffectOnTarget
Second	Delete	MilitaryDisadvantage MilitaryDisadvantageOnEntity
First and second	Rename	From EffectTypeTarget to MilitaryAdvantage From EffectOnTarget to MilitaryAdvatageOn From EffectOnTargetProbability to MilitaryAdvantageProbability From EffectTypeCollateral to CollateralDamage From EffectOnCollateral to CollateralDamageOn From EffectOnCollateralProbability to CollateralDamageProbability
First and second	Delete	CollateralEntity

Table 6.4. Considerations for the military-legal perspective

6.6. Evaluation and Results

To be able to demonstrate and evaluate the proposed model as a proof-of-concept (Peffers et al., 2008) in the operational context (as defined in Sections 1.2.2. and 6.5), two use cases/case studies of Counter-terrorism Cyber Operations were prepared between March-April 2019 together with military-technical experts from TNO (the Netherlands Organization for Applied Scientific Research) while considering the following facts: i) the plausibility of such Cyber Operations to be conducted in the current global political and military situation, and ii) the realism of such operations from a technological point of view. In this sense, these cases were thought taking into consideration the emergent threat that terrorism represents at global level since "the victims are not [in most cases] chosen on an individual basis but are struck either at random or for symbolic effect" (Dinstein, 2014) backed by the idea of proposing Cyber Operations perceived by the

consulted military-technical experts as being realistic (Couretas, 2019) future scenarios (Caton, 2013) as an alternative in counter-terrorism methods.

The evaluation was conducted in a Workshop (Focus Group) organized by TNO and the Netherlands MoD in one day in April 2019 with the name "From Effects Estimation to Targeting Decisions in Cyber Warfare" with four military-technical experts with more than 15 years of international military-technical experience (see Appendices-Annex F). The military-technical experts were asked 12 questions structured in five groups: opening, introductory, transition, key and ending questions, and relate to phases I-V of the targeting process described in Chapter I-Section 1.2.2. Furthermore, following the data model for representing and simulating Cyber Operations proposed by (Maathuis et al., 2018d), the following information was used for both evaluation use cases/case studies: Context, Actor, Type, Military Objective, Target, Phase, and Cyber Weapon. Both case studies/use cases consider a war context and are presented below.

6.6.1. Case Study I: Drone Counter-Terrorism Cyber Operation

Context: The ongoing war and humanitarian crisis in Aricikland motivated the government of Aricikland to further engage in the fight against terrorism while being assisted and supported by the Coalition (an alliance formed by 12 countries). From a just completed ISR (Intelligence, Surveillance, and Reconnaissance) mission, the Coalition assessed that the most active international terrorist group in the area – Terrmisous – are preparing a terrorist attack against the president of Aricikland using a suicide drone/UCAV (Unmanned Combat Aerial Vehicle) weaponized with 3 kg explosive munition. This is about to be done while the president gives a speech at the Conference Hall of the Aricikland National Security Centre located in the city centre of Aricikland's capital. This scenario is depicted in Figure 6.15.

Actor: Coalition vs. Terrmisous.

Type: Offensive Cyber Operation.

MilitaryObjective: To prevent the terrorist drone attack against its intended target (the president of Aricikland). This is to be achieved by manipulating the Operator Control (the Ground Control Station) of the drone in the sense of manipulating/altering the position and speed of the drone so that it will have a random flight pattern and will be (probably) prevented to reach its own target.

Phase: planning (before execution).

Target: A terrorist subsonic drone/UCAV (Military Target) that flies at medium altitude and has an electric propulsion system. The terrorist drone operates in two modes to conduct terrorist missions. First, in manual mode being controlled and programmed by the Operator Control. Second, in automatic mode being controlled and pre-programmed by the automated pilot from its board computer. Moreover, the terrorist drone carries 3 kg explosive munition that should be deployed with its self-destruction once its target is reached. The UCAV forms together with the Operator Control and communication system (wireless data link) the UAS (Unmanned Aerial System) that Terrmisous uses to reach its aim. The Operator Control has a standard Internet connection, a weak defense mechanism, and no direct collateral connections.

CyberWeapon: During the just completed ISR mission, a malware was implanted in the Operator Control system by exploiting an existing 0-day (unknown and unpatched software vulnerability). The malware is able to automatically manipulate/alter the direction and speed of the UAV during flight based on inserting a random factor. This manipulation implies the following actions and facts:

- The screen available at the Operator Control displays the modified direction and speed of the drone. At the same time, the Operator Control is able to receive near real-time un-modified (correct) video and/or photo packets from the drone which are compliant with the real values of direction and speed.
- The flight pattern of the drone is changed by being randomized which means that the drone is prevented to fly on its considered flight path to reach its target (the president of Aricikland). The terrorist operator is not able to bypass this situation and realizes that the military objective might not be achieved. Furthermore, the terrorist operator has two options:

a) To abort or suspend the mission. Therefore, the suicide drone will not reach its target.
b) To continue the mission by a fire order (engage target) taking a high risk knowing that it will not reach its real target. Therefore, the suicide drone will reach other collateral different entities (object(s), person(s), and/or environment) or will fall somewhere in the neighbourhood where it will be captured by the Coalition.

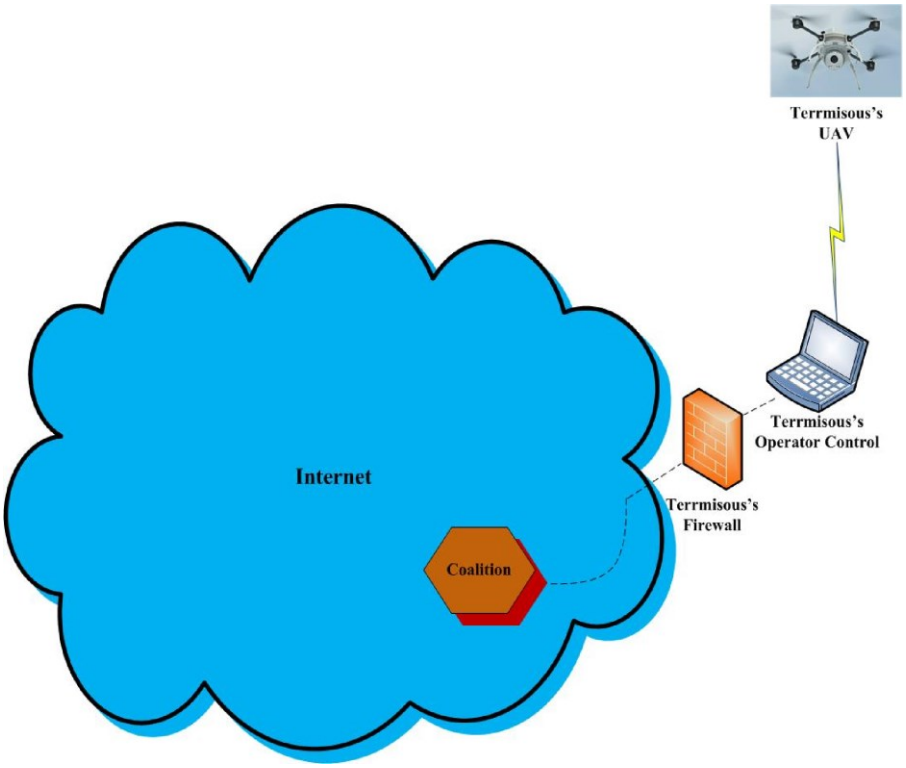


Figure 6.15. Cyber Operation Case I

6.6.2. Case Study II: Ship Counter-Terrorism Cyber Operation

Context: The ongoing war and humanitarian crisis in Aricikland motivated the government of Aricikland to further engage in the fight against terrorism while being assisted and supported by the Coalition (an alliance formed by 12 countries). From a just completed ISR (Intelligence, Surveillance, and Reconnaissance) mission, the Coalition assessed that the most active international terrorist group in the area – Terrmisous – are preparing a terrorist attack using a commercial cargo ship (civilian/dual use target) weaponized with chemical agents (dangerous/toxic chemical substances aboard) near the civilian port AricikPortus. Currently, the terrorist cargo ship is berthed (lies) at the civilian port VicikPortus where it needs to refuel to be able to go further to AricikPortus. This scenario is depicted in Figure 6.16.

Actor: Coalition vs. Terrmisous.

Type: Offensive Cyber Operation.

MilitaryObjective: To prevent the terrorist cargo ship from leaving the port VicikPortus to reach the port AricikPortus. This is to be achieved by neutralizing the services (make them temporary unavailable) of the civilian pump station from VicikPortus where the terrorists intend to load their cargo ship with fuel.

Phase: planning (before execution).

Target: A civilian cargo ship under terrorist control weaponized with chemical weapon agents and used by Terrmisous (Dual Use Target) that arrives at a pump station in VicikPortus to load with fuel. The pump station is a part of a fuel distribution network from Vicik and is directly connected to the distribution centre from Vicik. The targeted pump station is connected to Internet, has a weak defense mechanism, and direct collateral connections.

CyberWeapon: During the just completed ISR mission, the stage for a protocol based DDoS was prepared against the pump station by exploiting a discovered but not patched software vulnerability. This neutralization implies the following actions and facts:

- The services used by the pump station for loading ships with fuel are temporary unavailable, so the terrorist ship is not able to load with fuel.
- The terrorist ship might not be able to further leave the port and finish its mission, and has two options:

a) To abort or suspend the mission. Therefore, the chemical agents will not be deployed by the terrorist controlled cargo ship near the port AricikPortus.
b) To continue the manipulated mission taking a high risk of not being able to reach the target or reach collateral different entities (object(s), person(s), and/or environment.

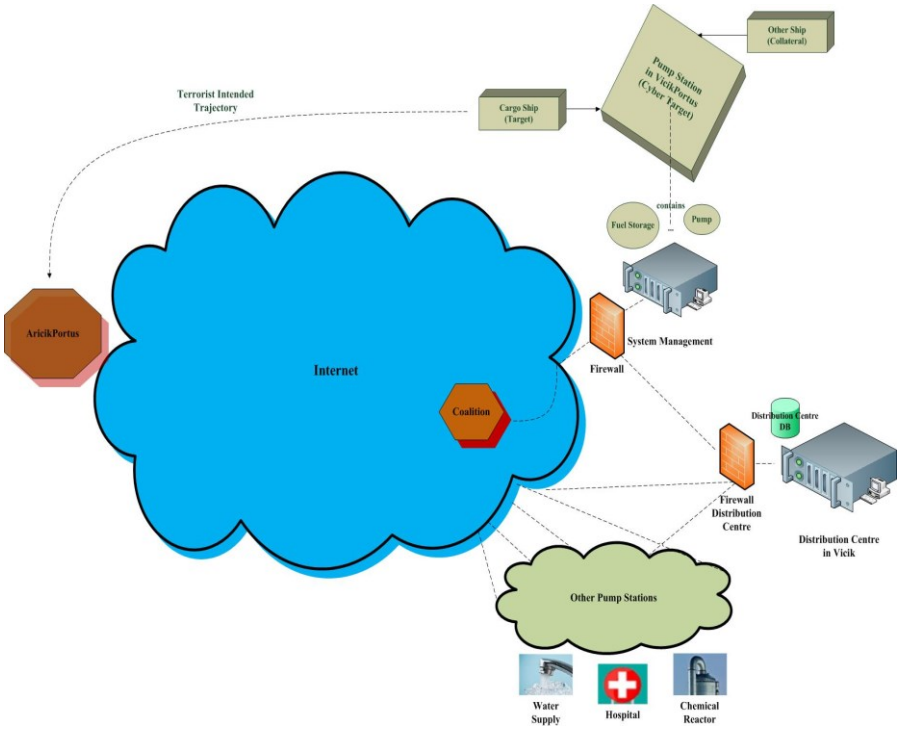


Figure 6.16. Cyber Operation Case II

6.6.3. Results

To evaluate the introduced model, the following evaluation criteria need to be fulfilled aligned with Design Science Research (Peffers et al., 2008; Mettler et al., 2014; McLaren et al., 2011):

- compatibility with the design requirements presented in Activity III in Section 6.3. of this chapter;
- usefulness meaning the "quality or state of being useful" (Cambridge Dictionary). The level of usefulness of the model was evaluated with the help of four military-technical experts in the Focus Group. During this process, the experts have assessed if this model could be useful to support targeting decisions in Cyber Operations and that implies if the model and the information received are compatible with their own intentions and /or expectations taking into consideration the fact that in this field we are still at the beginning of the road. The results of this evaluation are further below presented.

Furthermore, in Table 6.5. can be found for each Cyber Operation case study the final targeting decision provided by each expert that has

evaluated our model (columns two to four). The fifth column of the same table provides the final targeting decision provided by the model simulated with the evaluation data collected for each case from the military-technical experts. The input data is provided by the consulted experts based on the given information for each use case (see Sections 6.6.1. and 6.6.2.), analysed (see Section 1.4.3.), and run through simulations as described below using estimations for the parameters presented in the appendix (see Section 6.8.). The data is provided to the model and the final results consisting of output values and their interpretation are provided in the table below and further in this section.

Cyber Operation Use Case	Targeting Decision Expert 1	Targeting Decision Expert 2	Targeting Decision Expert 3	Targeting Decision Expert 4	Targeting Decision Model
1	Not-Disproporti onal	Disproportio nal	Disproportion al	Disproportion al	Disproportio nal (value: 0.75)
2	Not-Disproporti onal	Not-Disproportio nal	Not-Disproportion al	Not-Disproportion al	Not-Disproportio nal (value: 0.5)

Table 6.5. Targeting Decision in Cyber Operations model evaluation

This evaluation is done in MATLAB 2015b on an Intel(R) Core(TM) i7-5600U CPU with 2.6 GHZ, 8GB RAM, and Windows 7 64 bit OS. The model was developed on the same system. Through this evaluation process, the accuracy of the proposed model is tested on a dataset (with the two presented Cyber Operations) that was not used for training the model before and experts, as abovementioned. The results of the model are further discussed:

- for the first Cyber Operation use case (drone counter-terrorism), three out of four military experts (75%) have concluded that this engagement is disproportional. This is aligned with the advised decision provided by the model for this specific use case. Additionally, the model correctly estimated e.g. Military Advantage (Alter with impact on Integrity with values 0.27 and 0.61, respectively) and Collateral Damage InjuryOrLossOfLife with impact on InjuryOrLossOfLife with values 0.16 and 0.05, respectively), facts that match experts' effects assessment.
- for the second Cyber Operation use case (ship counter-terrorism), four out of four military experts (100%) have concluded that this engagement is not-disproportional. This is also aligned with the

advised decision provided by the model for this specific use case. In addition, the model correctly estimated e.g. Military Advantage and Collateral Damage as Degrade on Availability with values 0.49 and 0.72, respectively, facts that match experts' effects assessment.

– In this regard, in Figure 6.17. is depicted a sample of the area of simulation results from MATLAB for the proposed model and in Figure 6.18. is illustrated the entire output space as the space of all possible considered targeting decisions in Cyber Operations depicted here in relation to Military Advantage and Collateral Damage.

Figure 6.17. Targeting Decision in Cyber Operation Model sample area of simulation

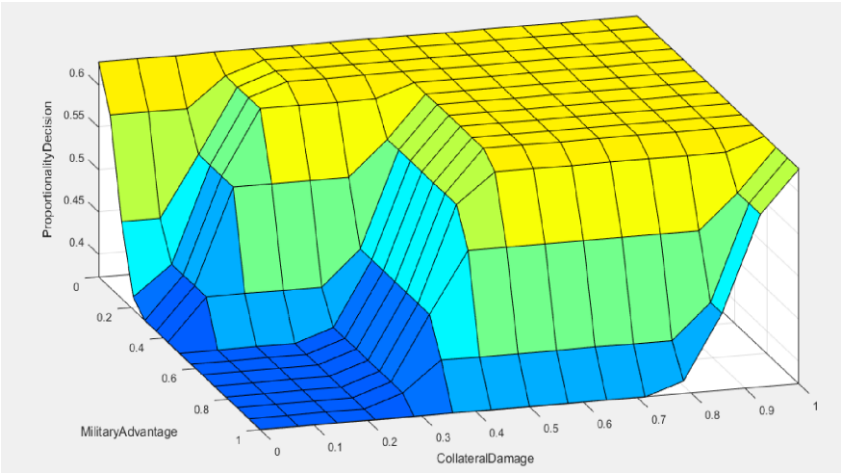


Figure 6.18. Targeting Decision in Cyber Operation Model entire output surface

Based on the evaluation process above presented, the proposed model was able to estimate the effects and advise proportionality decisions with an accuracy between 75% (in the first case) and 100% (in the second case), fact that allows us to conclude that the proposed model is worth further development using additional datasets and tuning.

Furthermore, to assess the usefulness of the introduced model, the experts have been asked to assess it using a three-point scale from 1 to 3, as follows: 1 = Not Useful, 2 = Neutral, and 3 = Useful. Their opinion is presented in Table 6.6., and implies that three experts out of four found that this model is Useful, and one expert as Neutral. Moreover, the experts were asked to elaborate their answer. The answers have been structured and are further presented:

- The model could successfully support targeting decision making by providing adequate decision support information as targeting decision based on the proportionality assessment (military-legal perspective of use as defined in Chapter I-Section 1.2.2.) and suitable as a base for further Courses of Action (CoAs) development (military-operational perspective of use as defined in Chapter I-Section 1.2.2.), since it is useful and understandable from a military-technical perspective.
- The model could help structuring the studied decision making process itself in Cyber Operations through its modular/layered architecture and reasoning (see Sections 6.5. and 6.8.). For instance, one of the experts said that the model "is clear and well structured". In this sense, the experts considered that such a modular/layered architecture and way of reasoning could be beneficial taking into consideration the following three facts. First, the fact that the model directly embeds and separates the core components of targeting decisions concerning proportionality assessment in Cyber Operations: the studied effects of engaging specific military targets and concrete decisions regarding the (dis)proportionality of such engagement in Cyber Operations. Second, the facts that the effects were classified considering on one side their military and civilian nature, and on the other side considering where these effects occur: on objects or humans. For instance, the experts agree on reasoning that degradation has effect on availability of systems, that altering the functionality of software applications, configurations, or data has effect on integrity of systems, and that a Cyber Operation that produces high not-human Collateral Damage and low not-human Military Disadvantage can be considered disproportional. And third, the fact that additional variables and/or parameters could be added to the model e.g. for estimating more types of effects or for advising more types of decisions in Cyber Operations.

– The experts suggested that the model is worth further development (i.e.. extension) based on more data(sets) with different case scenarios and similar evaluation processes with different expert audiences i.e. military political, military-technical, military-legal and/or political. For instance, one of the experts said that "the model shows the reality of this process" and another expert said that "the model captures the real 'grey' zone" since it is developed using a technique (fuzzy) that inherently embeds the uncertainty of this domain.

Usefulness Level	Expert 1	Expert 2	Expert 3	Expert 4
Usefulness	3	3	2	3

Table 6.6. Targeting Decision in Cyber Operations Model usefulness evaluation

Based on the usefulness evaluation just discussed, we can attribute an usefulness degree of 75% based on the evaluation provided by the consulted experts, which allows us to conclude (again) that the proposed model is worth further development using additional datasets and tuning.

In regards to the computing resources (performance indicator) used by the proposed model using the abovementioned system configuration, in average 15% of CPU resources and 1.2 GB RAM were used during singular tests, and up to in average 25% and 2 GB RAM during parallel tests.

Therefore, although dealing with limited data, the model succeeded in providing comparable results to the ones of the military experts that have evaluated it and complied with the evaluation criteria. This also means that the proposed model seems to be compatible with the design requirements. However, it is again important to mention that the multi-layered model just advises targeting decisions based on effects estimation, classification, and proportionality assessment/test. Human factors such as context, culture, stress etc. are not adopted in our modelling approach. These factors are considered by the research community (e.g. cognitive science, psychology) as being very difficult to measure or model (Staal, 2004; Vogt et al., 2010; Shiraev & Levy, 2017). We consider that future research should be conducted on investigating which human factors and aspects are involved during targeting decision making, and from there if or which ones should be involved in such a model.

As Figure 6.5 expresses and taking into consideration the fact that it is critical to consider control measures, the experts were asked for each Cyber Operation case study what kind of control measures they would propose and apply in order to avoid or (at least) minimize the expected Collateral Damage. These control measures can also be further considered as possible

Courses of Action (CoA) based on both cyber and kinetic options. Hence, their advice is further elaborated and structured as a set of three recommendations for each use case.

For the first Cyber Operation use case, as follows:

- Consider a different cyber weapon and other element of the target that could be engaged using this cyber weapon, in the sense of using a cyber weapon that would disturb the C2 data link.
- Consider a different cyber weapon that would facilitate full control of the Operator Control and provide the possibility of flying it into a different safe place where it could be captured.
- Cancel the event or change the speech location, date, and time so that the president could still give his/her speech.

For the second Cyber Operation use case, as follows:

- Consider integrating a method to transmit the confirmation of achievement of effects for the employed cyber weapon and immediately stop it.
- Consider requesting cooperation from Vicik's authorities (e.g. political, legal, technical) and consider other points of access in the sense of using a direct (joint) boarding team on the terrorist ship or using a different cyber weapon that would disconnect the fuel station from its distribution centre.
- Consider allowing the terrorist ship to refuel, but using a different type of oil that would produce damage to the ship or at least delaying it in order to capture it.

6.7. Conclusions

While planning, executing, and assessing Cyber Operations, the actor that either conducts them and/or is impacted by their actions, is confronted with (and sometimes benefiting from) facts such as the lack of object permanence, lack of measurement, rapid computational speed, and anonymity (Kallberg & Cook, 2017) labelled under the umbrella of vagueness, impreciseness or uncertainty. These facts are added to the human or social ones e.g. context, background, culture or risk appetite when Commanders (as decision makers) have to decide if the act of conducting a specific Cyber Operation is not-disproportional or disproportional, relying on the information given at the time by military intelligence and the advice provided by his/her military advisors (e.g. cyber, legal, political, media etc.).

This research was conducted in the fields of Cyber Security, Artificial, Intelligence, and Military Operations in order to propose a multi-layered fuzzy model as a proof-of-concept that estimates and classifies the effects of Cyber Operations, and by that advises targeting decisions that could be applicable in two contexts of use: military legal and military operational. Furthermore, the evaluation of the model was done with technical-military experts in the Netherlands considering the military legal perspective when advising targeting decisions concerning the proportionality assessment, and shows that the model is useful when targeting in Cyber Operations.

The main limitation of this research is the reduced amount of data(sets) publicly available on real Cyber Operations incidents as well as limited technical research available in this direction. However, to cope with this fact, multidisciplinary expertise was used from all the dimensions of this research: military, technical, technical-military, and military legal. As more data(sets) are expected to be publicly released and more research is expected to be conducted in the near future, this would facilitate an additional data driven approach to further fine tune and validate the model proposed for practical use.

Therefore, this research advances the current state of the art and space of artefacts in the cyber and military domains in the sense of both situation awareness and situation assessment. Furthermore, this research calls for further research and development in these fields considering the proposed model as a baseline model that can be further extended and trained based on new data(sets) and use cases using AI techniques for tuning, such as a) neuro-fuzzy approach as a combination of Fuzzy Logic and Artificial Neural Networks, b) deep learning approach, for instance Convolutional Neural Networks (CNN), c) Multi-Agent Systems using reinforcement learning, d) combining with Genetic or other Evolutionary algorithms for optimization purposes, and e) quantum-inspired Fuzzy Evolutionary algorithm or quantum-inspired Neural Networks.

Since Cyber Operations are now and will be clearly deployed also in future wars, the author considering further focusing (among others) on i) designing control measures to avoid and/or limit the unintended effects of Cyber Operations (e.g. Collateral Damage), ii) considering more the integration of multiple dimensions, factors, and aspects in (targeting decision making in) Cyber Operations keeping in mind that it is important to win battles in (cyber) war, but even more important is how they are won.

6.8. Appendix

Input / Output Variable and Definition	Value Variable (Fuzzy Set)	Membership Functions Definitions	Value Variable Definitions
MilitaryObjective = The aim / goal of a Cyber Operation.	ToManipulate	[0 0.15 0.3]	Altering or influencing an entity.
	ToCapture	[0.23 0.38 0.53]	Getting control on an entity.
	ToNeutralize	[0.463 0.613 0.763]	Making an entity unable to further function/perform.
	ToDestroy	[0.7 0.85 1]	Completely and permanently damage an entity.
TargetNature = The status of a human or a non-human/object considering the following criteria: nature, location, purpose or use, in determining if the human/non-human is targetable or not.	LegitimateMilitaryTarget	[0 0.3 0.6]	Legitimate or lawful military target.
	DualUseTarget	[0.4 0.7 1]	Entity that has a dual functionality or is shared by both military and civilian actors/systems.
TargetEntity = The type of the entity that can be directly engaged using cyber weapons.	DataOrInformation	[0 0.19 0.38]	Data
	SoftwareEnvironmentOrPlatformOrApplication	[0.31 0.5 0.69]	Software application
	ConfigurationOrLogOrAlert	[0.62 0.81 1]	File
TargetVulnerability = The status of target's vulnerability that	0Day	[0 0.19 0.38]	Unknown and unpatched vulnerability
	DiscoveredAndPat	[0.31 0.5 0.69]	Discovered but not

should be exploited.	chNotApplied		patched vulnerability
	DiscoveredAndPatchApplied	[0.62 0.81 1]	Discovered and patched vulnerability
TargetDefenseMechanism = The assessment of a target's defense mechanism(s).	Weak	[0 0.3 0.6]	Target has a weak defense mechanism
	Strong	[0.4 0.7 1]	Target has a strong defense mechanism
TargetConnectionToCollateral = The assessment regarding possible a target's open connection(s) to collateral entities.	NotConnected	[0 0.3 0.6]	Target is not connected to collateral entities.
	Connected	[0.4 0.7 1]	Target is connected to collateral entities.
TargetInternetConnection = The status of target's Internet connection.	NotConnected	[0 0.3 0.6]	Target is not connected to Internet.
	Connected	[0.4 0.7 1]	Target is connected to Internet.
CyberWeaponType = The type of cyber weapon.	Malware	[0 0.3 0.6]	Malicious software
	DDoS	[0.4 0.7 1]	Distributed Denial of Service
CollateralNature = The status of a collateral entity in the sense of being civilian, allied, friendly or neutral to this Cyber Operation.	CollateralAlliedOrFriendlyOrNeutralMilitary	[0 0.3 0.6]	Allied, Friendly or Neutral actors and / or systems
	CollateralCivilian	[0.4 0.7 1]	Collateral civilian actors and / or systems
CollateralEntity = The type of the entity that is not targeted in this Cyber Operation.	Human	[0 0.098 0.196]	Human being
	DataOrInformation	[0.166 0.264 0.362]	Data
	SoftwareEnvironmentOrPlatformOrApplication	[0.332 0.43 0.528]	Software application
	HardwareOrDevice	[0.498 0.596 0.694]	
	ConfigurationOrLogOrAlert	[0.664 0.762 0.86]	File

	Environment	[0.83 0.928 1]	Biotic and / or abiotic surroundings
CollateralEntityDefenseMechanism = The assessment conducted for the defense mechanism for collateral entity.	Weak	[0 0.3 0.6]	Collateral entity has a weak defense mechanism
	Strong	[0.4 0.7 1]	Collateral entity has a strong defense mechanism
EffectTypeTarget = The type of effect that impacts the target engaged.	No	[0 0.055 0.111]	No impact
	MentalOrPhysicalInjuryOrLossOfLife	[0.111 0.166 0.222]	Mental injury, physical injury or loss of life
	Alter	[0.222 0.277 0.333]	Modifying information, systems' aspects (e.g. functionality, performance), human behaviour or operations' aspects.
	Disclose	[0.333 0.388 0.444]	Extracting and revealing information about humans, systems, or operations.
	Degrade	[0.444 0.499 0.555]	Depriving or reducing functional, behavioural or quality aspects of an entity.
	Control	[0.555 0.61 0.666]	Managing and influencing a human, system or operation.
	Isolate	[0.666 0.72 0.777]	Closing or breaking external connections (including C2) of humans, systems or operations.
	Delete	[0.777 0.832 0.888]	Putting away resources while still being possible to be accessed by using recovering means

			(standard *delete* action) or permanently becoming inaccessible and unrecoverable (standard *erase/wipe* action).
	Destroy	[0.888 0.944 1]	Completely and permanently damage an entity so that it becomes useless and irreparable.
EffectOnTarget = The aspect or quality of the target that is impacted.	MentalOrPhysicalHealthOrLossOfLife	[0 0.055 0.111]	Mental injury, physical injury or loss of life
	Trust	[0.111 0.166 0.222]	Capability of being confident in someone or something.
	Reputation	[0.222 0.277 0.333]	(General) opinion or standing regarding a person or organization.
	Privacy	[0.333 0.388 0.444]	Ability or state in which information is selectively expressed/exposed by its owner and is free of intrusion or interference.
	Confidentiality	[0.444 0.499 0.555]	Required protecting measures and controls of resources and information to prevent access or disclosure of unauthorized users or systems.
	Integrity	[0.555 0.61 0.666]	Correctness and trustfulness of resources and information.

	Availability	[0.666 0.72 0.777]	Availability (in the sense of accessibility and usability) of resources and information to the authorized users or systems.
	Authenticity	[0.777 0.832 0.888]	State in which information is in its original form as from the source when for instance, exchanged.
	Accountability	[0.888 0.944 1]	Being able to trace the actions that were applied on a specific entity.
EffectOnTargetProbability = The probability of impacting the target.	No	[0 0.1 0.2]	0%
	Low	[0.2 0.3 0.4]	(0%, 25%]
	Medium	[0.4 0.5 0.6]	(25%, 50%]
	High	[0.6 0.7 0.8]	(50%, 75%]
	VeryHigh	[0.8 0.9 1]	(75%, 100]
EffectTypeCollateral = The type of effect that impacts a collateral entity.	No	[0 0.055 0.111]	See above
	MentalOrPhysicalInjuryOrLossOfLife	[0.111 0.166 0.222]	
	Alter	[0.222 0.277 0.333]	
	Disclose	[0.333 0.388 0.444]	
	Degrade	[0.444 0.499 0.555]	
	Control	[0.555 0.61 0.666]	
	Isolate	[0.666 0.72 0.777]	
	Delete	[0.777 0.832 0.888]	
	Destroy	[0.888 0.944 1]	
EffectOnCollateral = The aspect or quality of a collateral entity that is impacted.	MentalOrPhysicalHealthOrLossOfLife	[0 0.05 0.1]	
	Trust	[0.1 0.15 0.2]	
	Reputation	[0.2 0.25 0.3]	

	Privacy	[0.3 0.35 0.4]	
	Confidentiality	[0.4 0.45 0.5]	
	Integrity	[0.5 0.55 0.6]	
	Availability	[0.6 0.65 0.7]	
	Authenticity	[0.7 0.75 0.8]	
	Accountability	[0.8 0.85 0.9]	
	No	[0.9 0.95 1]	
EffectOnCollateralProbability = The probability of impacting a collateral entity.	No	[0 0.1 0.2]	
	Low	[0.2 0.3 0.4]	
	Medium	[0.4 0.5 0.6]	
	High	[0.6 0.7 0.8]	
	VeryHigh	[0.8 0.9 1]	
CollateralEntity = The type of the entity that is not targeted, but impacted in this Cyber Operation, and can be either collateral civilian, allied, friendly or neutral.	OnCollateralAlliedOrFriendlyOrNeutralMilitary	[0 0.3 0.6]	
	OnCollateralCivilian	[0.4 0.7 1]	

Table 6.6. Effects Estimation Model variables in Cyber Operations

Input / Output Variable and Definition	Value Variable (Fuzzy Set)	Membership function	Definition Value Variable
MilitaryObjectiveAchievement = The achievement of the already defined Military Objective.	No	[0 0.3 0.6]	Is not achieved
	Certain	[0.4 0.7 1]	Is achieved
EffectTypeTarget = see Table 1			See above
EffectOnTarget = see Table 1			

EffectOnTargetProbability = see Table 1	See Table 1		
CollateralEntity = see Table 1			
EffectTypeCollateral = see Table 1			
EffectOnCollateral = see Table 1			
EffectOnCollateralProbability = see Table 1			
MilitaryAdvantage = Intended effects that contribute to the achievement of military objectives.	No	[0 0.1 0.2]	0%
	Low	[0.2 0.3 0.4]	(0%, 25%]
	Medium	[0.4 0.5 0.6]	(25%, 50%]
	High	[0.6 0.7 0.8]	(50%, 75%]
	Very High	[0.8 0.9 1]	(75%, 100%]
MilitaryAdvantageOnEntity = The type of entity which is impacted by Military Advantage.	Human	[0 0.25 0.5]	Human being
	NonHuman	[0.5 0.75 1]	Not human being / object
MilitaryDisadvantage = Unintended effects that do not contribute to achieving military objective, but impact allies, friendly, neutral, even the target or conducting actors.	No	[0 0.1 0.2]	See above
	Low	[0.2 0.3 0.4]	
	Medium	[0.4 0.5 0.6]	
	High	[0.6 0.7 0.8]	
	Very High	[0.8 0.9 1]	

MilitaryDisadvantageOnEntity = The type of entity which is impacted by Military Disadvantage.	Human	[0 0.25 0.5]	
	NonHuman	[0.5 0.75 1]	
CollateralDamage = Unintended effects that do not contribute to achieving military objectives, but impact civilian assets, in the form of civilian injury or loss of life and/or damage or destruction to civilian objects and/or environment.	No	[0 0.1 0.2]	
	Low	[0.2 0.3 0.4]	
	Medium	[0.4 0.5 0.6]	
	High	[0.6 0.7 0.8]	
	Very High	[0.8 0.9 1]	
CollateralDamageOnEntity = The type of entity which is impacted by Collateral Damage.	Human	[0 0.25 0.5]	
	NonHuman	[0.5 0.75 1]	

Table 6.7. Effects Classification Model variables in Cyber Operations

Input / Output Variable and Definition	Value Variable (Fuzzy Set)	Membership function	Definition Value Variable
MilitaryAdvantage	No	[0 0.12 0.24]	See above
	Low	[0.19 0.31 0.43]	
	Medium	[0.37 0.49 0.61]	

	High	[0.56 0.68 0.8]	
	VeryHigh	[0.75 0.87 1]	
MilitaryAdvantageOnEntity	Human	[0 0.3 0.6]	
	NonHuman	[0.4 0.7 1]	
CollateralDamage	No	[0 0.12 0.24]	See above
	Low	[0.19 0.31 0.43]	
	Medium	[0.37 0.49 0.61]	
	High	[0.56 0.68 0.8]	
	VeryHigh	[0.75 0.87 1]	
CollateralDamageOnEntity	Human	[0 0.3 0.6]	
	NonHuman	[0.4 0.7 1]	
ProportionalityDecision = Proportionality assessment that considers as Not-Disproportional if Collateral Damage is not excessive in relation to Military Advantage.	Not-Disproportional	[0 0.25 0.5]	Engaging this specific target with this specific cyber weapon is not-disproportional (not excessive), in other words engaging this target in this Cyber Operation is allowed.
	Disproportional	[0.5 0.75 1]	Engaging this specific target with this specific cyber weapon is disproportional (excessive), in other words engaging this target in this Cyber Operation is prohibited.

Table 6.8. Targeting Decision Model variables in Cyber Operations

6.9. References

Additional Protocol I (1977). *Art. 48 – Basic rule*.

Additional Protocol I (1977). *Art 52(2) – General protection of civilian objects.*

Additional Protocol I (1977). *Art. 57(2)(a)(i)-(iii), (b) – Precautions in attack*.

Alali, M. , Almogren, M., Hassan, M.M., Rassan, I.A.L. & Bhuiyan, M.Z.A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system, *Compouters & Security*, 74, pp. 323-339.

Azimirad, E. & Haddadnia, J. (2015). Target threat assessment using fuzzy sets theory, International *Journal of Advances in Intelligent Informatics*, 1(2), pp. 57-74.

Baalman, M.A. (2010). Spatial composition techniques and sound spatialisation technologies, *Organised Sound*, 15(3), pp. 209-218.

Baturone, I., Barriga, A., Jimenez-Fernandez, C., Lopez, D.R. & Sanchez-Solano, S. (2000). Microelectronic design of fuzzy logic-based systems, CRC Press.

Boothby, W. H. (2012). *The law of targeting*, Springer, pp. 81, 126, 260, 476-478, 489.

Burstein, F., & Holsapple, C. W. (Eds.). (2008). *Handbook on decision support systems 2: variations*. Springer Science & Business Media.

Cambridge Dictionary. *Usefulness*. https://dictionary.cambridge.org/dictionary/english/usefulness Accessed March, 02, 2020.

Cannon-Bowers, J.A. & Bell, H.H. (1997). Training decision makers for complex environments: implications of the naturalistic decision making perspective, *Naturalistic decision making*, pp. 99-110.

Case, D.U. (2016). *Analysis of the cyber attack on the Ukrainian power grid*, Electricity Information Sharing and Analysis Center.

Caton, J.L. (2013). Complexity and emergence in ultra-tactical cyberspace operations; In Proceedings of the 5th International Conference on Cyber Conflict (pp. 1-14). IEEE.

Center for Army Lessons Learned. (2015). *Handbook of Military Decision Making*, pp. 15-6.

Chen, G., Pham, T. T., & Boustany, N. (2001). Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems.

Couretas, J.M. (2019). *An introduction to cyber modeling and simulation*, John Willey & Sons, Inc.
Dinstein, Y. (2014). *Non-international armed conflicts in international law*, Cambridge University Press.

Dilek, S., Huseyin, C. & Mustafa, A. (2015). Applications of artificial intelligence techniques to combating cyber crimes: a review, *International Journal of Artificial Intelligence and Applications*, 6(1).

Druzdzel, M. J., & Flynn, R. R. (2017). Decision support systems. In *Encyclopedia of Library and Information Sciences* (pp. 1200-1208). CRC Press.

Falliere, N., Murchu, L.O. & Chien, E. (2011). *W32 Stuxnet Dossier*, White paper, Symantec.

Fayi, S.Y.A. (2018). *What Petya/NotPetya ransomware is and what its remediations are*, Information Technology-New Generations, pp. 93-100.

Franz, T. (2011). The cyber warfare professional, *Air and Space Journal*.

Gill, T. D. & Fleck, D. (Eds.) (2011). The handbook of the international law of military operations, Oxford University Press, pp. 246, 253.

Goodfellow, I., Bengio, Y. & Courville, A. (2016). *Deep learning*, MIT.

Goztepe, K. (2012). Designing fuzzy rule based expert system for cyber security, *International Journal of Information Security Science*, pp. 13-19.

Graf, R., Skopik, F. & Whitebloom, K. (2016). A decision support model for situational awareness in national cyber operations centers, In the IEEE International Conference on Situational Awareness, Data Analytics and Assessment (pp. 1-6). IEEE.

Headquarters Department of the Army (1997). *Field Manual 101-5*, chapter V.

Hevner, A. & Chatterjee, A. (2010). Design Science Research in Information Systems, *Design research in information systems*. Springer, pp. 9-22.

Hollis, D. (2011). Cyberwar case study: Georgia 2008, Small Wars Journal 2011. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008: Accessed June, 14, 2019.

Huang, Z., Shen, C.C., Doshi, S., Thomas, N. & Duong, H. (2016). Fuzzy sets based team decision-making for Cyber Situation Awareness, In Proceedings of the 33th International Conference on Military Communications (1077-1082). IEEE.

ICRC (2005). Rule 1: The principle of distinction between civilians and combatants, International Committee of the Red Cross. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1: Accessed May, 10, 2019.

ICRC (2010). The Geneva Conventions of 1949 and their Additional Protocols, International Committee of the Red Cross. https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm: Accessed May, 10, 2019.

Inyaem, U., Haruechaiyasak, C., Meesad, P. & Tran, D. (2010). Terrorism event calssification using fuzzy inference system, International Journal of Computer Science and Information Security, 7(3).

Jachec-Neale, A. (2014). *The concept of military objectives in international law and targeting practice*, Routledge, pp. 204.

Kallberg, J., & Cook, T. S. (2017). The unfitness of traditional military thinking in cyber. *IEEE Access*, *5*, pp. 8126-8130.

Kanuck, S. (2009). Soverign discourse on cyber conflict under international law, *Texas Law Review*, 88, pp. 1571.

Klir, G.J. & Yuan, B. (1995). *Fuzzy sets and fuzzy logic: theory and applications*, pp. 574.

Kulkarni, S.S., Rai, H.M. & Singla, S. (2012). Design of an effective substitution cipher algorithm for information security using Fuzzy Logic, *International Journal of Innovations in Engineering and Technology*, 1(2).

Kumar, S.S. & Kathiresan, V. (2016). Alert system for controlling cyberbullying words using Fuzzy Logic and Fuzzy Inference Engine, *Asian Journal of Computer Science and Technology*, 5(2), pp. 29-31.

Kumar, S., Singh, A. & Kumar, M. (2019). Information hiding with adaptive stenography based on novel fuzzy edge identification, *Journal of Defence Technology*, 15(2), pp. 162-169.

Lipshitz, R., Klein, G., Orasanu, J. & Salas E. (2001). Taking stock of Naturalistic Decision Making, Journal of Behavioural Decision Making, 14, pp. 331-352.

Lu, J., Lv, F., Liu, H.Q., Zhang, M. & Zhang, X. (2018). Botnet detection based on fuzzy association rules; In Proceedings of the 24th International Conference on Pattern Recognition (pp. 578-584). IEEE.

Maathuis, C., Pieters, W. & Berg, v.d. J. (2016). Cyber Weapons: a Profiling Framework. In Proceedings of the 1st International Conference on Cyber Conflict U.S. (pp. 1-8). IEEE.

Maathuis, C., Pieters, W. & van den Berg, J. (2018b). A Knowledge-Based Model for Assessing the Effects of Cyber Warfare", In Proceedings of the 12th NATO Conference on Operations Research & Analysis.

Maathuis, C., Pieters, W. & van den Berg, J. 2018c, 'Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations', Proceedings of the IEEE Military Communications Conference (pp. 1-6). IEEE.

Maathuis, C., Pieters, W. & v.d. Berg, J. (2018d). Developing a computational ontology for Cyber Operations, *Journal of Information Warfare*, 17(3):32-51.

Malham, D.G. & Myatt, A. (1995). 3-D sound spatialization using ambisonic techniques, *Computer Music Journal*, 19(4), pp. 58-70.

Mandami, E.H. & Assilian, A. (1975). An experiment in linguistic synthesis with a fuzzy logic controller, *International Journal of Man-machine Studies*, 7(1), pp. 1-13.

McDonald, G., Murchu, L.O., Doherty, S. & Chien, E. (2013) *Stuxnet 0.5: The missing link*, Symantec.

McLaren, T., M.B.A. & Buijs, P. (2011), A Design Science approach for developing information systems research instruments.

Mettler, T., Eurich, M. & Winter, R. (2014). On the use of experiments in Design Science Research: a proposition of an evaluation framework, *CAIS*, 34, 10.

Mezler, N. (2008). *Targeted killing in international law*, Oxford University Press on Demand, pp. 359.

NATO (2013). *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim 2.0*.

NATO (2014). Wales Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_112964.htm. 2014: Accessed May, 24, 2019.

NATO (2016). *NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting*. NATO Standardization Office.

NATO (2016a). Allied Joint Doctrine for Intelligence Procedures, NATO Standardization Office, pp. 24-25.

NATO (2018). Cyber defence. https://www.nato.int/cps/en/natohq/topics_78170.htm: Accessed July, 07, 2019.

Newcomb, E.A. & Hammell, R.J. (2016). A fuzzy logic utility framework (FLUF) to support information assurance, *Software Engineering Research, Management and Applications*. Springer, pp. 33-48.

Orasanu, J. (2005). Crew collaboration in space: a naturalistic decision-making perspective, Aviation, space, and environmental medicine, 76(6).

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chaterrjee, A. (2008). A Design Science Research Methodology for Information Systems Research, *Journal of Management of Information Systems*. 2008, 24(3), pp. 45-78.

Prelipcean, G., Boscoianu, M. & Moisescu, F. (2010). New ideas on the artificial intelligence support in military applications. In Proceedings of the 9th WSEAS international conference on Artificial intelligence, knowledge engineering and data bases. World Scientific and Engineering Academy and Society.

Rath, A.K., Parhi, D.R., Das, H.C., Muni, M.K. & Kumar, P.B. (2018). Analysis and use of fuzzy intelligent technique for navigation of humanoid

robot in obstacle prone zone, *Journal of Defence Technology*, 14(6), pp. 677-682.

Rao, D. V. & Balas-Timar, D. (2014). A soft computing approach to model human factors in air warfare simulation system, *Innovation in Intelligent Machines-5*. Springer; pp. 133-154.

Romanosky, S. & Goldman, Z. (2017). Understanding Cyber Collateral Damage, *Journal of National Security Law and Policy*, 9, pp. 233.

Rospocher, M., & Serafini, L. (2012). An ontological framework for decision support. *Proceedings of Joint International Semantic Technology Conference*, Springer, pp. 239-254.

Sallam, H. (2015). Cyber security risk assessment using multi fuzzy inference system, International *Journal of Engineering and Innovative Technology*, 4(8), pp. 13-19.

Schmitt, M. N. (Ed.) (2013). Tallinn Manual on the international law applicable to cyber warfare; Cambridge University Press, pp. 68, 80.

Schmitt, M. N. (Ed.) (2017). Tallinn Manual 2.0. on the international law applicable to cyber operations; Cambridge University Press, pp. 375.

Schreier, F. (2015). *On cyberwarfare*, Geneva Centre for the Democratic Control of Armed Forces.

Shanmugavadivu, R. & Nagarajan, N. (2011). Network intrusion detection system using fuzzy logic, *Indian Journal of Computer Science and Engineering*, 2(1), pp. 101-111.

Shang, K. & Zakir, H. (2013). Applying fuzzy logic to risk management and decision-making, Canadian institute of actuaries.

Shiraev, E.B. & Levy, D.A. *Cross cultural psychology: critical thinking and contemporary applications*. Routledge Taylor & Francis Group.

Siler, W., & Buckley, J. J. (2005). *Fuzzy expert systems and fuzzy reasoning*. John Wiley & Sons.

Singhal, A. & Hema, B. (2013). Fuzzy logic approach for threat prioritization in Agile security framework using DREAD model, arXiv preprint arXiv: 1312.6836(2013).

Smith, E.S. (1994). *An application of fuzzy logic control to a classical military tracking problem*, U.S. Naval Academy.

Staal, M. A. (2004). *Stress, cognition, and human performance: A literature review and conceptual framework.* NASA.

Stone, S.W. (2015). Factors influencing agility in allocating decision-making rights for Cyberspace Operations, In Proceedings of the 20th International Command and Control Research and Technology Symposium, pp. 96.

Tavana, M., Trevisani, D.A. & Kennedy, D.T. (2014). A fuzzy cyber-risk analysis model for assessing attacks on the availability and integrity of the Military Command and Control systems, *International Journal of Business Analytics*, 1(3), pp. 21-36.

Tremblay, M. C., Hevner, A. R., & Berndt, D. J. (2010b). Focus groups for artifact refinement and evaluation in design research. *Cais*, *26*(27), pp. 599-618.

Tuija, K., Kuusisto, R. & Roehrig, W. (2016). Situation understanding for operational art in cyber operations, *Journal of Cyber Warfare and Terrorism*, 6(2), pp. 1-14.

United States Army (2013). *Joint Publication 3-60 Joint Targeting*. United States Army.

United States Army (2018). *Joint Publication Cyberspace Operations*. United States Army.

Wibowo, S. & Grandhi, S. (2018). Fuzzy multicriteria analysis for performance evaluation of Internet-of-Things-based supply chains, *Symetry*, 10(11), 603.

Wright, J.D. (2012). *'Excessive' ambiguity: analysing and refining their proportionality standard*, International Review of the Red Cross, pp. 819-854.

Yang, G., Yang, Y., Li, J., Liu, J., Ru, Y., Yuan, K., Wu, Y. & Liu, K. (2016), An assessment method of vulnerability in electric CPS cyber space. In the 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, pp. 379-402. IEEE.

Zadeh, L.A. (2008). Is there a need for fuzzy logic, *Information sciences,* pp. 2751-2779.

Zheng, C., Han, L., Ye, J., Zou, M. & Liu, Q. (2009). A fuzzy comprehensive evaluation model for harms of computer virus, In the 6th International Conference on Mobile Adhoc and Sensor Systems, pp. 708-713.

Zsambok, C. & Klein, G. (1996). *Naturalistic Decision Making*, Taylor & Francis.

Chapter 7. Conclusions

"Deep in the wood, in the dark, there's a way
Follow this path and you will meet a strange crowd
In the forest you will meet
Silhouettes of your dreams
Dancing on the path you walk
...
When you wake up
You wish you sleep again
...
In the deepest forest
In the deepest dark
You will find the fire
...
When you wake up you will believe it was a wonderful dream."
(Therion – Via Nocturna)

Includes parts of Boltjes, B. Maathuis, C., van den Berg, T. & Gouweleeuw, R. 2019, "Developing Standards for Including the Cyber Domain in Military Training and Exercises", *Proceedings of the Simulation Interoperability Standards Organization Simulation Innovation Workshop, SISO*.

In the last decades, Cyber Operations have proven to be a real option in achieving or as support to achieving military and/or political goals. It is generally believed that their use will further increase and that they will embed more intelligent and adaptive means. That is why, a critical aspect in regards with their design, execution, or use is the assessment of their effects.

This research aimed to understand and model Cyber Operations, assess their effects, and advise military targeting decisions based on proportionality assessment in order to support military targeting decision making process in Cyber Operations. Additionally, it aimed at supporting awareness raising, military training, simulations and exercises, and communication in this field and adjacent domains (e.g. political and legal). The resulting findings have been presented in Chapter 2 to 6 and resumed in the current chapter.

We first discuss our research findings, after that we continue by addressing our contributions as well as limitations. At the end we reflect on possible extensions that we have identified during the research.

7.1. Summary of Research Findings

This dissertation intends to provide an answer to the following main research question:

How to assess the effects of Cyber Operations in order to support military targeting decisions in Cyber Warfare?

To do so, the main research question was decomposed into five subordinate research questions, each treated in a separate chapter and represented by a corresponding designed artefact. The sub-sections 7.1.1-5. provide the related research findings. As the core of this research was the effects assessment in Cyber Operations, this corresponds with the vision on the term 'effects assessment' provided by (Remenyi & Wilson, 2018): "an attempt to attribute value to the result of creating, acquiring, operating, or abandoning a system or policy."

7.1.1. Conclusions Research Question 1

The first research question was defined as follows:

How to represent the entities involved in Cyber Operations?

This question implied both a comprehensive understanding of the Cyber Operations concept and of the phenomenon or activity itself as a combination of theoretical, empirical, design, and practical efforts. This was achieved by first defining the Cyber Operations concept as "a type of or a part of a military operation in which cyber weapons/capabilities are used to achieve military objectives in front of adversaries inside and/or outside cyberspace" (Maathuis et al., 2018b). This definition is aligned with scholars' vision and existing incipient doctrine for Cyber Operations (U.S. Army, 2018; Herr & Herrick, 2016; U.S. Army, 2013). Furthermore, the entities and relationships between these entities involved in Cyber Operations are represented as a knowledge/data model in the form of a computational ontology. This ontology is compliant with the requirements for developing a cyber warfare computational ontology established by (Dipert, 2013).

The upper-classes of this model are Context, Actor (i.e. agent), MilitaryObjective, Type, Phase, Target, CyberWeapon, Action, Geolocation, Asset, and Effect, and they describe at a higher or abstract level Cyber Operations as a military-technical (thus socio-technical) phenomenon, and completely map the definition. As each upper-class contains more child classes and several relationships are defined between them and their instances (objects) e.g. isExploiting and isProducingCollateralDamage, they could provide an in-depth understanding of this phenomenon.

Next to understanding, due to the properties of flexibility and reusability that this model contains, it aims at supporting decision making processes and communication between different actors involved in their planning, design, execution, and/or assessment by facilitating further understanding, representation, and simulation in distributed environments, for instance, when assessing targets' vulnerabilities. Moreover, the model was evaluated by technical means and with the help of military-technical experts (see Appendices-Annex G) which for instance suggested to integrate the role of the target in the model. Furthermore, the model was exemplified on three Cyber Operations case studies conducted on incidents from Georgia, Operation Olympic Games/Stuxnet, and Black Energy 3 in Ukraine. Therefore, the proposed model could represent a useful conceptualization as the context where the whole reasoning of this dissertation takes place. Additionally, the proposed model can be used in the same way in both military-legal and military-operational perspectives of use considered in this dissertation of use (as defined in Section 1.2.2.) which implies that it does not require any kind of additional changes.

7.1.2. Conclusions Research Question 2

The second research question was defined as follows:

What should a profiling framework for Cyber Weapons look like?

This question foreshadowed both a comprehensive understanding of the cyber weapons concept and a way to profile them. A cyber weapon was defined as "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" (Maathuis et al., 2016). This definition is compatible with the scholars' view illustrated in (Herr, 2014; Schmitt, 2013; Mele, 2013). The arena is prepared further to define a way to profile cyber weapons with the help of a profiling framework.

This is done by analysing a few cyber weapons and by that, identifying classes and characteristics of cyber weapons which are of further use when assessing their effects in Cyber Operations e.g. purpose, use, sophistication, and area of action. The proposed profiling framework is evaluated and exemplified on Cyber Operations case studies conducted on Operations Orchard, Operation Olympic Games/Stuxnet, and Black Energy 3. The results are presented in a profiling matrix (Table 3.1. in Chapter 3) that shows its effectiveness and applicability in helping decision makers and researchers to understand what these means of Cyber War are, what should be considered when designing and developing them as well as what are the dimensions to be taken into account when assessing their effects in Cyber Operations.

In this framework control measures for avoiding, limiting or controlling unintended effects of cyber weapons (as offensive cyber capabilities) such as Collateral Damage were considered since their context of use was set to be war. If these control measures fail to produce the expected results in the Testing phase of the cyber weapon to be deployed (Section 3.2. in Chapter 3), that means that the cyber weapon should not be deployed on the intended target, and an in-depth analysis should be considered. If a new target is selected that can imply that either a new cyber weapon has to be deployed or the existing cyber weapon has to be adapted to the new target, fact that is not always applicable. This means that the flow of actions goes back to one of the initial three phases of the cyber weapon's life cycle, as follows: Project definition (phase I, described in Section 3.2. in Chapter 3), Reconnaissance (phase II, described in Section 3.2. in Chapter 3), or Design (phase III, described in Section 3.2. in Chapter 3). Additionally, the proposed framework is applicable in the same way to both

perspectives or contexts of use considered (as defined in Section 1.2.2.) which means that it does not require any kind of additional changes.

7.1.3. Conclusions Research Question 3

The third research question was defined as follows:

What methodology is adequate to assess the effects of Cyber Operations?

This question signified building an effects assessment methodology for Collateral Damage and Military (Dis)Advantage in order to support targeting in Cyber Operations. These concepts have been defined in the context of Cyber Operations as follows. Military Advantage was defined as the "intended effects that contribute to achieving military objectives", Collateral Damage was defined as the "unintended effects that do not contribute to achieving military objectives, but impact civilian assets, in the form of civilian injury or loss of life and/or damage or destruction to civilian objects and/or environment", and Military Disadvantage was defined as the "unintended effects that do not contribute to achieving military objectives, and impact allies, friendly, neutral, even the target or conducting actors". These definitions are also compliant with the resources abovementioned in Section 7.1.2 and 7.1.2.. The proposed methodology embeds multidimensional factors such as spreading, duration, and probability of occurrence.

The methodology is structured in five phases, as follows: Target Identification and Validation, Target Analysis, Target Effects Assessment, Collateral Effects Assessment, and Minimization of Unintended Effects. The methodology begins when targets (of Cyber Operations) are identified and validated, and ends when control measures for avoiding or minimizing the unintended effects (Collateral Damage) are considered and applied when necessary. The methodology is compliant with methodologies used in kinetical Military Operations (Council of the European Union, 2016; NATO, 2011; Joint Chief of Staff, 2011), and was evaluated with the help of military-technical experts on a virtual (see Appendices- Annex D), but realistic Cyber Operation case study on a Ballistic Missile Defense System. Thereupon, the experts considered that the methodology is effective and applicable in realistic Cyber Operations use cases, and provides meaningful insights into the dynamics of targeting and targeting decisions in Cyber Operations in regards to intelligence and perception. In consequence, the introduced methodology embeds adequate aspects that need to be considered when further assessing and estimating the effects of Cyber

Operations. Additionally, considering the perspectives or contexts of use defined in Section 1.2.2., the proposed methodology could be used as it is in the military-operational perspective/context of use, and could be used in the military-legal perspective/context of use by just ignoring the assessment of Military Disadvantage.

7.1.4. Conclusions Research Question 4

The fourth research question was defined as follows:

How to assess the effects of Cyber Operations?

This question involved building an effects assessment model in the form of a knowledge-based model that could serve as a knowledge/data-based simulation environment for decision support in Cyber Operations (Maathuis et al., 2018). The model represents and proposes for reasoning information such as thirty types of effects together with thirty three aspects and qualities of systems that can be impacted. For instance, from the upper-class EffectType we recall sub-classes that contain different types of effects such as Alter, Control, Destroy, Disrupt, and Injury. From the upper-class EffectOn we recall sub-classes that contain different aspects and qualities of entities that are being impacted in Cyber Operations such as Authentication, Availability, Connectivity, Confidentiality, Functionality, Integrity, Physical Injury, and Privacy. The proposed model was evaluated by technical means considering its consistency and reusability, and was evaluated with the help of technical-military experts considering its accuracy, clarity, conciseness, and adaptability (see Appendices-in Annex G). Furthermore, the model was exemplified on Cyber Operations case studies conducted on incidents from Georgia and Ukraine, and as suggested by the experts consulted, is further integrated and used in distributed simulation environments for Cyber Operations at TNO. Additionally, the proposed model is applicable in the same way meaning that it does not require any kind of additional changes for both perspectives or contexts of use as defined in Section 1.2.2. That implies selecting which effects are of interest for each perspective/context of use according to the requirements of the Cyber Operation that is being conducted.

7.1.5. Conclusions Research Question 5

The fifth research question was defined as follows:

How to estimate the effects of Cyber Operations in order to support targeting decisions in Cyber Warfare?

This question meant building a multi-layered model that i), estimates the effects of Cyber Operations, ii) classifies the effects of Cyber Operations considering intention and nature as classification criteria, and iii) advices by supporting targeting decisions based on proportionality assessment/test in Cyber Operations. The proposed model was evaluated with the help of military-technical experts (see Chapter 6 and Appendices-in Annex F) on two virtual, but rather realistic Cyber Operations case studies on a suicide drone and a cargo ship. For the evaluation process, the model had to comply with the design requirements as well as the assessment of usefulness that the experts have conducted. From the evaluation process we have seen that the model complied with the design requirements and the experts have associated a high degree of usefulness (75%). In the light of these findings, the model is estimated to be useful for supporting targeting decisions considering limited data(sets), and represents a 'proof of concept' while advocating for further development with real data(sets) and further evaluation in modelling and simulations of military exercises that should be done by different categories of experts.

Additionally, the proposed model can be used in both perspectives or contexts of use defined in Section 1.2.2., and further context-specific adaptations can be made. This concerns for example the following:

- For the military-legal context, the researcher/user should consider:
  - That a series of variables should be ignored (e.g. Trust, Reputation, Privacy in order to remain in the borders of the military-legal definition for Collateral Damage) or renamed (e.g. from EffectTypeTarget to MilitaryAdvantage for naming compatibility) in the first and second layers (sub-models), as elaborated in Chapter 6 in Section 6.5. and Section 6.6. In this way, only Collateral Damage that is of physical nature and Military Advantage depicted with green and red colours in Figure 1.4. from Chapter 1 are considered in this assessment, while all the other effects are not taken in consideration.
  - That no actions are required for the third layer (sub-model) since the only values considered for assessing proportionality are Collateral Damage (restricted) and Military Advantage, and the output provided is represented by NotDisproportional and Disproportional values.

- For the military-operational context where both intended and unintended effects are computed (as extended to the legal context), the researcher/user should consider:

- That there are no actions required for the first and second layers (sub-models) of the proposed model.
- That all the effects depicted with green (Military Advantage), red (Collateral Damage that is of physical nature), orange (broader Collateral Damage that is of broader nature), and yellow (Military Disadvantage) colours in Figure 1.4. from Chapter 1 are considered in this assessment.
- That for the third layer (sub-model) multiple degrees of (dis)proportionality could be considered for the output variable in the sense of having an analogue nature, instead of a digital nature (e.g. NotDisproportional and Disproportional). That means using multiple degrees of (dis)proportionality which express different levels of (dis)proportionality. This can be done by using values such as NotDisproportional, LowDisproportional, MediumDisproportional, HighDisproportional, VeryHighDisproportional. In this sense, more or less values could be considered for defining such degrees of (dis)proportionality.

7.1.6. Conclusions Main Research Question

The answer to the main research question can be based on the combination of the developed artefacts which assess the effects of Cyber Operations in different contexts of use and provide targeting decision support concerning proportionality assessment in Cyber Operations. The proposed artefacts have benefited from the evaluation done and advises provided by the military-technical experts. We have identified two ways in which the proposed artefacts could be used, as described in the following two paragraphs.

First, the artefacts could be used stand-alone as follows. The first artefact (described in Chapter 2) could capture the whole context of a Cyber Operation in the sense of representing participant components such as actors, targets, and cyber weapons together with the relationships (causality) between them. The first artefact could be used for modelling and simulating Cyber Operations, for instance, for military training and exercises purposes. The second artefact (described in Chapter 3) could profile cyber weapons in the sense of identifying classes and characteristics of cyber means or capabilities used in Cyber Operations to achieve the intended effects. The second artefact could be used for feature engineering in designing future models for Cyber Operations as well as developing strategies and programs that consider the use of cyber weapons in different scenarios. The third

artefact (described in Chapter 4) could assess the effects of cyber weapons used in Cyber Operations in a systematic methodological way by following specific phases and steps that start identifying the targets and ending with proposing control measures for minimizing or mitigating the unintended effects of cyber weapons in Cyber Operations. The third artefact could be used as an effects assessment methodology for Cyber Operations as the extended equivalent of the existing methodology used in current military operations for assessing Collateral Damage (CDE) as well as support for designing an assessment methodology in post-engagement of targets in Cyber Operations (BDA). The fourth artefact (described in Chapter 5) could assess the effects of Cyber Operations through a model that classifies the effects on different qualities and aspects of the impacted entities. The fourth artefact could be used for modelling and simulating the effects of Cyber Operations, for instance, for military training and exercises purposes. The fifth artefact (described in Chapter 6) could be used (directly as it is, or accessed through a GUI or further extended, as explained in Section 7.3.) to estimate the effects of Cyber Operations and advise targeting decisions concerning proportionality assessment, in other words, a multi-layered model that could advise if engaging a specific target using a specific cyber weapon in a Cyber Operation is not-disproportional or disproportional (military-legal perspective of use as defined in Section 1.2.2.) as well as advising targeting decisions when a broader palette of effects are considered (military-operational perspective of use as defined in Section 1.2.2.).

Second, a way how the proposed artefacts could be together used for a specific Cyber Operation is further depicted. Once the entities participating in a Cyber Operation are represented using the first artefact integrating the information provided regarding the profiled cyber weapon from the second artefact, the third and fourth artefact could be used to systematically assess its effects depending on the perspective of use/context that is being considered i.e. military legal or military operational. Afterwards, once the information is gathered from the previous artefacts, the effects of Cyber Operations could be estimated in order to advise targeting decisions concerning proportionality.

7.2. Research Contributions and Limitations

This section discusses scientific and societal contributions followed by the limitations of the executed research.

7.2.1. Reflection on Research Contributions

The research presented proposes a set of artefacts that integrate both definitions for not yet defined or agreed defined concepts in Cyber Operations together with three models, an assessment methodology, and a profiling framework. Furthermore, the research contributions have both scientific and societal dimensions which are discussed below.

7.2.1.1. Reflection on Scientific Contributions

This dissertation contributes to the existing Cyber Warfare & Security, Military Operations, and Artificial Intelligence body of knowledge and space of corresponding artefacts, as follows:

Firstly, contributions to Cyber Warfare & Security and Military Operations domains:

- By providing a set of multidisciplinary artefacts in the form of three models, one methodology, and one profiling framework in Cyber Operations. To summarize, this research contributes in the following ways:

  - Provides understanding for concepts such as cyber weapons, Cyber Operations, as well as intended and unintended effects of Cyber Operations such as Military Advantage, Military Disadvantage, and Collateral Damage. Although some of these concepts have been addressed in the scientific literature (Herr & Herrick, 2016; Herr, 2014; Gallina, 2002; Romanosky & Goldman, 2017; Schmitt, 2013; Schmitt, 2017), Military Advantage and Military Disadvantage have not been previously defined in scientific literature, to the best of our knowledge.
    From the consulted military experts we have noticed more interpretations for the concept Collateral Damage. This is aligned with the need of considering two perspectives or contexts of use for the proposed artefacts in the sense of remaining in the military-legal perspective/context of use where Collateral Damage is perceived in a more physical way e.g. physical injury, and the military-operational context where Collateral Damage is contained and perceived in a broader way by including more types of unintended effects (from the second Focus Group).
  - Provides a way to represent and reason about Cyber Operations and their effects in the form of knowledge/data models that could be of further use in combination with other

Artificial Intelligence and/or Software Engineering techniques for different aims. The proposed artefacts are useful when assessing the effects of Cyber Operations which means both analysing and estimating them. This could be seen as a step forward of research conducted by (Dipert, 2013; Simmons et al., 2009; Applegate & Stavrou, 2013; Oltramari, 2015; Chan, 2015; Bodeau & Graubart, 2013; Bernier, 2013; Marinos, 2016).

- Provides an assessment methodology and a multi-layered model to estimate and classify the effects of Cyber Operations, and based on that targeting decisions support information based on proportionality assessment in Cyber Operations. The need for developing these types of artefacts for Cyber Operations has been addressed by (Couretas, 2019). In this research, these artefacts are directly aimed at supporting targeting decision making in Cyber Operations. In this way, these artefacts could assist military Commanders (as decision makers) and their advisors in their decision making process.

– By providing three case scenarios or use cases of virtual, but realistic Cyber Operations (Couretas, 2019; Bodeau, 2018; Fite, 2014) that could be considered for (distributed) simulations in the Modelling and Simulation domain in order to support military training and exercises in Cyber Operations or broader operations e.g. hybrid. These case scenarios were designed and developed from a military-technical perspective, and were evaluated by military-technical experts with significant international experience (between 15 and 20 years of experience in the military and cyber domains). Moreover, they were built based on researching their correspondent used technologies (e.g. ballistic missiles and suicide UAVs) as case studies in this research in order to exemplify and evaluate different proposed artefacts. Since these scenarios have been described in different scientific publications and in the present dissertation, they could be of use in future research not just for Cyber Warfare, but also e.g. for cyber terrorism (Lewis, 2002; Taylor et al., 2014; Korstanje, 2016; Pipyros et al., 2016).
– Granting the abovementioned facts, this research provides useful insights into Cyber Operations and introduces artefacts that could produce or enrich military situation awareness as well as situation assessment to different other scientific-communities such as political, ethical, medical, sociological etc. (Kott et al., 2015; Knott et al., 2013; Mancuso, 2014; Liles et al., 2012).

Secondly, contributions to the Artificial Intelligence (and broader Computer Science) domain (Allen & Chan, 2017; Prelipcean et al., 2010;

Dilek et al., 2015; Tyugu, 2011; Blowers & Williams, 2014; Hallaq, 2017; Hurley, 2018) through applying different techniques and opening new paths to possible future research in this domain. Taking into consideration the abovementioned aspects, the present research uses AI techniques (i.e. Knowledge Representation and Reasoning, and Fuzzy Logic) so it can be seen as an useful application of them in the domain of Cyber Operations that opens new doors to further research which will be further presented in Section 7.3. of this chapter.

7.2.1.2. Reflection on Societal Contributions

This dissertation contributes to domains such as technical, military, and political, as follows:

Firstly, it contributes to military and political decision making:

- Due to the fact that cyberspace is currently and will be in the future a significant warfare battlefield where different kinds of actors (state, hybrid, or non-state actors) will employ their force to achieve their aims ranging from influencing each other's perceptions to damage or destruction of physical or digital entities. Based on the proposed artefacts and their positive evaluation by experts from this field, this research could support military Commanders and their teams while targeting in Cyber Operations. Additionally, on a higher level, this research could contribute to the design and development of military doctrines and strategies, as well as to the development of TTPs (Tactics, Techniques, and Procedures) in Cyber Operations. At the same time, this research can contribute to the design and development of control measures and recommendations in regards with the avoidance, minimization and/or mitigation of collateral effects of Cyber Operations. Additionally, this research could also contribute to the design and development of (public) policies, as well as best practices and recommendations on different types of Cyber Security incidents and the assessment of their effects on targets and on collateral assets since current strategies and policies lack fundamental and simulated models and methodologies that could be used for such purposes.
- Due to exemplifying and evaluating the artefacts proposed on new Cyber Operations, this research could contribute with valuable data and features useful to model and simulate Cyber Operations and their effects. That could be possible for such operations being conducted either stand-alone or as part of broader complex operations. Hence, this research could support situation awareness

and decision making in training and exercises for military personnel at strategical, operational, and tactical levels on how to plan, design, execute, assess Cyber Operations and how to recognize and assess the effects of Cyber Operations. Additionally, it could support awareness towards proposing adequate measures necessary to be known or taken into consideration in order to minimize/mitigate the unintended effects of Cyber Operations.

Secondly, it contributes to technical practitioners from fields such as Cyber Security, AI, Data Science, and Software Engineering as well as congruent or correspondent stakeholders when analysing or performing (implying designing, developing, testing, executing, and evaluating) Cyber Operations or other types of cyber security incidents together with their effects that should be known a priori (assessment in the sense of estimation) or a posteriori (assessment in the sense of analysing).

By resuming and following the Ready-Set-Go information architecture model described by (Edvinsson & Aderinne, 2013) and adapted to this dissertation as it is in Figure 7.1. depicted, the contribution of this dissertation can be found in different scientific domains that could contribute through its results to different processes in the field (reality). These processes are: awareness (in the sense of situation awareness as reflected from the first, second and third proposed artefact), perspective (in the sense of illustrating different contexts and perspectives in this research and conducting it in a multidisciplinary way as reflected in all proposed artefacts), and support (in the sense of assessment and decision support as reflected in the proposed artefacts).

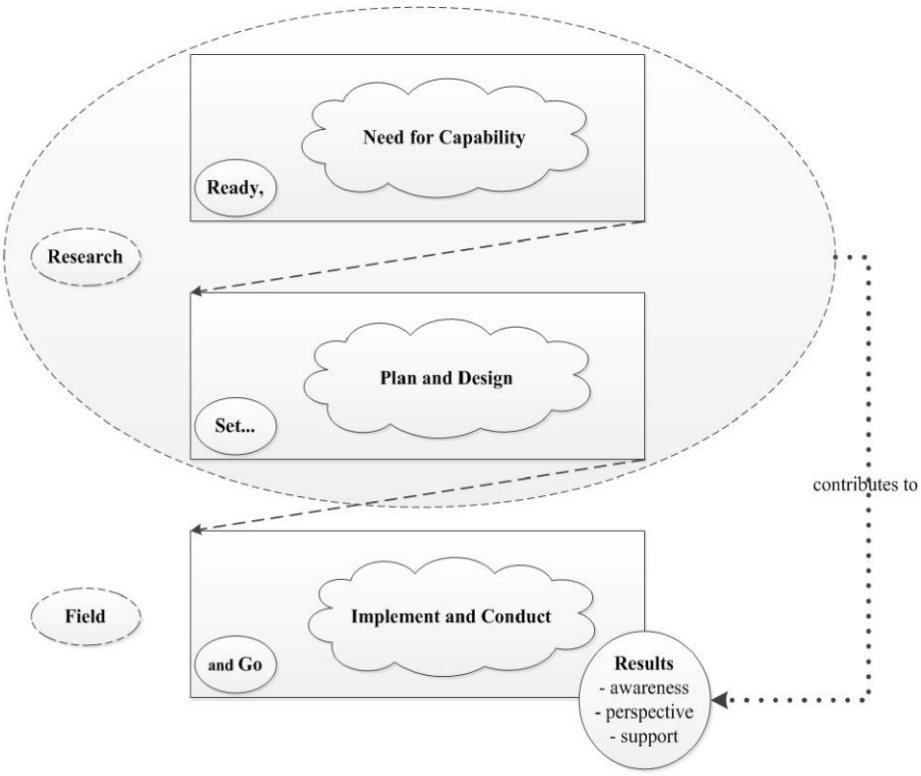


Figure 7.1. Ready-Set-Go model adapted from (Edvinsson & Aderinne, 2013)

7.2.2. Reflection on Research Limitations

This section discusses the identified limitations of this research. These limitations are classified as technological, theoretical/methodological, and governance, and are further described in dedicated sub-sections.

7.2.2.1. Reflection on Technological Limitations

From a technological point of view, while conducting this research we have been confronted with limitations related to data(sets) available in this field. These limitations are further elaborated together with the methods we have used in order to cope with them.

The first limitation is regarding the availability or openness of data(sets) of Cyber Operations incidents. Techniques and technologies that represent the basis for designing, developing, and using cyber weapons are

widely available as opposite to the availability of the ones for designing, developing, and using kinetic weapons which are more restricted and regulated (Osinga, 2012). However, data(sets) concerning the effects of using cyber weapons in different Cyber Operations is many times restricted or scarcely available through different forms of reports (e.g. from antivirus software companies or CERT-Computer Emergency Response teams teams) as opposite to data(sets) concerning the effects of different weapons used in other war settings. Additionally, (Osinga, 2012) argues that the level of intelligence required in Cyber Operations is much higher than the one necessary when attacking using conventional weapons. This is due to the dynamism and interconnectivity which characterize cyberspace. Thus, although we have considered in the beginning a purely data oriented approach based on other AI techniques than the ones used (i.e. neuro-fuzzy and deep learning), we did not to continue in this line since at the moment of speaking, we lack the necessary data(sets) for training and testing the models. We consider that if the data(sets) availability would not be a problem, a purely data oriented approach based on massive open data(sets) would drive targeting decisions with high accuracy. However, some aspects should be taken into account:

- Such an approach would lack the benefit of using the expertise of SMEs (Subject Matter Experts) in order to define and deal with the aim that has to be achieved as well as to integrate human factors and to evaluate it.
- Such an approach might imply significant processing and memory resources for the systems where it is implemented, so systems' performance might become an issue. Nonetheless, this limitation could be coped with by using High Processing Computing (HPC) which implies the use of super computers, parallel processing techniques, cloud solutions etc.

The second limitation concerns the following aspects about the case studies analysed, and is related to the first limitation already introduced on data(sets) availability:

- For the analysed real Cyber Operations i.e. Operation Orchard, Operation Olympic Games/Stuxnet, in Georgia, Black Energy 3, and Not Petya, we only had access to the publicly available source code which was incomplete as well as to limited log files captures. This limitation signifies an incomplete analysis of software security aspects evaluated on the considered targets and their networks.
- To designing and analysing the virtual, but realistic Cyber Operations case scenarios on a Ballistic Missile Defense System, a Suicide UAV/drone, and a cargo ship, a limited depth of data was

considered for the input variables in the sense of aggregating more features into one e.g. target vulnerability as an input variable of the last artefact presented in Chapter VI.

7.2.2.2. Reflection on Theoretical/Methodological Limitations

From a theoretical-methodological point of view, the following limitations have been identified.

The first limitation is related to the design of the proposed artefacts. This limitation is reflected in the design of the following two artefacts:

- In case of the second artefact, the introduced profiling framework does not consider characteristics applicable to ransomware although ransomware is a class of malware, and implicitly, a cyber weapon. This is due to the fact that the research conducted for building the first artefact focused on the use of cyber weapons in a war context and was done before NotPetya (cyber weapon in the form of a Trojan ransomware acting in 2017 in the war context from Ukraine) happened. That signifies that distinct characteristics such as encryption method/algorithm and message, decryption permission, and payment are not (yet) included. Nonetheless, NotPetya was studied after its occurrence in 2017, and became a Cyber Operation case study integrated in the exemplification and evaluation process of the fourth artefact and has no further influence in the development of the fifth artefact.
- The fifth and last artefact, the proposed multi-layered model for decision support embeds (due to the legal constraints in this research in regards to proportionality) on its third layer/model the legal perspective in perceiving the proportionality assessment/test with just two concepts: Collateral Damage and Military Advantage in Cyber Operations.

The second limitation is with reference to the integration of human cognition and behavioural aspects such as background and experience on one side, and stress, culture, and religion on the other side. If these aspects would have been integrated, for instance, in the conducted interviews, then more human aspects could have been integrated in the proposed artefacts as they have an influence into the targeting decision making process and they reflect the behaviour of decision makers (i.e. military Commanders). However, the proposed artefacts in this dissertation have partially addressed human and social factors in their design, as follows:

- For the first artefact by integrating sophistication of cyber weapons that is directly something depending on the ones (i.e. actors or agents) which are building them.
- For the second artefact by considering a broader palette of context dimensions expressed by classes like SocioCultural and Historical.
- For the third and fourth artefacts by integrating human impacted aspects in Cyber Operations such as Reputation and Trust.
- For the fifth artefact by expressing the human factors and aspects that exist in each phase of the introduced Targeting Decisions Modelling Framework in Cyber Operations, which is the fundament of the proposed artefact.

Hence, the human factors as the ones abovementioned (e.g. cognition and stress) in the beginning of the previous paragraph were not modelled since i) we had to deal with and integrate legal constraints as well as the difference of perspective that exists between military Commanders and military legal advisors, ii) they are very difficult to be expressed and measured given the limited data that we had to work with, and iii) are generally perceived difficult to comprehend, measure, and by that, model and simulate. For instance, a research study started in the Netherlands in 2005 named The Prospective Research In Stress-related Military Operations (PRISMO) initiated by the Research Centre of the Military Mental Healthcare at the Dutch Ministry of Defense (Van der Wal, 2019). The research aims to investigate the biological base of the mental health of the Dutch troops in stress conditions such as the ones experienced in Military Operations conducted in Afghanistan. Additionally, similar initiatives exist all over the world, and their results are important to be expressed and heard. One forum to do that are the EURO ISME Conferences where military, technical, ethical, and medical aspects of warfare are discussed. These initiatives can be an example and in some aspects inspirational for further integrating and researching human factors in Cyber Operations, and even further extending different aspects or artefacts proposed in this research, since “as humans have moved from land to sea then to space, they have taken the human condition with them” (Liles, 2010).

The third limitation concerns the evaluation process considered in this research. This limitation has the following elements. First, as previously mentioned, the limited number of Cyber Warfare existing incidents and their supportive data(sets) as well as the ones that we have designed for exemplification and evaluation purposes. Second, the fact that although the proposed artefacts were built based on international sources (e.g. case studies/use cases of Cyber Operations and interviews etc.), the military-technical experts who have evaluated our artefacts are Dutch, but with significant international experience (between 15 to 20 years of experience)

in real joint Military Operations and exercises. Additionally, the evaluation was not done in conditions of stress and (probably, depending on the case) in more limited time than real operations. However, this limitation and broader, generalization of the proposed artefacts, are partially addressed because the case studies conducted on real or virtual Cyber Operations are diverse by context, aim, target, and used cyber weapon, and the diversity of the consulted military-technical experts are from different countries i.e. the Netherlands, Germany, France, the US., and Canada. Therefore, an extended evaluation with international military-technical experts (in or without stress conditions) could be a further option and might provide interesting insights related to culture, religion, risk appetite or even stress for each decision maker, as well as future updates for the proposed artefacts.

7.2.2.3. Reflection on Governance Limitations

From a governance point of view, the following limitations have been identified.

The first limitation is about the availability of resources and is related to the military and political vision expressed by existing doctrines, strategies, policies, best practices in the form of standards, methods, and techniques applicable in Cyber Operations. Currently, several countries have publicly available cyber doctrines such as the U.S. and the U.K. which have even published new updated versions of them. Other countries already have an initial version of a cyber doctrine (e.g. the Netherlands) which are not (yet) publicly available, and other countries are developing their initial or first version. Currently, NATO is preparing to publish its cyber doctrine AJP 3-20 named "Doctrine for Cyberspace Operations". Additionally, eastern countries e.g. Russia and China as well as a set of other countries in the same region (still) consider and relate to the concept of *information* instead of *cyber,* and publish their doctrines, strategies, and policies in this way. The situation is different when discussing about strategies or reports instead of doctrines, since a significant amount of countries developed their own national cyber strategy or (set of) report(s) that are publicly available. In this regards, the Netherlands publishes every year a Cyber Security Report from the National Cyber Security Centre (NCSC). In regards to the existence and development of cyber policies and best practices in the form of methods and techniques is somehow aligned with the situation of cyber strategies, but with a higher degree of variety. This implies that inside a country or as a cooperation between different countries in the form of different organizations, groups, research institutes (e.g. ENISA, SANS, MITRE etc.) and universities publish own documents in the form of cyber policies, strategies, reports etc. which can be useful at national and international level.

The aspect that strikes from the abovementioned discussion is the availability of cyber resources that could be shared at (inter)national level between different stakeholders. To summarize, this fact goes to the willingness to share, secrecy around sharing as preventing exposure and future risks in front of other actors (state or non-state actors), and the existence of other different impediments (e.g. governmental and financial). However, it should be kept in mind that "global cyberspace superiority is not possible due to the complexity of cyberspace" (U.S. Army, 2018).

Due to different factors and impediments (i.e. privacy and secrecy concerns), we have tried and failed to collect additional data(sets) on other Cyber Operations incidents (both real and realistic synthetic) in order to research and use them in our process of building, i.e. either in the design or evaluation of our proposed artefacts, from different countries such as the Netherlands, Germany, the U.S., Romania, and Lithuania.

The second limitation relates to the accommodation of legal aspects with the latest warfare battlefield: cyberspace. Grounded on the fact that the information revolution triggered a societal and technical shift that brings "the non-physical to the fore and makes it as important and valuable as the physical one" (Taddeo, 2012), implied for several years that different schools of thoughts have pendulated on the applicability of the existing legal frameworks as they are now defined. This implied analysing why would this framework be applicable or wondering if some articles should be reinterpreted and updated or new ones should be proposed. Such a discussion considering 'data' as both a physical and digital sense as in the Computer Science paradigm and mindset, as well as reinterpreting Collateral Damage as both physical and psychological/mental injury.

However, this is an extremely difficult process when referring to the LOAC due to the fact this legal framework i) evolved from the 19th Century and goes back to thousand years ago from the rules that were governing wars (armed conflicts) back then. Thus, it needs time to grow and adapt to new technologies and challenges, and ii) is the result of both learning from previous wars and trying to make things better for the ones to come. Hence, in some aspects it might be impossible to reach a common understanding or agreement at such a scale of countries involved. However, recently, the schools of thought have moved from investigating *why* this legal framework would be applicable to *how* would it be applicable. In this regard, a first step in this direction was made by NATO at the Wales Summit in 2014 when it was considered that "our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace" (NATO, 2014). This recognition is aligned with the ones of

(Schmitt, 2013; Schmitt, 2017). Nonetheless, more multidisciplinary research should be done in this sense since Cyber Operations i) are a viable option to engaging some designated targets, ii) might be preferred in some cases as they could produce a low detection probability and/or no or limited physical damage, and iii) their higher-order effects on targets might also impact other elements, including retaliation attributed to their conducting actors (U.S. Army, 2018).

Additionally, important lessons could and should be learned from the laws applicable in other parts of the Cyber Security domain such as cyber crime and privacy. These sub-domains currently embed at both research and industry levels more flexibility, speed, and a multidisciplinary approach, meaning critical factors that could also contribute to the development of a global consensus and globally recognized regulation or advising system applicable to Cyber Warfare.

7.3. A Way Forward: Reflection on Research Extensions

Research Extension 1: Release data(sets)

Several times we mentioned in this dissertation the issue of dealing with limited data(sets) and the broader well known problem that researchers deal with while conducting research in Cyber Warfare/Operations as they are confronted with missing or incomplete data(sets). This issue was described earlier in this dissertation as it was one of the major limitations that triggered further development of ideas in slightly other directions. Hence, we argue and call for the release of publicly available or definitely broader available data(sets) of real, virtual or fictive, but realistic Cyber Operations incidents conducted by both state and non-state actors since research needs to rely on credible data (Couretas, 2019). We believe that this would help both academic researchers and practitioners in developing new ideas, services, and systems in and for Cyber Operations. We want to believe that in a near future efforts in this direction will be done and that this will be actually realized. Hence, we foresee the following possible extensions for the proposed artefacts in this dissertation:

- For the first artefact, being able to enlarge the context/universe of Cyber Operations by exemplifying it on more and different Cyber Operations with a broader palette of effects.
- For the second artefact, finding new dimensions in the sense of characteristics useful to profile cyber weapons and be able to exemplify the proposed framework in more and different Cyber Operations. Additionally, it might be interesting to further research

if the development and deployment of cyber weapons is worth being done when compared to other possible weapons that could be deployed to achieve military objectives considering the exposure that the use of cyber weapons brings after (and even during) their deployment (e.g. from a code re-use and logic perspective).

- For the third artefact, allowing to extend the introduced assessment methodology by (perhaps) considering new dimensions, factors, and sub-steps in the whole process. Additionally, new insights could also be obtained from more and different Cyber Operations that could be used to evaluate this methodology.
- For the fourth artefact, facilitating filling the proposed model with more and different Cyber Operations could imply instantiating existing classes as well as further developing the model towards identifying new metrics for each type of identified effect and impacted aspect or quality of the affected entity.
- For the fifth artefact, granting the possibility of extending the features to further train it as well as evaluating and comparing the results based on more and different realistic Cyber Operations. The way how both perspectives or contexts of use are captured in this research is provided by using AI techniques that easily facilitate operations such as specific extractions, modifications, interoperability with other models/tools or GUIs (Graphic User Interface), and extensions. Since the proposed artefact is flexible and adaptable, it could be directly used and/or adapted to limit and embed only physical injury with minimal technical effort or consider other ones in a different context/perspective of use. Additionally, if one would want to consider an analogical view towards (dis)proportionality in the sense of not having a digital or Boolean interpretation (disproportional and not-disproportional), then different levels or degrees of (dis)proportionality (e.g. very disproportional, slightly disproportional etc.) could be defined and this view would imply for this research limited technical effort i.e. only updating the third layer (sub-model) of the fifth artefact. This means defining different levels or degrees of (dis)proportionality as the output of the third layer (sub-model) of the fifth artefact and deciding the functional mechanism for it. Hence, this signifies that based on the levels or degrees of proportionality, a decision about the deployment of a cyber weapon should be established based on these levels or degrees of (dis)proportionality. In plus if one would want to address other types of effects such as geopolitical or economic, then the proposed artefacts in this research could be extended through the integration of additional variables and in particular for Artefact 5, more variables as well as rules could be integrated in the first and second layer.

Research Extension 2: Increase Synergy and Multidisciplinarity/Transdisciplinarity

Another aspect that we believe would facilitate the extension of this research and its correspondent proposed artefacts is synergy. We understand by synergy the interaction or cooperation between different parties such as different actors/agents, organizations, and/or projects towards reaching a common aim. This is possible in Cyber Operations by unifying efforts through a multidisciplinary approach towards reaching common greater goals such as new developments (e.g. of doctrine, strategies, policies, reports) and joint operations. We refer by that not just bringing actively together actors/agents, organizations, and/or projects of a similar nature (e.g. civilian or military, technical or non-technical), but actually merging them together (i.e. different nature) to reaching fruitful results. This synergy would help reaching common awareness, understanding, and assessment. Additionally, synergy would actively contribute to better comprehending behaviours and decision making aspects in Cyber Operations as critical key points present in different moments in their life cycle (e.g. planning, execution or assessment). In plus, synergy could benefit and trigger through multi-dimensional evaluation and future developments for the proposed artefacts or building new ones, for instance i) modelling Commanders' behaviour while targeting in Cyber Operations, ii) proposing control measures to avoiding or minimizing the unintended effects of Cyber Operations such as Collateral Damage and Military Disadvantage, iii) re-analyse legal aspects in Cyber Warfare (e.g. what is an attack, target, effect, Collateral Damage) through technical-legal or technical-military-legal lenses, iv) investigating what kind of degrees of disproportionality (e.g. very disproportional, slightly disproportional) in relation to degrees or grades of excessiveness could be defined, interpreted, and further integrated in the proportionality assessment and targeting decision making process, or v) investigating how a broader context (also outside war, during peace times) where political, international relations, economic, and societal dimensions are taken into consideration to see how they influence and weigh into different decision making processes such as the ones regarding cyber weapons' design, deployment, and use.

Research Extension 3: Increase the use of Artificial Intelligence techniques

The use of Artificial Intelligence techniques in the cyber or information domain has significantly increased in the last years as it enables designing automatic computing solutions to solve different relevant societal problems (Dilek et al., 2015). In particular, Fuzzy Logic is an AI technique

"heavily used" in cyber defense (Newcomb & Hammel, 2016) and military decision tools (Prelipcean et al., 2010). Furthermore, aligned with the aim of the present research and the call of extension to further use the same AI techniques utilized in this research combined with other Artificial Intelligence/Machine Learning techniques or directly other AI/ML techniques, we consider three main directions of extensions (somehow) related with the previous two considered extensions:

- Further estimating the effects of Cyber Warfare based on more available or open data(sets) using techniques such as i) neuro-fuzzy technique by combining additional data with the expertise already contained in and for the fifth artefact, ii) deep learning, and in particular Convolutional Neural Networks with several hidden layers. This approach could be considered directly integrating the modelling architecture of the fifth artefact, and iii) quantum inspired fuzzy evolutionary algorithms or quantum-inspired Neural Networks.
- Control measures for a) avoidance or minimization of, or b) mitigation of unintended effects of Cyber Operations that affect both military and civilian actors, in the sense of Military Disadvantage and Collateral Damage. As control measures for a) need to be a priori engaging targets in Cyber Operations, control measures that should be applied to b) need to be a posteriori engaging targets in Cyber Operations. In both extension situations, genetic or other evolutionary algorithms used alone or in combination with the already utilized AI techniques are suitable making use of the first, second, fourth, and fifth artefacts built in this research. These techniques are inspired from the natural selection phenomenon and could be used because they allow finding optimal solutions (optimization techniques) when not much is known about how to reach a good solution.
- Behaviour analysis of decision makers during targeting in Cyber Operations, such as military Commanders and military legal advisors. Additionally, profiling different entities involved in Cyber Operations like actor/agent, target, and cyber weapon. For both considered extension options, a Multi-Agent System (MAS) or Agent-based Modelling (ABM) combined with Reinforcement Learning (RL) approach are suitable and can use firstly, the first and fourth artefacts proposed in this research from a Software Engineering perspective, and secondly, the third and fifth artefacts for more information regarding targeting decision making together with behaviours and beliefs of consulted military experts as decision makers reflected in this research. These techniques could be used since they provide useful insights into agents' behaviour and reflect

ways on how they learn to behave, take actions, and relate with each other in special conditions.

Research Extension 4: Increase the use of Modelling and Simulation techniques

In the military domain, the use of computer-based simulations has a long history on modelling and simulating the development of new warfighting techniques as well as to train military personnel (troops) in different missions (Wihl, 2015; Marshall, 2015; Wihl, 2010). Since the Modelling and Simulation domain contains techniques that would facilitate the introduction and integration of new capabilities such as cyber capabilities in order "to enable dynamic and interactive force-on-force maneuvers at net-speed" (Caton, 2013) and achieve military and/or political objectives, it is considered both an intersecting field to this research as well as an extension one. Furthermore, in order to reflect some insights into this extension, a scientific publication (Boltjes et al., 2019) written together with Rudi Gouweleeuw, Bert Boltjes, and Tom van den Berg, and is further resumed. The co-authors of this further presentation are military-technical experts in Modelling and Simulation, Software Engineering, Military Operations, and Cyber Security from TNO (Netherlands Organisation for Applied Scientific Research) from the departments of Modelling, Simulation, and Gaming, and Military Operations, respectively.

Hence, (Boltjes et al., 2019) proposes the design of a Cyber Simulation Data Exchange Model (SDEM) that would facilitate the direct integration of Cyber Operations into military simulations in order to increase the level of cyber awareness, train personnel in the use of or deal with cyber capabilities/weapons, and to be able to assess the possible effects and impact on the simulated mission. This model directly uses the fourth artefact proposed in the present research – the Knowledge-based model to assess the effects of Cyber Warfare – (Maathuis et al., 2018), and implicitly the second artefact proposed in the present research – the Cyber Operations computational ontology (Maathuis et al., 2018b).

Correspondently, the steps in building the proposed SDEM are depicted in Figure 7.1. This model was designed using Domain Engineering Process activities described in (McClure, 2001; Peffers et al., 2008; IEEE 12207-2008, 2008), is aligned with the Distributed Simulation Engineering and Execution Process (DSEEP) (IEEE 1730-2010, 2010), and introduced, as follows (Boltjes et al., 2019):

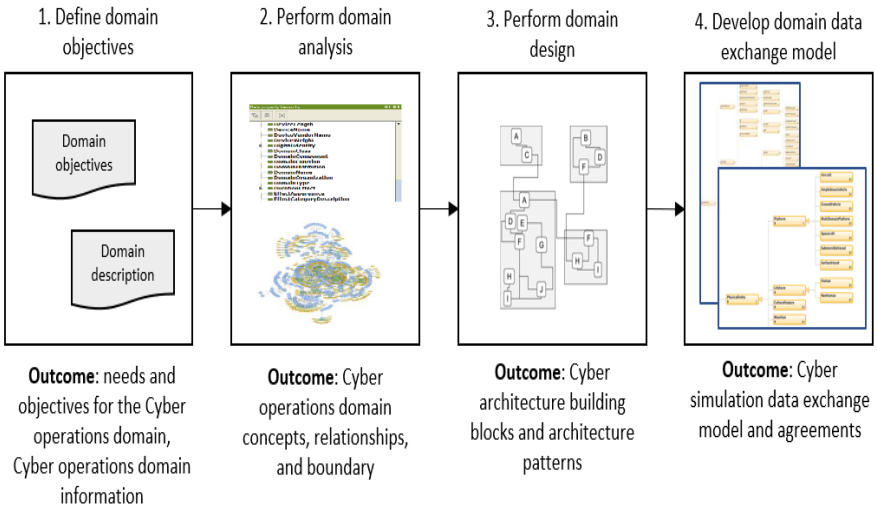


Figure 7.1. Cyber Simulation Data Exchange Model

Furthermore, the flow from the cyber simulation domain engineering process to the cyber simulation application process is illustrated in Figure 7.2. and its steps are further elaborated:

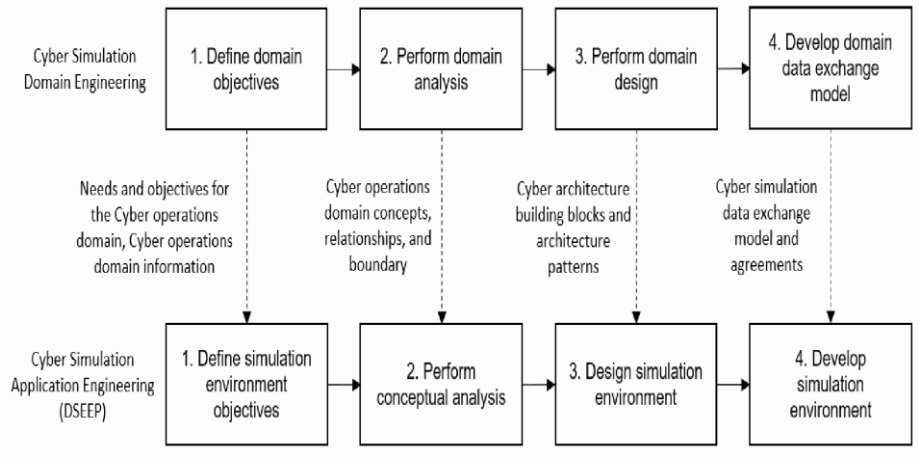


Figure 7.2. From cyber simulation domain engineering to cyber simulation application process

- In Step 1, the cyber application engineer uses the Cyber Operations domain information and the objectives for the domain in the needs and objectives settings for his/her simulation environment.
- In Step 2, the cyber application engineer uses the language and concepts of the Cyber Operations domain models as authoritative

domain information to develop the simulation conceptual model and simulation scenario for his/her simulation environment.

- In Step 3, the cyber application engineer uses the cyber architecture building blocks and patterns for the design of the simulation environment and for the selection and development of software applications. The engineer might also use Modelling and Simulations repositories for retrieval of existing cyber simulation assets for the domain.
- In Step 4, the cyber application engineer uses the cyber simulation data exchange model as a reference for the development of the data exchange model for his simulation environment.

Following the considered approach, the architecture of the cyber simulation domain engineering process also facilitates a higher level of interoperability between the models developed in the cyber simulation application engineering process, i.e. by using a common domain model (e.g. ontology), building blocks, data exchange model, etc.

Conclusively, new ways and possibilities exist for tackling and solving key points and dilemmas in Cyber Warfare. As the global interest for offensive Cyber Operations starts to grow, this research intended to contribute to a variety of audiences by embedding a military-technical view that opens new doors for future research since Cyber Operations (as a new domain of Military Operations) represent a new military option "that will likely reshape future warfare" (Sigholm, 2013), that will be present in relation to future hostilities (Boothby, 2016) while still considering and aiming that "wisdom will grow with our power and teach us that the less we use our power the greater it will be" (Thomas Jefferson).

"If you know the enemy and know yourself,
You need not fear the result of a hundred battles.
If you know yourself, but not the enemy,
For every victory gained, you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle."
(Sun Tzu – The Art of War in Sabaton's musical interpretation – Sabaton – The Art of War)

7.4. References

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs.

Additional Protocol I (1977). *Art 51(4) – Protection of the civilian population.*

Applegate, S.D. & Stavrou, A. (2013). Towards a cyber conflict taxonomy. In Proceedings of the 5th Conference on Cyber Conflict (pp. 1-8). IEEE.

Bernier, M. (2013). *Military activities and cyber effects (MACE) taxonomy. Taxonomy*. Defence Research and Development Canada, Centre for Operational Research and Analysis.

Blowers, M., & Williams, J. (2014). Machine learning applied to cyber operations. In *Network science and cybersecurity* (pp. 155-175). Springer.

Bodeau, D.J. and Graubart, R. (2013). *Characterizing effects on the cyber adversary: A vocabulary for analysis and assessment*. The MITRE Corporation.

Boltjes, B., Maathuis, C., van den Berg, T. & Gouweleeuw, R. 2019, "Developing Standards for Including the Cyber Domain in Military Training and Exercises", *SISO, Simulation Innovation Workshop*.

Bodeau, D.J., McCollum, C.D. & Fox, D.B. (2018). Cyber threat modelling: survey, assessment, and representative framework. Homeland Security Systems Engineering & Development Institute.

Boothby, W. H. (2016). *Weapons and the law of armed conflict*. Oxford University Press.

Caton, J. L. (2013). Complexity and emergence in ultra-tactical cyberspace operations. In Proceedings of the 5th International Conference on Cyber Conflict (pp. 1-14). IEEE.

Chan, P., Theron, J., van Heerden, R. & Leenen, L. (2015). An ontological knowledge base for cyber network attack planning. In Proceedings of the 10th International Conference on Cyber Warfare and Security.

Council of the European Union (2016). Avoiding and minimizing Collateral Damage in EU-led Military Operations concept.

http://data.consilium.europa.eu/doc/document/ST-5785-2016-INIT/en/pdf: Accessed June, 12, 2019.

Couretas, J.M. (2019). An introduction to cyber modeling and simulation; John Willey & Sons.

Dilek, S., Huseyin, C. & Mustafa A. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. International Journal of Artificial Intelligence and Applications, 6(1).

Dipert, R. (2013). The essential features of an ontology for cyberwarfare. *Conflict and cooperation in cyberspace.* P Yannakogeorgos & A Lowther (Eds.), Taylor & Francis, pp.35-48.

Edvinsson, H., & Aderinne, L. (2013). *Enterprise Architecture Made Simple: Using the Ready, Set, Go Approach to Achieving Information Centricity*. Technics Publications.

Fite, B.K. (2014). *Simulating Cyber Operations: a Cyber Security Training Framework*. SANS Institute.

Gallina, D., Gorman, P., Herman, M., MacDonald, J., & Ryer, R. (2002). *Military advantage in history*. Information Assurance Technology Analysis Center.

Hallaq, B., Somer, T., Osula, A. M., Ngo, K., & Mitchener-Nissen, T. (2017). Artificial Intelligence Within the Military Domain and Cyber Warfare. In Proceedings of the European Conference on Cyber Warfare and Security (pp. 153-156).

Herr, T. (2014). PrEP: A Framework for Malware & Cyber Weapons. *The Journal of Information warfare*, vol. 13(1), p. 87-106.

Herr, T., & Herrick, D. (2016). Military cyber operations: A primer. *American Foreign Policy Council Defense Technology Program Brief*, 14.

Hurley, J. S. (2018). Beyond the Struggle: Artificial Intelligence in the Department of Defense (DoD). In Proceedings of the 13th International Conference on Cyber Warfare and Security (Vol. 297).

IEEE (2008). *IEEE 12207-2008, Systems and software engineering - Software life cycle processes*. IEEE.

IEEE (2010). IEEE 1730-2010, Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP). IEEE.

Joint Chief of Staff (2012). *No-Strike and Collateral Damage Estimation Methodology*. United States Army.

Knott, B. A., Mancuso, V. F., Bennett, K., Finomore, V., McNeese, M., McKneely, J. A., & Beecher, M. (2013). Human factors in cyber warfare: Alternative perspectives. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. SAGE Publications, 57(1), pp. 399-403.

Korstanje, M. E. (Ed.). (2016). *Threat mitigation and detection of cyber warfare and terrorism activities*. IGI Global.

Kott, A., Wang, C., & Erbacher, R. F. (Eds.). (2015). *Cyber defense and situational awareness* (Vol. 62). Springer.

Liles, S. (2010). Cyber Warfare: As a form of low-intensity conflict and insurgency. In Proceedings of the *Conference on Cyber Conflict* (pp. 47-57). IEEE.

Liles, S., Dietz, J. E., Rogers, M., & Larson, D. (2012). Applying traditional military principles to cyber warfare. In Proceedings of the *4th International Conference on Cyber Conflict* (pp. 1-12). IEEE.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies.

Maathuis, C., Pieters, W. & Berg, v.d. J. (2016). Cyber Weapons: a Profiling Framework. In Proceedings of the 1st International Conference on Cyber Conflict U.S. (pp. 1-8). IEEE.

Maathuis, C., Pieters, W. & van den Berg, J. (2018). A Knowledge-Based Model for Assessing the Effects of Cyber Warfare", In Proceedings of the 12th NATO Conference on Operations Research & Analysis.

Maathuis, C., Pieters, W. & v.d. Berg, J. (2018b). Developing a computational ontology for Cyber Operations, *Journal of Information Warfare*, 17(3):32-51.

Maathuis, C., Pieters, W. & v.d. Berg, J. (2020). Decision Support Model for Effects Estimation and Proportionality Assessment for Targeting in Cyber Operations, *Journal of Defence Technology*, to appear.

Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014). Human factors in cyber warfare II: Emerging perspectives. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications, 58(1), pp. 415-418.

Marshall, H., Good., T., Gaughan, C. & McDonnell, J.S. (2015). *Development of a Distributed Cyber Operations Modeling and Simulation Framework*. SISO.

Marinos, L. (2016). *ENISA Threat Taxonomy: A tool for structuring threat information*. ENISA.

McClure, C. A. R. M. A. (2001). Software Reuse. *A Standards-Based Guide. Software Engineering Standards Series*. *IEEE Computer Society*.

Mele, S. (2013). *Cyber-weapons: legal and strategic aspects*. Istituto Italiano di Studi Strategici.

NATO (2011). Collateral Damage Estimation.

NATO (2014). Wales Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_112964.htm. 2014: Accessed May, 24, 2019.

Newcomb, E.A. & Hammell, R.J. (2016), A fuzzy logic utility framework (FLUF) to support information assurance, *Software Engineering Research, Management and Applications*. Springer; 33-48.

Oltramari, A., Cranor, L.F., Walls, R.J. & McDaniel, P. (2015). Computational ontology of network operations', In Proceedings Proceedings of the Military Communications Conference (pp. 318-23). IEEE.

Osinga, F. (2012). Introducing Cyber Warfare. *Cyber Warfare,* Asser Press, pp. 13.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chaterrjee, A. (2008). A Design Science Research Methodology for Information Systems Research, *Journal of Management of Information Systems*. 2008, 24(3), pp. 45-78.

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare. *Information & Computer Security*, *24*(1), 38-52.

Prelipcean, G., Boscoianu, M. & Moisescu, F. (2010). New ideas on the artificial intelligence support in military applications. In Proceedings of the 9th WSEAS international conference on Artificial intelligence, knowledge engineering and data bases. World Scientific and Engineering Academy and Society.

Remenyi, D., & Wilson, R. L. (2018). *Glossary of Cyber Warfare, Cyber Crime Cyber Security*. ACPIL.

Romanosky, S. & Goldman, Z. (2017). Understanding Cyber Collateral Damage. *Journal of National Security Law and Policy*, 9, 233,

Schmitt, M.N. (Ed.). (2013). *Tallinn Manual on the international law applicable to cyber warfare.* Cambridge University Press, pp. 68, 80.

Schmitt, M.N. (Ed.). (2017). *Tallinn Manual 2.0. on the international law applicable to cyber operations*. Cambridge University Press, pp. 451.
Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1-37.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A cyber attack taxonomy. Proceedings of 9th Annual Symposium On Information Assurance-ASIA, 14.

Smeets, Max. (2019) 'NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis', In Proceedings of the 11th *International Conference on Cyber Conflict (CyCon)*, IEEE, 4.

Taddeo, M. (2012). An analysis for a just cyber warfare. In Proceedings of the 4th international conference on cyber conflict (pp. 1-10). IEEE.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

Tyugu, E. (2011). Artificial intelligence in cyber defense. In *Proceedings of the 3rd International Conference on Cyber Conflict* (pp. 1-11). IEEE.

Tzu, S., Tzu, S., Sun, W., & Vu, S. C. (1971). *The art of war*. Oxford University Press, USA.

United States Army (2013). Joint Publication 3-12 (R). *Cyberspace Operations*. United States Army.

United States Army (2018). Joint Publication 3-12. *Cyberspace Operations*. United States Army.

Van der Wal, S.J., Gorter, R., Reijnen, A., Geuze, E., & Vermetten, E.(2019). Cohort Profile: The prospective research in stress-related military operations (PRISMO) study in the Dutch armed forces. *BMJ open*, *9*(3), e026670.

Vogt, J., Leonhardt, J., Köper, B., & Pennig, S. (2010). Human factors in safety and business management. *Ergonomics*, *53*(2), 149-163.

Wihl, L., Varshney, M., & Kong, J. (2010). Introducing a cyber warfare communications effect model to synthetic environments. In *The Interservice/Industry Training, Simulation & Education Conference.*

Wihl, L. (2015).Training for the Combined Cyber/Kinetic Battlefield.

Summary

Cyber Warfare is perceived as a radical shift in the nature of warfare. It can represent a real alternative next to other types of Military Operations to achieve military and/or political goals in front of adversaries. To this end, Cyber Operations use specific technologies i.e. cyber weapons/capabilities/means. With a short but intense history of incidents/ events labelled as Cyber Operations or Cyber Warfare incidents, their potential and scale of impact has proven to cross geographical and digital borders. In this way, their effects are impacting not only their engaged targets, but also other collateral actors and systems, at local, national, regional, and global scale.

Cyber Operations are increasingly integrated by military forces of state, hybrid, and non-state actors as a component of the existing or to be built toolboxes of options for military Commanders and a real option on the strategic/political agenda. They can be planned, executed, and assessed as independent operations or embedded as a component into other broader Military Operations with either a supportive or an amplifier role to achieving the intended effects.

In comparison with other types of Military Operations (e.g. land, air, sea, and space), Cyber Operations are surrounded by secrecy and still lack a comprehensive understanding as well as methodologies, models, and TTPs (Tactics, Techniques, and Procedures) that could support their efficient, effective, and performant planning, execution, and assessment. This is reflected in both as a gap in the existing body of knowledge of cyber and military domains as well as from a practitioner point of view.

As Cyber Operations are classified in three major classes i.e. intelligence, offensive, and defensive, this research is relevant for all three of them since it aims at assessing their effects. However, this research is mainly addressed to offensive Cyber Operations and is conducted through offensive lenses which embeds offensive and intelligence perspectives e.g. when analysing targets or the effects of Cyber Operations in order to support targeting decision making in Cyber Operations. Taking into consideration the fact that at the moment of speaking military Commanders and their teams lack methodologies and models to support their decisions in Cyber Operations, and the existing gap in the scientific literature and corresponding space of artefacts, the aim of this research is as follows:

To design a series of models, methodologies, and frameworks that assess the effects of Cyber Operations in order to support military targeting decisions in Cyber Warfare.

The aim was translated to the following main research question of this dissertation:

How to assess the effects of Cyber Operations in order to support military targeting decisions in Cyber Warfare?

The present research primarily aims at supporting military Commanders advised by their teams composed of cyber advisors, legal advisors etc. while targeting in Cyber Warfare. More specifically, both the research and its resulted artefacts could be used when planning, executing, and assessing Cyber Operations by assessing the effects of Cyber Warfare and advising targeting decisions concerning the proportionality assessment and further considerations for developing CoAs (Courses of Action) in Cyber Operations. In this way two perspectives or contexts of use were identified for the present research: military-legal and military-operational. In the legal context, the principle of proportionality requires to test in order to prevent that the unintended effects on civilians and civilian systems (Collateral Damage) are excessive in relation to the intended effects that would support the achievement of military objectives (Military Advantage). In the operational context, a broader perspective is considered in the sense of including the unintended effects of Cyber Operations that impact military actors and systems (Military Disadvantage) as well as including a broader view on the unintended effects of Cyber Operations that impact civilian actors and systems (Collateral Damage). In order to be able to achieve the abovementioned aim, to answer the main research question of this research, and to design the proposed artefacts, a multidisciplinary research in the fields of Cyber Security (i.e. incident analysis, threat, vulnerability, and impact assessment), Artificial Intelligence (i.e. Knowledge Representation and Reasoning, Fuzzy Logic), and Military Operations (i.e. military targeting, planning, air and space technologies such as Ballistic Missile and Unmanned Aerial Vehicles/Unmanned Aircraft Systems) was conducted from a military-technical perspective.

This research was conducted using a Design Science Research approach which allows the design, development, and evaluation of artefacts that can solve a specific aim. By using this methodology, the aim and implicitly, the main research question was split into five different and smaller research questions that were sequentially answered and for each a different artefact was proposed. Hence, the logic behind the decision to split into five artefacts relies on their use in Cyber Operations and on the fact that

in order to understand the phenomenon (Cyber Operations) and its effects, one first needs to tackle it through different angles and perspectives (technical-military) as a whole (Artefact I), followed by focusing on what the means (cyber weapons) are that are actually producing its effects (Artefact II) through a structured methodological approach (Artefact III) focusing on classifying and assessing its effects on different qualities and aspects of impacted entities (Artefact IV) and afterwards estimating these effects and proposing targeting decisions concerning the proportionality assessment (Artefact V). Hence, these artefacts together answer the main research question. Additionally, the artefacts have benefitted from the fact that they i) were designed and evaluated with the help of military-technical experts using research instruments such as semi-structured interviews and Workshops (structured focus groups), and ii) were brought directly to both the scientific community and practitioners through a series of peer-reviewed venues and presentations in national and international settings (i.e. conferences, journals, and workshops).

The scientific contributions of this research contribute to the body of knowledge and correspondent space of artefacts from the fields of Cyber Security, Military Operations, and Artificial Intelligence. This is represented by the five artefacts that have been built and proposed, and are further depicted in the following figure:

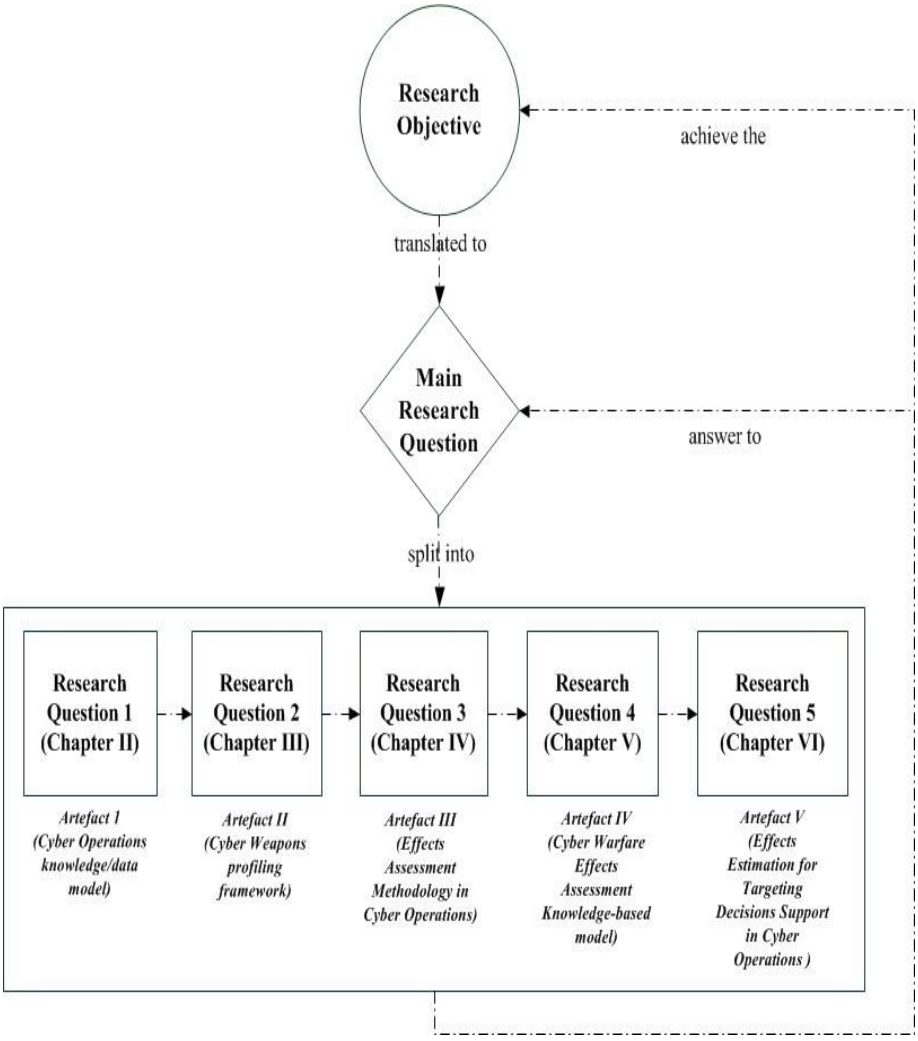


Figure S.1. Relation between Research Objective, Main Research Question, Research Questions, Dissertation Chapters, and Artefacts

The first artefact is a knowledge/data model to represent the definition and context of Cyber Operations. A Cyber Operation was defined as "a type or part of a Military Operation in which cyber weapons/capabilities are used to achieve military objectives in front of adversaries inside and/or through cyberspace". Accordingly, the entities involved in Cyber Operations as well as the relationships between these entities are further represented as a model in the form of a computational ontology. In order to do that, the following research instruments were used: literature review, reports, military doctrine, case studies on real Cyber Operations incidents, face-to-face meetings with military-technical experts,

plus direct participation and observation in joint military exercises. Hence, the upper-classes of this model are Context, Actor (i.e. agent), MilitaryObjective, Type, Phase, Target, CyberWeapon, Action, Geolocation, Asset, and Effect, and relationships considered are the ones such as isExploiting and isProducingCollateralDamage.

The second artefact is a profiling framework for Cyber Weapons that first establishes a definition for Cyber Weapons: computer programs 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. After that, analyses their life cycle, and further analyses their classification criteria and characteristics that are further used for developing the third artefact. To reach to that, the following research instruments were used: literature review and case studies on real Cyber Operations incidents.

The third artefact is an effects assessment methodology for intended and unintended effects of Cyber Operations such as Military Advantage, Collateral Damage, and Military Disadvantage. In this research, the following definitions for these effects have been proposed: Military Advantage as "intended effects that contribute to achieving military objectives", Collateral Damage as "unintended effects that do not contribute to achieving military objectives, but impact civilian assets, in the form of civilian injury or loss of live and/or damage or destruction to civilian objects and/or environment", and Military Disadvantage as "unintended effects that do not contribute to achieving military objectives and impact allies, friendly, neutral, even the target or conducting actors". To reach these definitions and methodology, the following research instruments were used: literature review, reports, military doctrine, two sets of interviews with eighteen military experts, case studies on real and virtual realistic Cyber Operations incidents, face-to-face meetings with military experts, direct participation and observation in joint military exercises, and a Focus Group/Workshop. Moreover, the assessment methodology contains multidimensional factors such as spreading, duration, and probability of occurrence, and is structured in five phases, as follows: Target Identification and Validation, Target Analysis, Target Effects Assessment, Collateral Effects Assessment, and Minimization of Unintended Effects. Thus, the methodology begins when targets (of Cyber Operations) are identified and validated, and ends when control measures for avoiding or minimizing the unintended effects are considered and applied when needed.

The fourth artefact is an effects assessment model in the form of a knowledge-based model that can serve as a knowledge/data-based simulation environment for decision support in Cyber Operations.

Accordingly, the model represents and proposes for reasoning information such as thirty types of effects (e.g. Alter, Disturb, LossOfLife) together with thirty three aspects and qualities of systems that can be impacted (e.g. Confidentiality, Functionality, Reputation). To achieve these results, the next research instruments were used: literature review, reports, military doctrine, three sets of semi-structured interviews with forty military experts, case studies on real and virtual realistic Cyber Operations incidents, face-to-face meetings with military experts, field work in joint military exercises, and a Focus Group/Workshop.

The fifth and last artefact is a multi-layered Fuzzy model that first, estimates the effects of Cyber Operations, second, classifies the effects of Cyber Operations considering intention and nature as classification criteria, and third, advises targeting decisions based on a proportionality assessment in Cyber Operations. In order to reach that, literature review, reports, military doctrine, three sets of semi-structured interviews with forty military experts, case studies on real and virtual realistic Cyber Operations incidents, field work in joint military exercises, and a Focus Group/Workshop were used.

Additionally, in this research three virtual, but realistic case scenarios/studies/use cases of Cyber Operations were designed and used for evaluation purposes for different advanced artefacts. These cases could be of further use in military training and exercises for Cyber Operations, broader integrated in Hybrid Operations/Warfare, or other types of cyber incidents e.g. (counter-) Cyber Terrorism. As they were built from a military-technical perspective based on intensive research on correspondent used technologies (i.e. ballistic missiles, suicide UAVs, and cargo ships), their realism and usefulness was successfully evaluated by the consulted military-technical experts. Moreover, this research raises situation awareness to different other scientific-communities from fields such as legal, politics, ethics etc., and represents a successful application of different AI techniques (i.e. Knowledge Representation and Reasoning, and Fuzzy Logic) for building some of the proposed artefacts.

The introduced artefacts in this research have been exemplified and evaluated from a double perspective: technical, and by military-technical experts with significant international experience in military training, exercises, and real operations (the youngest expert had 15 years of experience and the oldest expert had 35 years of experience). To evaluate the artefacts criteria such as consistency, accuracy, clarity, conciseness, usefulness, and adaptability were considered. The expert-based evaluation process was conducted through a series of face-to-face meetings and Focus

Groups with the experts who successfully validated the artefacts proposed in this dissertation.

Based on these facts, the answer to the main research question is the combination of the fifth proposed artefacts in this research and their use when aiming at assessing the effects of Cyber Operations and providing decision support information for targeting decision support concerning proportionality assessment in Cyber Operations.

The societal contributions of this research directly aims at supporting targeting decisions in Cyber Warfare by assisting military Commanders (as decision makers), their advisors, and by that broader to political awareness and decision making, in such a way that it:

- Provides useful insights (e.g. definitions and assessment of effects) for the design and development of military doctrines, strategies, TTPs in Cyber Operations as well as design and development of (public) policies, reports, best practices and recommendations for Cyber Operations.
- Provides three Cyber Operations case scenarios/use cases that represent three realistic, public, and usable data(sets) which could be of further use for the design and development of other artefacts for Cyber Operations.
- Provides awareness and a realistic starting point to technical practitioners from fields such as Cyber Security, Software Engineering, Artificial Intelligence/Machine Learning, as well as congruent or correspondent stakeholders when analysing or deploying them or other types of cyber incidents in regards with assessing and estimating their effects and support to decision making.

The main limitations of this research were the limited data(sets) publically available to use in this research, and the existing lack in other methodologies, models, and TTPs that could have been used in different states of this research and moments of building the proposed artefacts. However, to cope with these limitations, military experts have been consulted from the beginning of this research and implicitly from the design phase of the proposed artefacts and to their evaluation at the end. Hence, this research embeds and uses a hybrid approach i.e. being both knowledge and data oriented.

Conclusively, four recommendations for extensions for future work were identified. First, governments and organizations should publicly release by making available or definitely broader available data(sets) of real,

virtual or fictive, but realistic Cyber Operations incidents conducted by both state and non-state actors. Second, increase synergy by unifying efforts from different academic and practitioner communities through a multidisciplinary approach towards reaching common greater goals such as new developments (e.g. of doctrine, strategies, policies, reports) and joint operations. That means not just bringing actively together actors/agents, organizations, and/or projects of a similar nature (e.g. civilian or military, technical or non-technical), but actually merging them together (i.e. different nature) to reaching fruitful results. This synergy would help reaching common awareness, understanding, and assessment, and would actively contribute to better comprehending behaviours and decision making aspects in Cyber Operations. Third, increase the use of AI techniques in both academic and practitioner use in order i) to further predict or estimate the effects of Cyber Operations based on extended data(sets), ii) to provide and implement control measures for minimizing or mitigating the unintended effects of Cyber Operations, and iii) to analyse the behaviour of military decision makers when targeting in Cyber Warfare. Fourth, increase the use of Modelling and Simulation techniques that would facilitate the introduction and integration of new capabilities such as cyber weapons/capabilities in the battlefield as well as for supporting military training, exercises, and use of Cyber Operations.

Samenvatting

Cyber Warfare, oftewel cyberoorlog, wordt gezien als een radicale omslag in de aard van oorlogvoering. Cyber Warfare kan immers een reële alternatief zijn naast andere typen militaire operaties die gericht zijn op het verwezenlijken van militaire en/of politieke doelen in de confrontatie met tegenstanders. Hiertoe, Cyber Operations gebruiken specifieke technologieën zoals cyberwapens/-capaciteiten/-middelen. In de nog jonge-iets meer dan tien jaar omvattende-maar enerverende historie van incidenten/gebeurtenissen die algemeen worden aangeduid als Cyber Operations (cyberoperatie-) of Cyber Warfare (cyberoorlog-) incidenten is gebleken dat ze qua potentieel en impact zowel geografische als digitale grenzen overschrijden. Hun invloed reikt dan ook voorbij de aangevallen doelen en omvat tevens andere bijkomende actoren en systemen, op lokale, landelijke, regionale en wereldwijde schaal.

Cyber Operations worden steeds meer geïntegreerd door militaire strijdkrachten, alsmede door hybride en niet-gouvernementele actoren, in de zin dat ze een bestanddeel vormen van bestaande of nog te ontwikkelen toolboxes met opties voor militaire bevelhebbers. Daardoor worden ze een reële optie op de strategische/politieke agenda. Ze kunnen worden gepland, uitgevoerd en beoordeeld als zelfstandige operaties of als onderdeel worden ingebed in andere, bredere militaire operaties die een ondersteunende dan wel een versterkende rol vervullen bij het realiseren van de beoogde effecten.

Vergeleken met andere typen militaire operaties (bijvoorbeeld op land, in de lucht, op zee of in de ruimte) vinden Cyber Operations in strikte geheimhouding plaats. Er is nog geen sprake van fundamenteel inzicht of methodieken, modellen en TTP's (Tactieken, Technieken en Procedures) die een efficiënte, effectieve en performante planning, uitvoering en beoordeling mogelijk zouden maken. Dat manifesteert zich in een lacune in de huidige kennis op cyber- en militair gebied, maar ook vanuit uitvoerend perspectief.

Cyber Operations worden onderverdeeld in drie hoofdklassen, namelijk informatievergaring, aanval en verdediging. Dat maakt het huidige onderzoek relevant voor alle drie, aangezien het hier gaat om de inschatting van effecten. Dit onderzoek wordt echter uitgevoerd met offensieve lenzen die offensieve en intelligentieperspectieven omvatten, bijvoorbeeld bij het analyseren van doelen of de effecten van incidenten met Cyber Operations

ter ondersteuning van gerichte besluitvorming in Cyber Operations. Aangezien dat op dit moment militaire Commandanten en hun teams methodologieën en modellen missen om hun beslissingen in Cyber Operations te ondersteunen, en de bestaande kloof in de wetenschappelijke literatuur en overeenkomstige ruimte van artefacten, het doel van dit onderzoek wordt daarmee als volgt:

Het ontwerpen van een reeks van modellen, methodieken en kaders voor de beoordeling van de effecten van Cyber Operations ter ondersteuning van de besluitvorming betreffende militaire doelen in Cyber Warfare.

Dit doel is vertaald in de volgende belangrijkste onderzoeksvraag van dit proefschrift:

Hoe kunnen we de effecten beoordelen van de besluitvorming omtrent militaire doelen in Cyber Warfare?

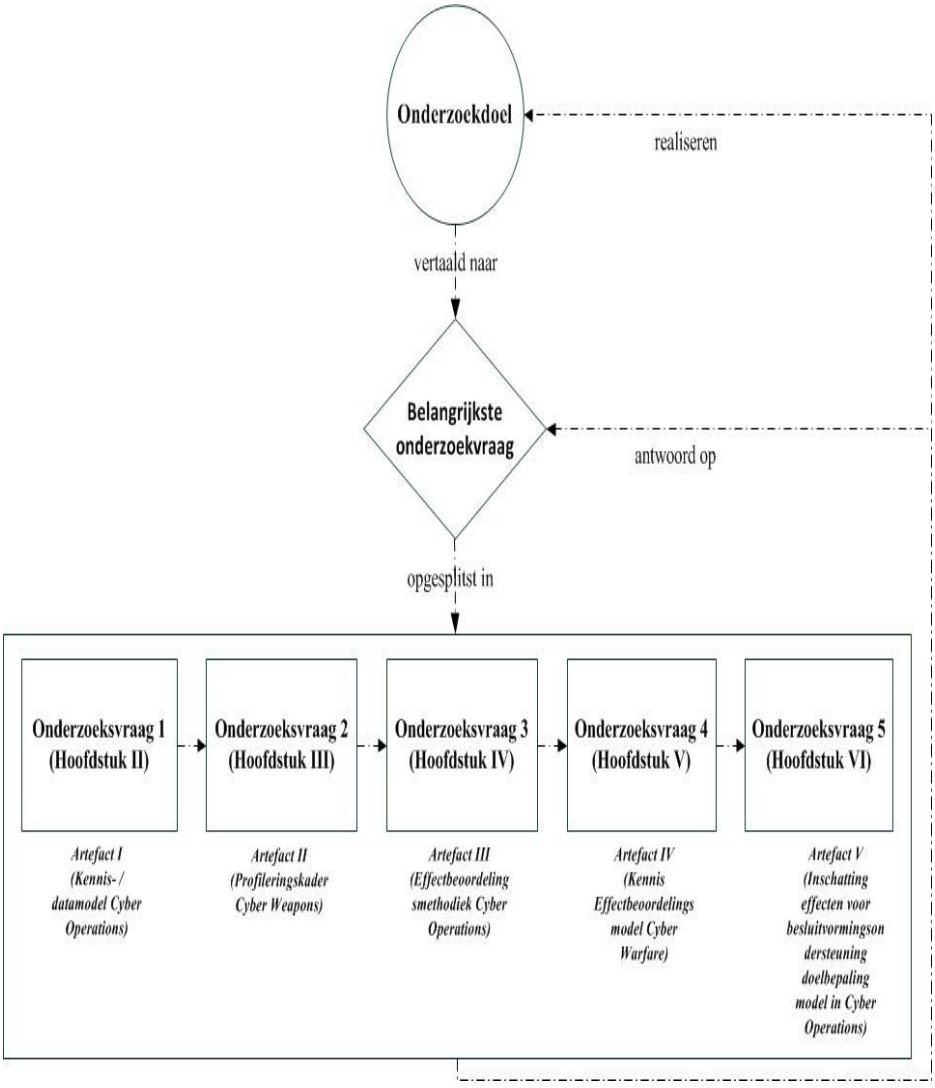
Het huidige onderzoek richt zich primair op de ondersteuning van militaire bevelhebbers die terzijde worden gestaan door teams van cyberadviseurs, juridische adviseurs etc. bij het bepalen van doelen in Cyber Warfare. In meer specifieke zin kan het onderzoek en de resulterende artefacten worden gebruikt bij het plannen, uitvoeren en beoordelen van Cyber Operations door het beoordelen van de effecten van Cyber Warfare en het adviseren met betrekking tot besluitvorming betreffende doelen in de context van proportionaliteitsbeoordeling, en ook verdere overwegingen voor het ontwikkelen van CoA's (Courses of Action) in Cyber Operations. Op deze manier werden twee perspectieven of gebruikscontexten geïdentificeerd voor het huidige onderzoek: juridisch en operationeel. In de juridische context, het proportionaliteitprincipe (evenredigheidsbeginsel) moet worden getest om te voorkomen dat de ongewenste effecten op burgers en civiele systemen (nevenschade) buitensporig zijn in verhouding tot de gewenste effecten die het bereiken van militaire doelen zouden kunnen ondersteunen (militair voordeel). In de operationele context, wordt een breder perspectief overwogen in de zin van het opnemen van de onbedoelde effecten van Cyber Operaties die van invloed zijn op militaire actoren en systemen (Military Disadvantage), evenals een bredere kijk op de onbedoelde effecten van Cyber Operaties die van invloed zijn op civiele actoren en systemen (Collateral Damage).

Teneinde bovenstaand doel te realiseren, de belangrijkste onderzoeksvraag te beantwoorden, en om de voorgestelde artefacten te ontwerpen, werd multidisciplinair onderzoek uitgevoerd op het gebied van cybersecurity (incidentanalyse en beoordeling van dreiging, kwetsbaarheid

en impact), kunstmatige intelligentie (kennisrepresentatie en -beredenering, fuzzy logic), en onderzoek naar militaire operaties/verdediging (kiezen van militaire doelen, planning, lucht- en ruimtevaarttechnologie zoals ballistische raketten en onbemande luchtvaartuigen/onbemande vliegtuigsystemen) vanuit militair-technisch perspectief.

Dit onderzoek is uitgevoerd op basis van een zogeheten Design Science Research-benadering, die het ontwerp, de ontwikkeling en evaluatie mogelijk maakt van artefacten die een specifiek doel kunnen verwezenlijken. Uitgaande van deze methodiek werd het doel en impliciet ook de belangrijkste onderzoeksvraag opgesplitst in vijf verschillende onderzoeksdeelvragen, die achtereenvolgens werden beantwoord en waarvoor telkens een ander artefact werd voorgesteld. De achterliggende logica van de keuze voor deze opsplitsing in vijf artefacten berust dan ook op het gegeven dat, teneinde inzicht te krijgen in het verschijnsel (Cyber Operations) en de effecten ervan, we de vraag eerst vanuit verschillende invalshoeken en gezichtspunten (technisch-militair) in zijn totaliteit zullen moeten benaderen (Artefact I). Vervolgens kunnen we inzoomen op de middelen (cyber wapens) die de effecten feitelijk bewerkstelligen (Artefact II) uitgaande van een gestructureerde methodologische benadering (Artefact III) die gericht is op de classificering en beoordeling van de effecten op diverse eigenschappen en aspecten van de getroffen entiteiten (Artefact IV), gevolgd door een beoordeling van deze effecten en het voorstellen van besluiten betreffende doelen met betrekking tot de proportionaliteitsbeoordeling (Artefact V). Tezamen beantwoorden deze artefacten dan ook de belangrijkste onderzoeksvragen. Bovendien hebben de artefacten hiervan geprofiteerd van het feit dat ze i) zijn ontworpen en beoordeeld met hulp van militair-technische deskundigen met gebruik van onderzoeksinstrumenten zoals interviews en workshops, en ii) rechtstreeks aan de wetenschappelijke gemeenschap en praktijkmensen zijn voorgelegd middels een reeks peer-reviewed locaties en presentaties op zowel landelijk als internationaal niveau (congressen, vaktijdschriften en workshops).

De wetenschappelijke bijdragen van dit onderzoek vergroten de kennis en bijbehorende ruimte voor artefacten op het terrein van cyberoorlog/-veiligheid, militaire operaties en kunstmatige intelligentie. Dit wordt weergegeven door middel van de vijf artefacten die zijn ontwikkeld en voorgesteld, zoals in de volgende afbeelding:



Afbeelding S.1. Relatie tussen onderzoeksdoel, belangrijkste onderzoeksvraag, onderzoeksvragen, proefschrifthoofdstukken en artefacten

Het eerste artefact is een kennis/gegevensmodel voor het weergeven van de definitie en context van Cyber Operations. Een Cyber Operation is gedefinieerd als "een type of onderdeel van een militaire operatie waarin cyberwapens/-capaciteiten worden ingezet om militaire doelen in de confrontatie met tegenstanders te verwezenlijken, binnen en/of via cyberspace". De entiteiten die zijn betrokken bij Cyber Operations alsmede de relaties tussen deze entiteiten zijn daarnaast weergegeven als model, in de vorm van een computationele ontologie. Voor dat doel werden de

volgende onderzoeksinstrumenten gebruikt: literatuuronderzoek, rapportage, militaire doctrine, casestudy's betreffende echte Cyber Operations-incidenten en persoonlijke ontmoetingen met militair-technische deskundigen, naast rechtstreekse deelname aan en observatie van gezamenlijke militaire oefeningen. De hoogste categorieën van dit model zijn dientengevolge Context, Actor (agent), MilitaryObjective (militair doel), Type, Phase (fase), Target (doel), CyberWeapon (cyberwapen), Action (actie), Geolocation (geolocatie), Asset en Effect, terwijl relaties in beschouwing worden genomen zoals isExploiting (maakt gebruik van) en isProducingCollateralDamage (richt bijkomende schade aan).

Het tweede artefact is een profileringskader voor Cyber Weapons dat allereerst een definitie voor Cyber Weapons vaststelt: computerprogramma's die zijn gemaakt en/of worden gebruikt om (een ICT-component van) een systeem te wijzigen of beschadigen om (militaire) doelen te bereiken tegen tegenstanders binnen en/of buiten cyberspace. Daarna, hun levensduur analyseert en de classificeringscriteria en kenmerken in detail analyseert, en verder worden gebruikt voor het ontwikkelen van het derde artefact. Om dat te realiseren werden de volgende onderzoeksinstrumenten gebruikt: literatuuronderzoek en casestudy's betreffende echte Cyber Operations-incidenten.

Het derde artefact is een effectbeoordelingsmethodiek voor bedoelde en onbedoelde effecten van Cyber Operations zoals Military Advantage (militair voordeel), Collateral Damage (bijkomende schade), en Military Disadvantage (militair nadeel). In dit onderzoek zijn de volgende definities voor deze effecten voorgesteld: Military Advantage als “bedoelde effecten die bijdragen aan het verwezenlijken van militaire doelen”, Collateral Damage als “onbedoelde effecten die niet bijdragen aan het verwezenlijken van militaire doelen, maar die een impact hebben op burgerbezit in de vorm van letsel of het overlijden van burgers en/of schade aan of verwoesting van burgerdoelen en/of de leefomgeving van burgers”, en Military Disadvantage als “onbedoelde effecten die niet bijdragen aan het verwezenlijken van militaire doelen, maar die een impact hebben op geallieerde, bevriende en neutrale objecten, met inbegrip van het doel zelf of uitvoerende actoren”. Voor de ontwikkeling van deze definities en methodieken werden de volgende onderzoeksinstrumenten toegepast: literatuuronderzoek, rapportage, militaire doctrine, twee reeksen interviews met 18 militaire deskundigen, casestudy’s betreffende echte en virtuele realistische Cyber Operations-incidenten, persoonlijke ontmoetingen met militaire deskundigen, rechtstreekse deelname aan en observatie van gezamenlijke militaire oefeningen, en een focusgroep/workshop. De beoordelingsmethodiek, die multidimensionale factoren zoals spreiding, duur en waarschijnlijkheid van optreden omvat, is gestructureerd in vijf

fasen: Target Identification and Validation (doelidentificatie en -validering), Target Analysis (doelanalyse), Target Effects Assessment (beoordeling doeleffecten), Collateral Effects Assessment (beoordeling bijkomende effecten), and Minimization of Unintended Effects (minimalisering onbedoelde effecten). Het beginpunt van de methodiek ligt dus daar waar doelen (of Cyber Operations) worden geïdentificeerd en gevalideerd, en de methodiek eindigt wanneer beheersmaatregelen voor het vermijden of minimaliseren van ongewenste effecten worden overwogen en toegepast, indien noodzakelijk.

Het vierde artefact is een effectbeoordelingsmodel in de vorm van een kennisgeoriënteerd model dat kan fungeren als kennis-/datageoriënteerde simulatieomgeving voor besluitvormingsondersteuning bij Cyber Operations. Het model vertegenwoordigt en oppert dan ook beredeneringsinformatie zoals 30 soorten effecten (bijvoorbeeld Alter (wijzigen), Disturb (verstoren), LossOfLife (verlies van levens) in combinatie met 33 aspecten en eigenschappen van systemen die beïnvloed kunnen worden (bijvoorbeeld Confidentiality (betrouwbaarheid), Functionality (functionaliteit) en Reputation (reputatie)). Om deze resultaten te verwezenlijken werden de volgende onderzoeksinstrumenten gehanteerd: literatuuronderzoek, rapportage, militaire doctrine, drie reeksen interviews met 40 militaire deskundigen, casestudy's betreffende echte en virtuele realistische Cyber Operations-incidenten, persoonlijke ontmoetingen met militaire deskundigen, veldwerk in gezamenlijke militaire oefeningen en een focusgroep/workshop.

Het vijfde en tevens laatste artefact is een meerlaags fuzzy model dat allereerst de effecten van Cyber Operations inschat, ten tweede de effecten van Cyber Operations classificeert, met intentie en aard als classificatiecriteria, en ten derde advies uitbrengt over besluitvorming omtrent doelen, op basis van een proportionaliteitsbeoordeling in Cyber Operations. Voor dit doel werd gebruik gemaakt van literatuuronderzoek, rapportage, militaire doctrine, drie reeksen interviews met 40 militaire deskundigen, casestudy's betreffende echte en virtuele realistische Cyber Operations-incidenten, persoonlijke ontmoetingen met militaire deskundigen, veldwerk in gezamenlijke militaire oefeningen en een focusgroep/workshop.

Voorts werden binnen dit onderzoek drie virtuele maar realistische casescenario's/-study's en usecases van Cyber Operations ontworpen en toegepast voor beoordelingsdoeleinden, voor diverse geavanceerde artefacten. Deze cases kunnen van verder nut zijn bij militaire training en oefeningen voor Cyber Operations, bredere integratie in Hybrid Operations/Warfare, of andere typen cyberincidenten, bijvoorbeeld

cyber(contra)terreur. Aangezien ze zijn ontwikkeld vanuit een militair-technisch perspectief, op basis van intensief onderzoek naar verwante toegepaste technologie (ballistische raketten, onbemande zelfmoordluchtvaartuigen en vrachtschepen), werden hun realiteitsgehalte en toepasbaarheid met succes beoordeeld door de geraadpleegde militair-technische deskundigen. Bovendien versterkt dit onderzoek de situationele bewustwording bij allerlei andere wetenschappelijke gemeenschappen op diverse terreinen: juridisch, politiek, ethiek, etc. Het vertegenwoordigt een succesvolle toepassing van verschillende AI-technieken (Knowledge Representation and Reasoning (kennisrepresentatie en -beredenering) en fuzzy logic) voor het ontwikkelen van een aantal voorgestelde artefacten.

De in dit onderzoek geïntroduceerde artefacten werden als voorbeeld gebruikt en beoordeeld vanuit tweeërlei oogpunt: enerzijds technisch, en anderzijds vanuit het perspectief van militair-technische deskundigen met aanzienlijke internationale ervaring op het gebied van militaire training, oefeningen en echte operaties. Ter beoordeling van de artefacten werden criteria zoals consistentie, nauwkeurigheid, helderheid, compactheid, bruikbaarheid en flexibiliteit in aanmerking genomen. Het beoordelingsproces werd uitgevoerd middels een reeks persoonlijke ontmoetingen en focusgroepen met de deskundigen, die de in dit proefschrift voorgestelde artefacten met succes hebben gevalideerd.

Op basis van deze feiten is het antwoord op de belangrijkste onderzoeksvraag de combinatie van de vijfde voorgestelde artefacten in dit onderzoek om de effecten van Cyber Operations te beoordelen en gerichte ondersteuning van beslissingen met betrekking tot proportionaliteitsbeoordeling in Cyber Operations.

Op basis van deze feiten is het antwoord op de belangrijkste onderzoeksvraag de combinatie van de vijfde voorgestelde artefacten in dit onderzoek en hun gebruik bij het beoordelen van de effecten van cyberoperaties en het verstrekken van informatie over besluitondersteuning voor besluitvormingsondersteuning met betrekking tot evenredigheidsbeoordeling bij Cyber Operations. En in bredere zin door versterking van politiek besef en besluitvorming. Op zo'n manier dat dit:

- Bruikbaar inzicht biedt (bijvoorbeeld definities en beoordeling van effecten) voor het ontwerpen en ontwikkelen van militaire doctrines, strategieën en TTP's in Cyber Operations, naast het ontwerpen en ontwikkelen van (openbaar) beleid, rapportage, best practices en aanbevelingen voor Cyber Operations.
- Leidt tot drie case-scenario's/usecases voor Cyber Operations die drie realistische, openbare en bruikbare data(sets)

vertegenwoordigen die van verder nut kunnen zijn voor het ontwerpen en ontwikkelen van andere artefacten voor Cyber Operations.
- Zorgt voor bewustwording en een realistisch uitgangspunt voor technische praktijkmensen op het gebied van o.a. cyberveiligheid, software-engineering, kunstmatige intelligentie/machine-learning, maar ook voor congruente of verwante stakeholders bij het analyseren of implementeren ervan, of van andere soorten cyberincidenten met betrekking tot het beoordelen en inschatten van de effecten, en ondersteunt besluitvorming.

De belangrijkste beperkingen van dit onderzoek werden gevormd door de beperkte data(sets) die publiek toegankelijk waren voor gebruik in dit onderzoek, en het huidige gebrek aan andere methodieken, modellen en TTP's die van pas hadden kunnen komen in verschillende fasen van dit onderzoek en bij het ontwikkelen van de voorgestelde artefacten. Om deze beperkingen het hoofd te bieden zijn er echter van begin af aan militaire deskundigen geraadpleegd, en is dit impliciet gebeurd vanaf de ontwerpfase van de voorgestelde artefacten tot de eindbeoordeling ervan. Dit onderzoek biedt dan ook inbedding en toepassing van een hybride aanpak, die zowel kennis- als datageoriënteerd is.

Ter afronding werden vier aanbevelingen voor toekomstig werk geïdentificeerd. Ten eerste dienen overheden en organisaties Cyber Operations-incidenten openbaar te maken door datasets van echte, virtuele of fictieve maar realistische Cyber Operations-incidenten uitgevoerd door overheidsactoren of andere actoren ter beschikking te stellen, of in ieder geval in ruimere mate ter beschikking te stellen. Ten tweede moet de synergie worden versterkt door het bundelen van krachten van verschillende universitaire en praktijkgemeenschappen door middel van een multi- of transdisciplinaire benadering gericht op het verwezenlijken van hogere gemeenschappelijke doelen, zoals nieuwe ontwikkelingen (bijvoorbeeld van doctrines, strategieën, beleid, rapportage) en gezamenlijke operaties. Dat betekent dat we niet alleen actief actoren/agenten, organisaties en/of projecten van soortgelijke aard bij elkaar moeten brengen (bijvoorbeeld burger of militair, technisch of niet-technisch), maar deze groepen echt met elkaar moeten vermengen (heterogeen maken) om bruikbare resultaten te verkrijgen. Deze synergie bevordert het bereiken van een gemeenschappelijke vorm van besef, inzicht en beoordeling, en draagt actief bij aan een beter begrip van gedrags- en besluitvormingsgererelateerde aspecten in Cyber Operations. Ten derde wordt het gebruik van AI-technieken aanbevolen in zowel universitaire als praktijkomgevingen, teneinde i) de effecten van Cyber Operations nauwkeuriger te kunnen voorspellen of inschatten op basis van uitgebreide data(sets), ii)

controlemaatregelen te bieden en te implementeren gericht op minimalisering of beperking van de onbedoelde effecten van Cyber Operations, en iii) het gedrag van militaire besluitvormers te analyseren bij het vaststellen van doelen in Cyber Warfare. Ten vierde moet meer gebruikgemaakt worden van modelontwikkelings- en simulatietechnieken die de invoering en integratie van nieuwe mogelijkheden zoals cyberwapens/-toepassingen op het slagveld mogelijk maken, alsmede ter ondersteuning van militaire training, oefeningen en het toepassen van Cyber Operations.

Propositions

accompanying the dissertation

Effects Assessment for Targeting Decisions Support in Military Cyber Operations

by

Clara Maathuis

1. Cyber Weapons can empower or weaken any kind of ICT-based activity, action, or system of an actor, and, by that, also the actor himself (Chapter II-IV, this dissertation).

2. Cyber Warfare has reshaped global beliefs, perceptions as well as political, military, and societal options (Chapter III, this dissertation).

3. Military Commanders perceive proportionality in a different way than military legal advisors (Chapter IV-VI, this dissertation).

4. AI techniques are beneficial when assessing and estimating the effects of Cyber Warfare (Chapter II, V, VI, this dissertation).

5. Governments and organizations need to develop open data infrastructures and release Cyber Operations data(sets) since technical experts need real and massive data(sets) to develop and materialize their ideas.

6. In order to rewrite existing and propose new laws of war we need to re-architect our minds.

7. Immigration is a challenging and sometimes overwhelming process implying losing the sense of *home*. However, *home* for one is where her/his heart is, and that can be in different places at the same time or nowhere.

8. In the coming decade, Space and the Arctic will become battlefields where ICT is playing at the same time an enabler and disabler role to different super powers/actors.

9. Conflicts and wars are conducted because of thirst of being complete in one or more senses.

10. Symphonic metal songs are just as complex and amazing as wars.

These propositions are regarded as opposable and defendable, and have been approved as such by the promotors Prof. dr. ir. J. van den Berg and Assoc.prof.dr.ir. W. Pieters

Stellingen

bij het proefschrift

Effects Assessment for Targeting Decisions Support in Military Cyber Operations

door

Clara Maathuis

1. Cyber Weapons kunnen elke vorm van ICT gebaseerde activiteit, actie, of systeem van een acteur, en daarmee ook de acteur zelf versterken of verzwakken (hoofdstuk II-IV, dit proefschrift).

2. Cyber Warfare heeft wereldwijde overtuigingen, percepties alsmede politieke, militaire en maatschappelijke opties op hun kop gezet (hoofdstuk III, dit proefschrift).

3. Militaire bevelhebbers kijken anders naar proportionaliteit dan militaire juridische adviseurs (hoofdstuk IV-VI, dit proefschrift).

4. AI-technieken zijn nuttig bij het beoordelen en inschatten van de effecten van Cyber Warfare (hoofdstuk II, V en VI, dit proefschrift).

5. Overheden en organisaties moeten open datainfrastructuren ontwikkelen en Cyber Operations-data(sets) vrijgeven, aangezien technische deskundigen behoefte hebben aan echte en omvangrijke data(sets) om hun ideeën te kunnen uitwerken en verwezenlijken.

6. Om oorlogswetten te kunnen herschrijven dan wel nieuwe oorlogswetten voor te stellen moeten we onze manier van denken van de grond af opnieuw opbouwen.

7. Immigratie is een uitdagend en soms ook overweldigend proces waarbij er sprake is van het verlies van een *thuis*gevoel. *Thuis* kan echter voor iemand de plek betekenen waar haar/zijn hart is, en dat kan op meerdere plaatsen tegelijkertijd of nergens zijn.

8. In het komende decennium zullen de ruimte en de noordpool een slagveld worden waar ICT zowel een constructieve als een destructieve rol zal vervullen voor de diverse supermachten/-actoren.

9. Conflicten en oorlogen worden uitgevochten vanuit de drang tot vervolmaking, in één of meerdere betekenissen van het woord.

10. Symfonische metal-nummers zijn even complex en bijzonder als een oorlog.

Deze stellingen worden opponeerbaar en verdedigbaar geacht en zijn als zodanig goedgekeurd door de promotores, prof. dr. ir. J. van den Berg en universitair hoofddocent dr. ir. W. Pieters

Appendices

Annex A: Interview Questions Collateral Damage in Cyber Operations

1. What is your role/function and experience in relation with Cyber Operations and Collateral Damage?
2. What does Collateral Damage in Cyber Operations for you mean?
3. What kind of information do you need to perform your role/function regarding estimating Collateral Damage?
4. What are your requirements and expectations from a Collateral Damage estimation methodology/model?
5. What kind of parameters, indicators or metrics could be used to estimate Collateral Damage?
6. What are the challenges you see in designing such a methodology/model?
7. What do you do when and if you do not get the information or results you need from such a methodology/model?
8. Would you be available for another interview/workshop in the future?

Annex B: Interview Questions Targeting Decisions in Cyber Warfare

1. What is your role/function and experience in relation with targeting in Cyber Operations?
2. Could you please explain your activities involved in the targeting decision making process as a military Commander?

3. What are the factors and aspects that influence your targeting decisions?

4. What are the factors and criteria that you consider when you put Collateral Damage against Military Advantage?

5. Considering the proportionality assessment, what does the word "excessive" for you means?

6. What would you advice to limiting Collateral Damage in case of expecting Collateral Damage to be excessive when weighted against Military Advantage?

7. What would you advice to avoiding Collateral Damage in case of expecting Collateral Damage to be excessive when weighted against Military Advantage?

8. Would you be available for another interview/workshop in the future?

Annex C: Interview Questions Military Advantage in Cyber Operations

1. What is your role/function and experience in relation with Cyber Operations and Military Advantage?

2. What does Military Advantage in Cyber Operations for you mean?

3. What kind of information do you need to perform your role/function regarding anticipating/assessing Military Advantage?

4. What are your requirements and expectations from a Military Advantage anticipation/assessment methodology/model?

5. How do you categorize/classify and describe each category/class of Military Advantage?

6. What kind of parameters, indicators or metrics could be used to anticipate/assess Military Advantage?

7. How do you perceive Military Advantage in conventional Military Operations in relation with Military Advantage in Cyber Operations?

8. Would you be available for another interview/workshop in the future?

Annex D: Focus Group 1 Questions: Effects Assessment and Targeting Decisions in Cyber Operations - Case Studies through a (Cyber) War Game Approach

1. Could you please briefly introduce yourself by telling your name and function?

2. Could you please tell how long have you been working in cyber and military domains?

3. Cyberspace is a complex and dynamic domain governed by uncertainty. At the same time, targeting it is not an exact science and often it is considered a form of "art". Taking these facts into consideration, how would you assess the uncertainty around targeting decisions in conducting Cyber Operations?

4. How would you assess [in the sense of estimate] Military Advantage considering all levels and domains of warfare and how would it contribute to achieving military objectives/goals?

5. How would you assess [in the sense of estimate] Collateral Damage?

6. What other categories of collateral effects do you expect to occur?

7. What kind of indicators would characterize Military Advantage and how do you estimate them?

8. What kind of indicators would characterize Collateral Damage in each mentioned category and how do you estimate them?

9. What kind of indicators would characterize the other collateral effects for each category and how do you estimate them?

10. Based on these facts what would you advise the military Commander? Engage this target in attack or not?

    Answer 10.1. Attack! (This means that Collateral Damage is negligible or acceptable).
    Answer 10.2a. Do not attack!
    Answer 10.2a.1. If the source of this answer is the fact that Collateral Damage is excessive, then what measures/controls would you consider to limit/mitigate or avoid Collateral Damage?
    Answer 10.2a.2. If the source of this answer is the fact that Collateral Damage is excessive, what would be acceptable as Collateral Damage (thus non-excessive) in order to attack?
    Answer 10.2.b. Do not attack!
    If the source of this answer is the fact that Military Advantage is not concrete and direct, what would you advice the Commander?

11. Besides these facts, what other factors or aspects you believe are influencing Commander's targeting decision?

12. Do you have another advice regarding this process?

13. Would you be available for another interview, expert meeting or workshop in the future?

Annex E: Focus Group 2 Questions: Assessing Injury in Cyber Warfare

1. Could you please briefly introduce yourself by telling your name and function?

2. Could you please tell how long have you been working in medical, military, and cyber domains?

3. What does injury from a medical and military perspective for you mean?

4. Do you see injury as Collateral Damage in Cyber Operations?

5. What types and forms of injury as Collateral Damage could exist in Cyber Operations from your perspective?

6. How should injury as Collateral Damage be measured in Cyber Operations?

7. What kind of aspects and indicators would you consider to assess injury as Collateral Damage in Cyber Operations?

8. What kind of control measures would you consider to limit/mitigate or avoid injury as Collateral Damage in Cyber Operations?

9. Would you be available for another interview, expert meeting or workshop in the future?

Annex F: Focus Group 3 Questions: From Effects Estimation to Targeting Decisions in Cyber Warfare

1. Could you please briefly introduce yourself by telling your name and function?

2. Could you please tell how long have you been working in cyber and military domains?

3. How would you assess proportionality in Cyber Operations?

4. What are the values for the following variables based on the information given for the considered Cyber Operation use/case scenario?

MilitaryObjective, TargetNature, TargetEntity, TargetVulnerability, TargetDefenseMechanism, TargetConnectionToCollateral, TargetInternetConnection, CyberWeaponType, CollateralNature, CollateralEntity, and CollateralEntityDefenseMechanism.

5. What are the values for the following variables regarding estimating the effects of the present Cyber Operation use case/scenario based on the given information?

EffectTypeTarget, EffectOnTarget, EffectOnTargetProbability, EffectTypeCollateral, EffectOnCollateral, EffectOnCollateralProbability, CollateralEntity.

6. What are the values for the following variables based on the information given and the results from Question 4 and 5 for the considered Cyber Operation use/case scenario? In other words, do you believe that the Military Objective of the present Cyber Operation is achieved?

MilitaryObjectiveAchievement: No, Certain.

7. What are the values for the following variables regarding classifying the effects of the present Cyber Operation use case/scenario based on the definitions presented for Collateral Damage, Military Advantage, and Military Disadvantage, the information given, and the results from Question 4-6?

MilitaryAdvantage, MilitaryAdvantageOnEntity, MilitaryDisadvantage, MilitaryDisadvantageOnEntity, CollateralDamage, and CollateralDamageOnEntity.

8. Based on these results (from Questions 4-7), do you consider the present Cyber Operation/engaging the given target, not-disproportional or disproportional?

9. Considering these facts, in case of an excessive Collateral Damage and implicitly dealing with a not-proportional Cyber Operation, what kind of control measures would you advice the military Commander in order to minimize or avoid Collateral Damage?

10. Do you have another advice regarding this process?

11. Would you be available for another interview, expert meeting or workshop in the future?

Annex G: Expert Meeting Questions for Artefact Evaluation

1. Could you please briefly introduce yourself by telling your name and function?

2. Could you please tell how long have you been working in cyber and military domains?

3. Do you consider this model/methodology as being accurate? Please explain your decision.

4. Do you consider this model/methodology as being clear? Please explain your decision.

5. Do you consider this model/methodology as being concise? Please explain your decision.

6. Do you consider this model/methodology as being applicable and adaptable to different contexts of Cyber Operations? Please explain your decision.

7. Would you be available for another interview, expert meeting or workshop in the future?

List of Publications

1. Maathuis, C., Pieters, W. & van den Berg, J. 2020, 'Decision Support Model for Effects Estimation and Proportionality Assessment for Targeting in Cyber Operations', *Journal of Defence Technology,* 2019(1), DOI: https://doi.org/10.1016/j.dt.2020.04.007, Elsevier.
2. Maathuis, C. 2019, 'A Transdisciplinary Approach to Cyber Warfare', *In Proceedings of the Technology, Management, and Policy Conference 2019,* George Washington University.
3. Boltjes, B., Maathuis, C., van den Berg, T. & Gouweleeuw, R. 2019, 'Developing Standards for Including the Cyber Domain in Military Training and Exercises', *In Proceedings of the Simulation Innovation Workshop 2019,* SISO, pp. 1-17.
4. Maathuis, C., Pieters, W. & van den Berg, J. 2018, 'A Knowledge-Based Model for Assessing the Effects of Cyber Warfare, *In Proceedings of the 12th NATO Conference on Operations Research & Analysis,* NATO, pp. 1-7.
5. Maathuis, C., Pieters, W. & van den Berg, J. 2018, "Developing a Computational Ontology for Cyber Operations", 2018, *Journal of Information Warfare*, vol. 17, issue 3, pp. 33-52.
6. Maathuis, C., Pieters, W. & van den Berg, J. 2018, 'Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations', *In Proceedings of the IEEE Conference on Military Communications,* pp. 1-6, IEEE.
7. Maathuis, C., Pieters, W. & van den Berg, J. 2018, 'A Computational Ontology for Cyber Operations', *In Proceedings of the 17th European Conference on Cyber Warfare and Security,* pp. 278-288.
8. Maathuis, C. 2018, 'Disambiguating Military (Dis)Advantage in Cyber Warfare', *In Proceedings of the 8th EURO ISME Annual Conference on The Ethical Implications of Emerging Technologies in Warfare*.
9. Maathuis, C. 2017, 'Fighters and Victims in the Cyber Battlefield: Towards Assessing the Impact of Cyber Warfare', *In Proceedings of the 3rd Cyber Security Workshop Nederland*.
10. Maathuis, C., Pieters, W. & van den Berg, J. 2016, 'Cyber Weapons: a Profiling Framework', *In Proceedings of the 1st International Conference on Cyber Conflict (CyCon U.S.),* IEEE Computer Society, pp. 1-8, IEEE.

Curriculum Vitae

Clara was born in an immigrant family and since she was interested in technology from a younger age, she finished her high school in Mathematics and Informatics, further earned her bachelor's degree in Computer Science and Automatic Control Engineering, and master's degree in Intelligent Systems – Artificial Intelligence. For both bachelor's and master's thesis she worked on topics related to Wireless Security and developed intelligent software platforms and applications. In parallel, she did professional music training in violin, piano, and vocal singing, and co-founded a former symphonic metal band.

Since her studies, she was eager to apply her knowledge and further develop in solving real world problems. Accordingly, she did an internship in telecommunications and continued working in international projects as Senior Software Engineer in telecommunications and control systems industries. Concurrently, she taught courses in Informatics and Mathematics for undergraduate students.

In September 2015, she started a joint PhD research at Delft University of Technology, TNO, and Netherlands Defense Academy on modelling the effects of Cyber Operations/Warfare for military targeting support. During her research, she collaborated with military-technical scientists from TNO i.e. Rudi Gouweleeuw, Bert Boltjes, and Tom van den Berg on integrating Cyber Operations in Modelling and Simulation systems for military training and exercises. This collaboration resulted in an article that is partially integrated in the Conclusions section of this dissertation.

During her PhD research, she published and presented in a series of blindly peer-reviewed venues in different international settings, served as a session Chair in Cyber Security at the 18th European Conference on Cyber Warfare and Security, and was a technical reviewer for a few scientific articles on different Cyber Security and AI topics. She was involved in co-supervising a Master student, advised multiple Master students, and was Teaching Assistant for the Cyber Risk Management and Security & Technology courses at Delft University of Technology.