Decision support model for effects estimation and proportionality assessment for targeting in cyber operations

Maathuis, C.; Pieters, W.; van den Berg, J.

DOI
10.1016/j.dt.2020.04.007

Publication date
2020

Document Version
Final published version

Published in
Defence Technology

Citation (APA)
Maathuis, C., Pieters, W., & van den Berg, J. (2020). Decision support model for effects estimation and proportionality assessment for targeting in cyber operations. *Defence Technology*, *17*(2), 352-374. https://doi.org/10.1016/j.dt.2020.04.007

KeAi
CHINESE ROOTS
GLOBAL IMPACT

Contents lists available at ScienceDirect

Defence Technology

journal homepage: www.keaipublishing.com/en/journals/defence-technology

Decision support model for effects estimation and proportionality assessment for targeting in cyber operations

C. Maathuis [a], [b], [c], [d], [*], W. Pieters [a], J. van den Berg [a]

[a] Delft University of Technology, Jaffalaan 5, 2628 BX, Delft, Netherlands
[b] TNO Military Operations, Oude Waaldorperweg 63, 2597 AK, Den Haag, Netherlands
[c] Netherlands Defense Academy, De la Reyweg 120, 4818 BB, Breda, Netherlands
[d] Open University of the Netherlands, Valkenburgerweg 177, 6419 AT, Heerlen, Netherlands

ARTICLE INFO

Article history:
Received 31 August 2019
Received in revised form
14 March 2020
Accepted 1 April 2020
Available online xxx

Keywords:
Cyber operations
Cyber warfare
Cyber weapons
Artificial intelligence
Fuzzy logic
Targeting

ABSTRACT

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.

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 [1,2] 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 [3], it relies on information and communications technology (ICT), which exists for decades. As cyberspace represents "a critical feature of modern society" [4], 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 [5], 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?

[*] Corresponding author. Delft University of Technology, Jaffalaan 5, 2628 BX, Delft, Netherlands.
E-mail address: clara.maathuis@tudelft.nl (C. Maathuis).
Peer review under responsibility of China Ordnance Society

https://doi.org/10.1016/j.dt.2020.04.007

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 [6,7]. 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 [8], Stuxnet conducted on a larger timescale but discovered in 2010 [9,10] or the ones conducted in Ukraine between 2015 and 2017 [11,12], 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 [13–17]. 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 [18–21] 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 article contributes with the embedded cyber operations use cases to designing realistic cyber wargames 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 article 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 article. The fourth section provides an overview of the AI technique used in this article to implement the model: Fuzzy Logic. The fifth 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.

2. Background and related research

In order to achieve the aim of this article, 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 article. The results of the review are discussed in the two sub-sections below.

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 Fig. 1 [22,23].

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. Furthermore, the targeting cycle contains the following six phases [13,22,24]:

- 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

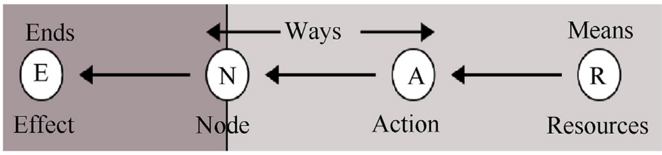


Fig. 1. Military Targeting: ends, ways, and means [20 at page 21].

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 was 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/principle 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. Additionally, different options 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.
- Phase IV – 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 warfare or military cyber operations [19]. As [25] 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" [26] 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" [13] 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" [27]. This vision is aligned with both editions of the Tallinn Manual [16,17].

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" [28]. 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 [29,30]. 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" [7] that it is a real lawful 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" [7]. Furthermore, they should not allow, avoid or limit an attack that would "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" [7].

The "excessive" term is interpreted by some military legal advisors as "shock to the conscience", "clearly unreasonable", "unreasonable" or "significant imbalance" [31]. 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 [32] together with commander's – as responsible authority and decision maker [33,34] – 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 [35] guided under the responsibility of a commander relies on their "creative application of knowledge, practice, cognition, imagination and intuition" [36]. 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" [37] and are by definition surrounded by uncertainty in dynamic environments in ill-defined or ill-structured problems [38,39]. Furthermore, as the aim of the present article 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 [40], in other words a decision support system [41–43] in cyber operations. 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.

2.2. Artificial intelligence: 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 [44]. In particular, fuzzy logic is an AI technique "heavily used" in cyber defence [45] and military decision tools [46]. Relevant research to this article is further outlined.

Reference [47] advances a fuzzy logic model for military C2 systems that estimates financial impact of an attack on the availability and integrity of assets.

In [48], 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.

Reference [49] 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 [50], a target threat fuzzy based assessment model is presented to support weapon assignment and intelligence sensor support systems.

In [51], a gray-based clustering algorithm for vulnerability assessment for electric cyber-physical systems is introduced integrating confidentiality, integrity, availability, and collateral damage potential as defining variables.

Reference [52] 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 [53], 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 article 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.

3. Research approach

The present article 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/defense studies expertise, techniques, and methods. Accordingly, a design science research [54,55] approach was followed as it facilitates the design, development, and evaluation of artefacts such as models, methods, and frameworks considering the following scientific activities:

3.1. 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 – 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, military doctrine, strategies, and reports, one can conclude 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 [20]. Accordingly, related research that tackles tangent points to this research is presented in the Related Work section of this article and Activity III.

3.2. 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 proportional or disproportional (proportionality principle).

3.3. 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 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 [19] and targeting decisions in cyber operations [20] was used as guidance and input in the present research.

3.4. 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.

3.5. 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 [53] 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 experts, and the results of this process are presented in the evaluation and results section of this article.

3.6. Activity VI: Communication

The results of the present research were communicated and presented through presentations, meetings, e-mails, and the present article.

4. Fuzzy logic

This article 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 [54] 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" [55] 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 2 of this article. 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 was used [56].

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 [57] – 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. 2.

Due to its major use in decision making applications, this article uses triangular membership functions [58–60]. These functions are described by 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 Eq. (1) and illustrated in Fig. 3.

$$\mu_U(x) = \begin{cases} 0,\ x < ll \\ \dfrac{x - ll}{m - ll},\ ll < x < m \\ \dfrac{hl - x}{hl - ll},\ m < x < hl \\ 0, x > hl \end{cases} \tag{1}$$

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

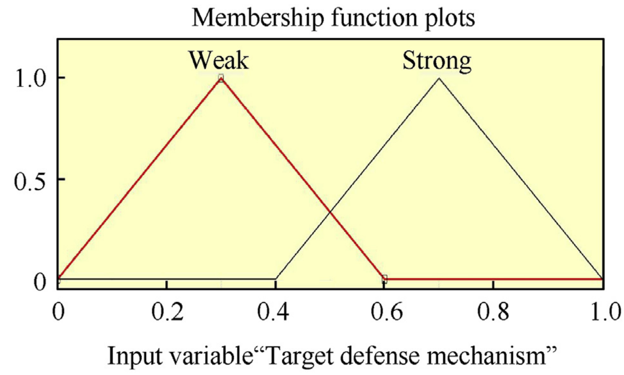


Fig. 2. TargetDefenseMechanism linguistic variable computed using triangular membership functions.

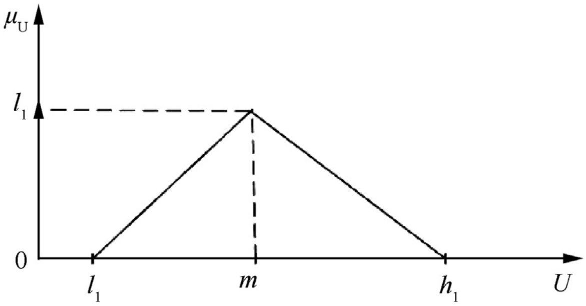


Fig. 3. Triangular membership functions.

the sentence after THEN is called consequent.

For instance, the mechanism of defense of a target is computed in the proposed model in this article using a linguistic variable named Target Defense Mechanism that is computed using triangular membership functions and has weak and strong as defined fuzzy sets. This variable is depicted in Fig. 2.

Moreover, a fuzzy inference system is able to extract conclusions from approximations of data using these linguistic variables and their membership functions [61]. Accordingly, the fuzzy inference system mechanism is presented and illustrated in Fig. 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.

There are three common inference systems known. These are Mamdani fuzzy models, Sugeno fuzzy models, Tsukamoto fuzzy models [62]. 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 such as artificial neural networks or genetic (evolutionary) algorithms. Hereby a short list of applications: intrusion detection [63], Internet of things performance evaluation [64], alert systems for controlling cyber bullying [65], cyber situation awareness [66], in information hiding with stenography [67], in cryptography for the substitution cipher algorithm [68], navigation of humanoid robot [69], terrorist event classification [70], and pilot's behaviour assessment in warfare simulations [71].

Hence, the illustrated technique has a diverse pallet of applications in different domains by representing a way to design and implement intelligent systems providing the main advantage of mathematically dealing with the uncertainty of information - "gray" (i.e. vague, ambiguous, imprecise) by nature [72]. Accordingly, in the coming section of this article, the design and implementation of the model are further presented.

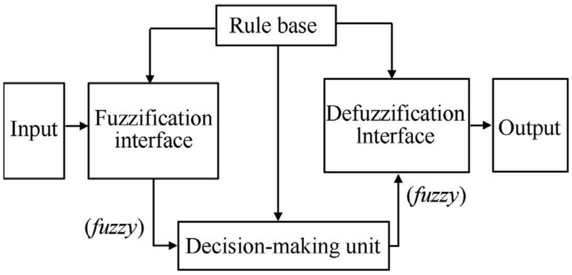


Fig. 4. Fuzzy inference system.

5. Design and implementation

To be able to introduce the design and the way the proposed model was implemented (see Activity III in Section 3.), a reflection on the underlying mechanism is necessary. This mechanism is depicted in Fig. 5 and embedded in Fig. 6, and contains the following key points:

- First, military advantage and collateral damage (A in Fig. 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 article, the coming remarks can be made. On one side, in past and current military operations, the estimation of military advantage is based on 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

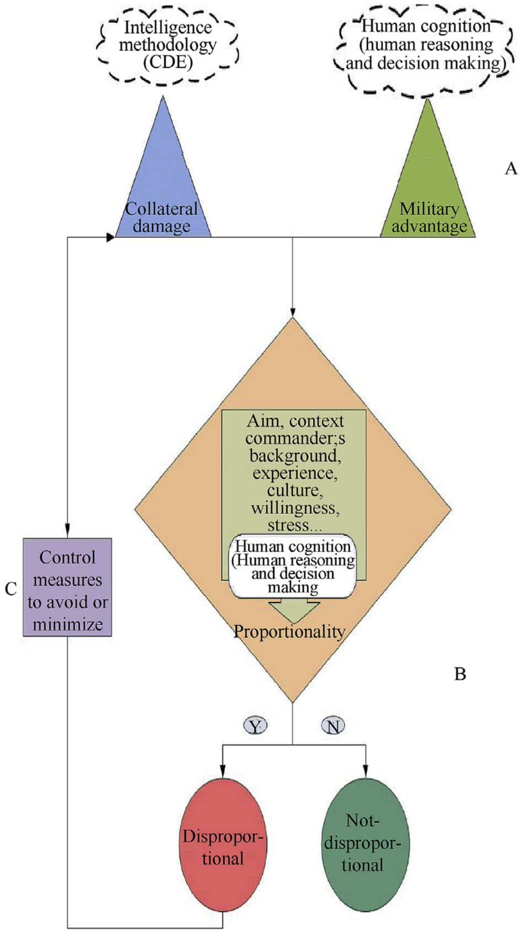

Intelligence methodology (CDE)
Human cognition (human reasoning and decision making)
A
Collateral damage
Military advantage
Aim, context commander;s background, experience, culture, willingness, stress...
Human cognition (Human reasoning and decision making
Proportionality
B
C
Control measures to avoid or minimize
Y
N
Dispropor-tional
Not-dispropor-tional

Fig. 5. Effects estimation and targeting decisions in cyber operations.

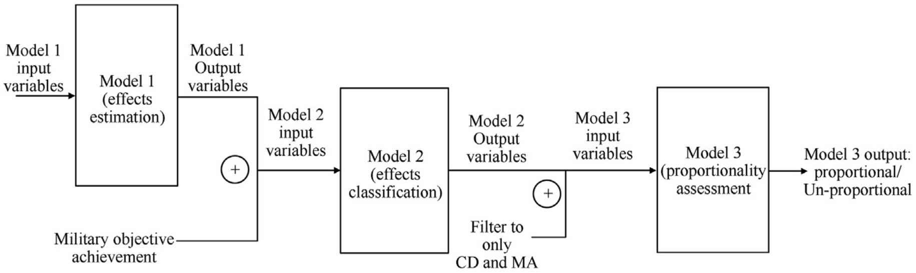

Model 1 input variables
Model 1 (effects estimation)
Model 1 Output variables
+
Military objective achievement
Model 2 input variables
Model 2 (effects classification)
Model 2 Output variables
+
Filter to only CD and MA
Model 3 input variables
Model 3 (proportionality assessment
Model 3 output: proportional/ Un-proportional

Fig. 6. Multi-layered model for effects estimation and targeting decisions in cyber warfare.

methodologies. On the other side, in past and current military operations, the estimation of collateral damage is based on the CDE methodology which is an estimation methodology done by the intelligence forces [73] 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. 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" [74], 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 Fig. 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 Fig. 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 [13,16].

Based on the underlying mechanism described, a multi-layered fuzzy model has been designed as an intelligent system [75] with its architecture illustrated in Fig. 6. The first and second layer/model depicted in Fig. 6 correspond to the blocks before the decision depicted in Fig. 5, and the third layer/model illustrated in Fig. 6 corresponds to the decision block illustrated in Fig. 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 [18], 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 [76] and previous work [18–21] 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.

Based on the abovementioned aspects and design decisions, two perspectives or contexts of use were considered for the proposed multi-layered model:

- The first perspective is of legal nature and is based on the (classical) interpretation of the proportionality assessment. This perspective brings together two elements (categories of effects): collateral damage and military advantage.
- The second perspective 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 Figs. 7- 9 clearly separates military targets from civilian objects (based on the principle of distinction), as follows: in Fig. 7 are depicted the input and output variables, in Fig. 8 is illustrated a membership function for one of the input variables, and in Fig. 9 are captured some rules. This model contains 11 input variables and 7 output variables identified in Refs. [19,20] and are based on information given before the execution of a cyber operation. These variables are characterized by triangular membership functions and are defined in the appendix of this article.

A detailed description for calculating the membership functions of the variables military objective and target vulnerability are further provided using Eq. (2) in Eq. (3) and Eq. (4) below. Further, in the Appendix section of this article are defined all the variables used.

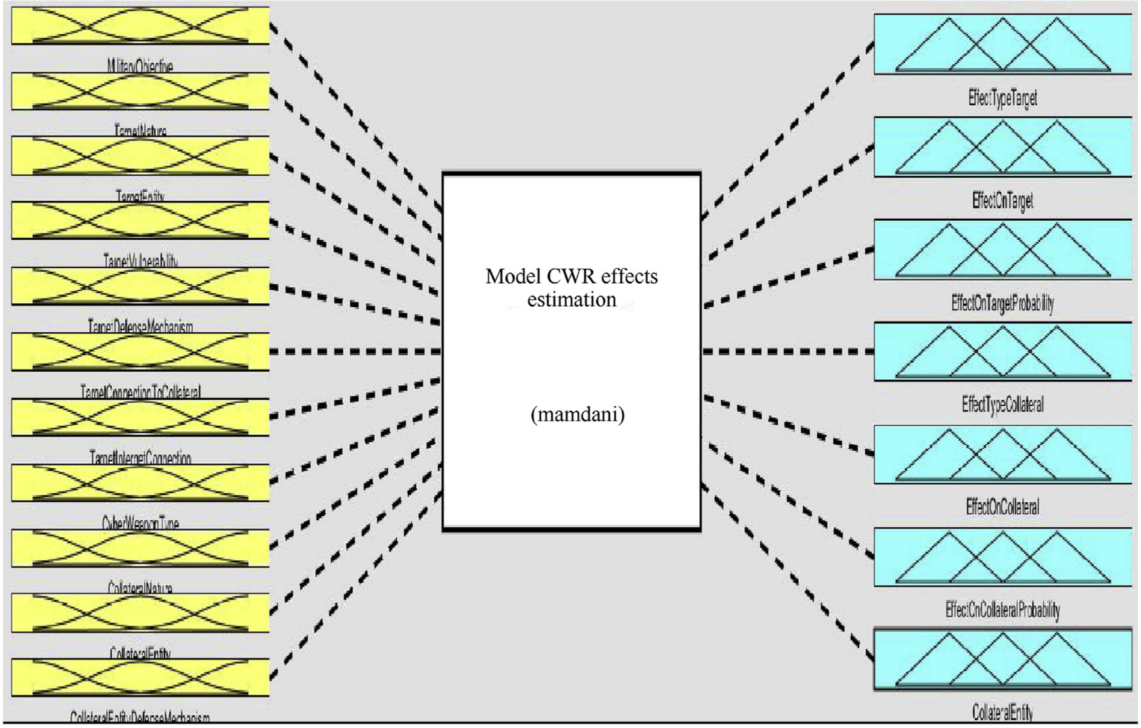
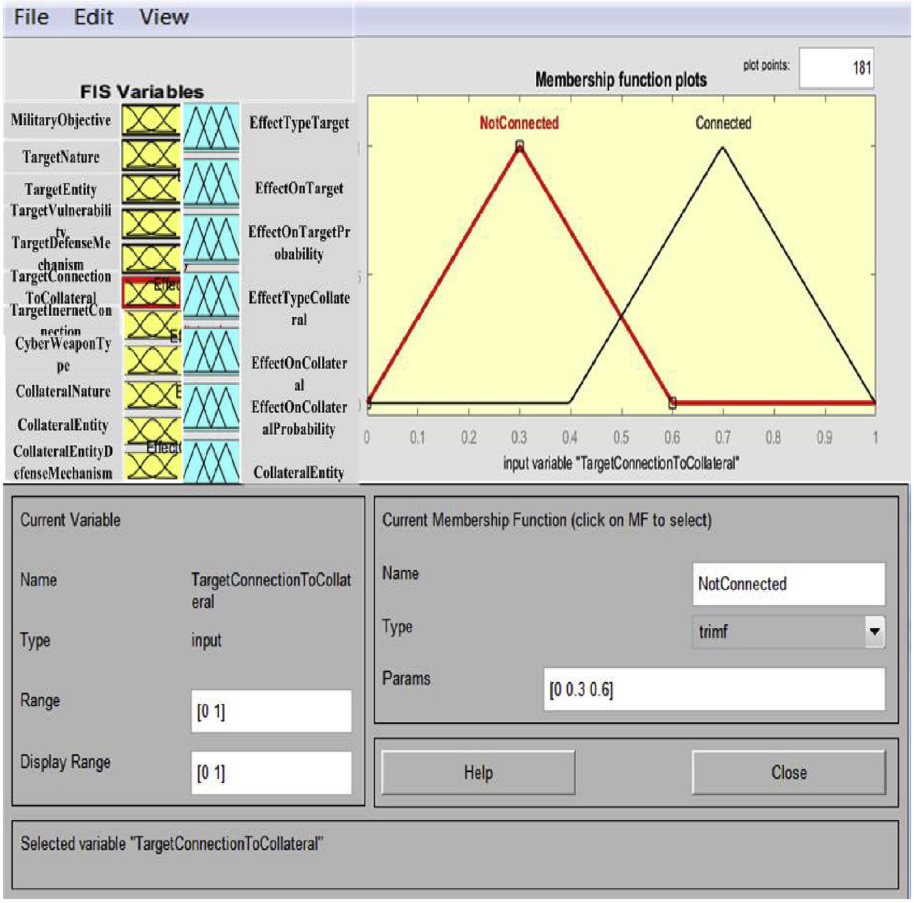


Fig. 7. Effects estimation model in cyber operations.



Current Variable

Name TargetConnectionToCollateral

Type input

Range [0 1]

Display Range [0 1]

Current Membership Function (click on MF to select)

Name NotConnected

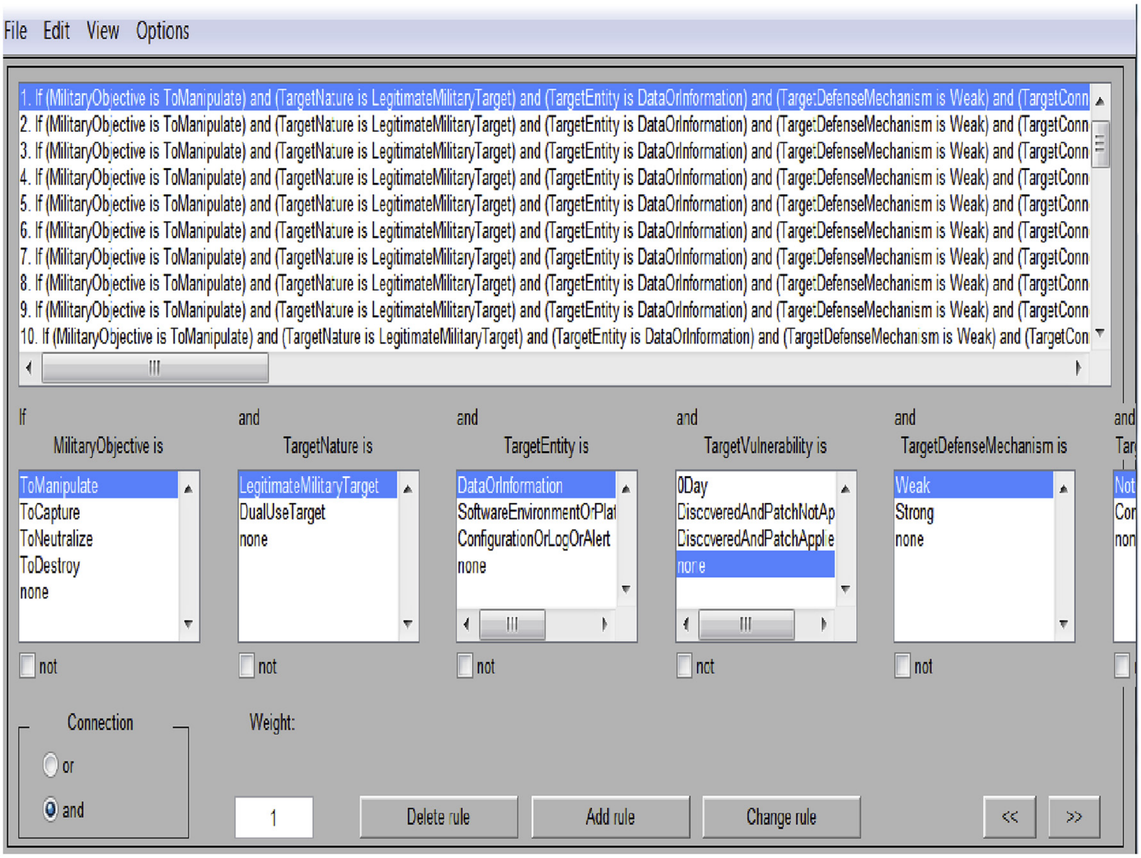
Type trimf

Params [0 0.3 0.6]

Selected variable "TargetConnectionToCollateral"

Fig. 8. Target connection to collateral input variable membership functions.

Please cite this article as: Maathuis C et al., Decision support model for effects estimation and proportionality assessment for targeting in cyber operations, Defence Technology, https://doi.org/10.1016/j.dt.2020.04.007


1. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
2. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
3. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
4. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
5. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
6. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
7. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
8. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
9. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (Targe:DefenseMechanism is Weak) and (TargetConn
10. If (MilitaryObjective is ToManipulate) and (TargetNature is LegitimateMilitaryTarget) and (TargetEntity is DataOrInformation) and (TargetDefenseMechanism is Weak) and (TargetCon

If MilitaryObjective is: ToManipulate
and TargetNature is: LegitimateMilitaryTarget
and TargetEntity is: DataOrInformation
and TargetVulnerability is: none
and TargetDefenseMechanism is: Weak
and Tar: Not

Connection: ○ or ● and

Weight: 1

Fig. 9. Effects estimation model rules in cyber operations.

$$\mu_{\text{MilitaryObjective}}(x) = \begin{cases} \left(\max\left(\min\left(\frac{x}{0.15},\frac{0.3-x}{0.15}\right),0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.23}{0.15},\frac{0.53-x}{0.15}\right),0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.463}{0.15},\frac{0.763-x}{0.15}\right),0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.7}{0.15},\frac{1-x}{0.15}\right),0\right)\right) \end{cases} \tag{2}$$

$$\mu_{\text{TargetVulnerability}}(x) = \begin{cases} \left(\max\left(\min\left(\frac{x}{0.19},\frac{0.38-x}{0.19}\right),0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.31}{0.19},\frac{0.69-x}{0.19}\right),0\right)\right) \\ , \\ \left(\max\left(\min\left(\frac{x-0.62}{0.19},\frac{1-x}{0.19}\right),0\right)\right) \end{cases} \tag{3}$$

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 [77,78].

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 article.

The second model is illustrated in Figs. 10-12, as follows. In Fig. 10 are depicted the input and output variables and in Fig. 12 are captured a part of the rules. The model contains 8 input variables and 6 output variables based on the effects classification presented in Ref. [18,20] characterized by triangular membership functions.

A detailed description for calculating the membership functions of the variable effect type target is further provided using Eq. (2) in Eq. (5) below. Further, in the Appendix section of this article are defined all the variables used.

Please cite this article as: Maathuis C et al., Decision support model for effects estimation and proportionality assessment for targeting in cyber operations, Defence Technology, https://doi.org/10.1016/j.dt.2020.04.007

Table 1
Effects Estimation Model variables in Cyber operations.

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
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
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
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

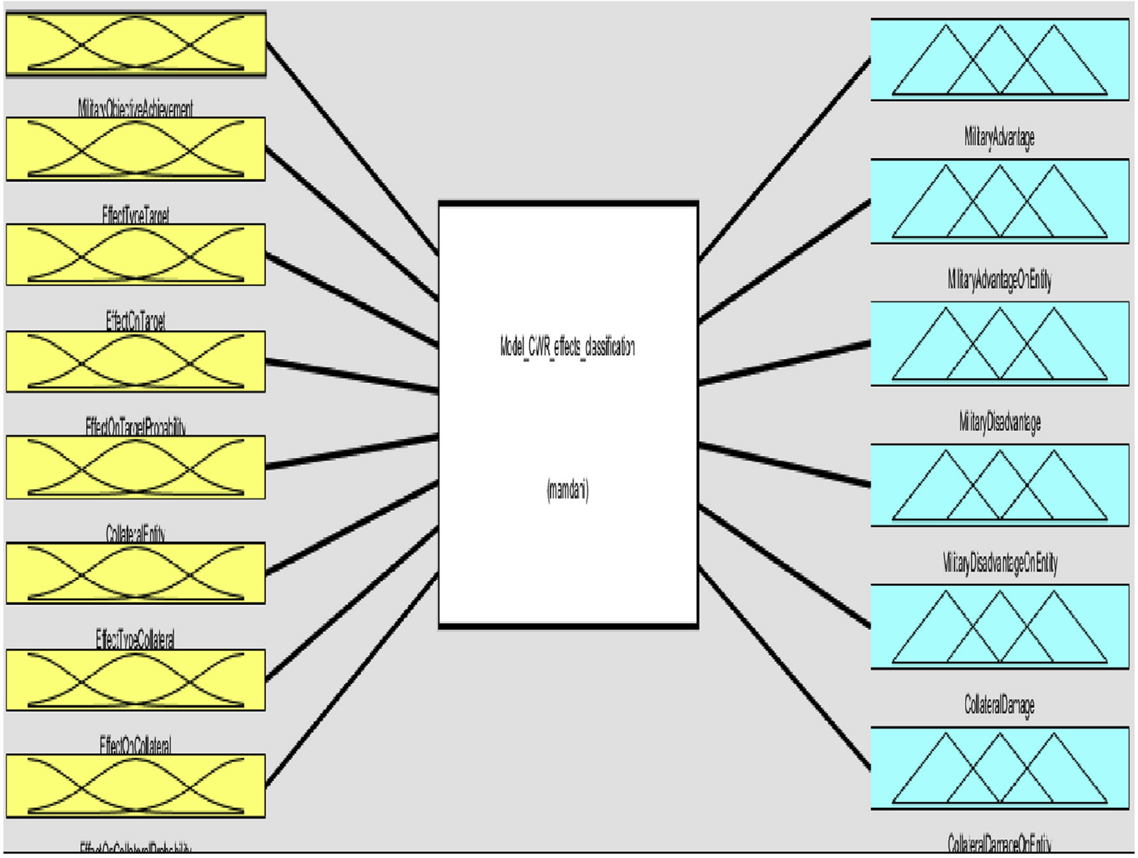


Fig. 10. Effects classification model in cyber operations.

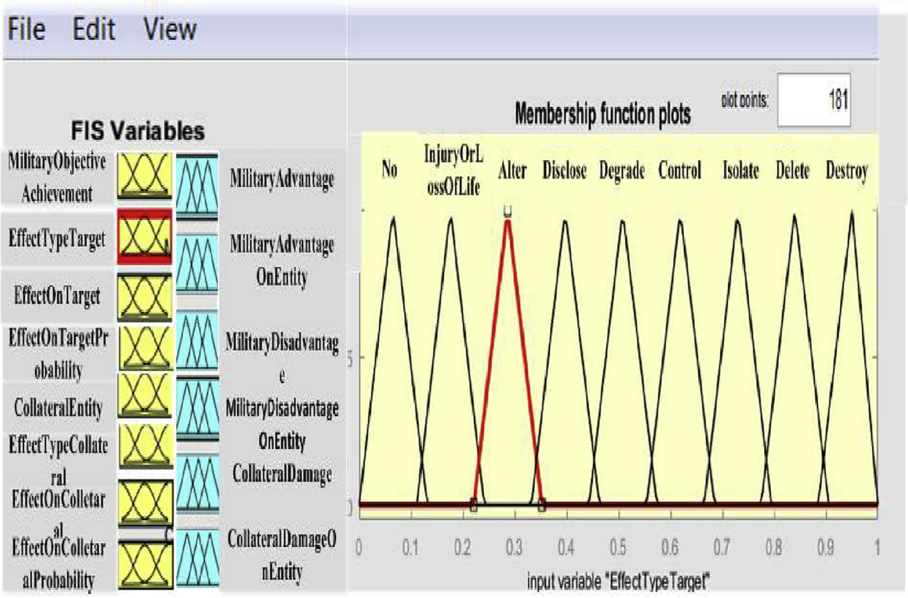
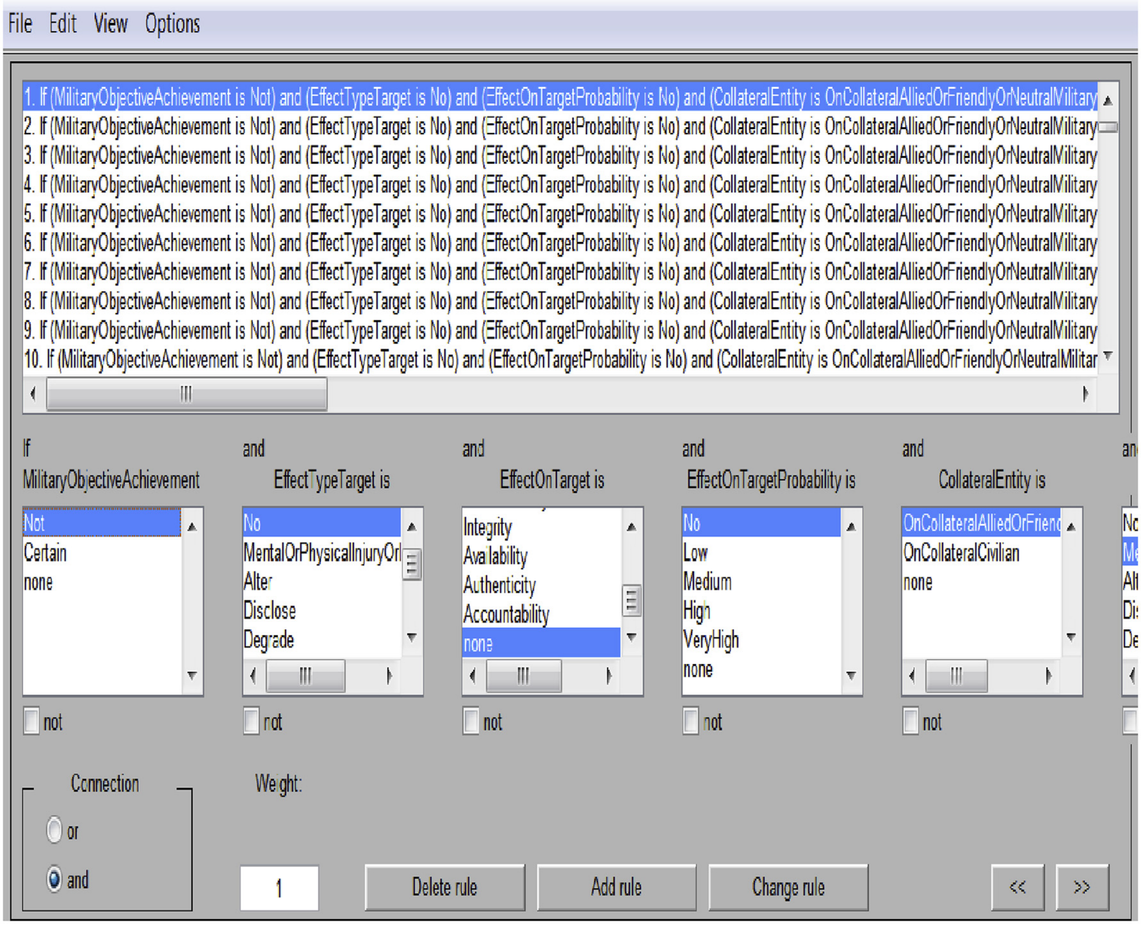


Fig. 11. Effect type target input variable membership functions.



1. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
2. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
3. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
4. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
5. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
6. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
7. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
8. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
9. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitary
10. If (MilitaryObjectiveAchievement is Not) and (EffectTypeTarget is No) and (EffectOnTargetProbability is No) and (CollateralEntity is OnCollateralAlliedOrFriendlyOrNeutralMilitar

If MilitaryObjectiveAchievement	and EffectTypeTarget is	and EffectOnTarget is	and EffectOnTargetProbability is	and CollateralEntity is	an
Not	No	Integrity	No	OnCollateralAlliedOrFriend	No
Certain	MentalOrPhysicalInjuryOr	Availability	Low	OnCollateralCivilian	Me
none	Alter	Authenticity	Medium	none	Al
	Disclose	Accountability	High		Di
	Degrade	none	VeryHigh		De
			none		
□ not	□ not	□ not	□ not	□ not	□

Connection
○ or
● and

Weight:
1

Fig. 12. Effects classification model rules in cyber operations.

$$\mu_{\text{EffectTypeTarget}}(x) = \left\{ \begin{array}{c} \left(\max\left(\min\left(\frac{x}{0.0555}, \frac{0.111-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.111}{0.555}, \frac{0.222-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.222}{0.555}, \frac{0.333-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.333}{0.555}, \frac{0.444-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.444}{0.555}, \frac{0.555-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.555}{0.555}, \frac{0.666-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.666}{0.555}, \frac{0.777-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.777}{0.555}, \frac{0.888-x}{0.0555}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.888}{0.555}, \frac{1-x}{0.0555}\right), 0\right)\right) \end{array} \right\} \tag{4}$$

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 article.

The third model is illustrated in Figs. 13-15 is based on the proportionality test, as follows. In Fig. 12 are depicted the input and output variables, in Fig. 13 is illustrated a membership function for one of the input variables, and in Fig. 15 are captured a part of the rules. The model contains 4 input variables and 1 output variables characterized by triangular membership functions (see Fig. 14).

A detailed description for calculating the membership functions of the variable collateral damage and proportionality decision further provided using Eqs. (5) and (6) below. Further, in the Appendix section of this article are defined all the variables used.

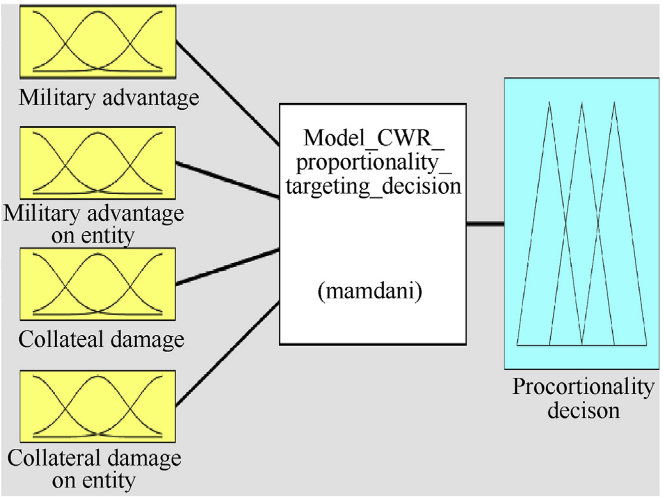

Military advantage
Military advantage on entity
Collateal damage
Collateral damage on entity
Model_CWR_proportionality_targeting_decision
(mamdani)
Procortionality decison

Fig. 13. Targeting decision model based on proportionality assessment in cyber operations.

$$\mu_{\text{CollateralDamage}}(x) = \left\{ \begin{array}{c} \left(\max\left(\min\left(\frac{x}{0.12}, \frac{0.24-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.19}{0.12}, \frac{0.43-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.37}{0.12}, \frac{0.61-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.56}{0.12}, \frac{0.8-x}{0.12}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.7}{0.12}, \frac{1-x}{0.13}\right), 0\right)\right) \end{array} \right\} \tag{5}$$

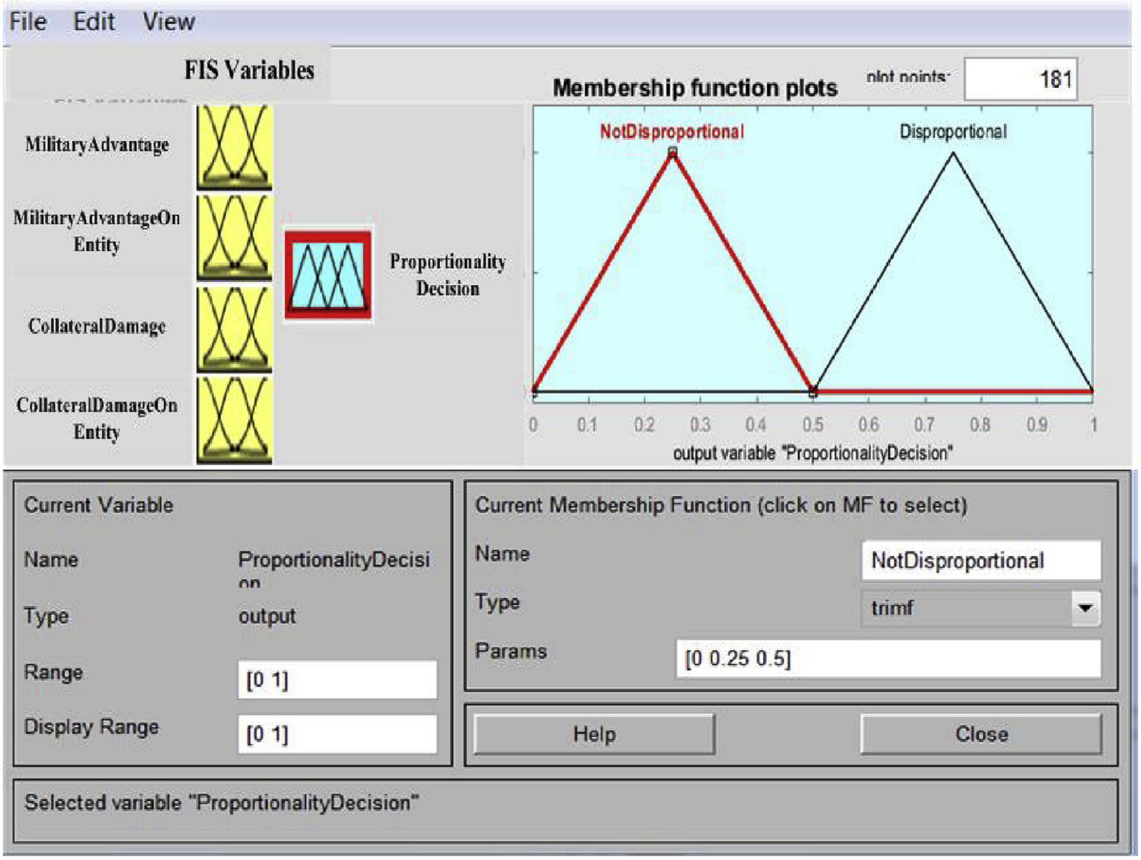
$$\mu_{\text{ProportionalityDecision}}(x) = \left\{ \begin{array}{c} \left(\max\left(\min\left(\frac{x}{0.25}, \frac{0.5-x}{0.25}\right), 0\right)\right), \\ \left(\max\left(\min\left(\frac{x-0.5}{0.25}, \frac{1-x}{0.25}\right), 0\right)\right) \end{array} \right\} \tag{6}$$

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

Table 2
Effects classification model variables in cyber operations.

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 objective(s)	No/Low/Medium/High/VeryHigh
MilitaryAdvantageOnEntity = The type of entity which is impacted by Military Advantage.	Human/NonHuman
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



Current Variable

Name ProportionalityDecision

Type output

Range [0 1]

Display Range [0 1]

Current Membership Function (click on MF to select)

Name NotDisproportional

Type trimf

Params [0 0.25 0.5]

Selected variable "ProportionalityDecision"

Fig. 14. Proportionality decision output variable membership functions.

IS NonHuman) AND (CollateralDamage IS High) AND (CollateralDamageOnEntity IS NonHuman) THEN ProportionalityDecision IS DisProportional.

Moreover, the output variable is defined in Table 3 with complete definitions for all variables presented in the Annex of this article.

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 5, the proposed model could be used:

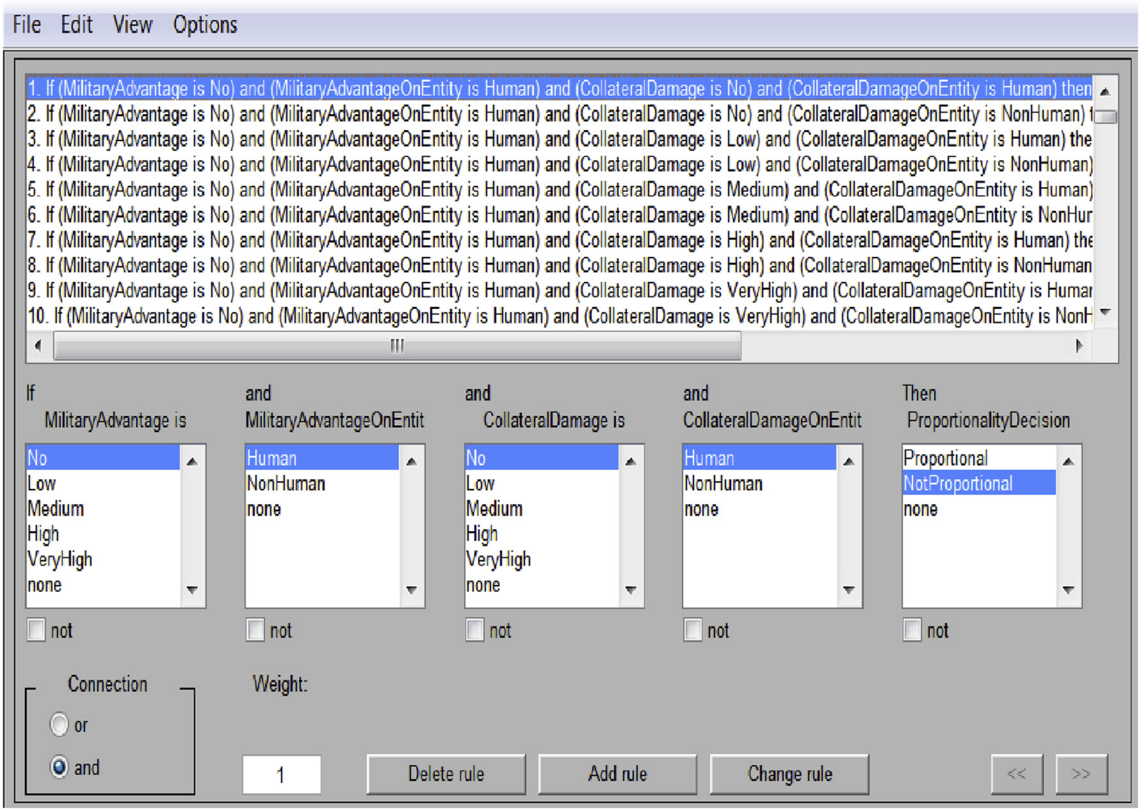
- In the operational context as it is or further considering multiple degrees of (dis)proportionality if an analogue approach is desired by using values such as Not Disproportional, Low Disproportional, Medium Disproportional, High Disproportional, Very High Disproportional in the last model (layer) of the proposed model.

In the legal context further considerations could be applied considering only integrating 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 4. Strictly for exclusion purposes the necessary action is deleting and for naming compatibility the necessary action is renaming. These actions imply that in the estimation process the additional variables used in the operational context would not be present in the legal context (delete action), and that the renamed variables are used in the same way according to their definitions (rename action).

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 Section 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 incidents to be conducted in the current global political and military situation, and ii) the realism of such incidents 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” [79] backed by the idea of proposing Cyber operations perceived by the consulted military – technical experts as being realistic [26] future scenarios [80] 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



1. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is No) and (CollateralDamageOnEntity is Human) then
2. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is No) and (CollateralDamageOnEntity is NonHuman) t
3. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is Low) and (CollateralDamageOnEntity is Human) the
4. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is Low) and (CollateralDamageOnEntity is NonHuman)
5. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is Medium) and (CollateralDamageOnEntity is Human)
6. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is Medium) and (CollateralDamageOnEntity is NonHur
7. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is High) and (CollateralDamageOnEntity is Human) the
8. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is High) and (CollateralDamageOnEntity is NonHuman
9. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is VeryHigh) and (CollateralDamageOnEntity is Humar
10. If (MilitaryAdvantage is No) and (MilitaryAdvantageOnEntity is Human) and (CollateralDamage is VeryHigh) and (CollateralDamageOnEntity is NonH

If MilitaryAdvantage is: No
and MilitaryAdvantageOnEntit: Human
and CollateralDamage is: No
and CollateralDamageOnEntit: Human
Then ProportionalityDecision: NotProportional
Connection: ● and
Weight: 1

Fig. 15. Targeting decision model rules based on proportionality assessment in cyber operations.

Table 3
Targeting Decision Model variables in Cyber operations.

Input/Output Variable and Definition	Value Variable (Fuzzy Set)	Definition Value Variable
ProportionalityDecision = Proportionality assessment that considers as Proportional if Collateral Damage is not excessive in relation to Military Advantage.	Proportional	Engaging this specific target with this specific cyber weapon is proportional (not excessive), in other words 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 4
Further considerations for the legal perspective of use.

Layer/Model No.	Action	Action on variable
First and second	Rename	From EffectTypeTarget to MilitaryAdvantage
First	Rename	From MentalOrPhysicalHealthOrLossOfLife to Physical Injury Or Loss Of Life
First and second	Rename	From EffectOnTarget to Military Advatage On
First	Delete	Trust, Reputation, Privacy for EffectOnTarget
First and second	Rename	From EffectOnTargetProbability to Military Advantage Probability
First and second	Rename	From EffectTypeCollateral to CollateralDamage
First and second	Rename	From EffectOnCollateral to Collateral Damage On
First and second	Rename	From EffectOnCollateralProbability to Collateral Damage Probability
First and second	Delete	CollateralEntity
Second	Rename	From EffectTypeTarget to MilitaryAdvantage
Second	Delete	MilitaryDisadvantage
Second	Delete	MilitaryDisadvantageOnEntity

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 Section 2. Furthermore, following the data model for representing and simulating Cyber operations proposed by Ref. [21], 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.

6.1. Case study/use case I: Drone counter-terrorism cyber operation

Context: The ongoing conflict 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/unmanned combat aerial vehicle (UCAV) 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 Fig. 16.

Actor: coalition vs. Terrmisous.

Type: offensive cyber operation.

Military objective: 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.

Cyber weapon: 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:

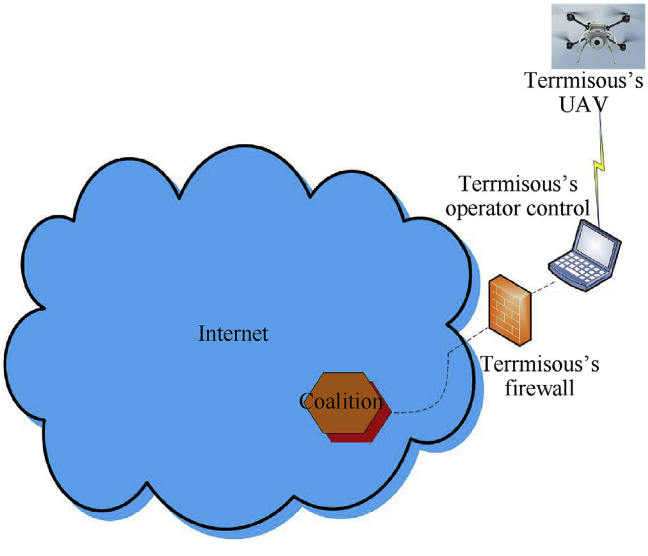


Fig. 16. Cyber operation Case I.

- 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.

6.2. Case study/use case II: ship counter-terrorism cyber operation

Context: The ongoing conflict 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 Fig. 17.

Actor: coalition vs. terrmisous.

Type: offensive cyber operation.

Military objective: 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.

Cyber weapon: 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.

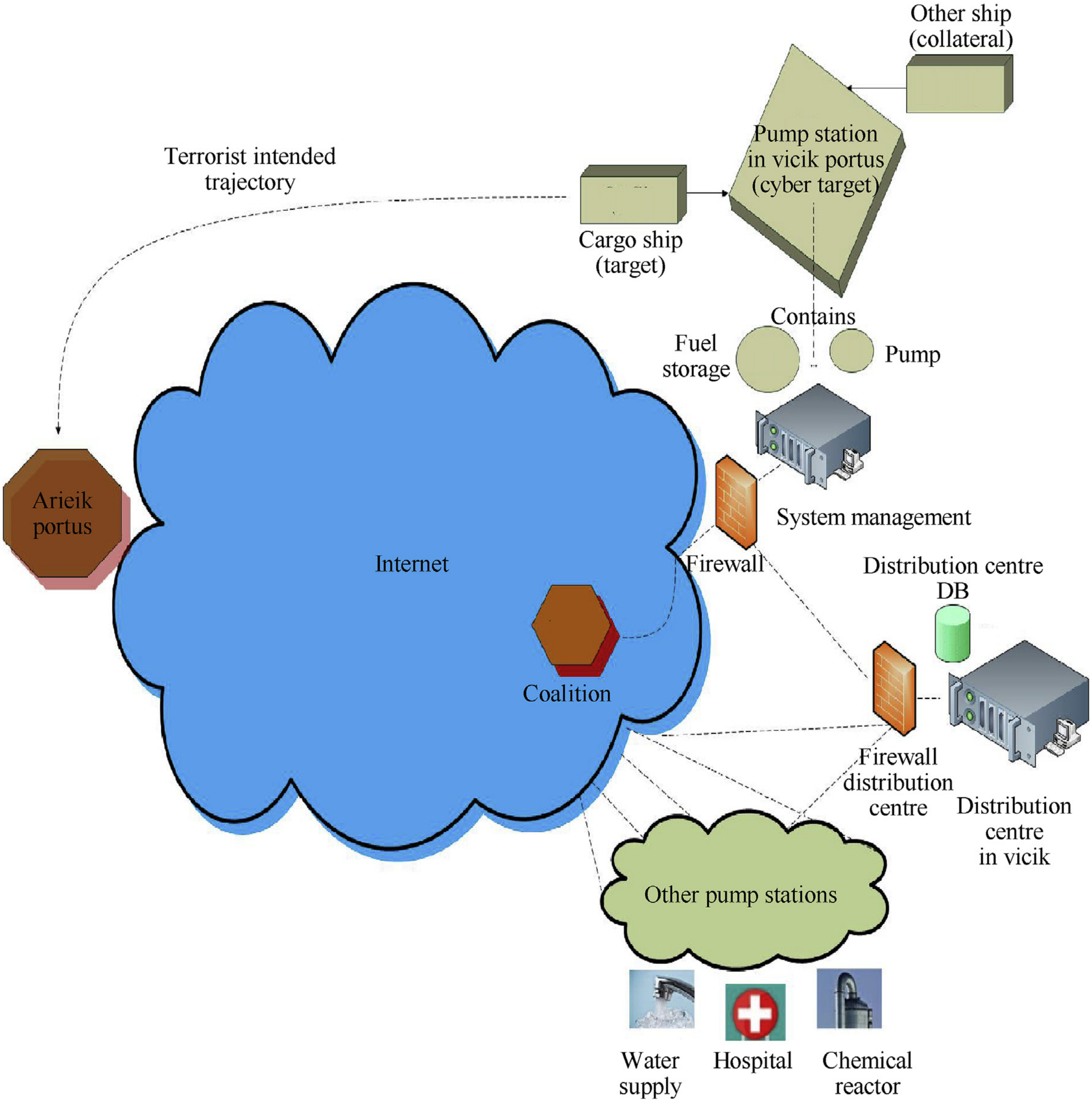


Fig. 17. Cyber operation Case II.

– 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.

6.3. Results

To evaluate the introduced model, the following evaluation criteria need to be fulfilled aligned with design science research [54,81,82]:

– compatibility with the design requirements presented in Activity III in Section 3 of this article.
– 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 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 Section 6.1 and Section 6.2), analysed (see Section 4), and run through simulations as described below using estimations for the parameters presented in the appendix. The data is provided to the model and the final results consisting of output values and their

Table 5
Targeting decision in cyber operations model evaluation.

Cyber operation Use Case	Targeting Decision Expert 1	Targeting Decision Expert 2	Targeting Decision Expert 3	Targeting Decision Expert 4	Targeting Decision Model
1	Proportional	Disproportional	Disproportional	Disproportional	Disproportional
2	Proportional	Proportional	Proportional	Proportional	Proportional

interpretation are provided in the table below and further in this section.

This evaluation is done in MATLAB 2015b on an Intel(R) Core(TM) i7-5600U CPU with 2.6 GHz, 8 GB 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 injury or loss of life with impact on injury or loss of life with values 0.16 and 0.05, respectively).
- 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.
- In this regard, in Fig. 17 is depicted a sample of the area of simulation results from MATLAB for the proposed model and in Fig. 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 (see Fig. 19).

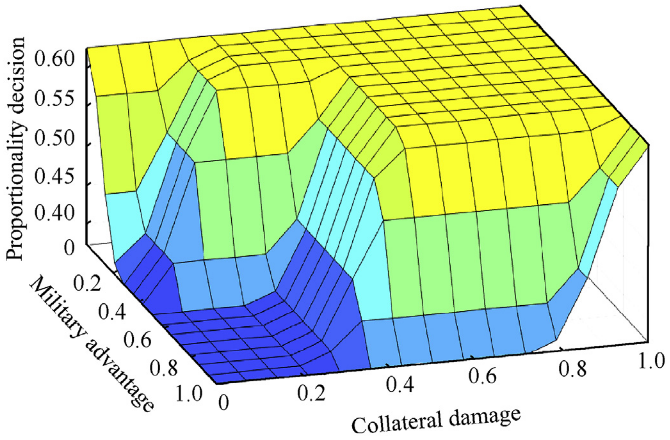


Fig. 19. Targeting decision in cyber operation model entire output surface.

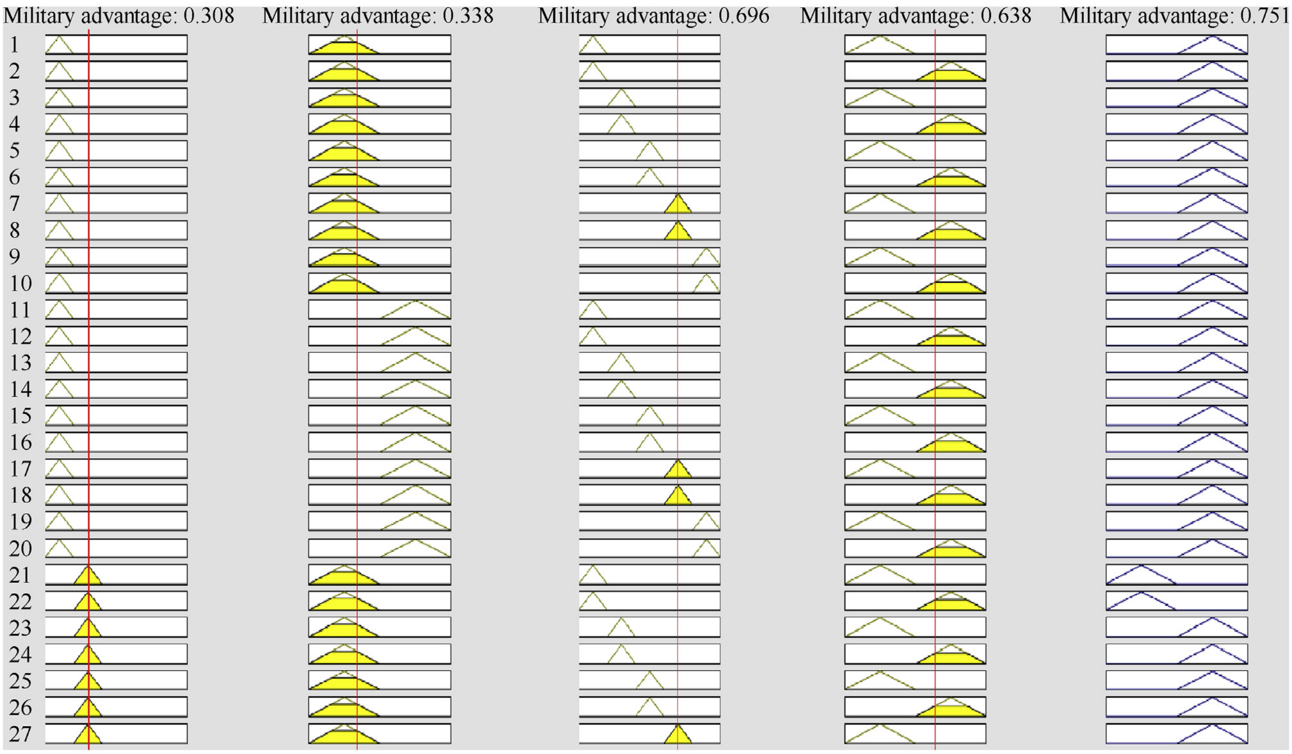

Military advantage: 0.308
Military advantage: 0.338
Military advantage: 0.696
Military advantage: 0.638
Military advantage: 0.751
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

Fig. 18. Targeting Decision in Cyber operation Model sample area of simulation.

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, 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 successfully supports targeting decision making by providing the right type of final decision support information as targeting decision based on the proportionality assessment (military legal perspective of use) and suitable as a base for further courses of action (CoAs) development (military operational perspective of use) since it is useful and understandable from a military – technical perspective.
- The model also helps to structure the decision making process itself in cyber operations and describes its important components and elements i.e. the variables and parameters contained (see Section 6 and Annex) and modelled using the methodology presented in Section 3 and Section 5. Additionally, the vision of experts is aligned with the way of reasoning embedded in this system (see Section 5).
- 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.

Therefore, 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 is 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, thus is just a technical (AI) based solution. Human factors and aspects such as context, culture, stress etc. are perceived by the research community (e.g. cognitive science, psychology, medicine) as being incredibly difficult or even impossible to measure or model. The authors consider that future research should be conducted on investigating which human factors and aspects are involved during targeting decision making from a multidisciplinary perspective, and from there if or which ones should be involved in such a model.

Table 6
Targeting decision in cyber operations model usefulness evaluation.

Usefulness Level	Expert 1	Expert 2	Expert 3	Expert 4
Usefulness	3	3	2	3

As Fig. 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.

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 [83] 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/defense studies 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: a legal and an operational one. Further, two possible perspectives were identified as applications for the proposed model: operational and legal. Furthermore, the evaluation of the model was done with technical – military experts in the Netherlands in an operational context, 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) full 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.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

We are thankful to LtCol(R) MSc Rudi Gouweleeuw and BG prof. dr. Paul Ducheine BG for their valuable support, and to all participating experts in this research.

Appendix

Table 7
Variables definition for model 1

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.
	Dual Use Target	[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 should be exploited.	0Day	[0 0.19 0.38]	Unknown and unpatched vulnerability.
	Discovered And Patch Not Applied	[0.31 0.5 0.69]	Discovered but not patched vulnerability.
	Discovered And Patch Applied	[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.	Collateral Allied Or Friendly Or Neutral Military	[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
	Hardware Or Device	[0.498 0.596 0.694]	Hardware or device
	ConfigurationOrLogOrAlert	[0.664 0.762 0.86]	File

(continued on next page)

Table 7 (*continued*)

Input/Output Variable and Definition	Value Variable (Fuzzy Set)	Membership Functions Definitions	Value Variable Definitions
	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]	

Table 7 (*continued*)

Input/Output Variable and Definition	Value Variable (Fuzzy Set)	Membership Functions Definitions	Value Variable Definitions
	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.	On Collateral Allied Or Friendly Or Neutral Military	[0 0.3 0.6]	
	OnCollateralCivilian	[0.4 0.7 1]	

Table 8
Variables definition for model 2

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 7	See Table 7		See Table 7
EffectOnTarget = see Table 7			
EffectOnTargetProbability = see Table 7			
CollateralEntity = see Table 7			
EffectTypeCollateral = see Table 7			
EffectOnCollateral = see Table 7			
EffectOnCollateralProbability = see Table 7			
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 Table 7
	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 9
Variables definition for model 3

Input/Output Variable and Definition	Value Variable (Fuzzy Set)	Membership function	Definition Value Variable
MilitaryAdvantage	No	[0 0.12 0.24]	See Table 8
	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 Table 8
	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.

References

[1] Malham DG, Myatt A. 3-D sound spatialization using ambisonic techniques. Comput Music J 1995;19(4):58–70.
[2] Baalman MA. Spatial composition techniques and sound spatialisation technologies. Organ Sound 2010;15(3):209–18.
[3] NATO. Cyber defence. 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm. [Accessed 15 May 2019].
[4] Kanuck S. Soverign discourse on cyber conflict under international law. Tex Law Rev 2009;88:1571.
[5] Center for Army lessons learned, handbook of military decision making. 2015. p. 15–6.
[6] Additional Protocol I. Art. 48 – basic rule. 1977.
[7] Additional Protocol I. Art 1977;57(2) [a)(i)-(iii)],(b) – Precautions in attack.
[8] Hollis D. Cyberwar case study: Georgia 2008. Small Wars J 2011. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008. [Accessed 12 March 2019].
[9] Falliere N, Murchu LO, Chien E. W32 Stuxnet dossier. Symantec: White paper; 2011.
[10] McDonald G, Murchu LO, Doherty S, Chien E. Stuxnet 0.5: the missing link. Symantec; 2013.
[11] Case DU. Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center; 2016.
[12] Fayi SYA. What Petya/NotPetya ransomware is and what its remediations are. Information Technology-New Generations; 2018. p. 93–100.
[13] Boothby WH. The law of targetingvol. 81. Springer; 2012. 126, 260, 476-478, 489.
[14] Gill TD, Fleck D, editors. The handbook of the international law of military operations, vol. 246. Oxford University Press; 2011. p. 253.
[15] Romanosky S, Goldman Z. Understanding cyber collateral damage. J Natl Secur Law Pol 2017;9:233.
[16] Schmitt MN, editor. Tallinn Manual on the international law applicable to cyber warfare, vol. 68. Cambridge University Press; 2013. p. 80.
[17] Schmitt MN, editor. Tallinn Manual 2.0. on the international law applicable to cyber operations. Cambridge University Press; 2017. p. 375.
[18] Maathuis C, Pieters W, van den Berg J. Cyber weapons: a profiling framework. In: IEEE 1st international conference on cyber conflict U.S.; 2016. p. 1–8.
[19] Maathuis C, Pieters W, van den Berg J. A knowledge-based model for assessing the effects of cyber warfare. In: 12th NATO conference on operations research and analysis; 2018.
[20] Maathuis C, Pieters W, van den Berg J. Assessment methodology for collateral damage and military (Dis)Advantage in cyber operations. In: IEEE 35th international conference on military communications; 2018. p. 1–6.
[21] Maathuis C, Pieters W, van den Berg J. Developing a computational ontology for cyber operations. J Inf Warf 2018d;17(3):32–51.
[22] NATO. Allied joint doctrine for joint targeting, vol. 28. NATO Standardization Office; 2016b.
[23] Joint staff 3-60, joint targeting. Joint Staff Publication; 2013.
[24] Mezler N. Targeted killing in international law. Oxford University Press on Demand; 2008. p. 359.
[25] Schreier F. On cyberwarfare. Geneva Centre for the Democratic Control of Armed Forces; 2015.
[26] Couretas JM. An introduction to cyber modeling and simulation. John Willey & Sons, Inc.; 2019.
[27] NATO, Wales. Summit declaration. 2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm. [Accessed 6 May 2019].
[28] ICRC. The Geneva Conventions of 1949 and their additional protocols. In: International committee of the red cross; 2010. https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm. [Accessed 9 May 2019].
[29] Additional Protocol I. Art. 48 – basic rule. 1977.
[30] ICRC, Rule 1. The principle of distinction between civilians and combatants. In: International committee of the red cross; 2005. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1. [Accessed 19 May 2019].
[31] Wright JD. 'Excessive' ambiguity: analysing and refining their proportionality standard. Int Rev Red Cross 2012:819–54.
[32] Joint Staff 2-01. Joint tactics, techniques, and procedures for intelligence support for targeting. Joint Staff Publication; 2003.
[33] NATO, Allied Joint Doctrine for Intelligence Procedures. NATO standardization office. 2016. p. 24–5.
[34] Jachec-Neale. The concept of military objectives in international law and targeting practice. Routledge; 2014. p. 204.
[35] Franz T. The cyber warfare professional. Air Space Power J 2011;25(2):87–99.
[36] Tuija K, Kuusisto R, Roehrig W. Situation understanding for operational art in cyber operations. JCyber Warfare Terror 2016;6(2):1–14.
[37] Stone SW. Factors influencing agility in allocating decision-making rights for Cyberspace Operations. In: 20th international command and control research and technology symposium, vol. 96; 2015.
[38] Lipshitz R, Klein G, Orasanu J, Salas E. Taking stock of naturalistic decision making. J Behav Decis Making 2001;14:331–52.
[39] Orasanu J. Crew collaboration in space: a naturalistic decision-making perspective. Aviat Space Environ Med 2005;76:6.
[40] Zsambok C, Klein G. Naturalistic decision making. Taylor & Francis; 1996.
[41] Burstein F, Holsapple CW, editors. Handbook on decision support systems 2: variations. Springer Science & Business Media; 2008.
[42] Rospocher M, Serafin L. An ontological framework for decision support. In: Proceedings of joint international semantic technology conference. Springer; 2012. p. 239–54.
[43] Druzdzel M, Flynn RR. Decision support systems. In: Encyclopedia of library and information sciences. CRC Press; 2017. p. 1200–8.
[44] Dilek S, Huseyin C, Mustafa A. Applications of artificial intelligence techniques to combating cyber crimes: a review. Int J Artific Intell Appl 2015;6(1).
[45] Newcomb EA, Hammell RJ. A fuzzy logic utility framework (FLUF) to support information assurance, Software Engineering Research, Management and Applications. Springer; 2016. p. 33–48.
[46] Prelipcean G, Boscoianu M, Moisescu F. New ideas on the artificial intelligence

support in military applications. In: 9th International Conference on Artificial Intelligence, knowledge engineering and data bases. World Scientific and Engineering Academy and Society; 2010.

[47] Tavana M, D A, Trevisani, Kennedy DT. A fuzzy cyber-risk analysis model for assessing attacks on the availability and integrity of the Military Command and Control systems. Int J Bus Anal 2014;1(3):21–36.

[48] Alali M, Almogren A, Hassan MM, Rassan IAL, Bhuiyan MZA. Improving risk assessment model of cyber security using fuzzy logic inference system. Comp Secur 2018;74:323–39.

[49] Sallam H. Cyber security risk assessment using multi fuzzy inference system. Int J Eng Innov Technol 2015;4(8):13–9.

[50] E. Azimirad, J. Haddadnia, Target threat assessment using fuzzy sets theory, Int J Adv Intell Inform 1(2)" 57-74.

[51] G. Yang, Y. Yang, J. Li, J. Liu, Y. Ru, K. Yuan, Y. Wu, K. Liu, An assessment method of vulnerability in electric CPS cyber space. In: IEEE 12th international conference on natural computation, fuzzy systems and knowledge discovery; 379-402.

[52] Graf R, Skopik F, Whitebloom K. A decision support model for situational awareness in national cyber operations centers. In: IEEE international conference on situational awareness. Data Analytics and Assessment; 2016. p. 1–6.

[53] Zheng C, Han L, Ye J, Zou M, Liu Q. A fuzzy comprehensive evaluation model for harms of computer virus. In: IEEE 6th international conference on mobile adhoc and sensor systems; 2009. p. 708–13.

[54] Peffers K, Tuunanen T, Rothenberger MA, Chaterrjee S. A design science research methodology for information systems research. J Manag Inf Syst 2008;24(3):45–78.

[55] Hevner A, Chatterjee S. Design science research in information systems, design research in information systems. Springer; 2010. p. 9–22.

[56] Prelipcean G, Boscoianu M, Moisescu F. 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; 2010.

[57] Shanmugavadivu R, Nagarajan N. Network intrusion detection system using fuzzy logic. Indian J Comp Sci Eng 2011;2(1):101–11.

[58] Mandami EH, Assilian A. An experiment in linguistic synthesis with a fuzzy logic controller. Int J Man Mach Stud 1975;7(1):1–13.

[59] Klir GJ, Yuan B. Fuzzy sets and fuzzy logic: theory and applications. 1995. p. 574.

[60] Goztepe K. Designing fuzzy rule based expert system for cyber security. Int J Inform Secur Sci 2012:13–9.

[61] Baturone I, Barriga A, Jimenez-Fernandez C, Lopez DR, Sanchez-Solano S. Microelectronic design of fuzzy logic-based systems. CRC Press; 2000.

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

[63] Lu J, Lv F, Liu HQ, Zhang M, Zhang X. Botnet detection based on fuzzy association rules. In: IEEE 24th international conference on pattern recognition; 2018. p. 578–84.

[64] Wibowo S, Grandhi S. Fuzzy multicriteria analysis for performance evaluation of Internet-of-Things-based supply chains. Symetry 2018;10(11):603.

[65] Kumar SS, Kathiresan V. Alert system for controlling cyberbullying words using fuzzy logic and fuzzy inference engine. Asian J Comp Sci Technol 2016;5(2):29–31.

[66] Huang Z, Shen CC, Doshi S, Thomas N, Duong H. Fuzzy sets based team decision-making for Cyber Situation Awareness. In: IEEE 33th international conference on military communications; 2016. p. 1077–82.

[67] Kumar Sanjeev, Singh Amarpal, Kumar Manoj. Information hiding with adaptive stenography based on novel fuzzy edge identification. J Def Technol 2019;15(2):162–9.

[68] Kulkarni SS, Rai HM, Singla S. Design of an effective substitution cipher algorithm for information security using Fuzzy Logic. Int J Innov Eng Technol 2012;1(2).

[69] Rath AK, Parhi DR, H C, Das, Muni MK, Kumar PB. Analysis and use of fuzzy intelligent technique for navigation of humanoid robot in obstacle prone zone. J Def Technol 2018;14(6):677–82.

[70] Inyaem U, Haruechaiyasak C, Meesad P, Tran D. Terrorism event classsification using fuzzy inference system. Int J Comput Sci Inf Secur 2010;7(3).

[71] Rao DV, Balas-Timar D. A soft computing approach to model human factors in air warfare simulation system. In: Innovation in intelligent machines-5. Springer; 2014. p. 133–54.

[72] Smith ES. An application of fuzzy logic control to a classical military tracking problem. U.S. Naval Academy; 1994.

[73] Joint Staff 3-12. Cyberspace operations. Joint Staff Publication; 2018.

[74] Cannon-Bowers JA, Bell HH. Training decision makers for complex environments: implications of the naturalistic decision making perspective. In: Naturalistic decision making; 1997. p. 99–110.

[75] Grosan C, Abraham A. Intelligent systems. Springer; 2011.

[76] Shang K, Zakir H. Applying fuzzy logic to risk management and decision-making. Canadian institute of actuaries; 2013.

[77] Chen G, Pham TT, Boustany. N. Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems. 2001.

[78] Siler W, Buckley JJ. Fuzzy expert systems and fuzzy reasoning. John Wiley & Sons; 2005.

[79] Dinstein Y. Non-international armed conflicts in international law. Cambridge University Press; 2014.

[80] Caton JL. Complexity and emergence in ultra-tactical cyberspace operations. In: IEEE 5th international conference on cyber conflict; 2013. p. 1–14.

[81] Mettler T, Eurich M, Winter R. On the use of experiments in Design Science Research: a proposition of an evaluation framework. CAIS 2014;34:10.

[82] McLaren T, M B A, Buijs P. A Design Science approach for developing information systems research instruments. 2011.

[83] J. Kallberg, T.S. Cook, The unfitness of traditional military thinking in cyber; IEEE Access, 5: 8126-8130.