A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual

Kosmas **Pipyros**[1], Christos **Thraskias**[2], Lilian **Mitrou**[1], Dimitris **Gritzalis**[1], Theodoros **Apostolopoulos**[1]

[1] Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business, Athens, Greece

[2] Dept. of Informatics, University of Peloponnese, Tripolis, Greece

{pipyrosk@aueb.gr, cthraskias@gmail.com, l.mitrou@aegean.gr, dgrit@aueb.gr, tca@aueb.gr}

Abstract. In this paper a systematic modelling methodology for evaluating the effects of cyber-attacks on States Critical Information Infrastructure (CII) is introduced. The analysis is focused on the United Nations Charter's normative scheme of the 'use of force', in order to define whether these attacks constitute a wrongful 'use of force' under the principles of international law. By using the qualitative criteria for recognizing the impact of cyber-attacks as proposed by the International Group of Experts in the Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) and by applying Multiple Attribute Decision Making (MADM) methods, cyber operations evaluation results are presented. For the analysis a case study of kinetic and cyber-attacks on Supervisory Control and Data Acquisition (SCADA) system is employed. Pros and cons of the Simple Additive Weighting (SAW) method and the Weighted Product Method (WPM) are evaluated. The weaknesses of applying the SAW method in cyber-attacks modelling, as well as the difficulty in defining an appropriate quantitative scale for the classification of such attacks when using WPM (due to the nonlinear relationship between attributes and overall score in WPM), lead us to present a new evaluation strategy. This new strategy combines the use of the above mentioned decision making algorithms and introduces a new grouping of Schmitt's criteria based on their properties for achieving an improved cyber-attacks modelling assessment. Different quantitative scales are applied in the distinct Schmitt's criteria groups in order to quantify them based on their characteristics. The correlation of the qualitative and quantitative methods of analysis lead to more accurate cyber-attack evaluation and classification.

Keywords: International Law; Multiple Attribute Decision Making; Cyber-attack; Cyber Operation; Cyber Warfare; Critical Information Infrastructure.

1 Introduction

In the 21st century, cyberspace is the new frontier, a new world full of possibilities to help advance prosperity. Cyberspace and the rapid development of Information and Communication Technologies (ICTs) have fundamentally transformed the global economy and the way of life by providing billions of people across the world with instant access to information, to communication and to new economic opportunities. At the same time, national security, education, government, health, public safety, as well as sectors such as energy, transportation and communication are closely related to, if not dependent on, cyberspace and updated ICTs. The more the systems, infrastructures, societies and economies are becoming independent the higher their vulnerability and the complexity to deal with new risks and treats that menace the sovereignty of States and the well-being of societies and citizens (Albanese et al., 2013). The integration of new technologies that are enabled with Cloud Computing services is growing with an interlinkage of infrastructures which are amounting to a new dimension of vulnerability (Albanese et al., 2014). The increasing number of cyber-attacks on States' Critical Information Infrastructure (CII) are transforming cyberspace also into a battlefield, "the mouse and keyboard being the new weapons" and bringing out 'cyber warfare' as the "5th dimension of war" (The Economist, 2010).

The wide range of cyber-attacks against Estonia's critical ICT's in 2007, following the country's spat with Russia over the removal of a war memorial, were the first large scale attacks that were meant to harm the functionality of the State and to cause a number of adverse effects on the operation of public administration and the economy. The specific assault quickly led to the cultivation of fear among citizens and to the destabilization of the country's financial system, threatening Estonia's national security (Tikk et al., 2010).

A smaller range of cyber operations followed, such as the cyber-attacks against Georgia (June 2008), Lithuania (August 2008), Kazakhstan (January 2009) and Ukraine (March and May 2014). Meanwhile, Advanced Persistent Threats (APT) (Virvilis et al, 2013) clearly demonstrate the fact that cyber warfare is an increasingly alarming phenomenon. Examples of such include "Ghostnet" (Kassner, 2009), a large-scale cyber spying operation against the US; "Operation Aurora" (Zetter, 2010), a targeted malware attack against at least 30 major US companies - including Google and Adobe; "Stuxnet" (Farwell et al, 2011), a zero-day malware leading to a sabotage against Iran's nuclear program; and "DarkSeoul" (Virvilis et al, 2013), a sophisticated malware that attacked South Korean financial institutions and the Korean broadcaster YTN (Sang-Hun, 2013).

In order to defend USA from cyber-attacks former US President Obama declared America's digital infrastructure a strategic national asset (The Economist, 2010). Such decisions reflect the need to address the challenges posed with regard to cyber-attacks that could be qualified as cyberwar actions. The continuous increase in both the number and the intensity of cyber-attacks on States' CII renders the research on defining and evaluating these categories of cyber-attacks into a pressing need.

A first range of questions relate to the adequacy and suitability of the existing "old" - developed over generations to be applied on attacks using kinetic weapons and armed violence - and the terminology used (such as force and aggression), to control "the brave new world of cyber warfare (Jolley, 2013). We have to bear in mind that terms themselves, such as CII, are steadily evolving due to the impacts of the advancing domination of online communications and cyberspace on the "real world" and ubiquitous computing. The difficulties to define and to identify the effects and impacts of a cyber-attack in order to be equated to an "armed attack" are obvious: if in the "traditional" *jus ad bellum* framework emphasis is given on human and/or material destruction, authors are arguing also for "unavailability" of CII as equivalent criterion (Tsagourias, 2012). Despite the progress made on regulation and research level to address the issues raised, there are still significant gaps in reaching a safe and definitive approach on when a cyber-attack constitutes "use of force" when the right to self-defence should be recognized (Robinson et al, 2015).

The paper contributes to the development of a systematic modelling methodology for evaluating the effects of cyber-attacks on States' CII in order to answer the question of whether these attacks have risen to the level of a "use of force" under the *jus ad bellum*, that body of international law that governs a State's resort to force as an instrument of its national policy. The threshold inquiry is crucial to assessing the level of violence between States in order to justify a lawful response. Because the UN Charter prohibits the unauthorized "use of force", a State must be able to quickly and safely assess whether a cyber operation constitutes a "use of force" triggering the international condemnation and economic sanctions, (active) "cyber self-defense" - or an "armed attack" (with the use of conventional military weapons) as forceful response.

This is primarily achieved by adopting the "effects-based" or "consequences-based" approach, which focuses on the overall effect of a cyber operation to the victim-State, as well as by using the qualitative criteria for recognizing the impact of cyber-attacks as proposed by the International Group of Experts in the Manual of the International Law applicable to Cyber warfare (Tallinn Manual). Furthermore, Multi-Attribute Decision Making (MADM) methods are also applied.

For the analysis, a case study of kinetic and cyber-attacks on Supervisory Control and Data Acquisition (SCADA) system is employed. The pros and cons of each MADM method are evaluated and cyber-attack evaluation results are presented. The weaknesses of each MADM

method lead us to present a new cyber-attack evaluation strategy that combines the use of decision making algorithms of MADM methods and introduces a new grouping of the International Group of Experts criteria based on their distinctive features. The correlations of both qualitative and quantitative methods lead us to achieve an improved cyber-attack evaluation assessment and as a result a more accurate and complete cyber-attack classification.

The paper is organised as follows: In section 2 the related work in cyber-attacks modelling assessment is presented. Furthermore, a comparative evaluation of the proposed methodology with previous cyber-attack evaluation methodologies is critically discussed. In section 3 the review of the existing international legal framework of cyber warfare is presented. Then, cyber operations are being categorized, based on their intensity. Furthermore, the "effect-based" model assessment and the qualitative criteria, as proposed by the International Group of Expert on the "Tallinn Manual of International Law Applicable to Cyber warfare", are described. In section 4 the descriptions of both Simple Additive Weighting (SAW) method and Weighted Product Method (WPM) are presented. Both methods are introduced as multi-criteria decision analysis ones for the evaluation of cyber-attacks. The pros and cons of each method lead us to propose a new cyber-attack evaluation methodology which includes both qualitative and quantitative methods of analysis and results to a more accurate and complete cyber-attack evaluation and classification. Finally, in section 5 the indicative results of the research are critically analysed.

2 Related work in cyber-attack modelling assessment

Being able to precisely define, evaluate and categorize cyber-attacks is becoming increasingly difficult. The technical complexity of systems, the growing variety of exploitable attack vectors and the ubiquitous integration of Internet technology into all aspects of our daily lives compound the problem. The failure to adopt a comprehensive approach to the problem is frequently the norm, leading to an incomplete understanding of cyber-attacks and a failure to provide an appropriate solution. A plethora of cyber-attack evaluation models exist today that help to understand cyber-attacks. Most of these models however focus on delivering insight from a unidimensional perspective: technical detail or understanding of human-centric factors. Moreover, these approaches do not provide a holistic evaluation of the effects of cyber-attacks on States' CII in order to establish a basic situational awareness understanding and to define the appropriate countermeasures.

According to Happa and Fairclough (2017) the existing literature on cyber-attack evaluation models can be divided in three broad categories: Technology-centric models, social-centric models and cyber-situational awareness and understanding models. Technology-centric models seek to define cyber operations from a technical perspective (e.g. how a piece of malware operates or how vulnerability can be exploited). Examples of this category include:

a) Bishop's taxonomy (1995) which expresses cyber-attacks in the form of six axes namely: Nature of a flaw, Time of introduction, Exploitation gain, Effect domain, Minimum number necessary and the source of the identification of the vulnerability).
b) Cohen's "cyber defence mirror model" (1997) which expresses network attacks based on a defined set of properties namely: Non-orthogonality, Correlation, Hardware non-specificity, Description, Applicability and Incompleteness.
c) Howard's process-based model (1998) which takes into account five stages of a cyber-attack namely: Attackers, Tools, Access, Results and Objectives in order to understand the nature of a cyber operation.
d) The "Validation Exposure Randomness De-allocation Improper Conditions Taxonomy" (VERDICT) proposed by Lough (2001). VERDICT is an insightful technical model to understand cyber-attacks based upon four characteristics namely: Improper validation, Improper exposure, Improper randomness and Improper de-allocation.
e) AVOIDIT which is a cyber-attacks taxonomy model proposed by Simmons et al. (2009). AVOIDIT is a classification methodology which uses five major classifiers to characterize the nature of a cyber-attack namely: Attack Vector, Operational Impact, Defense, Information Impact and Target.

f) "Cyber Kill-chain" proposed by Hutchins et al. (2011) which is a process-based model for describing the stages of a cyber-attack. The "Kill-chain" phases are Reconnaissance, Weaponization, Delivery, Exploit, Installation, Command & Control (C2) and Action on Objectives.

Social-centric models attempt to understand cyber-attacks from a human perspective. Approaches focus on the identification of non-trustworthy individuals who might represent a cyber security risk to the discovery of how human-behavioral failures can be exploited as part of the cyber-attack process. Examples of this category include:

a) Greitzer et al. (2009) describes an approach to predictive modelling for insider threat mitigation. Furthermore, methods and metrics for evaluating analytic insider threat tools are described by the same authors (Greitzer et al., 2013).
b) Kandias et al. (2010) proposes a model for insider threat prediction. Additionally, a method to predict the insider threat via social media is described by the same authors (Kandias et al., 2013).
c) Stavrou et al. (2014) proposed a business process modelling for insider threat monitoring and handling.

Cyber situational awareness and understanding models attempt to adopt a high-level approach to considering cyber-attacks and focus on the environment in which the cyber-attack occurs and the resultant impact upon different elements or layers within it. Examples of this category include:

a) The UK Defence and Science Technology Laboratory (DSTL) (2012) describes a layered mode for situational awareness in cyberspace. It consists of six layers of interaction namely: Social, People, Persona, Information, Network and Real World and attacks can exist on any one or more of these layers.
b) NATO Cyber Security Framework Manual (NATO, 2012) contains an interdisciplinary approach of legal, policy, strategic and technical perspectives of cyber security. This framework supports the NATO Cyber Defence Policy.
c) Conti et al. (2013) propose a framework for designing a "comprehensive cyber common operating picture (CCOP) in order to provide military decision-makers with a useful command and control operating tool to maintain situational awareness. CCOP uses techniques for network monitoring, intrusion detection, incident response, security visualization and military command center design.

However, as it has already become apparent, it is no longer possible to consider only the technological perspective of cyber-attacks but is essential to consider all generated aspects. Furthermore, the above-mentioned technology-centric, social-centric and cyber-situational awareness models failed to accurately identify the extent of impact on socioeconomic consequences such as public health, safety, economical and psychological impacts which are directly linked to the collapse or degradation of CII. In addition, none of the above-mentioned cyber-attack methods are linked to international law and the consequences related to interstate violence. For that reason, in the following sections a systematic modelling methodology is presented for evaluating the effects of cyber-attacks on States' CII in order to answer the question of whether these attacks have risen to the level of a "use of force" under *jus ad bellum* which is the body of international law that governs a State's resort to force as an instrument of its national policy. However, before we proceed to that, a useful review of the legal issues, focusing on the uncertainties when dealing with cyber-attacks using the regulatory framework of international law, is presented.

3 Cyber warfare under the prism of *Jus ad Bellum*

When the United Nations Charter was adopted (1945), States were menaced and threaten only by kinetic means and methods of warfare and in its context aggression was understood as the use of armed force against sovereignty, territorial integrity or political independence of another State (UN Resolution 3314). Aerial bombardment, ground assault, missile strikes and other territorial incursions were the traditional kinetic methods of warfare in the military battlefield. Military operations were always focused on destroying enemy forces through the application

of physical effects with the use of kinetic means of warfare. Death, injury and destruction provoked by kinetic attacks were the prerequisite criterion to define an attack as "unauthorized use of force". Actually neither the definition of "attack" nor the definition of cyber-attack is officially defined. As underlined by Tsagourias (2012), although no definition of what constitutes an "armed attack" is provided in the UN Charter, it has been accepted that an "armed attack" is a "use of force", defined as such by its gravity and its effects rather than by the instrument employed.

In 2009 the US National Research Council defined cyber-attacks as: *"the use of deliberate action to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks"* (Owens et al, 2009). Also, the International Group of Experts in the "Tallinn Manual" defines cyber-attack as "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects*" and cyber operations as *"The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace"* (Tallinn Manual, 2013). Furthermore, in accordance to Nguyen (2014) *"the standard definitions of the terms "cyber-attack" and "cyber operation" do not qualify the actions and operations that fall under their purview, leading to broad interpretations of the types of actions included"*.

Cyber warfare is inherently "international" in nature and thus, requires an international legal response (Morth, 1998). However, the only international legal instrument regulating quite comprehensively cyberspace remains the "International Convention of Cybercrime" (i.e., Budapest Convention). The Budapest Convention (2001) led to the creation of a reference framework aiming to address computer and internet crimes by introducing appropriate legislation and fostering international cooperation for law enforcement and exchange of respective information between governments and the private sector. Recognizing that an effective fight against cybercrime requires increased, rapid, and well-functioning international cooperation in criminal matters, the "Cybercrime Convention" aimed to achieve a common criminal policy. However, it was not the purpose of the Convention to introduce a legislative framework for cyber warfare. Moreover, despite the fact that there has been considerable progress at the European level towards the development of national cyber security strategies (DoD Cyber Strategy, 2015; ENISA, 2012) and the adoption of the "Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union" (L 194, 2016), it is doubtful if such strategies and rules can deal adequately and effectively with the challenges posed by cyber-attacks that are (to be) qualified as cyberwar acts (Jougleux et al, 2016). Furthermore, there are no specific rules of international law governing the international use of cyber force (Roscini, 2014). However, the uncertainty surrounding cyber legislation does not mean cyber operations are taking place in a normative void.

The first non binding document that attempted to address cyber-attacks using the instrumentarium of international law and to produce a manual on the law governing cyber warfare was produced in 2013. The "Tallinn Manual on the International Law Applicable to Cyber Warfare" (Schmitt, 2013) was a project launched by international law practitioners and scholars at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), in an effort to examine how extant legal norms applied to this "new" form of warfare. The main goal of the Tallinn Manual was to clarify the complex legal issues surrounding cyber operations, with particular attention paid to those involving the *jus ad bellum*, the body of international law that governs a State's resort to force as an instrument of its national policy, and the *jus in bello*, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict or international humanitarian law).

On the contrary, the International Group of Experts came to the unanimous conclusion that the general principles of international law should also apply to cyberspace. Its task was to determine how exactly this type of law can be applied and to identify any cyber-unique aspects thereof. The rules set forth in the Tallinn Manual provide specific provisions (Rules) on the topic intending to act as customary international law.

Yet, at present, there is a confusion regarding the implementation of international law rules to cyber warfare. More specifically, the following have not been clarified: (a) in which cases cyber-attacks constitute a "threat or use of force" so that the prohibition of article 2(4) of the UN Charter can apply (Chapter of the UN, 1945); (b) in which cases cyber-attacks constitute a "threat to the peace, breach of the peace, or act of aggression" (Chapter VII of the UN, 1945) so that the Security Council may decide upon measures to restore international peace and security under Article 42 of the UN Charter; and (c) in which cases cyber-attacks can be treated as "armed attack", making it possible for a UN member State to respond by exercising its legitimate right of self-defense under article 51 of the UN Charter (Chapter VII of the United Nations, 1945).

3.1 Level of Intensity of Cyber Operations

In the cyber context, the identification and classification of the type of conflict to which particular hostilities apply as a matter of law, is proving problematic. The difficulty in applying the traditional rules of international law, so as to deal effectively with cyber-attacks, stems from a number of factors. The most important of them is the failure to estimate properly the impact of a cyber-attack on the attacked-State and on the international environment. Also, the inability to positively identify the key actor of an attack makes it almost impossible to handle the "attribution problem" (Schmitt, 2011; Pipyros et al. 2016). Moreover, the identification and classification of the conflict in question is always the first step in any international humanitarian law analysis, for the nature of the conflict determines the applicable legal regime. Accordingly, classification is a subject of seminal importance (Schmitt, 2013).

Cyber operations, based on their intensity and according to international law, can be categorised as follows:

(a) The lowest level of intensity includes those cyber-attacks that there are nothing more than mere inconvenience for the State's functionality. They do not provoke serious problems, nor have any impact for the stakeholders of the attack. These cyber-attacks do not constitute a "use of force" or threat thereof in violation of international law.

(b) The second level of intensity includes those cyber-attacks reaching the level of "use of force". As foreseen in article 2(4) of the UN Charter *"all Members shall refrain, in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations"*. To elaborate further, this means that uses or threats of force that endanger national or international stability fall within article 2(4)'s prescriptive envelope (Schmitt, 1999).

(c) The third level of intensity refers to cyber operations in which the Security Council is actively involved by taking action so as to maintain or restore international peace and stability. In those cases the Security Council Resolution determines if there is a threat to the peace, breach of the peace or act of aggression, and calls for provisional measures (economic or trade sanctions), or gives authority to its peacekeeping forces to use force as may be necessary.

(d) The highest level of intensity is for cyber operations reaching a level of an armed attack. In these cases there is an inherent right of self-defence under Chapter VII of the UN. Figure 1 illustrates the level of intensity of cyber operations according to the provisions of the UN Charter.

However, the UN Charter does not provide any criteria for determining when an act amounts to "use of force" or to an "armed attack". Moreover, it does not provide any specifications for the Security Council in deciding what measures, and to which extent, must be taken to maintain or to restore international peace and security. Moreover, Rule 10 of the Tallinn Manual, based on article 2(4) of the United Nations Charter, entitled "Prohibition of the use of force" notes that *"a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful"* (Tallinn Manual, 2013).

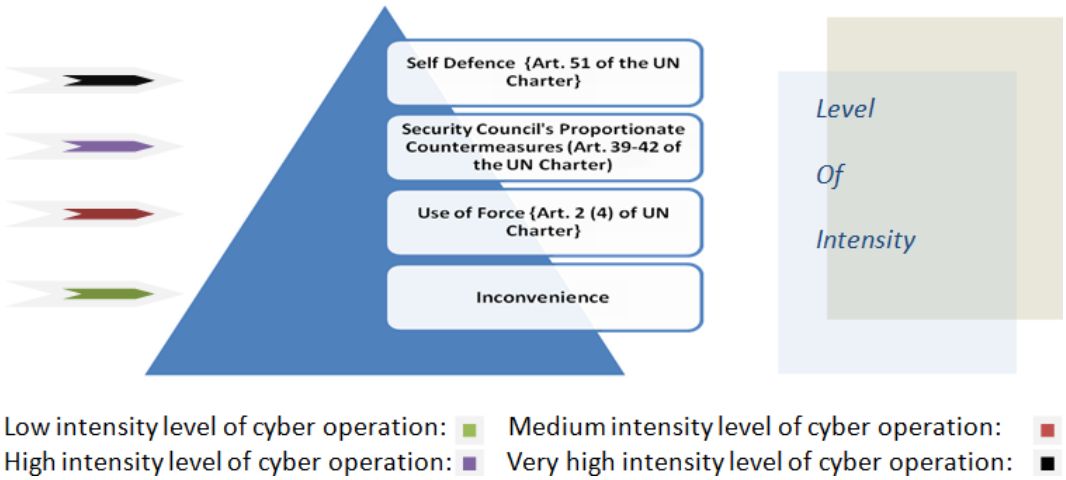

Fig. 1. Level of intensity of cyber operation

Nevertheless, this rule does not specify in which cases cyber operations can be considered as attacks that rise to the level of a "use of force" calling thus for the application of the prohibition of article 2(4) of the UN Charter (extended to Rule 10 of the Tallinn Manual). A potential answer to this question could be given by the next Rule of the Tallinn Manual, i.e. Rule 11 stating that *"a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"* (Tallinn Manual, 2013). It is therefore understood that in order for a cyber operation to be characterized as a "use of force" a parallel result logic is being employed, meaning that an effort is being made to identify cyber operations that are equivalent in terms of their results to other actions, kinetic or not, that would be described, in conventional terms, as "uses of force".

Based on the same logic, and following article 51 of the UN Charter, Rule 13 of the Tallinn Manual entitled "Self-Defence against Armed Attacks" States that *"a State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects"* (Tallinn Manual, 2013). However, in this case also, it is not clear in which cases cyber-attacks meet the scale and effects requirements so that they can be regarded, classified and handled as an "armed attack", allowing a UN Member State to respond by exercising its legitimate right of self-defense, under article 51 of the UN Charter. So it can be understood that in both Rule 11 and Rule 13 of the Tallinn Manual, the term "scale and effects" is a shorthand term that refers to those quantitative and qualitative criteria that should be analyzed in order for someone to be able to determine whether a cyber operation qualifies as a "use of force" or an "armed attack".

3.2 The "Scale and Effects" Model Assessment

The "scale and effects" concept, which was initially introduced in the so-called Nicaragua Judgment of the International Court of Justice (June 27, 1986) in a "case concerning military and paramilitary activities in and against Nicaragua", refers to a set of criteria that gather the qualitative and quantitative characteristics for determining whether or not, a hostile act rises to the level of "use of force" or to the level of "armed attack". In the Nicaragua Judgment, the International Court of Justice identified the "scale and effects" criteria as those qualitative and quantitative elements that help differentiate an "armed attack" from "a mere frontier incident" (Westlaw, 2007). More specifically, the International Court of Justice noted the need to *"distinguish the most grave forms of force (those constituting an armed attack) from other less grave forms"*, but chose to give no further details on the subject at hand. As a result, the parameters relating to a clear detection of the "scale and effects" criteria have not been further identified apart from the indication that they need to be grave. Therefore, the question remains in relation to the specification of the criteria required to identify which cyber-attacks qualify as

"use of force" and, by extension, in relation to the handling of those cases that do not meet the necessary criteria to qualify as "use of force".

Taking into consideration that the UN Charter does not provide any criteria for determining when an act amounts to a "use of force", the International Group of Experts (Tallinn Manual, 2013) adopted an interpretation according to which the critical element for identifying an attack as "use of force" or as "armed attack" is the breadth of the impact of this attack. More specifically, they concluded that a cyber operation shall amount to a "use of force" or to an "armed attack", if its impact is analogous to the one resulting from an action otherwise qualifying as a kinetic armed attack. By this logic, any attack producing similar results to the ones generated by an attack with the use of conventional weapons, resulting thus in death or destruction, shall meet the requirements of the "scale and effects" criteria.

Although, the International Group of Experts acknowledged the existence of a legal gap in relation to the identification of the exact point (threshold) at which an event such as death, injury, damage, destruction or suffering caused by a cyber operation, fails to qualify as an "armed attack", they were assertive as to what does not qualify as an "armed attack", i.e., *acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services"* (Tallinn Manual, 2013).

3.3 The Qualitative Criteria for Cyber-attacks Evaluation

Taking for granted the fact that the law is unclear as to the characterization and evaluation of a number of cyber-attacks, especially in the case of "use of force", whose impact is not immediately visible, and taking into account the total absence of an institutional framework for the evaluation of the "use of force" and "armed attack" concepts in cyberspace, the International Group of Experts proceeded to adopt an approach, following Schmitt's consequences-based analysis (Schmitt, 1999), that aims objectively to identify the likelihood of classifying a cyber operation as a "use of force".

This approach focuses on recognizing the impact of cyber-attacks and on equating them to the corresponding impact caused by other actions (non-kinetic or kinetic) that the international community would describe as "uses of force". In these cases, the parallelism and the subsequent analogous treatment of conventional operations that verge on being characterized as "uses of force" will be the outcome of the evaluation of non-exclusive criteria (factors) based on a case-by-case assessment. Table 1 provides the criteria, as proposed by the International Group of Experts. The criteria mentioned above have a non-binding nature. They are predictive tools, not normative standards and shall serve as indicators that States are likely to take into consideration when making "use of force" appraisals. Moreover, as Schmitt Stated, *"the factors must operate in concert"*. As an example, a highly invasive operation that causes only inconvenience, such as temporary denial of service, is unlikely to be classified as "use of force". By contrast, a number of States may categorize massive cyber operations that cripple an economy as "use of force" even though economic or political coercion is presumptively lawful.

Schmitt himself appear to have never intended to provide an absolute algorithm for solving what are some of the most technically and legally challenging questions a State may face. Instead, the International Group of Experts, following Schmitt's approach, saw it as a framework for analysing the effects of key factors on the legal nature of a cyber-attack and the appropriate responses. As such, the Schmitt analysis is useful as a "legal interpretation tool" as an analysis method for highlighting areas of uncertainty or disagreement in multiple legal analyses and for providing a framework for evaluating differences in the interpretation of the law.

Michael et al (2003) demonstrated, via a case study of kinetic and cyber-attacks on SCADA system, the application of the Schmitt Analysis to the question of whether the attacks have risen to the level of "use of force" under international law. Their aim was to perform a more academically rigorous evaluation of the factors affecting a lawful response to a cyber-attack on safety-critical software-intensive information system. This was achieved by taking into account both the quantitative and the qualitative aspects of the attacks, so as to reduce the "grey areas" of legal uncertainty and disagreement to an absolute minimum and to allow the most complete range of effective responses against those who attack a nation's critical infrastructure.

Severity	Is determined by the scope, duration and intensity of the caused consequences of a cyber operation.
Immediacy	Refers to the speed at which consequences manifest themselves.
Directness	Examines the chain of causation.
Invasiveness	Refers to the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State.
Measurability of effects	Refers to the fact that the more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess a situation when determining whether the cyber operation in question has reached the level of a use of force.
Military Character	Is a nexus between the cyber operation in question and military operations that heighten the likelihood of characterizing a cyber-attack as a use of force.
State Involvement	Refers to the fact that the clearer and closer a nexus between a State and cyber operations, the more likely it is that other States will characterize them as uses of force.
Presumptive Legality	International law is generally prohibitive in nature. Acts that are not forbidden are permitted. Absent an express treaty or accepted customary law prohibition, an act is presumptively legal.

Table 1. The qualitative criteria for cyber-attack evaluation

Two case scenarios of kinetic and cyber-attacks on the Washington Metro, i.e., the Washington DC's subway system, were demonstrated. The first case scenario involved terrorists released chemical gas on the Washington Metro during rush hour. The terrorists were citizens of countries with which the US, at the time of attack, was normally at peace. The second case scenario, as in the first, involved again an attack on the Washington Metro at rush hour. However, in this case scenario the terrorists used malicious code to strike the software-intensive automatic train protection system of the Metro. The attack was orchestrated from outside the US by using compromised administrative computers that were used by Metro officials to monitor operations.

Michael et al (2003) applied a quantitative scale to each of the seven identified factors (namely, Severity, Immediacy, Directness, Invasiveness, Measurability, Presumptive Legitimacy, and Responsibility) in order to evaluate the effects of both the kinetic and cyber-attack case scenarios. In their analysis each factor is graphically reproduced providing a brief description of the importance or distinctiveness of the factor, formulation of questions that would satisfy the requirements of the factor and a vertical scale of the factor itself with one quantitative choice located at the bottom and the other located at the top. Schmitt divided the spectrum into three broad bands, one each for relatively clear cases of each qualitative choice, and a central "gray area" for factually uncertain determinations. By applying the quantitative scale to each of the seven identified factors, any given operation could be described in qualitative terms as being closer to the one end of the spectrum or the other. In other words, an action's qualitative nature (in seven more or less binary areas) could be determined by applying any fixed quantitative figure (say, a one-to-ten scale). Schmitt's contribution in translating the qualitative Charter paradigm into its quantitative components - the legal equivalent of going from analogue to digital - provides a framework for scholars and practitioners to organize analysis in something other than a quantum cloud of subjective uncertainty.

In the following section a systematic modelling methodology is presented aiming to evaluating the effects of cyber-attacks on States CII in order to answer the question of whether these attacks have risen to the level of "use of force" under the principles of international law. In order for this to be achieved two approaches are taken into consideration. First, the use of the

International Group of Expert's approach, which is a transformation of the current Schmitt's consequence-based approach (Tallinn Manual, 2013). More specifically this approach has been differentiated by the replacement of the factor "Responsibility" with the factor "State Involvement", which however has similar conceptual and semantic interpretation, and by the adoption of the factor "Military Character" as a crucial factor for the determination of a cyber-attack as a "use of force". Secondly, Multiple Attribute Decision Making (MADM) methods are applied. The analysis is based on the same case scenarios of kinetic and cyber-attacks on SCADA system as argued by Michael et al (2003). Taking into account both the qualitative and quantitative aspects of such attacks and adding for the first time the "Military Character" attribute, as defined by the Tallinn Manual in the calculation procedure, a more accurate and complete evaluation of such attacks is proposed.

4 Multi Criteria Decision Analysis Methods

Multiple Attribute Decision Making (MADM) involves *"making preference decisions (such as evaluation, prioritization and selection) over the available alternatives that are characterized by multiple, usually conflicting attributes"* (Hwang and Yoon, 1981). The problems of MADM are diverse, and can be found in virtually any topic. Franklin, more than 200 years ago, recognized the presence of multiple attributes in everyday decisions, and suggested a workable solution (MacCrimmon, 1973).

By using Schmitt's analysis, three different MADM methods are applied for evaluating the effects of cyber-attacks in order to answer the question of whether these attacks have risen to the level of "use of force" under the principles of international law. Using the same case study of kinetic and cyber-attack scenarios as did Michael et al (2003) in the context of Schmitt's analysis (Schmitt, 1999), in this study the MADM methods are applied in order to evaluate these attacks.

Each decision table (or decision matrix) in MADM methods has four main parts, namely: (a) alternatives, (b) attributes, (c) weight or relative importance of each attribute, and (d) measures of performance of alternatives with respect to the attributes. The decision table is shown in Table 2 and identifies alternatives as A_i (i=1,2,…,N), attributes as B_j (j=1,2,…,M), weights of attributes as w_j (j=1,2,…,M) and the measures of performance of alternatives as m_{ij} (i=1,2, …,N and j=1,2,…,M). Given the decision table information to the decision-making method, the task of the decision maker is to find the best alternative and/or to rank the entire set of alternatives. Additionally, all the elements in the decision table must be normalized to the same units, so that all possible attributes in the decision problem can be considered (Rao, 2007).

Alternatives	**Attributes**			
	B_1	B_2	-	B_M
	(W_1)	(W_2)	-	(W_M)
A_1	m_{11}	m12	-	m_{1M}
-	-	-	-	-
A_N	m_{N1}	m_{N2}	-	m_{NM}

Table 2. The decision table in MADM methods

4.1 The Simple Additive Weighting (SAW) Method

In this section the SAW methodology is described in detail for ranking cyber-attacks on safety-critical information systems. The SAW method is probably the best known and most widely used. This method calculates the overall score of an alternative as the weighted sum of the attribute scores or utilities.

This is also called the weighted sum method (Fishburn, 1967). It is the simplest and still the widest used MADM method. Here, each attribute is given a weight, and the sum of all weights must be 1. Each alternative is assessed with regard to every attribute. The overall or composite performance score of an alternative is given by the following equation:

$$P_i = \sum_{j=1}^{M} W_j m_{ij}$$

Equation 1. Overall score with SAW method

where P_i is the overall, or composite, score of the alternatives A_i. The alternatives with the highest value of P_i are considered the best alternatives.

Table 3 demonstrates the decision matrix for a kinetic and a cyber-attack on SCADA system, as presented by Michael et al (2003). It is important to note that besides the criteria that the above mentioned authors used, in our study and in the calculation procedure one more attribute is added, i.e., the "Military Character" as defined by the International Group of Experts in the Tallinn Manual. The same weights are given to the attributes as in Michael, et al (2003). They are normalized in a scale of 1. Moreover, "Military Character" attribute was given the maximum weight of 0.16, as it is a crucial factor for the characterization of a cyber operation in such a question as a "use of force".

Alternatives	**Attributes**							
	Severity	Immediacy	Directness	Invasiveness	Measurability of effects	Presumptive Legality	State Involvement	Military Character
	0.15	0.12	0.08	0.16	0.09	0.12	0.12	0.16
Kinetic-Attack	8	8	8	9	8	8	5	8
Cyber-Attack	8	9	9	5	9	5	5	4

Table 3. The decision table for kinetic and cyber-attacks (Michael, Wingfield, Wijesekera (2003))

In Table 4, the kinetic and cyber-attack, which are described in the decision matrix of Table 3, are evaluated using the SAW method. It appears that the kinetic attack is more critical than the cyber one.

Alternatives	**SAW (P_i)**
Kinetic-Attack	7.8
Cyber-attack	6.45

Table 4. Ranking using the SAW method

Schmitt (1999) divided the spectrum into 3 broad bands, one for relatively clear cases of each qualitative choice and a central "grey area" for factually uncertain determinations (Fig. 2).

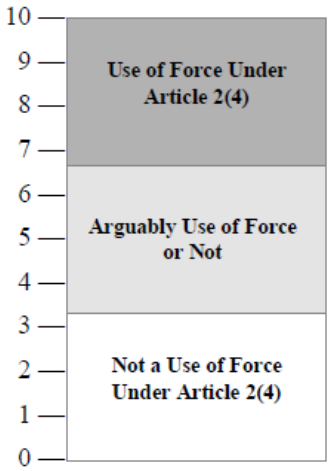

Fig. 2. The qualitative scale for cyber-attacks evaluation proposed by M. Schmitt

Using the quantitative scale of Figure 2 and taking into account the results of Table 4, the impact of the kinetic attack can be placed on the low end of the high range on the Schmitt scale. The impact the cyber-attack can be placed on the high end of the central "grey area" on the Schmitt scale. Therefore, a "use of force" occurred only in the first scenario (kinetic attack).

Taking into account both the qualitative and the quantitative aspects of such attacks and adding the "Military Character" attribute, as defined by the International Group of Experts in the calculation procedure, a more accurate and complete evaluation of such attacks is achieved. Nonetheless, there are still specific weaknesses using the SAW method. In order to show these weaknesses, the following example is presented.

Using the kinetic attack of Michael et al (2003), let us assume a hypothetical attack where the "State Involvement" attribute is given a value of zero and the other attributes hold the same values as presented above. The SAW method for this case will place the consequences of the attack on the high end of the central "grey area" on the Schmitt scale where it cannot be identified if an armed attack occurred or not. However, it is generally known that when the "State Involvement" attribute value of an attack is next to zero, this attack is unlikely to be classified as a "use of force". This is because the clearer and closer a nexus between a State and a cyber operation, the more likely is to be characterized as a "use of force". Absent a "State Involvement" it is unlikely that a cyber operation will be characterized as a "use of force". Therefore, it should be classified in the low range on the Schmitt scale, not in the central area. This example shows that it cannot appropriately model such kinds of attacks when applying the SAW methodology (Pipyros et al., 2016).

4.2 The Weighted Product Method (WPM)

The Weighted Product Method was introduced by Bridgeman (1922). According to Yoon and Hwang (1995) the method possesses sound logic and is computationally simple, but has not been widely utilized. Contrary to the SAW method, the different measurement units here do not have to be transformed into a dimensionless scale by a normalization process. This is because in the WPM method the attributes are connected by multiplication. The weights become exponents associated with each attribute value. In this method, the overall or composite performance score of alternatives is given by Equation 2:

$$P_i = \prod_{j=1}^{M} \left[m_{ij} \right]^{w_j}$$

Equation 2. Overall score with WPM method

Each value of an alternative with respect to an attribute, i.e. m_{ij}, is raised to the power of the relative weight of the corresponding attribute. The alternative with the highest P_i value is considered the best alternative.

In Table 5, using the WPM method we evaluate the kinetic and cyber-attacks described in the decision matrix of Table 3. We observe again that the kinetic attack is more critical than the cyber one. WPM operates on the premise that, in the absence of a conclusive definitional threshold with widespread acceptance within the international community, States must be highly sensitive to the international community's probable assessment of whether a cyber operation violates the prohibition on the "use of force".

Alternatives	**WPM (P_i)**
Kinetic-Attack	7.7051
Cyber-Attack	6.1392

Table 5. Ranking using the WPM method

Assuming again the hypothetical attack of the previous section, where the "State Involvement" attribute of kinetic attack is given with a value of zero while keeping the same values for

other attributes, it is easily understood that the overall performance score (which is a product) becomes zero now. This is because in the WPM method, the attributes are connected by multiplication. Thus, the WPM method for this case will place the consequences of the attack as not a "use of force" whichever quantitative scale someone decides to use. Although applying WPM in some kind of attacks gives better results than SAW, the lack of a definitional threshold for the appropriate ranking and classification of them seems to be a major drawback. Moreover, the nonlinear relationship between attributes and overall score in WPM makes more difficult the definition of a quantitative scale for the classification of attacks than using the SAW method (where a linear relationship exists).

In the following section we present a new strategy for cyber-attacks evaluation that combines the use of the first two methodologies and introduces a new grouping of Schmitt's criteria for achieving a better modelling of attacks.

4.3 A New Strategy for Cyber-attack Evaluation

In this section we continue our analysis by presenting a new modelling methodology that introduces a new calculation procedure and a new usage of the Schmitt's criteria for the better evaluation of cyber-attacks. This new strategy combines the use of the previous two decision making algorithms and introduces a new grouping of Schmitt's criteria based on their properties for achieving a better modelling of attacks. Figure 3 is a schematic diagram of this new strategy for cyber operations evaluation. The next paragraphs describe our methodology.

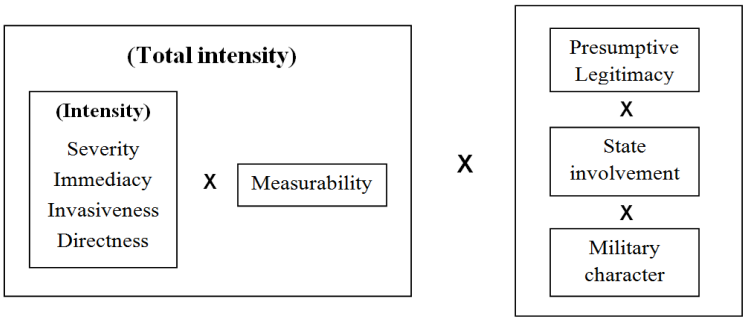

Fig. 3. The schematic diagram of the new strategy for cyber-attack evaluation

Firstly, as shown in Figure 3, "Severity", "Immediacy", "Invasiveness" and "Directness" are grouped together giving a new group named "Intensity". "Severity" refers to the degree of destruction of critical infrastructure or loss of human lives. It is, self-evidently, the most significant factor of the analysis. "Immediacy" focuses on the temporal aspects of the consequences in question whereas "Directness" examines the chain of causation (the indirect causal connection between the initial act and its effects). Furthermore "Invasiveness" refers to the degree to which cyber-attacks intrude into the target State or its cyber systems contrary to the interests of that State. The more secure a targeted cyber system, the greater the concern as to its penetration.

The four criteria are grouped together for two reasons: a) they are referred to the magnitude (intensity) of a cyber-attack, and b) they can be quantified by using the same quantitative scale (say, a one-to-ten scale). These attributes are the base of our calculation procedure and by applying the SAW method we can calculate the "Intensity" group score of a cyber-attack. Table 6 demonstrates the decision matrix for the above mentioned kinetic and cyber-attack on SCADA system so as to calculate the "Intensity" score of such attacks. For doing so, we should use in the decision matrix the four Schmitt's criteria: "Severity", "Immediacy", "Directness" and "Invasiveness". The weights of these attributes need to be redefined again in this example such that they could meet the requirement that the sum of all weights must be 1.

Alternatives	Attributes			
	Severity	**Immediacy**	**Directness**	**Invasiveness**
	0.29	0.24	0.16	0.31
Kinetic-Attack	8	8	8	9
Cyber-Attack	8	9	9	5

Table 6. The decision table for kinetic and cyber-attacks for "Intensity" score calculation

In Table 7 and by using the SAW method, we calculate the "Intensity" score of the kinetic and of the cyber-attacks described in the decision matrix of Table 6. It appears that the "Intensity" score of the kinetic attack is higher than the cyber one.

Alternatives	Intensity (P_i)
Kinetic-Attack	8.31
Cyber-Attack	7.47

Table 7. Ranking using the SAW method

Next, as presented in Figure 3, we multiply the "Intensity" score of an attack by the "Measurability" attribute to calculate the "Total Intensity" score. The more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a "use of force". The "Measurability" attribute can be quantified by using the quantitative scale from 0 to 1. By using a value of 1 it means that a complete and accurate (100%) measurement of the effects of an attack can be achieved. By using zero it means that the effects of an attack are not measurable. In Table 8, we calculate the "Total Intensity" score of the kinetic and cyber-attacks described in the decision matrix of Table 6.

Alternatives	Intensity (P_i)	Measurability	Total Intensity
Kinetic-Attack	8.31	0.9	7.479
Cyber-Attack	7.47	0.8	5.976

Table 8. Calculating the "Total Intensity" score

Last but not least, "State Involvement", "Military Character" and "Presumptive Legitimacy" are some of the most valuable factors for the characterization of a cyber operation as a "use of force" or not. The extent of "State Involvement" in a cyber operation lies along a continuum from operations conducted by a State itself to those in which its involvement is peripheral. The clearer and closer a nexus between a State and cyber operations, the more likely is that other States will characterize them as uses of force by that State. Furthermore, a nexus between the cyber operation in question and military operations heightens the likelihood of characterization as a "use of force". The "use of force" has traditionally been understood to imply force employed by the military or other armed forces. This contention supported by the fact that the UN Charter is particularly concerned with military actions. Finally, absent an express treaty or accepted customary international law prohibition, an act is presumptively legal. This being so, acts like propaganda, espionage, psychological operations are less likely to be considered by States as uses of force. Only if the criteria of "State Involvement", "Military Character" and "Presumptive Legitimacy" are met, a State can characterize a cyber-attack as a 'use of force'. For this reason, in order to quantify them we use binary logic assigning to them the values 0 or 1 (false or true).

In Figure 3, the attributes "Total Intensity", "Military Character", "State Involvement" and "Presumptive Legitimacy" are connected with multiplication. Thus, the last three should be "true" in order to have a non-zero overall score as a final result in the evaluation procedure. If one of them is zero, the overall score will be also zero. Therefore, for the evaluation of cyber-

attacks by using this methodology it is of fundamental importance to be able to decide if these three criteria are met or not.

In Table 9, we calculate the overall score of the kinetic and cyber-attacks described in the decision matrix of Table 6 by using our methodology. It is observed that the kinetic attack is more critical than the cyber one.

Alternatives	Total Intensity	State Involvement	Military Character	Presumptive Legitimacy	Overall Score
Kinetic Attack	7.479	1	1	1	7.479
Cyber-attack	5.976	0	0	0	0

Table 9. Calculating the overall score

Thus, using again the quantitative scale of Figure 2 and taking into account the results of Table 9, the consequences of the kinetic attack can be placed on the low end of the high range on the Schmitt scale and the consequences of the cyber-attack on the low range on the Schmitt scale. Therefore, a "use of force" occurred only in the first scenario (kinetic attack).

In conclusion the existing legal norms do not offer a comprehensive framework in the way that States can shape policy to the threat of hostile cyber operations. Furthermore, State practice is lacking in characterizing a cyber operation as a "use of force" or not. Even though there were many cyber operations that could be reach the level of a "use of force", in none of these cases States have been identified as the initiator of the cyber operation which might amount to a "use of force". The threshold of a "use of force" must be balanced between on the one hand State's willingness to avoid any harmful consequences caused by the actions of others States and one the other hand its motivation to preserve their freedom of action. The evaluation criteria proposed by the International Group of Experts in the Tallinn Manual seek to balance these conflicting objectives through consideration. However, as Schmitt admitted (2011) *"the criteria are admittedly imprecise, thereby permitting States significant latitude in characterizing a cyber operation as a 'use of force' or not"*. Furthermore, a State, depending on the attendant circumstances, may look also to other factors such as the prevailing political environment, whether the operation portends the future "use of force", the identity of the attacker and the nature of the target. In fact, a finding that a cyber or a kinetic attack is a "use of force" is a political and not legal decision, as it shows a State willingness to involve itself in a particular matter.

For the above mentioned reasons the authors of this paper have chosen to present this work in a manner to provide clear structure for discussion. It was not their intent to provide an absolute algorithm for producing the "right answer" given any input. The proposed systematic methodology is applied in order to portray a better modelling evaluation of cyber-attacks. It contributes in areas where there is uncertainty or disagreement in a number of a legal analysis and for making available means for addressing all issues related to the "use of force" concept.

5 Conclusions

In this paper, the aim was to present a new systematic modelling methodology for evaluating the effects of cyber-attacks on States' CII in order to define whether these attacks constitute a wrongful "use of force" under the *jus ad bellum*, that body of international law that governs a State's resort to force as an instrument of its national policy. We have adopted the "effects-based" or "consequences-based" approach, which focuses on the overall effect of a cyber operation to the victim-State, as well as by using the qualitative criteria for recognizing the impact of cyber-attacks as proposed by the International Group of Experts in the Manual of the International Law applicable to cyber warfare. Furthermore, Multi-Attribute Decision Making (MADM) methods and more specifically the Simple Additive Weighting (SAW) method and the Weighted Product Method (WPM) were applied.

Evidently, the characterization and classification of cyber-attacks on State's CII depends largely on the extent of their consequences. In other words, the categorization of the type of attack lies heavily on its impact level both in terms of the loss of human lives and in terms of

the destruction of critical infrastructures. Consequently, the degree of the immediate as well as of the long-term effects of a cyber-attack constitutes a critical factor for its categorization. Furthermore, the greater the degree of impact of a cyber-attack, the greater the chances are that it will be characterized as "use of force", or even worse, as "armed attack" when its magnitude is so great as to cause loss of human lives. Thus, the main issue of investigation is to define the method of measurability of the impact of a cyber-attack.

The main contribution of the paper relies on the development of a new modelling strategy that combines the International Group of Experts qualitative criteria with MADM methods. For the analysis, a case study of kinetic and cyber-attacks on Supervisory Control and Data Acquisition (SCADA) system is employed. The pros and cons of each MADM method are evaluated and the results of cyber-attack evaluation were presented. The weaknesses of each MADM method lead us to present a new cyber-attack evaluation strategy that combines the use of decision making algorithms of MADM methods and introduces a new grouping of the International Group of Experts criteria based on their distinctive features. The correlations of both qualitative and quantitative methods lead us to achieve an improved cyber-attack evaluation assessment and as a result a more accurate and complete cyber-attack classification.

Despite the constructive contribution of the "Tallinn Manual" the international legal regime is lagging behind the problems to deal with. The existing norms do not offer a comprehensive legal framework in the way that States can shape policy to the threat of hostile cyber operations. Furthermore, the use of interpretative methods such as analogies and teleological and systematic understanding is lacking the necessary legal safety. Additionally, state practice is lacking in characterizing a cyber operation as a "use of force" or not. However, for the sake of multiple safety decision making with regard to respond to a cyber attack has to be based on commonly accepted principles and pre-existing norms. Assessing the feasibility, legitimization and legality of responses of cyber-attacks, equivalent to armed attacks, seems to remain to a large extent "a matter of speculation and hypothetical reasoning (Kessler et al, 2013). Therefore, the systematic modelling methodology could be used as a "legal interpretation tool" in areas where there is uncertainty or disagreement in multiple legal analyses and for providing a framework for evaluating differences in interpretation of the law. The proposed systematic methodology is applied in order to portray a better modelling evaluation of cyber-attacks. However, it was not the purpose of the authors to provide an absolute algorithm for producing the "right answer" given any input.

The threshold of a "use of force" must be balanced between on the one hand State's willingness to avoid any harmful consequences caused by the actions of others States and one the other hand its motivation to preserve their freedom of action. The evaluation criteria proposed by the International Group of Experts in the Tallinn Manual seek to balance these conflicting objectives through consideration. As such, the usefulness of the methodology is perceived in areas where there is uncertainty or disagreement in a number of legal analyses, and for making available a means for addressing all issues having to do with "use of force". In addition, this methodology could act as a basis for the assessment and classification of cyber-attacks that are intended towards software-intensive IS that may constitute a component of a CII.

The above mentioned results demonstrate that there is a long way ahead for further research in the field of cyber-attack evaluation methodologies so as to achieve a more accurate modelling of cyber operations. Future work will be focused on the application of the suggested methodology in real-life cyber operation cases in order to enable their characterization and classification under the principles of international law and to achieve a more accurate and complete cyber-attack modelling assessment.

References

Massimiliano Albanese, Sushil Jajodia, Ravi Jhawar and Vincenzo Piuri. 2013. Reliable mision deployment in vulnerable distributed systems. In Proc. of the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks, 1-8.

Massimiliano Albanese, Sushil Jajodia, Ravi Jhawar and Vincenzo Piuri. 2014. Securing mision-centric operations in the Cloud. In Secure Cloud Computing. S. Jajodia et al. (Eds). Springer, 239-260.

Matt Bishop. 1995. A Taxonomy of UNIX System and Network Vulnerabilities. Technical Report CSE 95-10. Department of Computer Science, University of California at Davis.
Percy Williams Bridgman. 1922. Dimensionless Analysis. New Haven. Yale University Press.
Fred Cohen.1997.Information system attacks: A preliminary classification scheme. Computers & Security, 16, 1, 29-46.
Gregory Conti, John Nelson and David Raymond. 2013. Towards a Cyber Common Operating Picture. In Proc. of the 5th International on Cyber Conflict. K. Podins, J. Stinissen, M. Maybaum (Eds.). NATO CCD COE Publications, Tallinn.
Centre for Defence Enterprise. 2012. Cyber Situational Awareness. Defence Science and Technology Laboratory. Ministry of Defence, UK
http://nationalarchives.gov.uk/webarchive/
Council of Europe. 2001. Convention on Cybercrime. European Treaty Series 185.
European Commission. 2016. On critical information infrastructure protection. 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'. Communication 149.
European Parliament and the Council. 2016. Directive 1148 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union.
European Network and Information Security Agency. 2012. National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace.
James P. Farwell, Rafal Rohozinski. 2011. The new Cyber Threat: Stuxnet and the Future of Cyber war. IISS Survival Global Politics and Strategy, 53, 1, 23-40.
Peter Fishburn. 1967. Additive utilities with incomplete product set: Applications to priorities and assignments. Operations Research, 15, 3, 537-542.
John D. Howard and Thomas A. Longstaff. 1998. A common language for computer security incidents. Sandia National Laboratories.
Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin. 2011. Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. In Proc. of the 6th Annual International Conference on Information Warfare and Security, Washington, DC.
Ching-Lai Hwang, Kwangsum Yoon. 1981. Multiple Attribute Decision Making: Methods of Application. A State of the Art Survey. Springer.
Jason Jolley. 2013. Article 2(4) and Cyber warfare: How do Old Rules Control the Brave New World?. Canadian Center of Science and Education, 2, 1.
Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou. 2016. The Legal Regulation of Cyber Attacks. In Ioannis Iglezakis (editor). Kluwer Law International.
Miltiadis Kandias, Alexios Mylonas, Nikos Virvilis, Marianthi Theoharidou and Dimitris Gritzalis. 2010. An Insider Threat Prediction Model. In Proc. of the 7th International Conference on Trust, Privacy and Security in Digital Business, Springer, Spain, 26-37.
Miltiadis Kandias, Vasilis Stavrou, Nick Bozovic, Lilian Mitrou and Dimitris Gritzalis. 2013. Predicting the insider threat via social media: The YouTube case. In Proc. of the 12th Workshop on Privacy in the Electronic Society, ACM Press, Berlin, 261-266.
Michael Kassner. 2009. Ghostnet: Why it's a big deal.
www.techrepublic.com/blog/it-security/ghostnet-why-its-a-big-deal/
Oliver Kessler and Wouter Werner. 2013. Expertise, Uncertainty and International Law: A Study of the Tallinn Manual on Cyber warfare. Leiden Journal of International Law, 26, 793-810.
Alexander Klimburg (Ed.). 2012. National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence Publication, Tallinn.
Daniel Lowry Lough. 2001. A taxonomy of computer attacks with applications to wireless networks. Blacksburg. University Libraries. Virginia Polytechnic Institute and State University.
KR MacCrimmon. 1973. Multiple Criteria Decision Making: An Overview of Multiple Objective Decision Making. University of South Carolina Press, 18-44.
James Michael, Thomas Wingfield and Duminda Wijesekera. 2003. Measured Responses to Cyber-attacks using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System. In Proc. of the Twenty-seventh Annual International on Computer Software and Applications Conference, IEEE.
Todd Morth. 1998. Considering our position: Viewing information warfare as a use of force prohibited by article 2(4) of the UN Charter. Case Western Reserve Journal of International Law, 30, 2, 567-600.
Reese Nguyen. 2013. Navigating Jus Ad Bellum in the Age of Cyber Warfare. California Law Review. 101, 4, 1079-1130.

William Owens, Kenneth Dam and Herbert Lin. 2009. Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities. The National Academies Press.
Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis and Theodoros Apostolopoulos. 2014. A Cyber-attack Evaluation Methodology. In Proc. of the 13th Conference on Cyber Warfare and Security, ACPI, 264-270.
Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis and Theodoros Apostolopoulos. 2016. A review of obstacles in applying international law rules in cyber warfare, Information & Computer Security, 24, 1, 38-52.
Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis and Theodoros Apostolopoulos. 2016. Cyber-Attacks Evaluation Using Simple Additive Weighting Method on the Basis of Schmitt's Analysis, In Proc. of the 10th Mediterranean Conference on Information Systems, MCIS Proceedings, 41.
General Assembly. 1974. Resolution adopted by the General Assembly A/RES/29/3314: Definition of Aggression. United Nations.
Frank L. Greitzer and Thomas A. Ferryman. 2013. Methods and Metrics for Evaluating Analytic Insider Treat Tools. In Proc. of the 2013 IEEE Security and Privacy Workshops, California, USA, 90-97.
Frank L. Greitzer, Patrick R. Paulson, Lars J. Kangas, Lyndsey R. Franklin, Thomas W. Edgar, Deborah A. Frincke. 2009. Predictive Modeling for Insider Threat Mitigation. Technical report PNNL-60737, Pacific Northwest National Laboratory.
Jassim Hapa and Graham Fairclough. 2017. A Model to Facilitate Discussions about Cyber Attacks. In Ethics and Policies for Cyber Operations. M. Taddeo, L. Glorioso (eds.), Philosophical Studies Series 124, Springer International Publishing Switzerland, 169-185.
R. Venkata Rao. 2013. Decision Making in the Manufacturing Environment Using Graph Theory and Fuzzy Multiple Decision Making (MADM) Methods. Springer – Verlag London.
Michael Robinson, Kevin Jones and Helge Janicke. 2015. Cyber warfare: Issues and Challenges. Computers & Security, 49, 70-94.
Marco Roscini. 2014. Cyber Operations and the Use of Force in International Law. Oxford University Press.
Choe Sang-Hun. 2013. Computer Networks in South Korea are paralyzed in Cyber-attacks. The New York Times.
Michael Schmitt. 1999. Computer Network Attack and the Use of Force in International Law: Thoughts on a normative framework. Columbia Journal of Transnational Law, 37, 885-937.
Michael Schmitt. 2011. Cyber Operations and the Jus ad Bellum Revisited. Villanova Law Review, 56, 3, 569-606.
Michael Schmitt. 2013. Classification of Cyber Conflict. Journal of Conflict and Security Law, 17, 2, 245-260.
Michael Schmitt (Ed.). 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.
Michael Schmitt and Liis Vihul. 2014. Proxy Wars in Cyberspace: The Evolving International Law of Attribution. Fletcher Security Review, 1, 2, 53-72.
Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta and Qishi Wu. 2009. AVOIDIT: A Cyber Attack Taxonomy. Technical report: CS-09-003, University of Memphis.
Vasilis Stavrou, Miltiadis Kandias, Georgios Karoulas and Dimitris Gritzalis. 2014. Business Process Modeling for Insider Threat Monitoring and Handling. In Proc. of the 11th International Conference on Trust, Privacy & Security in Digital Business, Springer, Germany, 119-131.
The Department of Defense Cyber Strategy. 2015. United States of America.
The Economist. 2010. Cyber War in the fifth domain: Are the mouse and the keyboard the new weapons of conflict?
www.economist.com/node/16478792
Nicholas Tsagourias. 2012. Cyber-attacks, self-defence and the problem of attribution. Journal of Conflict & Security Law, 17, 2, 229-244.
Eneken Tikk, Kadri Kaska and Liis Vihul. 2010. International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence (CCD COE).
United Nations. 2001. Yearbook of the International Law Commission: Draft Articles on Responsibilities of States for Internationally Wrongful Acts, 2, 2.
United Nations and Statute of the International Court of Justice. 1948. The Universal Declaration of Human Rights.
www.un.org/en/universal-declaration-human-rights/index.html

Nikos Virvilis and Dimitris Gritzalis. 2013. The Big Four – What We Did Wrong in Advanced Persistent Threat Detection?. In Proc. of the 8th International Conference on Availability, Reliability and Security, Springer, 248-254.

Nikos Virvilis and Dimitris Gritzalis. 2013. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?. In Proc. of the 10th IEEE International Conference on Autonomic and Trusted Computing. IEEE Press, 396-403.

Westlaw. 1986. Case concerning military and paramilitary activities in and against Nicaragua. www.ilsa.org/jessup/jessup08/basicmats/icjnicaragua.pdf

K Paul Yoon and Ching-Lai Hwang. 1995. Multiple Attribute Decision Making: An Introduction. Sage University Paper Series on Quantitative Applications in the Social Sciences, 7-14.

Kim Zetter. 2010. Google Hack Attack was Ultra Sophisticated, New Details Show. Wired. www.wired.com/2010/01/operation-aurora/