Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2016 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2016

Cyber-Attacks Evaluation Using Simple Additive Weighting Method on the Basis of Schmitt's Analysis

Kosmas Pipyros
Athens University of Economics & Business, pipyrosk@aueb.gr

Christos Thraskias
University of Peloponnese, cthraskias@gmail.com

Lilian Mitrou
University of the Aegean, L.MITROU@AEGEAN.GR

Dimitris Gritzalis
Athens University of Economics & Business, dgrit@aueb.gr

Theodore Apostolopoulos
Athens University of Economics & Business, tca@aueb.gr

Recommended Citation

Pipyros, Kosmas; Thraskias, Christos; Mitrou, Lilian; Gritzalis, Dimitris; and Apostolopoulos, Theodore, "Cyber-Attacks Evaluation Using Simple Additive Weighting Method on the Basis of Schmitt's Analysis" (2016). *MCIS 2016 Proceedings*. 41.
http://aisel.aisnet.org/mcis2016/41

CYBER-ATTACKS EVALUATION USING SIMPLE ADDITIVE WEIGHTING METHOD ON THE BASIS OF SCHMITT'S ANALYSIS

Completed Research

Pipyros, Kosmas, Athens University of Economics & Business, Greece, pipyrosk@aueb.gr
Thraskias, Christos, University of Peloponnese, Greece, cthraskias@gmail.com
Mitrou, Lilian, University of the Aegean, Greece, l.mitrou@aegean.gr
Gritzalis, Dimitris, Athens University of Economics & Business, Greece, dgrit@aueb.gr
Apostolopoulos, Theodore, Athens University of Economics & Business, Greece, tca@aueb.gr

Abstract

A systematic modelling methodology is presented in this paper, so as to evaluate the effects of cyber-attacks on states' Critical Information Infrastructure, in order to answer the question of whether these attacks have risen to the level of a '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 the Simple Additive Weighting method, the widely used Multiple Attribute Decision Making method, cyber-operations evaluation results are presented. For the analysis a case study of kinetic and cyber-attacks on Supervisory Control and Data Acquisition system is employed. Taking into account 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 complete evaluation of such attacks is achieved.

Keywords: *Cyber-attack, International Law, Simple Additive Weighting Method, Use of Force.*

1. Introduction

In the 21st century, cyberspace is the new frontier, a new world full of possibilities to help advance security and prosperity. Major public sector industries, such as national security, education, government, health, public safety, as well as sectors such as energy, economics, transportation and communication are closely related to, if not dependent on, cyberspace and new information and communication technologies (ICT). Cyberspace and the rapid development of updated ICT 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. Yet, with these possibilities also come new perils. The increasing number of cyber-attacks on states' Critical Information Infrastructure (CII) has transformed cyberspace into a battlefield bringing out 'cyber warfare' as the 'fifth dimension of war' (The Economist, 2010) with an emphasis on governments' need to effectively protect their people against these attacks.

L. Panetta, former US Secretary of Defense (2011-13), during his speech 'Defending the nation from cyber-attack' (2011), pointed out that this is a "pre-9/11" moment and that 'a cyber-attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11'. This phrase seems to have been proven over the years. 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 and Lithuania in June and August 2008, respectively, against Kazakhstan in January 2009, and recently, the cyber-attacks against Ukraine in March and in May 2014. Meanwhile, Advanced Persistent Threats (APT) (Virvilis and Gritzalis, 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 and Rohozinski, 2011), a four zero-day malware leading to a sabotage against Iran's nuclear program; and 'DarkSeoul' (Virvilis, et al, 2013), a sophisticated malware that paralyzed South Korean financial institutions as well as the Korean broadcaster YTN (Sang-Hun, 2013).

More recently, in April 2016 Robert Work, US Deputy Secretary of Defense, declared that "the US Cyber Command Units are dropping cyber-bombs" on ISIS. Though possibly rhetorically, this statement demonstrates that cyber capabilities are now seen as weapons (Sanger, 2016). In spite of the fact that much remains unclear about the future relevance of cyberspace as a domain for military operations, it is undeniable that cyber capabilities can launch attacks that may cause death and destruction (Veenendaal et al, 2016). At the same time, the increase in both the number and the intensity of cyber-attacks on states' CII calls for an in-depth study in order to bring out the points that differentiate this category of operations from other types of hostile actions (such as attacks using kinetic weapons, armed violence, etc.) (Pipyros et al, 2014) (Gritzalis, 2014).

2. Cyber warfare under the prism of jus ad bellum

Although most interactions between cyberspace and the law occur at the national level, involving criminal activity by either individuals or private groups for personal gain or take the form of a plethora of other 'non-criminal' activities (i.e. commercial transactions, advertising, defamation) that are regulated by domestic law (Roscini, 2014), cyber warfare is inherently 'international' in nature and thus, requires an international legal response (Morth, 1998). Yet, at present, there are no specific rules of international law governing the international use of cyber force. The only treaty regulating cyberspace per se remains the International Convention of Cybercrime (*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. Recognising 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-attacks. Moreover, there are no treaties at all that deal directly with cyber warfare.

The first nonbinding document that attempted to interpret cyber-attacks through the prism of international law and to produce a manual on the law governing cyber warfare was produced in 2013. The *Manual on the International Law Applicable to Cyber Warfare* or the *Tallinn Manual* (Schmitt, 2013) was a project launched by distinguished international law practitioners and scholars at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)[1], in an effort to examine how extant legal norms applied to this 'new' form of warfare. The main focus of the *Tallinn Manual* was to bring some degree of clarity to 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). The uncertainty surrounding cyber legislation does not mean cyber operations exist in a normative void. 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 such law can be applied and to identify any cyber-unique aspects

[1] An international military organization based in Tallinn (Estonia) and accredited in 2008 by NATO as a 'Centre of Excellence'. However, NATO CCD COE is not part of NATO's command or force structure, but a part of a wider framework supporting NATO Command Arrangements.

thereof. Since there are neither treaty provisions that directly deal with cyber warfare nor state cyber practise and publicly available expressions of *opinion juris* (Article 38 of the Statute of the International Court of Justice, UN Charter), it is difficult to accurately conclude that any cyber-specific customary international law norms exist. The rules set forth in the *Tallinn Manual* provide specific provisions (rules) on the topic intending to act as customary international law.

However, despite the fact that there has been considerable progress at the European and international levels towards the development of National Cyber Security Strategies[2] and the adoption of an effective comprehensive legal framework of prevention measures against cyber-attacks (European Commission, 2009 & 2013), (Council of the European Union, 2016) confusion remains regarding the application of these rules. More specifically, the following have not been clarified: 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 United Nations, 1945); in which cases cyber-attacks constitute a ‘threat to the peace, breach of the peace, or act of aggression’ (Chapter VII of the United Nations, 1945), so that the Security Council may decide upon measures to restore international peace and security under Article 42 of the UN Charter; and in which cases cyber-attacks can be treated as ‘armed attacks’, making it possible for a UN member state to respond by exercising its legitimate right of self-defence under Article 51 of the UN Charter (Chapter VII of the United Nations, 1945).

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 extremely problematic. Cyber operations have the potential for producing vast societal and economic disruption without causing the physical damage typically associated with armed conflict (Schmitt, 2011).The difficulty in applying the traditional rules of international law in order 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 in the victim-state and in the international environment. Additionally, the inability to positively identify the key actor of an attack makes it often quite hard to handle the issue of ‘attribution’ (Pipyros et al, 2016) (Gritzalis, 2014). 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, can be separated into four categories. 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 and, according to international law, they have no consequences for the stakeholders of the cyber-attack. The second level of intensity includes those cyber-attacks that are at the level for ‘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’. This means that uses or threats of force which endanger national or international stability fall within article 2(4)’s prescriptive envelope (Schmitt, 1999). The state under attack which falls under the provisions of article 2(4) of the UN Charter has a legal ground to take precautionary measures (e.g. diplomatic protests, economic sanctions) and actions (kinetic or cyber) short of uses of force that qualify as lawful ‘counter measures’ under specific circumstances (Draft articles on Responsibility of States for Internationally Wrongful Acts, 2001). Moreover, the measures to be taken depend on the state’s perspective as far as it concerns the interpretation of the provisions of article 2(4). It is important to emphasize the US’s position in these cases regarding the width of applicability of this article. The US position on this matter is that they can retaliate even with armed force when there is a violation of the article. Moreover, in the third level of intensity there are specific cyber operations in which the Security Council can take action in order to determine if there is a threat to the peace, breach of the peace, or act of aggression, and to call for provisional measures (economic/trade sanctions), or to give authority to its peacekeeping forces to use force as may be necessary to maintain or restore international peace and security. Finally, 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 (Chapter VII of the

[2] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

United Nations, 1945). Figure 1 illustrates the level of intensity of cyber operations, according to the provisions of the UN Charter.

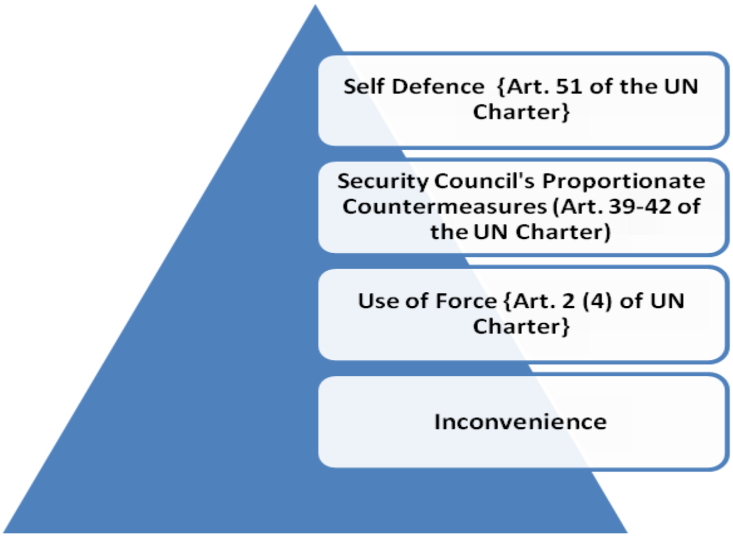
Self Defence {Art. 51 of the UN Charter}
Security Council's Proportionate Countermeasures (Art. 39-42 of the UN Charter)
Use of Force {Art. 2 (4) of UN Charter}
Inconvenience

Figure 1. Level of Intensity of cyber-operations under the prism of 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 they must be taken in order to maintain or to restore international peace and security.

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 consequence-based approach (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 a number 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 below do not have legal status. 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 (2014) said, ‘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 never intended to provide a mechanical 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 useful 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 algorithm, but it is even more useful as a method for highlighting areas of uncertainty or disagreement in multiple legal analyses and for providing a framework for evaluating differences in interpretation of the law.

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 criteria for a cyber-attack evaluation

James and Wijesekera (2003) have demonstrated how the Schmitt analysis can be used 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 (IS), aiming to reduce the ‘grey areas’ of legal uncertainty to an absolute minimum, and allow the most complete range of effective responses against those who attack a nation’s critical infrastructure. James and Wijesekera (2003) used Schmitt’s analysis in order to evaluate the effects of a cyber-attack. By applying a quantitative scale to each of the eight identified factors, any given operation could be described in qualitative terms as being closer to one end of a spectrum or the other. In other words, an action’s qualitative nature (in eight 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 analog to digital - provides a framework for scholars and practitioners to organize analysis in something other than a quantum cloud of subjective uncertainty. James and Wijesekera (2003) demonstrate, 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, taking into account both the quantitative and the qualitative aspects of the attacks.

In the following section 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 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 Tallinn Manual, and by applying the Simple Additive Weighting method (SAW) as a widely used Multiple Attribute Decision Making (MADM) method, cyber-operations evaluation results are presented. For the purpose of the analysis the same case study of kinetic and cyber-attacks on SCADA system is employed as James and Wijesekera (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 achieved.

3. 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. Even Franklin, more than two centuries ago, recognized the presence of multiple attributes in everyday decisions and suggested a workable solution (MacCrimmon, 1973).

For this paper, using Schmitt's analysis, the Simple Additive Weighting (SAW) method is applied for evaluating the effects of cyber-operations in order to answer the question of whether these attacks have risen to the level of 'use of force' under international law. Using the same case study of kinetic and cyber-attack scenarios as did James and Wijesekera (2003) in the context of Schmitt's analysis (Schmitt, 1999), in this study the abovementioned MADM method is applied in order to evaluate these attacks.

Each decision table (also called a decision matrix) in the SAW method 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 (where i = 1,…,N), attributes as B_j (where j = 1,…,M), weights of attributes as w_j (where j = 1,…,M), and the measures of performance of alternatives as m_{ij} (where i= 1,…,N and j=1,…,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. Also, 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_3	-	-	B_M
	(W_1)	(W_2)	(W_3)	(-)	(-)	(W_M)
A_1	m_{11}	m_{12}	m_{13}	-	-	m_{1M}
-	-	-	-	-	-	-
A_N	m_{N1}	m_{N2}	m_{N3}	-	-	m_{NM}

Table 2. Decision table in MADM methods

Table 3 demonstrates the decision matrix for a kinetic and a cyber-attack on a SCADA system, as presented by James and Wijesekera (2003). It is important to note that besides the criteria that the above authors used, in this study in the calculation procedure one more attribute is added, namely the 'military character' as defined by the international group of experts. The same weights it is given to the attributes as did James and Wijesekera (2003), and are normalized in a scale of 1. Moreover, 'military character' attribute was given the maximum weight of 0.16, as it is an important factor for the characterization of a cyber operation in such a question as a 'use of force'.

Alternatives	**Attributes**							
	Sev.	**Imm.**	**Dir.**	**Inv.**	**Meas.**	**Pres.**	**Res.**	**Mil.**
	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	1
Cyber-attack	8	9	9	5	9	5	5	1

Table 3. Decision table for kinetic and cyber-attacks

4. The Simple Additive Weighting method

In this section, the Simple Additive Weighting (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) and is a simple and widely 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

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.

In Table 4, using the SAW method, the kinetic attacks and the cyber-attacks are evaluated that were described in the decision matrix of Table 3. It is observed that kinetic attacks are more critical than are cyber-attacks.

Alternatives	SAW (P_i)
Kinetic- attack	6.68
Cyber-attack	5.97

Table 4. Ranking using the SAW method

Schmitt divided the spectrum into three broad bands, one each for relatively clear cases of each qualitative choice, and a central 'grey' area for factually uncertain determinations, as shown in Figure 2.

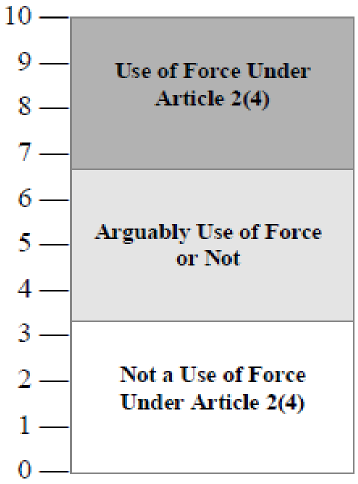
10
9
8
7
6
5
4
3
2
1
0
Use of Force Under Article 2(4)
Arguably Use of Force or Not
Not a Use of Force Under Article 2(4)

Figure 2. The quantitative scale for cyber-attacks evaluation

Using the quantitative scale of Figure 2 and taking into account the results of Table 4, the consequences can be placed of the kinetic attack on the low end of the high range on the Schmitt scale and the consequences of the cyber-attack on the high end of the central 'grey area' on the Schmitt scale. Therefore, it can be said that 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 applying the SAW method, it can be argued that assessing cyber-attacks on states' CII by using the SAW method leads to a more complete evaluation of cyber-attack classification under the principles of international law. Nonetheless, there are still some weaknesses using the SAW method. In order to show these weaknesses, the following example is presented.

Using the kinetic attack of James and Wijesekera (2003), let us assume a hypothetical attack where the 'Responsibility' 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 'Responsibility' attribute value of an attack is next to zero, this attack is unlikely to be classified 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.

5. Conclusions

As it has become clear, the characterization and classification of cyber-attacks on state's CII depends largely on the size of their consequences. In other words, the categorization of the type of attack lies heavily on its impact level both in terms of loss of human lives and in terms of destruction of critical infrastructures. So, the degree of the immediate as well as of the long-term effects of a cyber-attack constitutes a critical factor for its categorization.

Additionally, the greater the degree of impact of a cyber-attack, the greater the chances that it will be characterized as 'use of force', or even worse, as 'armed attack' when its size is so great as to cause loss of human lives. So the critical issue here is the method of measurability of the impact of a cyber-attack. In this work, using Schmitt's analysis, it was introduced a new modelling strategy for improving cyber-attack evaluation by taking into account the qualitative criteria as proposed by the international group of experts and applying the SAW method.

This framework could be used for stressing 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 can 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 critical infrastructure.

The above results demonstrate that a lot of research has to be conducted in the field of cyber-attack evaluation methodologies for the better and more accurate modelling of cyber operations. In the future, the recommended study will be focused on a more accurate approach of the abovementioned cyber-attack-modelling strategy, applying further MADM methods in order to determine and to evaluate the impact factors of a cyber-attack on states' CII, on the basis of its type and intensity, for enabling its categorization under the principles of international law.

References

Council of Europe (2001). "Convention on Cybercrime", *European Treaty Series 185*, Hungary.

Council of the European Union (2016). "Concerning measures for a high common level of security of network and information systems across the Union", *Legislative acts and other Instruments* 5581, Brussels, 21.04.2016

European Commission (2009). "On critical information infrastructure protection, protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience (Communication) COM", 149 final, Brussels, 30.03.2009.

European Commission (2013). "Cyber security Strategy of the European Union: An open safe and secure cyberspace", *Joint Communication to the European Parliament and the Council*, JOIN, 1 Final, Brussels, 07.02.2013.

Farwell, J. and Rohozinski, R. (2011). "Stuxnet and the Future of Cyber War", IISS, *Survival: Global Politics and Strategy*, 53 (1), 23-40.

Fishburn, P.C. (1967). *Additive Utilities with Incomplete Product Set: Applications to Priorities and Assignments*, USA: Operations Research Society of America (ORSA).

Hwang C., Yoon K., (1981). *Multiple Attribute Decision Making: Methods and Applications*, Berlin: Springer.

James M. and Wijesekera D. (2003). "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System", *27th Annual International Computer Software and Applications Conference*, IEEE, USA.

Gritzalis, D. (2014), "Insider threat prevention through Open Source Intelligence based on Online Social Networks", *13th European Conference on Cyber Warfare and Security*, Keynote address, Univ. of Peiraeus, Peiraeus: Greece.

Kassner, M. (2009). *Ghostnet: Why it's a big deal*, URL:http://www.techrepublic.com/blog/itsecurity/ghostnet-why-its-a-big-deal/1339/ (visited on 13/12/2015).

Panetta, L. (2012). *Defending the Nation from Cyber Attack, Business executives for National Security*, October 2012, USA, URL: http://www.bens.org/document.doc?id=188 (visited on 16/12/ 2015).

MacCrimmon K. (1973). *An Overview of Multiple Objective Decision Making*, In: J. Cochrane & M. Zeleny (Eds.), *Multiple Criteria Decision Making*, pp. 18-43, USA: Univ. of South Carolina Press.

Morth, T. (1998). "Considering our position: Viewing information warfare as a use of force prohibited by article 2(4) of UN Charter", *Case Western Reserve Journal of International Law*, 30, 567-600.

Pipyros, K., Mitrou, L. Gritzalis, D., Apostolopoulos, T. (2014). "Cyber Attack Evaluation Methodology", In: *Proc. of the 13th European Conference on Cyber Warfare and Security*, Univ. of Peiraeus, Peiraeus: Greece.

Pipyros, K., Mitrou, L., Gritzalis, D., Apostolopoulos, T. (2016). "A review of obstacles in applying international law rules in cyber warfare", *Information & Computer Security*, 24(1), 38-52.

Rao, R. (2013), "Decision Making in the Manufacturing Environment Using Graph Theory and Fuzzy Multiple Attribute Decision Making (MADM) Methods", vol. 2, 227-229, London: Springer.

Roscini, M. (2014). *Cyber operations and the use of force in international law*, Oxford: Oxford University Press.

Sang-Hun, C. (2013). *Computer Networks in South Korea are paralyzed in Cyber-attacks*, URL:http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes .html?pagewanted=all&_r=0 (visited on 10/10/2015).

Sanger, D. (2016). *Cyber-attacks Target ISIS in a New Line of Combat*, The New York Times, URL:http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0/ (visited on 30/05/2016).

Schmitt, M. (1999). "Computer Network Attack and the Use of Force in International Law: Thoughts on a normative framework", *Columbia Journal of Transnational Law*, 37, URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800 (visited on 30/06/2015).

Schmitt, M. (2011). "Cyber operations and the jus ad bellum revisited", *Villanova Law Review*, pp. 569-606, URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id_2184850 (visited on 1/07/2015).

Schmitt, M. (2013). "Classification of Cyber Conflict", *Journal of Conflict & Security Law*, 17(2), 245-260.

Schmitt, M. (2014). "Proxy wars in cyberspace: the evolving international law of attribution", *Fletcher Security Review*, 1(2) URL:https://ccdcoe.org/sites/default/files/multimedia/pdf/ c28a64_ 2fdf4e7945e9455cb8f8548c9d328ebe.pdf (visited on 30/10/2015).

Schmitt, M. (Ed.) (2013). *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press, URL: http://nuclearenergy.ir/wpcontent/uploads/2013/11/Tallinn _manual.pdf. (visited on 16/10/2015)

The Dept. of Defence Cyber Strategy, USA (2015), URL: http://www.defense.gov/Portals/1/features/ 2015/0415_cyber strategy/ Final_2015_DoD _CYBER_STRATEGY_for_web.pdf. (visited on 16/ 12/2015).

The Economist (2010). *Cyber war in the fifth domain, Are the mouse and the keyboard the new weapons of conflict?* URL: http://www.economist.com/node/16478792/ (visited on 31/08/2015).

Tikk, E., Kaska, K. and Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence (CCD CoE) Publications.

United Nations, *Draft articles on Responsibilities of States for Internationally Wrongful Acts,* 2001, URL: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. (visited on 16/ 12/2015).

United Nations and Statute of the International Court of Justice, *Universal Declaration of Human Rights*, URL: http://www.un.org/en/documents/udhr/ (visited on 14/08/2015).

Veenendaal, M., Kaska, K. and Brangetto, P. (2016). *Is NATO Ready to Cross the Rubicon on Cyber Defence?,* NATO Cooperative Cyber Defence Centre of Excellence, Estonia
URL: https://ccdcoe.org/publication-library.html (visited on 24/10/2015).

Virvilis, N. and Gritzalis, D. (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, pp. 248-254.

Virvilis, N. and Gritzalis, D. (2013). "Trusted computing vs advanced persistent threats: Can a defender win this game?", In: *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, IEEE Press, pp. 396-403, Italy.

Virvilis, N., Tsalis, N., Mylonas, A. and Gritzalis, D. (2015). "Security busters: Web browser security vs. suspicious sites", *Computers & Security*, 52, 90-105.

Zetter, K. (2010). *Google Hack Attack was Ultra Sophisticated*, New Details Show, URL: http://www.wired.com/threatlevel/2010/01/operation-aurora/#ixzz0deHCunGn (visited on 31/08/2015).