A CYBER ATTACK EVALUATION METHODOLOGY

Kosmas Pipyros[1], Lilian Mitrou[1,2], Dimitris Gritzalis[1], Theodore Apostolopoulos[1]

[1] University of Economics and Business, Athens, Greece
[2] University of the Aegean, Samos, Greece
pipyrosk@aueb.gr
l.mitrou@aegean.gr
dgrit@aueb.gr
tca@aueb.gr

ABSTRACT

Following the identification on an international basis of cyberspace as a new “domain of warfare”, it has become widely (though not fully) accepted that the traditional rules of International Humanitarian Law are also applicable to Computer Network Attacks (CNAs). Despite the fact that there has been considerable progress at the European and International level towards the development of National Cyber Security Strategies and the adoption of an effective comprehensive legal framework of prevention measures against cyber attacks, there is confusion regarding the application of these rules. More specifically, it has not been clarified: a) in which cases do cyber attacks constitute a ‘threat or use of force’ so that the prohibition of article 2(4) of the UN Charter can apply, b) in which cases do cyber attacks constitute a ‘threat to the peace, breach of the peace, or act of aggression’ 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 an “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.

The difficulty in applying the traditional rules of International Humanitarian Law to categorize 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 host country 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’.

The aim of this paper is to propose a model for detecting the effects of cyber attacks and for enabling their categorization on the basis of their type and intensity. The above method requires the identification of the Critical Information and Communication Infrastructures of each State and their ranking in terms of their intensity and seriousness.

Keywords: Cyber Warfare, Computer Network Attack (CNA), Information and Communication Systems and Technologies (ICT), Critical Infrastructures, International Humanitarian Law (IHL).

1. INTRODUCTION

The rapid development of Information and Communication Technologies (ICTs) over the last decades has contributed a lot to the advancement of humanity. The access of new technologies in every aspect of human life has extended to such a degree that, major public sector industries, such as National Security, Education, Government, Health, Public Safety, as well as sectors such as Nutrition, Energy, Economics and Transportation & Communication, are closely related to the new ICTs. Thus, information and communication systems and technologies are currently playing an important role in ensuring a State's proper functioning and the well-being of its citizens, and cyberspace, the common ground of all these, acts as the connecting link between them.

Although there is no universal definition of cyberspace one could adopt the definition proposed by the US Department of Defense Strategy for operating in cyberspace. This definition which focuses mainly on cyber security issues, states that cyberspace is defined as 'an interdependent and interrelated infrastructural IT network, including the internet, telecommunication networks, computer systems and the systems managing production processes and control in strategic sectors connected to national security'.[1] However, taking into consideration the widespread and growing use of social media one cannot overlook the fact that cyberspace is defined more by the social interactions involved rather than its technical implementations and that it is a domain that is becoming more and more a communication channel of information exchange between people.[2] For this reason cyberspace could also be defined as a system of exchange and processing of information (data), functioning in accordance with formal rules, legal regulations in use in the territories of particular countries, operating thanks to the connection of technical resources located on the territory of every single country.[3]

2. REAL LIFE CYBER INCIDENTS FROM THE PERSPECTIVE OF INTERNATIONAL LAW

The advances in ICTs go hand in hand with the first cyber-attack incidents that become more and more sophisticated and specialized with the passing of time. The first cyber incidents to be regarded of a military nature were those that emerged during the Kosovo era involving conflicts conducted by non state actors i.e. by the so-called 'patriotic hackers', who seemed however to act under the umbrella of the respective national governments. These types of conflict were characterized '…as the first war on the Internet, in recognition of not only the cyber-attacks but also the broader role played by the Internet, especially in the dissemination of information about the conflict'.[4]

[1] US Department of Defense Strategy for operating in Cyberspace (2011) [online] http://www.defense.gov/news/d20110714cyber.pdf.

[2] Morningstar, C. and Farmer, F. (2003) *The Lessons of Lucas film's Habitat: The New Media Reader*, The MIT Press, Cambridge and London.

[3] Nowak, A. (2013) "Cyberspace as a new quality of hazards", *NDU Scientific Quarterly*, no 3(92), pp 5-25.

[4] Berson, T. and Denning, D. (2011) "Cyberwarfare" [online] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06029359.

In terms of wide range attacks, the leading one took place in April 2007 in Estonia. That cyber attack was directed against Estonia's critical ICTs leading to the deregulation of the country's financial system and threatening its national security.[5] The Estonia attack was followed by a number of large-scale cyber incidents such as the 'hit' against Georgia, following the increase in intensity of the political conflict between Georgia and Russia.[6] That assault was based mainly on the launching of Distributed Denial of Service (DDOS) attacks against the country's information infrastructure and led to the defacement of the country's public websites. The aforementioned aggressions as well as the persistent attacks on U.S ('Operation Aurora',[7] 'Ghostnet'[8] and DDoS attacks against the New York Stock Exchange)[9], Iran (the recent sabotage against Iran's nuclear program with the 'Stuxnet' computer worm)[10,11] and South Korea (aggressions that took place in 2013 and paralyzed three TV stations and part of the country's banking system)[12] clearly demonstrate the fact that cyber warfare is a phenomenon that is today more relevant than ever.[13] At the same time, the increasing number of cyber events reported on a regular basis has transformed 'Cyberspace' into a battlefield, bringing to light 'Cyber warfare' as "the fifth domain or warfare" after land, sea, air and space.[14,15] In parallel, all these incidents brought about a series of discussions over the issue of Computer Network Attacks (CNAs) and their eventual political, economical

[5] Tikk, E., Kaska, K. and Vihul, L. (2010) International Cyber Incidents: Legal Considerations, Cooperative Cyber Defense Center of Excellence (CCD COE), Tallinn.

[6] Bumgarner, J. and Borg, S. (2009) "*Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008"*, *A US-CCU Special Report.*

[7] Zetter, K. (2010) "*Google Hack Attack was Ultra Sophisticated, New Details Show"* [online] http://www.wired.com/threatlevel/2010/01/operation-aurora/#ixzz0deHCunGn

[8] Kassner, M. (2009) "*Ghostnet: Why it's a big deal"* [online] http://www.techrepublic.com/blog/it-security/ghostnet-why-its-a-big-deal/1339/

[9] Robert, P. (2012) "*Leading US banks targeted in DDoS attacks"*, [online] http://nakedsecurity.sophos.com/2012/09/27/banks-targeted-ddos-attacks/

[10] Farwell, J. and Rohozinski, R. (2011) "*Stuxnet and the Future of Cyber War"*, 53(1) Survival: Global Politics and Strategy [online], http://www.iiss.org/en/publications/survival/sections/2011-2760/survival--global-politics-and-strategy-february-march-2011-f7f0/53-1-05-farwell-and-rohozinski-f587

[11] Virvilis, N. and Gritzalis, D. (2013) "The big four-What we did wrong in advanced Persistent Threat detection?", Proc. of the 8th International Conference on Availability, Reliability and Security, Germany, September.

[12] Sang-Hun, Ch. (2013) "*Computer Networks in South Korea are paralyzed in Cyber attacks"* [online] http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=0

[13] Virvilis, N., Gritzalis, D., and Apostolopoulos, T. (2013) "*Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?*", Proc. of the 10th IEEE International Conference on Autonomic and Trusted Computing, Italy, December.

[14] Lynn, W. (2010) "*Defending a New Domain: The Pentagon's Cyberstrategy*", [online], http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[15] The Economist (2010) "*Cyberwar: War in the fifth domain"* [online] http://www.economist.com/node/16478792

and social impact on the host State of a Cyber attack but also the international impact regarding this new kind of warfare and its consequences in the global strategic environment.

Following that, the critical question that has arisen is whether cyber attack incidents should be met by employing the traditional international law rules in force, or whether they should be considered as something completely different, asking for the introduction of new legislation – new agreements on an international/multinational level. Despite the fact that Russia, China and other countries favor an international treaty, similar to those agreed on chemical weapons, and have pushed for such an approach to regulating cyberspace, the U.S and the EU have repeatedly resisted proposals for an international treaty.[16] As a matter of fact, despite the opposing viewpoints on the subject according to which 'cyber space is a new military domain and must be understood in its own terms',[17] it has become widely accepted (in EU and NATO members) that the traditional rules of International Law apply also to Computer Network Attacks (CNAs). Besides, all recent institutional documents at European and International level share the same view.

More specifically, both at the European and the International level, the prevailing view is that international law suffices to handle issues relating to cyberspace operations. In fact a number of official papers confirm this fact. For example, the International Group of Experts[18] involved in the production of "the Manual of the International Law applicable to Cyber Warfare",[19] a project launched in the hope of bringing some degree of clarity to the legal issues surrounding cyber operations, rejects any characterization of cyberspace as a separate domain calling for its handling by a distinct body of law. On the contrary, the International Group of Experts unanimously has come to the conclusion that the general principles of international law should apply also to cyberspace.[20] Similarly, at the European level the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, published, on February 2013, a proposal for a cyber security strategy, followed by a draft directive, which aimed to address the issue of Network and Information Security (NIS) and which highlighted the fact that "the EU does not call for the creation of new international legal instruments for cyber issues" and that "the legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online".[21] The same text, in another point, resumes that "if armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand".[22] This same view was reflected as early as 2011, in the U.S International Strategy for Cyberspace where it was clearly stated that 'the development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international

[16] O'Connell, M. (2012) Cyber security without Cyber War, Journal of Conflict & Security Law, Oxford University Press.

[17] Libicki, M. (2009) Cyber deterrence and cyber war, The Rand Corporation.

[18] A Group of distinguished International Law practitioners and scholars.

[19] From now on 'Tallinn Manual'.

[20] Tallinn Manual, p 19.

[21] European Commission, Cyber security Strategy of the European Union: An Open Safe and Secure Cyberspace -JOINfinal-, p 15.

[22] European Commission, Cyber security Strategy of the European Union: An Open Safe and Secure Cyberspace -JOINfinal-, p 16.

norms obsolete. Long-standing international norms guiding State behavior - in times of peace and conflict - also apply in cyberspace".[23]

Moreover, the aforementioned Tallinn Manual, based on article 2(4) of the United Nations Charter notes in its Rule 10, entitled "Prohibition of the use of force", 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."[24]

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, ie. 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'.[25] 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 United Nations Charter, Rule 13 of the Tallinn Manual entitled "Self-Defense 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".[26] However, in this case also, it's not clear in which occasions cyber attacks meet the scale and effects requirements so that they can be 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. SCALE AND EFFECTS ANALYSIS

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 the 'Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America)', 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 that 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".[27] More specifically, the International Court of Justice noted the need to 'distinguish

[23] The White *House* (2011) "*International Strategy for Cyberspace: Prosperity, Security and Openess in a Networked World*" [online] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cybers pace.pdf

[24] Tallinn Manual, p 45.

[25] Tallinn Manual, p 47.

[26] Tallinn Manual, p 53.

[27] Westlaw, 1986 I.C.J. 14, p 84.

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 United Nations Charter does not provide any criteria for determining when an act amounts to a ‘use of force’, the International Group of Experts 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 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”, namely ‘acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services’.[28]

Taking thus 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 the adoption of an approach (following Schmitt’s consequence-based approach),[29] that aims to identify, in an objective way, 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 it 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’, with corresponding cyber operations that meet the ‘scale and effects’ requirements, will be the outcome of the evaluation of a number of non exclusive criteria (factors) based on a case-by-case assessment. These criteria (factors) are ‘severity’ (severity of attacks), ‘immediacy’ (the speed with which consequences manifest themselves), ‘directness’ (the causal relation between a cyber attack and its consequences), ‘invasiveness’ (the degree to which a cyber operation interferes with the targeted systems), ‘measurability of the effects’, ‘military character of the cyber operation’, ‘extent of State involvement’ and ‘presumptive legality’ (acts not expressly prohibited by international law). Nevertheless, it should be kept in mind that, as the International Group of Experts have clearly clarified, these factors cannot be considered as formal legal criteria.

[28] Tallinn Manual, p 55.

[29] Schmitt, M. (1999) “*Computer Network Attack and the Use of Force in International Law: Thoughts on a* normative *framework”*, 37 CJTL [online] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800.

4. A CYBER ATTACK EVALUATION METHODOLOGY

As it can been understood, the characterization and categorization of cyber attacks depends largely on the size of their consequences. In other words, the categorization of this type of attacks lies heavily on their impact level both in terms of loss of human lives and in terms of destruction of critical infrastructures. So, the degree of the visible as well as the long-term effects of a cyber attack constitute a critical factor for its categorization and the greater the degree of impact of a cyber attack the more the chances to be characterized as a 'use of force', or even worst, as an '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 cyber attack. Unfortunately, as it has already become apparent, the relevant criteria proposed by the International Group of Experts have failed to accurately identify the precise extent of impact of a cyber attack, since its effects are often not readily visible on the short hand and the measurability of the effects of a cyber attack is frequently a matter of subjective interpretation. If the impact level of cyber attacks could be determined through the use of qualitative and quantitative criteria, it would be possibly much easier to classify and categorize them based on the principles of International law.

On the other hand, one can easily notice that the same impact factors proposed by the International Group of Experts for the categorization and characterization of cyber attacks are also employed as criteria in risk criticality analysis methodologies to prioritize assets and infrastructures. For example, at the European level, the Council Directive 2008/114/EC of 8 December 2008 'on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection'[30], following a relevant European Commission Communication,[31] identified the following criteria as the minimum set of criteria that should be considered by member states when attempting to assess their critical infrastructures: (i) public safety–including issues such as population affected, loss of life, medical illness, serious injury, evacuation, (ii) economic effect – which takes into consideration the GDP effect, the significance of economic loss and/or the degradation of products or services, (iii) environmental effect – i.e. effect on the public and the surrounding environment, (iv) interdependency – which has to do with interdependencies between critical infrastructure elements, (v) political effects – that is, confidence in the government and (vi) psychological effects – i.e. psychological effects on the population. The evaluation of these criteria takes place in terms of their scope (local, regional, national and international) and time (during and after the incident).[32]

Respectively, at the international level, the U.S. National Infrastructure Protection Plan identifies the following criteria for evaluating consequences: (i) public health and safety – including their effect on human life and physical well-being, (ii) economic – which takes into consideration direct and indirect economic losses (iii) psychological – i.e. their effect on public morale and the degree of confidence of the people in economic and political institutions and (iv) governance/mission – which related to the effect on

[30] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection OJ L 345/75.

[31] European Commission, 'On a European Programme for Critical Infrastructure Protection' (Communication) COM (2006) 786 final.

[32] Theoharidou, M., Kotzanikolaou, P., and Gritzalis, D. (2009) "*Risk-based criticality analysis",* Critical Infrastructure Protection III, Springer, Vol. 311 pp 35-49.

the ability of the government or industry to maintain order, deliver essential services, ensure public health and safety and carry out national security – related missions.[33]

From everything mentioned above, it becomes clear that there is a direct link between cyber attacks and the corresponding methods used for assessing critical infrastructure and networks (ICTs) since in both cases the impact factors employed for their characterization are almost the same. In addition, the evaluation criteria used for assessing critical ICTs, are focused more on evaluating risks related to external impacts that is, impacts associated with socioeconomic consequences and their effect on citizens, since they are directly linked to the critical infrastructures affected per se and indirectly associated to the implications of the collapse or degradation of these critical ICTs for the well being of the citizens. This approach comes in contrast to the traditional risk analysis methodologies that focus more on the implications of the collapse or deterioration of infrastructure in the respective department or agency that relates to it (internal impacts), rather than on the external impacts of this collapse or deterioration to the citizens.

Based on everything mentioned above, one could proceed to an assessment of cyber attacks by adopting risk-based criticality analysis methodologies. A case in point is the generic risk-based criticality analysis methodology proposed by Theoharidou et al.[34] by which, a detailed list of impact criteria is presented for assessing the criticality level of infrastructures. What differentiates this method from traditional risk analysis methodologies is the fact that it assumes the same societal and sector-based impact factors used by the International Group of Experts for characterizing and assessing the intensity of cyber attacks, allowing thus the parallelism and the adoption of the same evaluation criteria for assessing cyber attacks.

This criticality analysis methodology, whose primary role is to be used as a base for assessing risk associated with critical ICTs, can also serve as a scale for measuring the intensity of cyber attacks in order to enable a quantification of the ‘scale and effect’ criteria, using qualitative and quantitative variables such as the ones recommended by the International Group of Experts in the Tallinn Manual, and possible adopting other criteria, so that it can become easier to identify when such acts verge on the so-called ‘use of force’ standard, which is used for determining whether or not a State has violated Article 2(4) of the United Nations Charter and the related customary international law prohibition. Furthermore, the same methodology could be used to indicate whether a cyber operation comes to the level of being characterized as a ‘use of force’ or as an ‘armed attack’ allowing thus a UN Member State to respond by exercising its legitimate right of self-defense according to Article 51 of the UN Charter. Similarly, the above method could serve as a scale for the Security Council to decide when a cyber attack constitutes ´threat to the peace, breach of the peace or act of aggression´, so that the required measures to restore international peace and security under Article 42 of the UN Charter can be adopted. In other words, the adoption of the criticality risk analysis methodology can serve as a means for estimating the impact of a cyber attack in the host country and in the international environment.

Based on everything mentioned above, one can draw the conclusion that the discussed evaluation methodology, using as a reference point the above mentioned criteria, could be used as a method for stressing areas where there is uncertainty or disagreement in an 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 systems that may constitute a component of a critical infrastructure.

[33] U.S. Department of Homeland Security, National Infrastructure Protection Plan 2009, Washington, DC.

[34] Theoharidou, M., Kotzanikolaou, P. and Gritzalis, D. (2009) ““*Risk-based criticality analysis”,* Critical Infrastructure Protection III, Springer, Vol. 311 pp 35-49..

Moreover, taking a reverse approach to this subject and trying to proceed, in advance, to the identification of the critical ICTs and their ranking in terms of their intensity and seriousness, each State could create an evaluation system of its critical information and communication infrastructures at a national level, possibly through linking them to its respective national cyber security strategy, and then attempt to extend this system at a European and international level. It is self-evident that such a wide system, based on specific evaluation criteria, would include a commonly accepted bundle of critical infrastructures and services, the potential destruction or impairment of which could be characterized, depending on the severity of the attack and the corresponding parameterization of its impact to the community, as a ‘threat to the peace, breach of the peace, or act of aggression’. Consequently it could fall under the categorization of a ‘use of force’ or of an ‘armed attack’, giving thus the right of self-defense to the State under attack.

Our future work will be focused on a more accurate approach of the above mentioned cyber attack methodology in order to determine and evaluate the impact factors of a cyber attack on the basis of their type and intensity, for enabling their categorization under the principles of International Law.

References

1. Barmpatsalou, K., Damopoulos, D., Kambourakis, and G., Katos, V. (2013) “*A critical review of 7 years of Mobile Device Forensics*”, Digital Investigation [online] http://www.researchgate.net/publication/258273700_A_critical_review_of_7_years_of_Mobile_Device_Forensics

2. Berson, T. and Denning, D. (2011) “Cyberwarfare” [online] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06029359

3. Bumgarner, J. and Borg, S. (2009) “*Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008”*, *A US-CCU Special Report.*

4. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection OJ L 345/75.

5. European Commission (2013) Cyber security Strategy of the European Union: An Open Safe and Secure Cyberspace, JOIN final.

6. European Commission (2006) On a European Programme for Critical Infrastructure Protection COM 786 final.

7. Farwell, J. and Rohozinski, R. (2011) “*Stuxnet and the Future of Cyber War”*, 53(1) Survival: Global Politics and Strategy [online], http://www.iiss.org/en/publications/survival/sections/2011-2760/survival--global-politics-and-strategy-february-march-2011-f7f0/53-1-05-farwell-and-rohozinski-f587.

8. Libicki, M. (2009) Cyber deterrence and cyber war, The Rand Corporation.

9. Lynn, W. (2010) “*Defending a New Domain: The Pentagon’s Cyberstrategy*” [online] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

10. Morningstar, C., and Farmer, F. (2003) *The Lessons of Lucas film's Habitat: The New Media Reader*, The MIT Press, Cambridge and London.

11. Mylonas, A., Kastania, A., and Gritzalis, D. (2013) “*Delegate the smartphone user? Security awareness in smartphone platforms*”, Computers & Security, Vol. 34, pp. 47-66.

12. Mylonas, A., Meletiadis, V., Mitrou, L., and Gritzalis, D. (2013) “*Smartphone sensor data as digital evidence*”, Computers & Security (Special Issue: Cybercrime in the Digital Economy), Vol. 38, pp. 51-75.

13. Schmitt, M. (1999) “*Computer Network Attack and the Use of Force in International Law: Thoughts on a* normative framework*”*, 37 CJTL [online] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800.

14. The Economist (2010) “*Cyberwar: War in the fifth domain*” [online] http://www.economist.com/node/16478792.

15. The White House (2011) International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World.

16. The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), General Editor M. Schmitt (2012) Tallinn Manual on International Law Applicable to Cyber Warfare.

17. Theoharidou, M., Kotzanikolaou, P., and Gritzalis, D. (2009) “Risk-based criticality analysis“, Critical Infrastructure Protection III, Springer, Vol. 311, pp. 35-49.

18. Tikk, E., Kaska, K. and Vihul, L. (2010) International Cyber Incidents: Legal Considerations, Cooperative Cyber Defense Center of Excellence (CCD COE), Tallinn.

19. U.S. Department of Homeland Security, National Infrastructure Protection Plan 2009, Washington, DC.

20. Virvilis, N., and Gritzalis, D. (2013) “The big four - What we did wrong in advanced Persistent Threat detection?”, Proc. of the 8th International Conference on Availability, Reliability and Security, Germany, September.

21. Virvilis, N., Gritzalis, D., and Apostolopoulos, T. (2013) “*Trusted Computing vs. Advanced Persistent Threats: Can a* defender *win this game?*”, Proc. of the 10th IEEE International Conference on Autonomic and Trusted Computing, Italy, December.

22. Westlaw, 1986 I.C.J. 14