LEGAL CHALLENGES IN SECURING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP): AN AMERICAN EMPATHY

Written by ***Irfan Ali Thanvi***

PHD Student, AIKOL-IIUM Gombak, Malaysia

DOI: doi.org/10.55662/CYLR.2023.2101

ABSTRACT

Among the main achievements of the CIIP policy are establishment of the European Forum for Member States and of the European Public-Private Partnership for Resilience; carrying out of pan-European exercises (Cyber Europe 2010 and 2012); adoption, by ENISA, of a minimum set of baseline capabilities and services and related policy recommendations for National/Governmental Computer Emergency Response Teams (CERTs) to function effectively.

In some cases, the Cybersecurity strategy is taking forward such actions (for example, in carrying out pan-European exercises). In other cases, the voluntary approach of the CIIP policy would be strengthened by the proposal for a Directive on network and information security, which would require the Member States to put in place a minimum level of capabilities at national level and to co-operate cross-border. This paper alludes to the legal challenges confronted by the authorities' in implementing them.

Keywords: Cyber-warfare, Cyber-attack, Cyber law, CIIP

INTRODUCTION

The identification of Critical Information Infrastructure Protection (CIIP) priorities and strategies is a complex but imperative topic for Governments. States and members of society depend on the proper functioning of their Critical Infrastructure (CI) services such as energy supply, telecommunications, financial systems, drinking water and governmental services. In turn, these CIs often critically depend on the proper functioning of Critical Information Infrastructures (CII). CIs are widely defined as: *"Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences".*[i] Critical Infrastructure Protection is also defined as: *"All activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability."*[ii]

Ever since March 30th, 2009, the European Commission adopted a Communication on Critical Information Infrastructure protection (CIIP) focusing on the protection of Europe from cyber disruptions by enhancing security and resilience. The Communication launched an action plan, also involving Member States and the private sector. It is based on five pillars:

a) preparedness and prevention,
b) detection and response,
c) mitigation and recovery,
d) international cooperation and
e) Criteria for European Critical Infrastructures in the field of ICT.[iii]

Two years later, in March 2011, the Commission took stock of the results achieved that far and announced follow-up actions in the Communication on CIIP on "Achievements and next steps: towards global cyber-security"[iv]. This Communication concluded that purely national approaches to tackling security and resilience challenges are not sufficient, and that Europe should continue its efforts to build a coherent and cooperative approach across the EU.

In its Conclusions on CIIP of 27th of May 2011,, the Council of the European Union stressed the pressing need to make ICT systems and networks resilient and secure to all possible disruptions, whether accidental or intentional; to develop across the Union a high level of preparedness, security and resilience capabilities and to upgrade technical competences to help Europe face the challenge of network and information infrastructure protection; and to foster Member States' cooperation by developing incident cooperation mechanisms between them.

Two Ministerial Conferences on CIIP took place respectively in Tallinn in 2009 and in Beglamoured in 2011[v]. Tallinn started the debate on the general direction of the European efforts towards an increased network and information security for the future. Beglamoured provided a forum to take stock of progress, assess lessons learnt and discuss the challenges ahead and next steps. It also investigated the way forward to engaging all stakeholders and in particular the private sector.

The European Parliament Resolution of 12th of June 2012 on “Critical Information Infrastructure Protection: towards global cyber-security”, broadly endorsed the 2011 Communication and made recommendations to the Commission for the way forward. Many of these recommendations have been taken on board in the Cybersecurity strategy and proposal for a Directive on network and information security published in 2013.[vi]

THE CIIP UNIT IN PRACTICE: THE LEGAL CHALLENGES[vii]

Critical Information Infrastructure Protection (CIIP) is universally acknowledged as a vital component of national security policy. For the sake of protection of their critical infrastructure, some countries (in particular, the Western European and North American states) have established sophisticated and comprehensive CIIP organizations and systems, involving governmental agencies from different ministries, with a variety of initiatives. These programs try to cover all the different facets of CIIP, ranging from reducing vulnerabilities and fighting computer crime to defense against cyber-terrorism. However, due to their complexity and country context, these CIIP models are not necessarily applicable to other countries. Hitherto, many existing solutions are resource-intensive and therefore not suitable for most countries in the world. For states that are starting to develop their own CIIP policy, it is often difficult to identify best practices and good examples. Many of these states may not have the same resources as the industrialized nations and cannot build complex and comprehensive organizations; rather, they can only focus on implementing only the most urgent measures. This paper provides a generic framework to help these countries to determine their response to the challenges of CIIP. It draws on different existing CIIP models the Swiss CIIP model, to suggest a functional model for a CIIP unit that can promote collaboration between existing stakeholders to protect the state's critical infrastructure and services. Over the last couple of years, the Swiss Reporting and Analysis Center for Information Assurance (MELANI) has proved a good example of a small, but effective CIIP organization.[viii] The generic model for CIIP presented here is not a cure-all; instead, this paper offers a few building-blocks for a functional CIIP unit. By concentrating on top priorities, cooperation between various stakeholders, flexibility and adaptability, relatively inexpensive solutions can be developed to meet country-specific needs. As the structure of the CIIP unit must be designed in relation to its essential tasks, identifying the main duties and responsibilities is vital.

Although we have described the structure and organization of the CIIP unit in this section, we would be polite to a fault to evade the influence of the European Laws on the American legislative, primarily because, Europe experienced the Estonia Cyber Attack and promulgated her laws through the EU Parliament. The USA, on the other hand has not to date experienced, such a disaster, but she is vulnerable to be exposed to such an attack in the future. Hitherto, in this Section we examine how the unit could work in practice using a case study to illustrate the internal and external processes that are triggered by incidents. The case study presented in the following is fictitious and represents an ideal response; the attack (a phishing attack, currently one of the most frequent types of targeted attacks) and the reaction of the CIIP unit are described based on realistic assumptions. The phases of detection, incident response and follow-up are shown, albeit this case study describes only one of many possible scenarios.

Phase 1: Detection of the Attack

The case study assumes of a phishing attack on a bank that is a member of the Closed Customer Base (CCB). Because such an attack may be detected in different ways, the detection process is described in three different scenarios. • Scenario 1: the bank reports the attack. In this scenario, the affected bank directly notifies the CIIP unit via its representative(s) and seeks assistance. The bank may have detected the attack either during a routine checkup or because it has investigated irregularities, or after having been notified by its clients. In this scenario, the CIIP unit is not directly involved in detection. It may verify the suspicion by asking the CERT team and the analysts of the Situation Center to investigate; otherwise, it may proceed immediately to incident response. • Scenario 2: a client of the bank reports the attack. A key feature of phishing attacks is their focus on the clients of a bank as the weakest link in the chain of defense. Thus, clients are often the first to detect the attack. In scenario 2, clients who received suspicious e-mails in which they were asked to indicate their passwords contact the cyber-crime unit of the police. This unit passes that information to the CIIP unit, which analyzes the information and informs the affected bank. In this scenario, the reporting of incidents by citizens (via the cyber-crime unit) results in the early detection of attacks. Thus, in this scenario, the CIIP unit acts as central platform for information exchange and makes sure that imperative information is conveyed in a timely manner to the appropriate people. • Scenario 3: the attack is detected by investigations of the CIIP unit. Both the CERT team and the analysts of the Situation Center are constantly monitoring critical indicators. In addition, they have access to a worldwide network of contacts in other CERT teams and analysts. Thus, in scenario 3, the CIIP unit detects the attack due to its own investigations or to information from various contacts. The CIIP unit should verify the findings and notify the target as soon as possible. In this scenario, the CIIP unit plays a leading part in the whole process of detection. These three scenarios indicate the importance of the national and international network and of both customer bases. In order to detect an attack as early as possible, the CIIP unit needs to remain vigilant in every direction. The process of incident response and the follow-up is the same, however, regardless of how the attack was detected.

Phase 2: Incident Response

Since time is a crucial factor in countering attacks, the CIIP unit must initiate incident response measures promptly. Attacks are carried out at any time; therefore, the CIIP unit must be ready to respond to incidents at night or over weekends. For the purposes of our example, it is supposed that the phishing-attack is detected by the bank (according to scenario 1) on a Sunday morning. In the afternoon, the bank alerts the CIIP unit via the 24/7 helpdesk. Due to its prior close cooperation with the responsible bank staff, the CIIP unit can be sure that the alert is justified. Thus, the incident response process is initiated immediately. First of all, further damage must be avoided. The CERT team – informed by the help desk – begins to take down the redirect servers. The major redirect servers are placed in other countries; therefore, the CERT team uses its contacts with other international CERTs. Despite its well-established international contacts, taking down all redirect servers requires several days. In the meantime, the CIIP unit tries to alleviate the consequences of the phishing attack by filtering the phishing mails. In order to set up such filters, contacts in the telecommunication sector are activated. Since the scenario of phishing attacks has recently been discussed in workshops and was part of an exercise, the partners of the telecommunication sector are familiar to the problem. In close collaboration with the CERT team, the filters are installed only a few hours after the detection of the attack. From the start of the incident response phase, the Situation Center keeps the affected bank informed about all measures taken. With the consent of the target, it also informs the other members of the financial sector about the nature of the phishing attack in order to allow them to take precautions. In addition, a staff member of the Situation Center briefs the public on phishing in a news broadcast on Sunday evening, so that people who read their e-mails on Monday morning will not be taken in by the phishing attack. The incident response phase ends three days later, when the CERT team reports that due to the close collaboration with a CERT team in another country, the major redirect server has been taken down. The immediate threat of the attack is now eliminated, and the follow-up phase starts.

Phase 3: Follow-up Treatments

Learning from incidents is a key element of future protection measures. In order to gain insights into future trends, the CERT team analyzes the technical characteristics of the attack and discusses the attack with national and international experts. Meanwhile, the analysts of the Situation Center draw up a final report of the incident in cooperation with the affected bank. Again, with the consent of the target, all lessons learned are made available to other members of the Closed Customer Base. For the target, the most imperative follow-up treatment is the prosecution of the perpetrators of the attack. Since the bank may lack experience or resources for the prosecution of Internet frauds, it appreciates the advice supplied by the CIIP unit. The CIIP unit cannot take charge of the prosecution itself, but it refers the target to the responsible authorities. Of course, the CIIP unit supplies all results of its investigations (e.g., the location of the redirect server) to the law enforcement agency.

Summary of the Proceedings

As follow-up efforts are not very time-consuming, the basic work with regard to the phishing attack may be completed within several days. However, this is only possible if the CIIP unit cooperates with various national and international partners and if the CERT team and the Situation Center share the work efficiently. The fictitious case study presented here illustrates an ideal case – in reality, delays and other problems can occur. Nevertheless, the case study offers valuable insights as to how the CIIP unit could work in practice.

INFORMATION SHARING

Albeit the sharing of information has been the centerpiece of both the government's and the private sector's efforts over the past several years to protect critical information systems, most information sharing still occurs through informal channels. Fundamental questions persist about who should share what information, when, how, why, and with whom. One reason for the lack of progress, according to private industry representatives, has been the lack of clarity regarding the benefits and associated liabilities in sharing information within and between industry sectors and with the government. For example, information sharing could lead to allegations of price fixing, restraint of trade, or systematic discrimination against certain customers; it could raise privacy concerns, expose proprietary corporate secrets, or reveal weaknesses and vulnerabilities that erode consumer confidence and invite hackers. Overcoming these concerns requires an informed position on the existing legal framework—an imperfect understanding of the law is both excuse and explanation for some observed limits to sharing.

Freedom of Information Act

Many private sector companies believe that proprietary CIIP-related information shared with federal government entities may be disclosed to third parties under the Freedom of Information Act (FOIA). Therefore, private sector companies have proposed amending FOIA to create a new exemption that would protect critical infrastructure information from disclosure. Opponents of such an exemption argue that the case law and agency interpretations demonstrate that the information—that is, information that is a trade secret or information that is commercial or financial, obtained from a person, and privileged or confidential—already is protected under the existing FOIA Exemption 4. Changing the FOIA, opponents argue, could upset the existing FOIA framework and open up the possibility for new litigation. Albeit the Homeland Security Act of 2002 did feature such an exemption, the fundamental issues remain.

A key problem is whether the federal government has the processes in place to protect information that should be protected under existing FOIA rules from inappropriate or accidental disclosure. The government may need to strengthen its formal controls on disclosure of information under FOIA, disclose to the private sector what those controls entail, and strengthen its programs to better educate federal agency employees (who respond to the FOIA requests) about the types of information that cannot be released under existing law.

Antitrust Law

An additional concern of many in the private sector is that sharing CIIP-related data with competitors could be viewed as a violation of the provisions of the Sherman Antitrust Act. As a result, many in the private sector have called for a new antitrust exemption. Opponents argue that a new exemption is not needed to protect firms from allegations of anticompetitive behavior. They suggest that firms can obtain informal legal advice from antitrust experts or formal advice from the Department of Justice—in the form of a business review letter—on whether its proposed future conduct would be viewed as a violation of the antitrust laws. In addition, an exemption would create a new body of law that would upset 30 years of case history and lead to years of new litigation. Hence, the American Bar Association opposes new antitrust exemptions. Like FOIA, the existing antitrust law does not prevent the private sector from sharing critical infrastructure information. However, because official reviews of proposed information sharing activities require time and money to obtain, the use of such reviews may be a barrier to the types of ad hoc information sharing that are most likely to uncover well-planned attacks on the infrastructure. Also, as with FOIA, there are persistent perception problems related to what may be deemed permissible and what may be deemed illegal.

LIABILITY

Experts observe that criminal law alone is not sufficient to deter hackers and prevent cybercrime; civil liability is necessary to ensure proper disincentives are in place to deter would-be cybercriminals. Ideally, civil liability allows a victim to recover losses from third parties if such parties were negligent or engaged in intentional misconduct and if such negligence or misconduct was the proximate cause of the loss. Because contract law does not provide an adequate remedy for third parties that have no privacy of contract, many experts have suggested the use of tort law as a model for computer-related cases. Proponents of tort liability argue that companies that control the computer networks are in the best position to implement appropriate security measures. If a company knows or has reason to know that its computer network is being used to cause harm, and it has the capacity to stop such harm from occurring, the company could be subject to liability if it does not take some corrective action. The applicability of tort law and the potential for civil lawsuits and monetary damages could encourage companies to invest in computer security measures. Debate continues in the private sector on whether there is a legal duty on the part of the company to secure its critical information infrastructure.[ix]

THE WAY FORWARD

The law, which is mainly a tool for implementing policy, does not exist in a vacuum. The legal framework for critical information infrastructure protection must be considered in the larger context of the business, social, and technical environment. Phil Reitinger, former deputy chief of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, argues that critical information infrastructure requires a multidisciplinary response. First, he suggests, we need technical solutions. Vendors must produce more secure products, and systems and customers must demand and implement better security. Second, we need management solutions. Companies must adopt and share best practices. The third approach recommended by Mr. Reitinger is to develop public education efforts to help all users better understand computer ethics (just as throwing a stone through a neighbor's window is wrong, so is breaking into someone else's computer system). Reducing nuisance attacks will allow government to focus resources on the greater threat. Finally, he proposes that we need knowledge solutions.[x] The private sector and law enforcement must gather and share information about threats, vulnerabilities, and remedies. He argues, “[w]e have got to figure out how we can spread the information and better secure systems while protecting privacy and not increasing the threat.” The highly publicized distributed denial-of-service attacks and worm incidents of 2000-2001 were seen as costly to victims, whose attention to Y2K had already underscored dependence on the information infrastructure. Thefts of or damage to intellectual property also have been growing for corporations.[xi] Against this backdrop, the events of September 11 heightened awareness and concern, and they spurred consideration of enhanced communication and coordination at three levels—within enterprises, within and among industries, and between industry and government—to respond to threats to infrastructure. A lingering challenge is how to achieve a greater understanding of the problem and possible solutions in smaller companies, particularly those that cannot afford an information technology support staff. Small businesses often are not aware that they need better computer security than what they have—if they have any at all. Frederick R. Chang, president and CEO of SBC Technology Resources, Inc., argues that the convergence of the voice and data networks compounds the problem and suggests possible solutions. The new awareness extends to an understanding that the practices that have helped companies to thrive, meticulously towards the betterment of the society. Plausible solutions have brought about significant development in awareness, R&D, technological advancement, and incredible realms of Artificial Intelligence.

CONCLUSION

Albeit the necessity of CIIP is practically acknowledged, many countries have not yet established a dedicated organizational unit. Hitherto, responsibility is scattered across organization within the government’s nomenclature. Hitherto, several private entities are involved. Since all of these entities are trying to shape the topic according to their interests, there is a danger of fragmentation. In order to counteract this danger, some countries have established sophisticated CIIP organizations. Unfortunately, these concepts may be less applicable to other countries, as they are often associated with high costs. This generic framework has thus sought to offer building blocks for a national CIIP unit that is able to achieve the demanding tasks of CIIP, without consuming too many resources. The following features are key elements of such a unit:

• With regard to the range of potential tasks, the CIIP unit should clearly define its responsibility. Its essential tasks are prevention and early warning, detection, reaction, and crisis management.

• The CIIP unit must cooperate with all relevant stakeholders of CIIP. It should be designed as a partnership involving a well-established government agency, a team of analysts from the intelligence services (Situation Center) and a center of technical expertise (CERT).

• The CIIP unit must be nationally and internationally connected. All partners should contribute their networks to the partnership. The CIIP unit can only act effectively with the help of various partners.[xii]

• The establishment of Public-Private Partnerships with the operators of CII, based on strong mutual trust, is essential for the success of the CIIP unit. In order to reduce vulnerabilities, information and experiences need to be shared. However, information-sharing in the area of information security is very sensitive for private firms. Thus, clear and strict rules of conduct (e.g., concerning the classification and circulation of information) is a vital for the success of any Public-Private Partnership.

• The CIIP unit should also address SMEs and private users, but cannot be responsible for the general information security of the country.

BIBILIOGRAPHY

ABELE-WIGERT, ISABELLE AND MYRIAM DUNN (2006), “INTERNATIONAL CIIP HANDBOOK 2006, VOL. I: AN INVENTORY

OF 20 NATIONAL AND 6 INTERNATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES” (ZURICH: CENTER FOR

SECURITY STUDIES).

AMITAI, AVIRAM (2005): “NETWORK RESPONSES TO NETWORK THREATS, “THE EVOLUTION INTO PRIVATE CYBERSECURITY ASSOCIATIONS”, IN GRADY, MARK AND FRANCESCO PARISI

(EDS.), “THE LAW AND ECONOMICS OF CYBERSECURITY” (CAMBRIDGE: CAMBRIDGE UNIVERSITY PRESS), PP. 143–92.

AMITAI, AVIRAM AND AVISHALOM TOR (2003), “OVERCOMING IMPEDIMENTS TO INFORMATION SHARING”, ALABAMA

LAW REVIEW, 55, PP. 231–79.

ANDERSSON, JAN J. AND ANDREAS MALM (2006), “PUBLIC-PRIVATE PARTNERSHIPS AND THE CHALLENGE OF CRITICAL

INFRASTRUCTURE PROTECTION”, IN DUNN, MYRIAM AND VICTOR MAUER (EDS.), “INTERNATIONAL CIIP HANDBOOK 2006,

VOL. II: ANALYZING ISSUES, CHALLENGES, AND PROSPECTS” (ZURICH: CENTER FOR SECURITY STUDIES), PP. 139–68.

BRANSCOMB, LEWIS M. AND ERWANN O. MICHEL-KERJAN (2006), “PUBLIC-PRIVATE COLLABORATION ON A NATIONAL

AND INAERNATIONAL SCALE”, IN PHILIP E. AUERSWALD ET AL. (EDS.), “SEEDS OF DISASTER, ROOTS OF RESPONSE: HOW

PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY” (CAMBRIDGE: CAMBRIDGE UNIVERSITY PRESS), PP. 395–403.

CUKIER, KENNETH N., VIKTOR MAYER-SCHOENBERGER, AND LEWIS M. BRANSCOMB (2005), “ENSURING, (AND

INSURING?) CRITICAL INFORMATION INFRASTRUCTURE PROTECTION” (KSG WORKING PAPER).

DACY, ROBERT F. (2004), “CRITICAL INFRASTRUCTURE PROTECTION: ESTABLISHING EFFECTIVE INFORMATION SHARING WITH

INFRASTRUCTURE SECTORS” (WASHINGTON, DC: UNITED STATES GENERAL ACCOUNTING OFFICE).

DUNN MYRIAM AND ISABELLE WIGERT (2004), “CIIP HANDBOOK 2004: AN INVENTORY AND ANALYSIS OF PROTECTION

POLICIES IN FOURTEEN COUNTRIES” (ZURICH: CENTER FOR SECURITY STUDIES).

DUNN, MYRIAM (2005), “A COMPARATIVE ANALYSIS OF CYBERSECURITY INITIATIVES WORLDWIDE”, PAPER PRESENTED

AT THE ITU WSIS THEMATIC MEETING ON CYBERSECURITY (GENEVA, 2005).

DUNN, MYRIAM AND VICTOR MAUER (2006), INTRODUCTION, IN DUNN, MYRIAM AND VICTOR MAUER (EDS.):

“INTERNATIONAL CIIP HANDBOOK 2006, VOL. II: ANALYZING ISSUES, CHALLENGES, AND PROSPECTS” (ZURICH: CENTER

FOR SECURITY STUDIES), PP.7–23.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA) (2005), “RAISING AWARENESS IN INFORMATION

SECURITY: INSIGHT AND GUIDANCE FOR MEMBER STATES”. AVAILABLE AT:

HTTP://WWW.ENISA.EUROPA.EU/DOC/PDF/DELIVERABLES/ENISA_CD_AWARENESS_RAISING.PDF.

GOVERNMENT ACCOUNTABILITY OFFICE (GAO) (2004), “CRITICAL INFRASTRUCTURE PROTECTION: IMPROVING INFORMATION

SHARING WITH INFRASTRUCTURE SECTORS” (WASHINGTON DC, WHITE HOUSE).

GRADY, MARK AND FRANCESCO PARISI (EDS.) (2005), “THE LAW AND ECONOMICS OF CYBER-SECURITY” (CAMBRIDGE:

CAMBRIDGE UNIVERSITY PRESS).

HENAUER, MARC (2004), “CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: A SWISS APPROACH”, IN: CENTRE FOR

INTERNATIONAL SECURITY POLICY (CISP): EAPC/PFP WORKSHOP ON CRITICAL INFRASTRUCTURE PROTECTION & CIVIL

EMERGENCY PLANNING: DEPENDABLE STRUCTURES, CYBERSECURITY AND COMMON STANDARDS (BERN, CENTRE FOR

INTERNATIONAL SECURITY POLICY).

HOLDEREGGER, THOMAS (2006), "THE ASPECT OF EARLY WARNING IN CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

(CIIP)", IN DUNN, MYRIAM AND VICTOR MAUER (EDS.), "INTERNATIONAL CIIP HANDBOOK 2006, VOL. II: ANALYZING

ISSUES, CHALLENGES, AND PROSPECTS" (ZURICH: CENTER FOR SECURITY STUDIES), PP. 111–35.

JUSTER KENNETH I. AND JOHN S. TRITAK (2002), "CRITICAL INFRASTRUCTURE ASSURANCE: A CONCEPTUAL OVERVIEW", IN

JOINT ECONOMIC COMMITTEE, UNITED STATES CONGRESS, "SECURITY IN THE INFORMATION AGE: NEW CHALLENGES,

NEW STRATEGIES" (WASHINGTON, DC: WHITE HOUSE).

KILLCRECE, GEORGIA ET AL. (2003), "STATE OF THE PRACTICE OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS

(CSIRTS)" (PITTSBURGH: PITTSBURGH UNIVERSITY PRESS).

PERSONICK, STUART D. AND CYNTHIA A. PATTERSON (EDS.) (2003), "CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

AND THE LAW: AN OVERVIEW OF KEY ISSUES" (WASHINGTON DC: NATIONAL ACADEMIC PRESS).

POULSEN, KEVIN (2005), "U.S. INFO-SHARING CALLED A FLOP", IN "SECURITY FOCUS", 11 FEBRUARY 2005. AVAILABLE

AT: HTTP://WWW.SECURITYFOCUS.COM/NEWS/10481.

PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (PCCIP) (1997): CRITICAL FOUNDATIONS:

PROTECTING AMERICA'S INFRASTRUCTURES (WASHINGTON DC: WHITE HOUSE).

PRIETO, DANIEL B. (2006), "INFORMATION SHARING WITH THE PRIVATE SECTOR: HISTORY, CHALLENGES, INNOVATION, AND PROSPECTS", IN PHILIP E. AUERSWALD ET AL. (EDS.), "SEEDS OF DISASTER, ROOTS OF RESPONSE: HOW PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY" (CAMBRIDGE: CAMBRIDGE UNIVERSITY PRESS), PP. 404–28.

RYTZ, RUEDI (2007), "REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI", PRESENTATION GIVEN AT THE INTERNATIONAL TELECOMMUNICATION UNION (ITU), FEBRUARY 2007.

SCHECHTER, STUART E. AND MICHAEL D. SMITH (2004), "HOW MUCH SECURITY IS ENOUGH TO STOP A THIEF? THE ECONOMICS OF OUTSIDER THEFT VIA COMPUTER SYSTEMS AND NETWORKS" (CAMBRIDGE: CAMBRIDGE UNIVERSITY PRESS).

Cases:

ICJ

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) Judgment of 26 February 2007, (2007) 2007 ICJ, (Bosnia Genocide).

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) Judgment of 19 December 2005, (2005) ICJ Rep. (Congo v. Uganda).

Case Concerning Legality of Use of Force (Yugoslavia v. Belgium) Verbatim Record, 10 May 1999, CR 99/15.

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of 27 June 1986, [1986] ICJ Rep. 14 (Nicaragua).

Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, (2003) ICJ Rep. 161 (Oil Platforms).

Gabcˇíkovo-Nagymaros Project (Hungary/Slovakia), Judgment of 25 September 1997, (1997) ICJ Rep. 7 (Hungary/Slovakia

Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt, Advisory Opinion of 20 December 1980, (1980) ICJ Rep. 67 (WHO/Egypt).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, including in and around East Jerusalem, Advisory Opinion of 9 July 2004, (2004) ICJ Rep.136 (Palestinian Wall).

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, (1996) ICJ Rep. 227 (Nuclear Weapons).

Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion of 11

April 1949, (1949) ICJ Rep. 174 (Reparation for Injuries).

Books, Articles and Internet Sources:

Barkham (2001) Information Warfare and International Law on the Use of Force. New York University Journal of International Law and Politics 34:57–113.

Buchan R (2012) Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict and Security Law 17:212–227.

Boebert E (2010) A Survey of Challenges in Attribution. In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy. National Research Council, National Academies Press, pp 41–54.

Bowett D (1972) Reprisals Involving Recourse to Armed Force. American Journal of International Law 66:1–36.

Bowett (2009) Self-Defence in International Law. The Lawbook Exchange, ltd. Originally published: Praeger, New York (1958).

Brownlie I (1963) International Law and the Use of Force by States. Oxford University Press, Oxford.

Brown G (2011) Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, NDU press, Washington 63:70–73.

Bull H (1984) Intervention in World Politics. Clarendon Press, Oxford.

Clark D and Landau S (2010) Untangling Attribution. In Proceedings of a Workshop on Deterring

Cyberattacks: Informing Strategies and Developing Options for US Policy. National Research Council, National Academies Press, pp 25–40.

Chatham House Principles of International Law on the Use of Force in Self-Defence. (2006) International and Comparative Law Quarterly, 55:963–972.

Dinstein Y (2002) Computer Network Attacks and Self-defence. In: Schmitt and O'Donnell, Computer Network Attack and International Law. International Law Studies – Naval War College 76:99–119.

Dinstein Y (2010) War, Aggression and Self-Defence. Cambridge University Press.

Dutch Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law (2008) Netherlands Yearbook of International Law, T.M.C. ASSER Press, The Hague.

European Commission, Sanctions or Restrictive Measures (2008) http://eeas.europa.eu/cfsp/sanctions/index_en.htm. Accessed 26 February 2013.

Foltz A (2012) Stuxnet, Schmitt Analysis, and the Cyber ''Use-of-Force'' Debate, Joint Force Quarterly 67:40. http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_schmitt_oct2012.pdf, Accessed 28 February 2013.

Gardam J (2004) Necessity, Proportionality and the Use of Force by States. Cambridge University Press, Cambridge.

Gazzini T (2006) The Changing Rules on the Use of Force in International Law. Manchester

University Press, Manchester.

Gorman S and Barnes J (2011) Cyber Combat: Act of War. The Wall Street Journal.

Gray C (2008) International Law and the Use of Force, 3rd ed., Oxford University Press, Oxford.

Greenwood C (2012) Self-Defence. Max Planck Encyclopedia of Public International Law

online.

Hargrove J (1987) The Nicaragua Judgment and the Future of the Law of Self-Defence, American

Journal of International Law 81:135–143.

Jennings R, Watts A (2008) Oppenheim's International Law. Vol 1 Peace. 9th edn, Oxford

University Press, Oxford.

Jensen E (2002) Computer Attacks on Critical State Infrastructure: A Use of Force Invoking the

Right of Self-Defence. Stanford Journal of International Law, 38:207–240.

Lin H (2010) Offensive Cyber Operations and the Use of Force. Journal of National Security Law and Policy 4:63–86.

Lubell N (2010) Extraterritorial Use of Force Against Non-State Entities. Oxford University Press, Oxford.

Roscini M (2010) World Wide Warfare—Jus ad Bellum and the Use of Cyber Force. Max Planck Yearbook of United Nations Law 14:85–130.

Ruys T (2010) 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law

and Practice. Cambrige University Press, Cambridge.

Sadurska R (1988) Threats of Force. American Journal of International Law 82:239 et seq.

Schmitt MN (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.

Schmitt MN (2011) Cyber Operations and the Jus Ad Bellum Revised. Villanova Law Review

56:576 et seq.

Schmitt MN (2012) The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski. 4th

International Conference on Cyber Conflict, available at http://www.ccdcoe.org/publications/

2012proceedings/5_4_Schmidt_ResponseToZiolkowski.pdf. Accessed 26 February 2013.

Sharp WG (1999) Cyberspace and the Use of Force. Aegis Research Corporation, Falls Church.

Simma B, Khan D-E, Nolte G, Paulus A (ed) (2012) The Charter of the United Nations. Oxford

University Press, Oxford.

Schachter (1984) The Right of States to Use Armed Force. Michigan Law Review 82:1620 et seq.

Sloan RD (2012) On the Use and Abuse of Necessity in the Law of State Responsibility.

American Journal of International Law 106:447–508.

Tams C (2009) The Use of Force against Terrorists. European Journal of International law

20:359–397.

Trump K (2011) State Responsibility for International Terrorism. Oxford University Press,

Oxford.

Tsagourias N (2010) Necessity and the Use of Force: A Special Regime. Netherlands Yearbook of International Law 41:11–44.

Tsagourias N (2011) Non-State Entities and the Use of Force. In D'Aspremont J (ed), Participants in the International Legal System: Theoretical Perspectives. Routledge, London, p 326 et seq.

Tsagourias N (2012) Cyberattacks, Self-defence and the Problem of Attribution. Journal of Conflict and Security Law 17:229–245.

Waxman (2011) Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). 36 Yale Journal of International Law 36:421 et seq.

Wedgwood R (1999) Legal personality and the role of non-governmental organisations and nonstate political entities in the United Nations system. In Hofmann R (ed) (1999) Non-State Entities as New Subjects of International Law, Duncker & Humblot, Berlin, pp 21–36.

Wet E de, Vidmar J (2012) Hierarchy in International Law: The Place of Human Rights, Oxford University Press, Oxford.

Ziolkowski K (2012) Jus ad bellum in Cyberspace – Some Thoughts on the ''Schmitt-Criteria'' for Use of Force. 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn. http://www.ccdcoe.org/publications/2012proceedings/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf. Accessed 26 February 2013.

Scientific books:

1. Carr, J. (2012). Inside Cyber Warfare, 2nd Edition, Sebastopol: O’Reilly Media, Inc.

2. Encyclopedia of Cyber Warfare (2017). / Eds. Paul J. Springer, ABC-CLIO

3. Green, L. (2000). The contemporary law of armed conflict, 2nd Edition, Manchester: Manchester University Press

4. Henckaerts, J-M., Doswald-Beck, L. (2005). Customary International Humanitarian Law Volume I: Rules, Cambridge University Press

5. International Humanitarian law: Answers to your questions (2005)/ ICRC. Accessible: https://shop.icrc.org/droit-international-humanitaire-reponses-a-vos-questions-2598.html (4 December 2017)

6. Research Handbook on International Law and Cyberspace. (2015). / Eds. N. Tsagourias, R. Buchan. Cheltenham: Edward Elger Publishing Limited

7. Roscini, M. (2014) Cyber Operations and the Use of Force in International Law, Oxford: Oxford University Press, p 45.

8. Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace, Cambridge University Press

9. The Ethics of Information Warfare (2014). /Eds. L. Floridi, M. Taddeo. Law, Governance and Technology Series, Springer International Publishing

Scientific articles:

10. Ayalew, Y.E. (2015) Cyber Warfare: A New Hullaballoo under International Humanitarian Law – Beijing Law Review, Vol. 6, No. 4, 209-210

11. Bannelier-Christakis, K. (2016) Marco Roscini, Cyber Operations and the Use of Force in International Law – Journal of Conflict and Security Law, Vol. 21, No. 2, 367.

12. Boer, L. (2013) ’Restating the Law ”As It Is”’: On the Tallinn Manual and the Use of Force in Cyberspace - Amsterdam Law Forum, Vol. 5, No. 3, 5

13. Buchan, R. (2012) Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? - Journal of Conflict & Security Law, Oxford University Press, Vol. 17, No. 2, 218-219
37

14. Cate, F. H., Kuner, C., Svantesson, D.J.B., Lynskey, O., Millard, C. (2017) The Rise of Cybersecurity and Its Impact on Data Protection - International Data Privacy Law, Vol. 7. No. 2, 73

15. Changeta, T. (2016)., Measuring Autonomous Weapon Systems against International Humanitarian Rules. – Journal of Law and Cyber Warfare, Vol. 5, No. 1, 75

16. Clough, J. (2012), The Council of Europe Convention on Cybercrime: Defining 'Crime' in a digital world - Criminal Law Forum, No. 23, 363

17. Crawford, E. (2013) Virtual Backgrounds: Direct Participation in Cyber Warfare – I/S: A Journal of Law and Policy for the Information Society, Vol. 9, No. 1, 2-3

18. Farwell, J. P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War, Survival: Global Politics and Strategy, Vol. 53, No.1, 23

19. Fitz, C. (2017), ALL IS FAIR IN LOVE AND CYBERWAR: INTERNATIONAL LAW AND CYBER-ATTACKS - Houston Journal of International Law, Vol. 1, No. 1, 4

20. Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual - Journal of Conflict & Security Law, Vol. 18 No. 2, Oxford University Press, 331-332

21. Gamreklidze, E. (2014), Cyber security in developing countries, a digital divide issue - The Journal of International Communication. Vol. 20, No. 2, 201-202

22. Gervais, M. (2012) Cyber Attacks and the Laws of War – Journal of Law & Cyber Warfare, Vol. 1, No. 8, 10.

23. Gill, T.D., Ducheine, P.A.L. (2013). Anticipatory Self-Defence in the Cyber Context – International Law Studies (Naval War Collage), Vol. 89, 461-462.

24. Haataja, S. (2017) The 2007 Cyber attacks against Estonia and international law on the use of force: an informational approach – Law, Innovation and Technology, Vol. 9, No. 2, 166

25. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), The law of Cyber-Attack – California Law Review, Vol. 100, No. 817-837.

26. Heintschel von Heinegg, W. (2014) Chapter 1 The Tallinn Manual and International Cyber Security Law - Yearbook of International Humanitarian Law, Vol. 15, 3-4

27. Hollis, D. (2011) Cyberwar Case Study: Georgia 2008 - Small Wars Journal, Small Wars Foundation, 2-4.

28. Kessler, O., Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare – Leiden Journal of International Law, Vol. 26, pp 793-798.

38

29. Lindsay, J. R. (2013) Stuxnet and the Limits of Cyber Warfare - Security Studies, Vol. 22, No. 3, 366.

30. Lunn, B. (2014) Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine – Journal of Law & Cyber Warfare, Vol. 4, 113.

31. Mavropoulou, E. (2015). Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber-Attacks - Journal of Law & Cyber Warfare, Vol. 4, No. 2, 24-26.

32. McGhee, J. (2014) Hack, Attack or Whack; The Politics of Imprecision in Cyber Law – Journal of Law & Cyber Warfare, Vol. 4, 15-16.

33. Mele, S. (2014). Legal Considerations on Cyber-Weapons and Their Definitions - Journal of Law & Cyber Warfare, Vol. 3, 56-57

34. Nguven, R. (2013) Navigating Jus Ad Bellum in the Age of Cyber Warfare - California Law Review, Vol.101, 1087-1091.

35. Ochmannova P., Thibault, A. (2013). Respoding to Change – Legal Challenges in the Future Security Environment: Report of the 2013 NATO Legal Conference on 24 -28 June 2013 in Tallinn - Military Law and Law of War Review, Vol. 52, 453

36. Preciado, M. (2012) If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare – Journal of Law & Cyber Warfare, Vol. 1, No. 1, 102.

37. Raboin, B. (2011) Corresponding Evolution: International Law and the Emergence of Cyber Warfare – Journal of the National Association of Administrative Law Judiciary, Vol. 31, No. 2, 609-640.

38. Schaap, A. (2009) Cyber Warfare Operations: Development and Use under International Law -Air Force Law Review, Vol. 64, No. 1, 158.

39. Simmons, N. (2014) A Brave New World: Applying International Law of War to CyberAttacks – Journal of Law & Cyber warfare, Vol. 4, 42-43.

40. Solce, N. (2008) The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force, Albany Law Journal of Science & Technology, Vol. 18, 297-298

41. Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict - Loyola of Los Angeles International and Comparative Law Review, Vol. 32, No. 2, 306

42. Tsagourias, N. (2013) Chapter 2: The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II- The Use of Force – Yearbook of International Humanitarian Law, Vol. 15, 20.

39

Websites and other material:

43. Council of Europe, Convention on Cybercrime, No. 185 of 23 November 2011, European Treaty Series, 08.11.2017

44. Cybercrime Convention Committee (2017), T-CY Guidance Notes, Accessible: https://rm.coe.int/16806f9471, 8 November 2017.

45. ICRC (2008), How is the Term “Armed Conflict” Defined in International Humanitarian Law?, Accessible: https://www.icrc.org/eng/assets/files/other/opinion-paper-armedconflict.pdf, 8 November 2017.

46. INTERPOL, The threats. Accessible: https://www.interpol.int/Crimeareas/Cybercrime/The-threats, 8 November 2017.

47. McGuinness, D. (2017) How a Cyber attack transformed Estonia. Accessible: http://www.bbc.com/news/39655415, 6 December 2017

48. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

49. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. CCDCOE, Accessible:
https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf, 25 October 2017.

Cases:

50. IT-94-1-AR72

LIST OF ABBREVIATIONS

AECERT: THE CYBER EMERGENCY RESPONSE TEAM

C: C PROGRAMMING LANGUAGE FILE

CI: CRITICAL INFRASTRUCTURE CCB CLOSED CUSTOMER BASE

CERT COMPUTER EMERGENCY RESPONSE TEAM

CI CRITICAL INFRASTRUCTURES

CII CRITICAL INFORMATION INFRASTRUCTURES

CIIP CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

CSIRT COMPUTER SECURITY INCIDENT RESPONSE TEAM

DPI: DEEP PACKET INSPECTION

FIRST FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS

GDP: GROSS DOMESTIC PRODUCT

GTM: GROUNDED THEORY METHOD

GZ/SIT: COMPRESSED FILE ARCHIVE CREATED BY GZIP

ICT INFORMATION AND COMMUNICATION TECHNOLOGY

IMF: INTERNATIONAL MONETARY FUND

ISAC INFORMATION SHARING AND ANALYSIS CENTER

IT: INFORMATION TECHNOLOGY

ITU INTERNATIONAL TELECOMMUNICATION UNION

ITAA INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

MELANI MELDE- UND ANALYSESTELLE INFORMATIONSSICHERUNG (REPORTING AND ANALYSIS CENTER FOR INFORMATION ASSURANCE)

NBS: NATIONAL BUREAU OF STATISTICS OF THE UNITED ARAB EMIRATES

OCB OPEN CUSTOMER BASE

PCCIP PRESIDENTIAL COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

PPP PUBLIC-PRIVATE PARTNERSHIP

PL: PERL SOURCE CODE FILE

SME SMALL AND MEDIUM-SIZED ENTERPRISE

SH: UNIX SHELL SCRIPT

TRA: TELECOMMUNICATION REGULATORY AUTHORITY

TXT: TEXT FILE

WARP WARNING ADVICE AND REPORTING POINT

ZIP: COMPRESSED FILE ARCHIVE CREATED BY PKZIPENISA EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

ENDNOTES

[i] Luiijf, H. A. M., T. C. C. van Schie, T. W. J. van Ruijven, and A. W. W. Huistra. "The GFCE-MERIDIAN good practice guide on critical information infrastructure protection for governmental policy-makers." (2016).

[ii] Pursiainen, Christer. "Critical infrastructure resilience: A Nordic model in the making?." *International journal of disaster risk reduction* 27 (2018): 632-641.

[iii] COM(2009) 149

[iv] Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009/C 321/01)

[vv] Joint communication on a partnership for democracy and shared prosperity with the Southern Mediterranean ; COM(2011)200 of 08.03.2011.

[vi] https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip

[vii] Manuel Suter, Center for Security Studies, ETH Zurich, A Generic National Framework For Critical Information Infrastructure Protection (CIIP). August 2007. Retrieved 27th January 2020.

[viii] http://www.melani.admin.ch/index.html?lang=en 2

[ix] Cynthia A. Patterson, Stewart D. Personick. Critical Information Infrastructure Protection and the Law: An Overview of Key Issues, (Washington, D.C.: National Academies Press, 2003), 4.

[x] Education efforts most likely would need to be international in scope, given that many computer-related problems originate overseas; recent incidents have come from countries such as Russia, the Philippines, and Romania.
National Academies of Sciences, Engineering, and Medicine. 2003. Critical Information Infrastructure Protection and the Law: An Overview of Key Issues. Washington, DC: The National Academies Press. https://doi.org/10.17226/10685.

[xi] Harriet Pearson also commented on an increase in corporate attention to security, referring to discussions she had been having with companies in the Midwest.
National Academies of Sciences, Engineering, and Medicine. 2003. Critical Information Infrastructure Protection and the Law: An Overview of Key Issues. Washington, DC: The National Academies Press. https://doi.org/10.17226/10685.

[xii] Abele-Wigert and Dunn (2006): p. 394. 21