Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

Applicability of Criminal Law and Jus ad Bellum to Cyber-Incidents

Oscar Serrano & Florin-Răzvan Radu & Ele-Marit Eomois

Despite current efforts to adapt existing legal instruments to regulate hostile activities in cyber space, there is uncertainty about the legal situation of actors affected by these actions. Part of this uncertainty is due to the fact that being the cyber domain technically complex, there is a strong need for collaboration between technical and legal subject matter experts, collaboration which is difficult to achieve. This paper aims to narrow the gap existing between the legal work in the area and the technical situations that arise during the day to day defence of computer networks. With this purpose, it defines a taxonomy of possible cyber-incidents, and analyses the predictable consequences of each type of cyber-incident with the purpose of mapping cyber-incidents to either Jus ad Bellum or criminal law.

Not surprisingly, this mapping justifies that most cyber operations fall outside Jus ad Bellum and usually account only to harassment, criminal acts or espionage, and as such they shall be prosecuted using national or international criminal law. The paper identifies the very few cases in which cyber-incidents could theoretically account to an armed attack (i.e. a cyber-attack).

Keywords Cyber-attack, taxonomy, legal issues

Citation: Serrano, O., Radu, F.-R. & Eomois, E.-M. (2016). Applicability of Criminal Law and Jus ad Bellum to Cyber-Incidents. *Magdeburger Journal zur Sicherheitsforschung*, *12*, 715–724. Retrieved December 22, 2016, from http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

1 Introduction

The number of cyber-incidents against public and private assets has increased steadily over the last years. Even though to date no nation has accepted being involved in them, there is evidence that hostile actions are not only conducted by non-state actors; also nations are taking part either by directly executing them or by indirectly supporting non-state actors [1]. As the number of connected devices and use cases for the Internet grows, the expectation is that this threat continues to grow in importance. Following the current surge in cyber hostilities, nations have increased efforts to regulate the cyber domain but to date there is no international consensus on a universal instrument against cybercrime.

Legal research in the area of cyber-incidents has tried to find definitions to terms like »cyber-attack«, »cybercrime« or »cyber warfare«, and to determine properties and thresholds under which these actions could be considered equivalent to use of force or even to an armed attack. Typical properties proposed in the literature are the addressee (state/non-state), the effects, or the political or national security purpose of the incident. Unfortunately, this approach has limited practical use, there is no consensus on the definitions and it is difficult to identify the real purpose of an incident.

This paper tries to overcome these difficulties by limiting the analysis to the data that is always available: target, type and assessed damage of the incident. Based on this technical and measurable information, we identify whether Jus ad Bellum or Criminal Law are applicable to each type of cyber incident. The approach is to build a taxonomy of possible types of cyber-incidents together with the potential foreseeable harm caused by each of them. Based on this, we identify which of the two legal frameworks is applicable, irrespective of »subjective« factors such as attribution, intention or other contended legal definitions.

The paper is structured as follows: Section 2 presents related work on the topic. Section 3 summarizes some of the existing legal frameworks. In Section 4 we propose a taxonomy for cyber-incidents. Section 5 further analyses how different incident types identified can be approached by existing legal instruments. In Section 6 examples of practical use are described and finally, conclusions are reported in Section 7.

2 Related Work

During the last years, in the lack of international accepted framework, legal experts have been analysing the applicability of existing law to the cyber domain. There are two main schools of thought, the permissive approach defending that the threat of cyber-incidents has been blown out of proportion and that the real challenges to cyber security are cybercrime and espionage. This school emphasises the utility of national and international criminal law to prosecute cyber offenses. Proponents of this thought there are authors like O'Connell [2] who argues that in order to identify the most relevant law we need to move away from military analogy in general, Gartzke [3] who dismissed the possibility of cyberwar and described cyber-attacks as an evolving, nuanced set of issues or Rid [4] who stated that:

»Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage.«

While it is certain that cyber-war has not taken place, the idea that cyber-incidents can have similar effects as the kinetic ones cannot be dismissed in view of the recorded cyber-incidents (e.g. Op. Orchard or Stuxnet). Based on this premise, the more restrictive approach tries to compare cyber-attacks to the armed attacks necessary to trigger UN Charter Article 5. However, they generally recognize the difficulty to equate cyber-attacks to use of force; other international rules such as those of non-intervention, countermeasures or economic law should also be considered. Most of these authors agree that these laws are only applicable to a small slice of cyber-incidents, those that could be referred as cyber-attacks, and even for those, the law is deficient and needs to be improved. Some of the authors defending this position are Schmitt [5], Roscini [6], Waxman [7] and Hathaway [8]. Finally this was also the approach proposed by the CCD-COE when drafting the Tallinn Manual on the international law applicable to cyber warfare [9].

Our article tries to bring these two schools of thought together and to clearly define, which cyber-incidents are affected by criminal law and which by other international laws such as the law of war.

With this aim we first have to define a taxonomy, which unambiguously classifies cyber-incidents. Mainly due to growing importance of sharing cyber security data, a number of taxonomies aimed at classifying security threats have evolved in the last years. Early taxonomies such as the Protection Analysis [10] or the Research in Secured Operating Systems [11] focused on categorising security flaws. The concepts set have since been used on newer taxonomies. Bishop [12] and later Howard [13] focused on defining a common language for the exchange and comparison of computer security incidents. Howard's work is notable because in addition to technical detail he considered more intangible factors such as attacker's motivation for conducting an attack. Meyers [14] proposed a taxonomy of attacks containing nine classes of cyber-incidents, work similar to our aim. Recent research has been done by Shiva [15] to define a taxonomy able to capture variants of attacks that may exploit more than one vulnerability. The result is a tree with 5 dimensions, which is far more complex and technically detailed than what is required for our work.

Other authors have worked only on taxonomies for a particular purpose, such as Mirkovic and Reihner [16] for Distributed Denial of Service (DDoS) attacks, King [17] for attacks against network log anonymization, Debar [18] for Intrusion Detection Systems (IDS) or Kjaerland [19] for computer crime profiling. Our work is more similar to these ideas in the sense we only pretend to define the taxonomy for our very specific use case. A detailed review of security taxonomies covering work from 1974 to 2006 was written by Igure [20].

To the best of our knowledge there has been no work trying to define a taxonomy that could be used to analyse legal implications of cyber-incidents.

3 Legal Frameworks

The international community has taken so far quite modest steps in regulating cybercrime. The adoption of a United Nations' (UN) legal instrument against cybercrime was subject of discussion for many years, but because of the divergent positions of the states, a universal convention on this matter is not feasible for the moment.

At European level, the Council of Europe (CoE) has assumed the lead and made important efforts to expand its norms against cybercrime beyond Europe, especially in Asia and South America. Thus, two months after the 9/11 terrorist attacks, the CoE has open for signature its Convention on Cybercrime, done in Budapest, on 23 November 2001.

The so called »Budapest Convention« was a very important measure in fighting cybercrime, which has determined major changes in national legislations not only in the member states of the CoE, but also in third countries, due to the fact that this instrument is open for accession to non-members. It represents a regional convention with universal vocation, and this is one of the reasons why a UN Convention on this matter is not likely to be adopted soon. However, so far the Budapest Convention was ratified only by 44 states, of which only 38 of the 47 members of the CoE[1]. It has to be mentioned that the Russian Federation, one of the suspects of cyber-incidents, did not sign the Budapest Convention, while it is allegedly in favour of a UN convention against cyber-crime. On the other hand, the US has signed the CoE Convention on cybercrime on the very day of its opening for signature and has ratified it on 29.09.2006. So far, apart from the US, five other countries are parties to the Budapest Convention beyond Europe: Australia, Dominican Republic, Japan, Mauritius and Panama. Canada and South Africa have signed, but not yet ratified this multilateral instrument.

The main added value of the convention is that it not only governs international cooperation against cybercrime, but also contains important provisions of substantive and procedural criminal law, which have to be implemented as a minimal standard by its states parties. The convention also obliges for extradition of criminal offenders in cybercrime cases. The EU has taken its own legislative measures against cyber-incidents. Thus, apart from the CoE standards, applicable in those EU Member States which have ratified it, the Council of the EU has adopted a Directive 2013/40/EU on attacks against information systems. The directive obliges the Member States to criminalise offences of illegal access to information systems, illegal interference to such systems, illegal data interference, as well as incitement, aiding and abetting and attempt to commit these offences, and to apply dissuasive penalties for such crimes.

Another approach proposed by international lawyers is the application of international humanitarian law. The Jus ad Bellum, governed by the UN Charter, define a set of criteria to regulate the use of armed force and is always attributed to a state (in a broad sense). Relevant Jus ad Bellum provisions are Article 2(4) (prohibition of the use of force), Article 51 (the right of self-defence), as well as Articles 39, 41, and 42. Also were applicable (e.g. art. 51) legal principles of necessity and of proportionality should be considered, as has been recognized by the International Court of Justice.

While it is commonly agreed that the prohibition of use of force includes kinetic armed attack, leaving thus aside attacks of political and economic nature, the notion »armed« continues to be discussed among scholars in order to be able to justify the application of Jus ad Bellum to cyber-attacks [21]. There are three approaches to determine whether a cyber-attack is considered an armed attack. According to the »instrument-based« approach, a cyber-attack is considered as an armed attack only if conventional military weapons are used (e.g. bombing computer servers). The »target-based« approach considers a cyber-attack any action that targets a sufficiently important computer systems, even if it does not necessarily result in physical damages. Thirdly, professor Michael Schmitt [5] is the main proponent of the »effects-based« approach that argues that in order to be considered an armed attack, a cyber-attack foreseeable consequence should be causing physical or property damage, with a severity resembling the consequences of an armed attack. In addition authors like L.J.M. Boer [22] argue that none of these approaches will provide an answer, as there is an implicit paradox in the Art 2(4) that excludes similar cases based on different rules (e.g. exclusion of economic coercion although it can have devastating effects that can resemble those of an armed conflict).

There are several other legal frameworks such as international telecommunications law, aviation law or law of space that might be of application for certain cyber-incidents. However we will not consider them

[1] Updated and complete chart of signatures and ratifications may be found in the Treaty Office portal of the Council of Europe, at the following URL address: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=12/12/2014&CL=ENG

for our work as they are applicable only to specific cases.

4 A Taxonomy of Cyber Incidents

The taxonomies discussed in Section 2 are too detailed and not suitable for our task. For example, most of them consider the attack vector one of their main classification attributes (e.g. [25], [13]), but from a legal perspective the technical details listing the families of malware used or Common Vulnerabilities and Exposures (CVE) exploited are not relevant, a higher view describing that the attack used for example social engineering or misuse of computer resources (e.g. by a malware) is more valuable. Therefore we propose in this section a new taxonomy, simple enough to fulfil our needs, and providing only the details that are of use from a legal perspective. To this respect, it can be argued for example that the international law principle of non-intervention requires coercion. And it can indeed be relevant to understand the vector or means of insertion to analyse whether requisite coercion is present to constitute a violation of the principle. Similarly, whether a vector of attack overcame resistance or defenses may be relevant to coercion analysis. Although it could be possible to extend the proposed taxonomy to cover these cases, at the moment these considerations are beyond the analysis for which we are designed it.

4.1 Types of Taxonomies

Howard [13] evaluated the main taxonomies used to classify cyber incidents and vulnerabilities. He identified the following main types of taxonomies:

- List of Terms: The most popular and the simplest taxonomy but it generally fails to achieve the mutual exclusion of the terms.
- Lists of Categories: A variation of the list of terms in which only categories are listed. It provides an improvement to the list of terms but has the same problems.
- Results Categories: Group incidents in categories, which describe the result of the incident.
- Empirical Lists: Results on longer lists of categories based on actual occurrences of incidents. These lists tend to be exclusive, exhaustive, unambiguous, and repeatable but they are complex to use due to the lack of any logical schema.
- Dimensions: Classify incidents based on 2 (matrices) or more dimensions, each representing a characteristic of the incident. Each category is defined by the combination all dimensions. The result is primarily a sophisticated list in several dimensions, each with the limitations of the lists discussed earlier.

We have decided for a results based category because this categorization allows, in most cases, to associate incidents with a unique category unambiguously.

4.2 Dimensions

Igure [20] identified the common basic dimensions for incident classification: impact, target, source, and vulnerability. For our work the impact and target are of major importance, the source is difficult to attribute and we will not use it; also the vulnerabilities are not interesting from a legal point of view and we substitute them by the incident type, which we categorize based on the effects of the incident.

Based on this works our taxonomy is divided into three dimensions:

- Incident type: Categorized as a results category.
- Target: Categorized as a list of categories.
- Damage: Categorized as a list of categories.

The main dimension of our taxonomy is the incident type. Target and damage dimensions will help differentiating variations of the same types of incidents.

4.3 Proposed Taxonomy

4.3.1 Incident type

The incident type identifies all potential hostile cyber activities. We consider here incidents originated in the cyber space can have physical effects, however we do not consider in this category incidents that originate from the physical space and have effect on the cyber domain, as for example sabotage of a data centre or supply chain attacks. We have identified the following categories:

- Fingerprinting: Discovery, classification and monitoring of potential target devices for cyberattacks.
- Vulnerability Scanning: Passive or active assessment of target devices for weaknesses. We include is this category fuzzing and reverse engineering. The first one involves use of invalid, unexpected or random data to search for unexpected program terminations. Those terminations can be used to find perform memory based attacks to the systems. Reverse Engineering consists of recovering the source code form the binary executable code, in this context with the aim to analyse it searching for vulnerabilities.
- Logical Denial of Service: Prevents legitimate users from accessing logical resources such as a website, a network or a system.
- Misuse: The use of system resources for unplanned purposes, typically of criminal interest. This incident type covers malware installation between other activities; its main manifestation would be the unknown participation of computing resources in BotNets.
- Spoofing: Attempts to masquerade a user, site or system with the intention to gain an illegitimate benefit.
- Social Engineering: Cover attempts to obtain information using social techniques such as Phish-

ing, Pharming, Spamming or Spear phishing. If the attempt is successful it might lead to information disclosure.

- Traffic analysis/monitoring: Used to gain knowledge about the content of communication, based on the analysis of metadata such as the origin, destination, volume and frequency of the exchanges, without access to the information itself and without altering it.
- Data Leakage: Unauthorized access to information, without the information itself being altered. This covers cyber-incidents such as eavesdropping or certain types of man-in-the-middle attacks.
- Data Tampering: Intentional alteration of information to obtain a benefit or to cause damage. This category includes data destruction and manipulation of SW.
- Physical Denial of Service: A denial of service to systems that control physical resources, preventing legitimate users from using them. As an example of systems controlling are the access to a building or the distribution of electricity or water.
- Physical Tampering: Exploitation of system vulnerabilities with the aim to tamper with the correct functioning of physical devices. The most well-known example of this type of incident would be Stuxnet [26].

4.3.2 Target

We differentiate two possible types of targets:

- Critical infrastructures: The 16 critical infrastructure sectors identified by the US Presidential Policy Directive 21: Chemical, Commercial facilities, Communications, Critical manufacturing, Dams, Defence Industrial Base, Emergency Services, Energy, Financial Services, Food and agriculture, Government facilities, Healthcare and public health, IT, nuclear reactors, transportation and waste and wastewater systems.
- Others: Any other target that cannot be considered as part of the critical infrastructures.

4.3.3 Severity

We define three categories of severity depending on the effects of the incident:

- Low: The incident is detrimental to the interest or effectiveness of the target.
- Medium: The incident is damaging to the target.
- High: Consequences of the incident resemble those of an armed attack and result in an exceptionally grave damage to the target.

5 Legal Framework of Applicability

This section discusses whether Jus ad Bellum or Criminal Law would be more appropriated to respond to each type of incident. When discussing about Jus as Bellum we consider only the »effects« approach, we agree with Hathaway [8] that the target based approach is too over-inclusive and would lead to superfluous escalation of conflicts and that the instrument based approach is outdated as cyber-attacks do not need to use traditional military weapons to cause large damages. In this context we use the definition of cyber use of force provided in the Tallinn manual: »its scale and effects are comparable to non-cyber operations rising to the level of a use of force« [9]. Table 1 presents a summary of this section.

5.1 Fingerprinting

Is the collection of information about the target using Open Source Intelligence tools, with the aim of enumerating users, shares, e-mails addresses and other information relevant for the cyber-incident. While this is a first step towards a cyber-incident it is generally not recognized as a criminal offense. These actions are not likely to be prosecuted, which is realistic considering that the large number of these actions makes their prosecution impractical.

5.2 Traffic analysis/monitoring

A powerful signals intelligence tool consistent in ignoring the data, which mostly cannot be accessible, and analysing the available metadata. It can be used for example to decrypt encrypted communications [27] or to de-anonymise users in protected communication channels [28], [29]. The legality of these actions depends on the legality of acquiring the required metadata under the different national laws. Regardless of its legality, traffic analysis and monitoring will never fall under Jus ad Bellum using the effect-based approach.

5.3 Spoofing

The process of forging data with the intention to masquerade a legitimate user or programme is a criminal act in some legislations while it is perfectly legal in others as long as it is not used to commit fraud or otherwise perpetrate a crime.

5.4 Vulnerability Scanning

Similarly to fingerprinting, it is conducted during the reconnaissance phase of a cyber-incident, and its goal is to list the vulnerabilities present in the systems previously fingerprinted. There are nations that have legislations that could be used to prosecute the search or disclosure of vulnerabilities as criminal acts, as it is arguably the case of the US Digital Millennium Copyright Act [30]. However this is a grey area and in most nations and for most cases the search or disclosure of vulnerabilities is not prosecuted.

5.5 Social Engineering

It covers a wide array of incidents that are usually the main entry point for cyber-incidents. Attackers use spear-phishing or spam to distribute malware to the end users or obtain information to gain unauthorized access to systems. Social engineering can be prosecuted using criminal law under charges such as wire fraud, fraud or related activities in connection with access devices (e.g. unauthorized use of credit cards). In addition, most countries have approved legislations addressing these criminal acts. For example the US has the CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act) of 2003 or the UK Privacy and Electronic Communications (EC Directive) Regulations 2003. Social engineering also has a physical component that might include meeting with people in public, physical interviews or dumpster diving, actions that are usually not illegal.

5.6 Logical Denial of Service (DoS)

DoS incidents are one of the most prevalent types of attacks, characterized by an explicit attempt to prevent legitimate users of a service from using it. DoS incidents are illegal under most national laws, especially those which have implemented the provisions of Article 4 of the Budapest Convention, which imposes to states parties to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. For example, the US Computer Fraud and Abuse Act (the »CFAA«) prohibits to »knowingly causing the transmission of a program, information code, or command, and as a result of such conduct, intentionally causes damages without authorization to a protected computer« (see 18 U.S.C. § 1030(a)(5)(A)). In this context, damage is defined as »any impairment to the integrity or availability of data, a program, a system, or information«. In addition, DoS attacks are usually distributed by making use of BotNets, what requires the misuse of systems by deploying malware. The most extreme case for this category of cyber-incident could involve the denial of service to critical infrastructures (e.g. air control systems) without causing direct or indirect physical damages. But even then, as long as the DoS incidents are not performed as part of an armed conflict or their effects are restricted to the cyber domain there is no reason to consider these incidents outside of the criminal law context. This is supported by the UN Charter Article 41 that lists between the measures not involving the use of force the »partial or complete interruption of … telegraphic, radio and other means of communication«.

However we agree with [] that although these cyber-incidents do not raise to the level of a use of force they do however a violations of international law that can be

5.7 Misuse

Covers the unauthorized access to computer systems and the deployment of malware, and is generally prosecuted by criminal law under charges such as for example unauthorised access to computer material, access with intent to commit or facilitate commission of offence or unauthorised modification of computer material. At European level, Article 2 of the Budapest Convention and Article 3 of the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems require the criminalisation of illegal access in information systems. In US, the mentioned Computer Fraud and Abuse Act is relevant. In addition, the UK Computer Misuse Act states that an offence of »unauthorized acts with the intent to impair, or with recklessness as to impairing, operation of computers« is committed if a person intentionally »does any unauthorized act in relation to a computer« intending to »impair the operation of any computer«, »prevent or hinder access to any program or data held in any computer« or »impair the operation of any such program or the reliability of any such data«.

None of the approaches to justify that a cyber-incident has escalated to an attack (i.e. instrument, effect or target) can justify that misuse could be considered a cyber-attack. As long as the misuse does not cause As for most of incident types analysed, there is no need to consider misuse outside of the criminal law context, even if the targeted systems belong to the critical infrastructure sector.

5.8 Data Leakage

The illegal collection of computer data without altering it is a growing matter of concern [31], which is also known as cyber espionage. Cyber espionage is defined by the Tallin manual as: »any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather information with the intention of communicating it to the opposing party« [9]. It is the posture of most nations that espionage does not fall under international laws, and the same posture is observed in respect to cyber espionage, which is not regarded as use of force even if the actions are highly invasive[32]. Most countries have laws that criminalise data theft, as for example the German Penal Code (§§ 202c and 202a): »whoever gathers information or produces or acquires (hacking) tools with the intention to gain unjustified access to somebody else's data«. Such criminal law provisions exist for example in all states parties to the Budapest Convention and the Member States of the EU implementing the Directive 2013/40/EU.

5.9 Data Tampering

Is usually covered under the same laws that protect misuse, and usually also requires the misuse of the computer systems. For example the UK Computer Misuse Act states that an offence of »unauthorized acts with the intent to impair, or with recklessness as to impairing, operation of computers« is committed if a person intentionally »impair the operation of any such program or the reliability of any such data«. A Cyber incident impacting critical systems that only results in the modification or destruction of non-essential data would not rise to the threshold of an armed attack. However in certain cases tampering with data in critical systems could be equivalent to the physical use of force. A theoretical example is tampering of financial data; damage caused by such an incident could severely hamper the financial sector of a nation causing property damage of severity high enough to be considered an act of force [33]. To be considered as use of force, the incident would have to produce extensive and permanent damage. However, financial institutions (as most critical infrastructure services) have developed business continuity and disaster recovery plans that allow the mitigation and recovery from such attacks. For example US regulates business continuity plans using the Federal Financial Institutions Examination Council (FFIEC) that requires banks to put in place Business continuity and disaster recovery plans to ensure continuous operations and limit losses, the GAO/IMTEC-91-56 Financial Markets: Computer Security Controls which covers the security of U.S. Stock Exchanges and the FFIEC Inter-Agency Policy 1997 that covers business continuity for any outsourced service. In practice that means that data could be recovered from alternate sites in the case of a disruptive event, by temporally moving systems offline and recovering from offsite backups. Therefore, although theoretically it could be possible, in practice the attack would need to extend concurrently to the main servers as well as the backup sites (that in some cases might not even be online) in order to be able to cause major damages. Therefore, although theoretically possible, it is difficult that data tampering attacks without mirrored effects in the physical world can be considered an act of force.

5.10 Physical Denial of Service

This type of cyber-attack aims to use cyber tools to cause a denial of service attack to a service used in the physical world. These are serious attacks which can involve severe losses for the organizations affected. If the attack targets critical sector organizations and the severity is commensurable with that of an armed attack, this could be a case for resorting to the law of armed conflict. Examples of such attacks include denying access to emergency services, Automatic Teller Machines (ATMs), electricity, water or sensors networks.

5.11 Physical Tampering

It consists on modification of computer systems that have effects on the correct functioning of physical devices. This is the most dangerous type of cyber-attack, in the sense that it can have destructive effects in the physical world. This type of attack, if targeting critical infrastructures with enough severity could be considered an act of force.

6 Practical Use

6.1 Stuxnet

Stuxnet was an advanced malware discovered in 2010 and designed to target Siemens SCADA systems controlling Iranian nuclear centrifuges. The aim was to delay the Iranian Nuclear Programme. The cyber-attack is widely considered at least an act of force, but there are discrepancies about whether it constitutes an Armed Attack. Following our analysis Stuxnet would be considered Physical Tampering against critical infrastructures, the severity could be arguably »Medium« or »High«, that would perhaps justify the use of armed actions.

Stuxnet is attributed to the US [1], with possible cooperation with Israel. Although Iran has not officially acknowledged it, it is generally accepted that after this incident they retaliated by attacking US banks [34], attacks to which the US did not officially respond. This sequence of cyber-attacks and retaliation, describe the most likely case for cyber-attacks.

6.2 Advanced Persistent Threats

APTs are reported to be involved on widespread intellectual property theft, targeting insider information related to governments, militaries, and private organizations. We shortly analyse two well-known APT.

6.2.1 APT 1

It is believed to be a Chinesse sponsored group linked to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department [35]. APT 1 has stolen terabytes of data from at least 141 English speaking organizations. For this they maintain an extensive infrastructure of computer systems around the world, with at least dozens, but potentially hundreds of human operators.

6.2.2 APT 28

A group targeting information about NATO, the Caucasus region and Eastern European governments and militaries [36]. It uses a modular malwares ecosystem that is customized for each target and presents a high level of complexity, including counter analysis capabilities such as runtime checks to identify an analysis environment, obfuscated strings unpacked

Type of Incident	Target	Severity		
		Low	Medium	High
Fingerprinting	Any	Criminal Law	N/A	N/A
Traffic analysis/monitoring	Any	Criminal Law	N/A	N/A
Spoofing	Any	Criminal Law	N/A	N/A
Vulnerability Scanning	Any	Criminal Law	N/A	N/A
Social Engineering	Any	Criminal Law	Criminal Law	N/A
Logical Denial of Service	Any	Criminal Law	Criminal Law	N/A
Misuse	Any	Criminal Law	Criminal Law	N/A
Information Disclosure	Any	Criminal Law	Criminal Law	Criminal Law
Data Tampering	Others	Criminal Law	Criminal Law	Criminal Law
Data Tampering	Critical inf.	Criminal Law	Criminal Law	Criminal Law / Jus ad Bellum
Physical Denial of Service	Others	Criminal Law	Criminal Law	Criminal Law
Physical Denial of Service	Critical inf.	Criminal Law	Criminal Law	Jus ad Bellum
Physical Tampering	Others	Criminal Law	Criminal Law	Criminal Law
Physical Tampering	Critical inf.	Criminal Law	Criminal Law	Jus ad Bellum

Table 1: Summary of applicable frameworks per type of attack.

at runtime, and the inclusion of unused machine instructions to slow analysis. Its design is similar to other malware samples used for international espionage and sabotage including Stuxnet, Duqu, Flamer, Red October and Weevil. Atribution is not clear but is believed to be a Russian sponsored group.

These groups employ highly developed cyber tools and they attack regularly private and governmental organizations using: Misuse, Spoofing, Social Engineering and Data Leakage. No known actions have been taken regarding APT 28 due to attribution problems; however the US Department of Justice indicted five members of the Chinese military after the release of the APT 1 report, accused of 31 charges including computer hacking, economic espionage or theft of trade secrets against US nuclear power, metals and solar products industries [37]. Although it is highly unlikely that these persons will be extradited by China, it demonstrate that customary criminal law or the use of non-forcible countermeasures are the most likely response to advanced and persistent state sponsored cyber-attacks. The recent Sony Pictures case reinforces our ideas [38].

7 Conclusions

This paper presents a taxonomy for classification of cyber-incidents that is useful to evaluate if criminal Law or Jus ad Bellum can be applied to different types of cyber-incidents. The paper shows that except in exceptional cases, criminal law is the most appropriate response to cyber-incidents, despite its categorization and independently of its attribution.

In this sense, the Budapest Convention is a step in the right direction. However, its legal efforts against cyber-attacks are seriously jeopardised by the limited number of ratifications, which lead to a significant number of »black holes« in this area, as well as by the difficulties in obtaining extradition of cybercrime offenders, especially because of obstacles related to »dual criminality« rule and non-extradition of own nationals.

Our work identifies only three situations in which a military response would be arguably legal and they mainly involve large physical effects to critical infrastructure sectors. These types of attacks have not been witnessed to date, but if they would ever be materialized, existing international legislation offer certain legal grounds to justify actions.

8 About the Authors

Oscar Serrano has worked as Scientist and consultant for major international organizations such as the Austrian Research Centres, Siemens or Eurojust for the last 15 years. In his role as Senior Scientist in Cyber Defence, he currently he advices a major international military organization about Cyber Security policy and Risk Management. He is author of several research papers and part of the program committee of the ACM Workshop on Information Sharing and Collaborative Security. His research interests include Threat Information Management, Cyber Law and Detection of Advanced Persistent Threats.

Florin-Răzvan Radu, PhD is a seconded national expert at Eurojust, in the Secretariat of the European Judicial Network, as of 1 October 2014. Previously, Mr Radu was director for European Affairs, International Relations and Programs within the Superior Council of Magistracy in Romania (September 2011 - October 2014), and he has been working 12 years with the Romanian Ministry of Justice, where he was the director of the Directorate for International Law and Treaties, from July 2003 to January 2009. He was for the first time seconded as national expert to the Secretariat of the European Judicial Network (EJN), in The Hague, from 2009 to 2011. In 2007 he was appointed head of the Romanian delegation to the Council of Europe Committee on Crime Problems (CDPC) and in June 2007 he was elected by the members of CDPC as member of the Bureau of CDPC. Between 2002 and 2008, he was the head of the Romanian delegation for the negotiation of several bilateral treaties in the field of judicial cooperation. He is also the drafter or co-drafter of several important pieces of Romanian legislation on judicial cooperation and author of two books in this field. From 2002, he was the Romanian coordinator Contact Point for the EJN.

Ele-Marit Eomois, L.L.M., M.A.S., is a Legal Specialist at Eurojust, in the Secretariat of the European Judicial Network. She has been working in the field of EU law and international affairs for the last 10 years. Over these years, she has given legal advice to public authorities and NGOs. She has also been a co-drafter of national legislation in justice and home affairs.

9 References

[1] D. E. Sanger, Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power. Crown Publishers, 2012.

[2] M. E. O’Connell, »Cyber Security without Cyber War,« Journal of Conflict and Security Law, vol. 17, no. 2, pp. 187–209, 2012.

[3] E. Gartzke, »The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,« International Security, vol. 38, no. 2, pp. 41–73, Oct. 2013.

[4] T. Rid, Cyber War Will Not Take Place. New York, NY, USA: Oxford University Press, Inc., 2013.

[5] M. Schmitt, »Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,« in Essays on Law and War at the Fault Lines, T. M. C. Asser Press, 2012, pp. 3–48.

[6] M. Roscini, »World Wide Warfare - Jus ad Bellum and the Use of Cyber Force,« Max Planck Yearbook of United Nations Law, vol. 14, pp. 85–130, 2010.

[7] M. C. Waxman, »Cyberattacks and the Use of Force: Back to the Future of Article 2(4),« Yale Journal of International Law, vol. 36, no. 2, Mar. 2011.

[8] O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, »The Law of Cyber-Attack,« California Law Review, vol. 100, no. 4, 2012.

[9] M. N. Schmitt, Ed., Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

[10] R. Bisbey and D. Hollingworth, »Protection Analysis: Final Report,« Information Sciences Institute, University of Southern California, 4676 Admiralty Way, Marina del Rey, California, 90291, May 1978.

[11] D. A. W. R. P. Abbott, J. S. Chin, J. E. Donnelley, W. L. Konigsford, S. Tokubo, »Security Analysis and Enhancements of Computer Operating Systems.«

[12] M. Bishop and D. Bailey, »A Critical Analysis of Vulnerability Taxonomies,« 1996.

[13] J. D. Howard and T. A. Longstaff, A Common Language for Computer Security Incidents. 1998.

[14] C. A. Meyers, S. S. Powers, and D. M. Faissol, »Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches,« 2009.

[15] S. Shiva, C. Simmons, C. Ellis, D. Dasgupta, S. Roy, and Q. Wu, »AVOIDIT: A cyber attack taxonomy.,« University of Memphis, Aug. 2009.

[16] J. Mirkovic and P. Reiher, »A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,« SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, Apr. 2004.

[17] J. King, K. Lakkaraju, and A. Slagell, »A Taxonomy and Adversarial Model for Attacks Against Network Log Anonymization,« in Proceedings of the 2009 ACM Symposium on Applied Computing, New York, NY, USA, 2009, pp. 1286–1293.

[18] H. Debar, M. Dacier, and A. Wespi, Eds., »Towards a Taxonomy of Intrusion-detection Systems,« Comput. Netw., vol. 31, no. 9, pp. 805–822, Apr. 1999.

[19] M. Kjaerland, »A taxonomy and comparison of computer security incidents from the commercial and government sectors,« Computers & Security, vol. 25, no. 7, pp. 522 – 538, 2006.

[20] V. Igure and R. Williams, »Taxonomies of attacks and vulnerabilities in computer systems,« Communications Surveys Tutorials, IEEE, vol. 10, no. 1, pp. 6–19, First 2008.

[21] M. N. Schmitt, »The Law of Cyber Warfare: Quo Vadis?,« Stanford Law & Policy Review, vol. 25, Sep. 2013.

[22] L. J. M. Boer, »’Echoes of Times Past’: On the Paradoxical Nature of Article 2(4),« Journal of Conflict and Security Law, 2014.

[23] K. Ziolkowski, »Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention,« Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Jan. 2014.

[24] J. Crawford, A. Pellet, S. Olleson, and K. Parlett, The Law of International Responsibility. OUP Oxford, 2010.

[25] S. Hansman and R. Hunt, »A taxonomy of network and computer attacks,« Computers & Security, vol. 24, no. 1, pp. 31 – 43, 2005.

[26] R. Langner, »Stuxnet: Dissecting a Cyberwarfare Weapon,« Security Privacy, IEEE, vol. 9, no. 3, pp. 49–51, 2011.

[27] D. X. Song, D. Wagner, and X. Tian, »Timing Analysis of Keystrokes and Timing Attacks on SSH,« in Proceedings of the 10th Conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 2001.

[28] Y. Gilad and A. Herzberg, »Spying in the Dark: TCP and Tor Traffic Analysis,« in Proceedings of the 12th International Conference on Privacy Enhancing Technologies, Berlin, Heidelberg, 2012, pp. 100–119.

[29] S. J. Murdoch and G. Danezis, »Low-Cost Traffic Analysis of Tor,« in Proceedings of the 2005 IEEE Symposium on Security and Privacy, Washington, DC, USA, 2005, pp. 183–195.

[30] A. Maurushat, Disclosure of Security Vulnerabilities: Legal and Ethical Issues. Springer Publishing Company, Incorporated, 2013.

[31] G. O'Hara, »Cyber-Espionage: A Growing Threat to the American Economy,« CommLaw Conspectus, vol. 19, p. 241, 2010.

[32] M. N. Schmitt, »Cyber Operations and the Jus ad Bellum Revisited,« 56 VILLANOVA LAW REVIEW 569-606, Apr. 2011.

[33] »Cyber Warfare,« Advisory Committee on Issues of Public International Law, The Hague, No 77, AIV / No 22, Dec. 2011.

[34] N. Perlroth and Q. Hardy, »Bank Hacking Was the Work of Iranians, Officials Say,« The New York Times, 01-Aug-2013.

[35] Mandiant, »APT1: Exposing One of China's Cyber Espionage Units,« Feb. 2013.

[36] Mandiant, »APT28: A Window into Russia's Cyber Espionage Operations?,« Feb. 2013.

[37] »United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui,« United States District Court for the Western District of Pennsylvania (Pittsburgh), Pennsylvania, Criminal No. 14-118, May 2014.

[38] »Sony cyber-attack: North Korea faces new US sanctions,« BBC News, Jan. 2015.