Received 14 December 2014
Revised 24 May 2015
Accepted 24 August 2015

Cyberoperations and international humanitarian law

A review of obstacles in applying international law rules in cyber warfare

Kosmas Pipyros
Department of Informatics, Athens University of Economics and Business, Athens, Greece

Lilian Mitrou
Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece, and

Dimitris Gritzalis and Theodoros Apostolopoulos
Department of Informatics, Athens University of Economics and Business, Athens, Greece

Abstract

Purpose – The increasing number of cyber attacks has transformed the "cyberspace" into a "battlefield", bringing out "cyber warfare" as the "fifth dimension of war" and emphasizing the States' need to effectively protect themselves against these attacks. The existing legal framework seem inadequate to deal effectively with cyber operations and, from a strictly legal standpoint, it indicates that addressing cyber attacks does not fall within the jurisdiction of just one legal branch. This is mainly because of the fact that the concept of cyber warfare itself is open to many different interpretations, ranging from cyber operations performed by the States within the context of armed conflict, under International Humanitarian Law, to illicit activities of all kinds performed by non-State actors including cybercriminals and terrorist groups. The paper initially presents major cyber-attack incidents and their impact on the States. On this basis, it examines the existing legal framework at the European and international levels. Furthermore, it approaches "cyber warfare" from the perspective of international law and focuses on two major issues relating to cyber operations, i.e. "jurisdiction" and "attribution". The multi-layered process of attribution in combination with a variety of jurisdictional bases in international law makes the successful tackling of cyber attacks difficult. The paper aims to identify technical, legal and, last but not least, political difficulties and emphasize the complexity in applying international law rules in cyber operations.

Design/methodology/approach – The paper focuses on the globalization of the "cyber warfare phenomenon" by observing its evolutionary process from the early stages of its appearance until today. It examines the scope, duration and intensity of major cyber-attacks throughout the years in relation to the reactions of the States that were the victims. Having this as the base of discussion, it expands further by exemplifying "cyber warfare" from the perspective of the existing European and International legal framework. The main aim of this part is to identify and analyze major obstacles that arise, for instance in terms of "jurisdiction" and "attribution" in applying international law rules to "cyber warfare".

Findings – The absence of a widely accepted legal framework to regulate jurisdictional issues of cyber warfare and the technical difficulties in identifying, with absolute certainty, the perpetrators of an attack, make the successful tackling of cyber attacks difficult.

Information & Computer Security
Vol. 24 No. 1, 2016
pp. 38-52

2056-4961
DOI 10.1108/ICS-12-2014-0081

Originality/value – The paper fulfills the need to identify difficulties in applying international law rules in cyber warfare and constitutes the basis for the creation of a method that will attempt to categorize and rank cyber operations in terms of their intensity and seriousness.

Keywords Accountability, Attribution, Jurisdiction, Cyber operations, Cyber warfare

Paper type Research paper

1. Cyber incidents and their impacts

The rapid development of information and communication technology (ICTs), its presence in every aspect of human life and the high degree of dependency on cyberspace make cyber security a common objective for a society's proper functioning and the well-being of its citizens. As the European Commission states in its most recent communication on the European Union (EU)'s Cyber Security Strategy (JOIN,European Commission, 2013), cyber security:

> […] commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.

Moreover, Hathaway *et al.* (2012) state that those threats, commonly referred to as cyber-attacks, include actions "[…] taken to undermine the functions of a computer network for a political or national security purpose". Ultimately, as the US National Research Council (2009) defines them, they are "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks".

It is not the first time that cyber-attacks have aroused the interest of governments as well as the scientific community. The primary instances of this type of offence can be traced back in the late 1980s, and they seem to evolve together with the rapid technological changes including the internet itself. The early attack on NASA's networks with the WANK worm in 1989 quickly gave its place to a number of more advanced cases including the attack on the French Government's websites with the Strano Network's "netstrike" in 1995, the Electronic Disturbance Theatre's "Web sit-ins" focusing against websites in Mexico and USA and aiming at the support of Mexican Zapatistas in 1998 or the Internet Black Tigers' "suicide email bombings" targeting Sri Lanka embassies and used as a means of opposing the governmental propaganda (Berson and Denning, 2011). All these incidents, although limited in range, brought about a series of discussions over the issue of cyber operations and their eventual political, economic and social impacts in the host State of a cyber-attack but also the impact on international relationships regarding this new kind of warfare and its consequences in the global strategic environment.

However, the incidents mentioned above were small-scale incidents of limited range and intensity in terms of the extent of damage caused to the victims of cyber-attacks. Moreover, none of these attacks was perpetrated by the Governments or tied to State-level conflicts. The perpetrators were mainly individuals or small groups acting independently, presumably without anyone's guidance or control. Their aim was to draw attention to themselves in relation to their political, social or economic goals. The first cyber operations to be regarded as of military nature, were those that emerged during the Kosovo era involving conflicts conducted by non-State actors, the so-called "patriotic hackers", who seemed, however, to act, if not under the umbrella, certainly

under the tolerance of the respective national governmental agencies. These types of conflict were characterized:

> […] as the first war on the Internet, in recognition of not only the cyber-attacks but also the broader role played by the Internet, especially in the dissemination of information about the conflict (Berson and Denning, 2011).

One of the most famous wide-range attacks that ever took place was the cyber-attack in Estonia in April 2007 that lasted for almost three weeks. This cyber-attack seemed to be the result of the Estonian Government's decision to defy Russian threats and to remove from the city center the Bronze Soldier monument, a memorial of the Soviet liberation of Estonia in World War II; a decision that caused diplomatic tension with Russia and a wave of protests in central Tallinn (Tikk *et al.*, 2010). Reactions were transferred from the streets to cyberspace with "patriotic hackers" engaging in a coordinated large-scale cyber-attack, which was directed against Estonia's critical ICTs – such as electronics and telecommunications infrastructures. The choice to shift the "battle field" from the streets to cyberspace was not random. As early as the mid-1990s, Estonia had been characterized as an e-State, as all of its critical services were provided to its citizens through the Web: e-banking, health care and e-government services, as well as internet voting for the national elections. These attacks were meant to harm the functionality of the State, causing a number of adverse effects to the operation of public administration and the economy (Tikk *et al.*, 2010) and leading to the destabilization of the country's financial system and threatening its national security. As Blank (2008) states:

> the specific assault which quickly led to the cultivation of fear among citizens and of a sense that nothing was functioning in the country, aimed at the undermining of Estonia's social cohesion.

The case in question, which was clearly an unprecedented act of psychological terror, demonstrated in its full range the close interrelation that exists between cyber security and national security and the key role that the former plays in ensuring a country's social stability and the prosperity of its citizens. At the same time, it revealed the insufficiency of the European security institutions such as the EU, NATO and the Security Council to stand by Estonia while the country was under cyber-attack. The Estonia cyber operation was followed by a number of smaller-range ones such as the attacks against Georgia and Lithuania in June and August 2008, respectively; against Kazakhstan in January 2009; and against Ukraine in March and May 2014. All these assaults were related to military interventions undertaken by Russia in these areas during the same time period (Tikk *et al.*, 2008).

The aforementioned aggressions as well as the persistent attacks on the USA ["Operation Aurora" (Zetter, 2010), "Ghostnet" (Kassner, 2009) and distributed denial-of-service (DDoS) attacks against the New York Stock Exchange (Roberts, 2012)], Iran [the recent sabotage against Iran's nuclear program with the "Stuxnet" computer worm (Farwell and Rohozinski, 2011; Pipyros *et al.*, 2014, Virvilis and Gritzalis, 2013a; 2013b, Virvilis *et al.*, 2015) and South Korea [aggressions that took place in 2013 and paralyzed three TV stations and part of the country's banking system (Sang-Hun, 2013)] clearly demonstrate that cyber threats is an increasingly alarming phenomenon. But should cyber operations of this art and these impacts be considered as something new, requiring the formulation of new legal instruments on an international level or should they be met by using the traditional international law rules in force?

On one side, Russia, China and other countries favor an international treaty, similar to those agreed on chemical weapons, and they have pushed for such an approach to regulating cyberspace. On the other side, the USA and the EU have repeatedly resisted such proposals arguing in favor of an update of the international law rules so that they can address these issues properly (O'Connell, 2012). The European Commission, in its proposal for a cyber security strategy, emphasized that:

> […]the legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online, pointing out that if armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand (JOIN, 07.02.2013, European Commission, 2013).

Additionally, the International Group of Experts involved in the production of the so-called "Tallinn Manual" – a project launched at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, in the hope of bringing some degree of clarity to the legal issues surrounding cyber operations – rejects any characterization of cyberspace as a separate domain calling for its handling by a new institutional framework. On the contrary, the experts came to the unanimous conclusion that the general principles of international law should also apply to the cyberspace (Schmitt, 2013).

Thereafter, the existing legal framework dealing with cyber threats at the European and international levels will be presented.

2. The regulatory framework for an "open, safe and secure cyberspace"

On a multinational level, the first attempt to deal with information technology (IT)-specific offences and the challenges posed by the – often transborder – nature of cybercrime, was the adoption by the Council of Europe of the International Convention on Cybercrime, also known as the Budapest Convention (CETS 185, 23.11.2001, Council of Europe, 2009). The Budapest Convention led to the creation of a reference framework aiming to address computer and internet crimes by introducing not only substantial rules but also (and perhaps mainly) procedural rules and the basis of international cooperation for law enforcement and exchange of respective information. The Convention on Cybercrime addressed direct threats arising from cyberspace, now legally defined as acts aimed toward confidentiality, integrity and availability of computer data and systems (Chapter II, Section 1, CETS 185, 23.11.2001, Council of Europe, 2009). The specific Convention, which dealt with crimes that were mainly, but not exclusively, carried out by private individuals without State intervention, aimed at the protection of private property and public goods, and it laid the ground for the harmonization by Member States of their relevant national laws focusing ultimately on the protection of society against cybercrime.

Following the cyber-attacks, especially against Estonia and Georgia, it became obvious that the existence of critical infrastructures plays a key role in ensuring a country's national security. As a result, the Council Directive 2008/114/EC of December 8, 2008 "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" adopted a framework for the identification of critical infrastructures in the sectors of energy, transportation and ICTs, which would serve as a first step toward the adoption of an overall strategy for their protection in the fight against terrorism. The high dependence of all actors (in the

public and private sector) on Critical Information Infrastructures (CIIs), the cross-border interconnectedness and interdependencies of CIIs with other Infrastructures, as well as the vulnerabilities and the threats they face, raised the need to address their security and resilience in a systemic perspective as the frontline of defense against cyber operations. Member States have to conduct a risk analysis based on major threat scenarios to select and prioritize important assets and implement security counter-measures for their protection and indicate at the national level those infrastructure and operations-services whose eventual deterioration or malfunction could have serious effects on public health, the financial system and the prosperity and security of citizens.

The next European initiative addressing large-scale events was the 2009 Communication (COM 149, 30.03.2009; European Commission, 2009) from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on CII Protection entitled "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". That Communication emphasized the need for coordinated collective action by pointing out that "Cyber-attacks have risen to an unprecedented level of sophistication. Simple experiments are now turning into sophisticated activities performed for profit or political reasons". The Commission also emphasized the huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam.

More recently, in February 2013, the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, presented a proposal for a cyber security strategy along with a draft Directive (JOIN, 07.02.2013, European Commission, 2013), addressing the issue of Network and Information Security (NIS). As referred to in the EU's relevant press release (IP/13/17, 07.02.2013):

> […]the cyber security strategy, for an Open, Safe and Secure Cyberspace, represents the EU's comprehensive vision on the best possible way to prevent and respond to cyber disruptions and attacks.

The specific strategy, aiming at further promoting the European values of freedom and democracy, serves not only as a means of communicating the EU's idea of cyber security but also as a basis for the adoption of a common legal framework relating to cyber-attacks, their overall impact and the potential ways of addressing them.

In addition, the European Parliament and the Council of the EU proceeded in August 12, 2013 to the adoption of Directive 2013/40/EU "on attacks against information systems and replacing Council Framework Decision 2005/222/JHA". The specific Directive aims at the establishment of a common institutional framework for approximating the constituent elements of criminal offences relating to attacks on information systems and seeks to improve cooperation between the competent authorities and institutions (ENISA, EUROJUST and EUROPOL) to fight cybercrime effectively. To this end, Member States should take appropriate measures to increase the resilience of their information systems so that they are protected more effectively against cybercrime. Directive 2013/40/EU aims to harmonize the criminalization of specific types of conduct (such as illegal access to information systems or illegal system and data interference) and does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact. The Directive's ultimate

goal is to address large-scale events and to contribute to the creation of a safer information society and of an area of freedom, security and justice.

Last but not least, on September 5, 2014, the Heads of State and the Government of the member countries of the North Atlantic Alliance endorsed at their Wales Summit an enhanced Cyber Defence Policy in which it was recognized that international law (including humanitarian law and the UN Charter) also applies to cyberspace. Acknowledging the sophisticated and potentially threatening nature of cyber-attacks for the Euro-Atlantic prosperity, security and stability and the fact that their effect could be as harmful to modern societies as a conventional attack, the North Atlantic Alliance decided to allow for their inclusion in NATO's core task of collective defense. In other words, given the right of the Alliance to take all the necessary measures (including the use of armed force) to restore international peace and security, it was agreed that the security council will be able to decide, on a case-by-case basis, whether a cyber attack leads or not, to the invocation of Article 5, so that appropriate action is taken. Additionally, at the Wales Summit, the Alliance was committed to further developing the national cyber defense capabilities by enhancing the national cyber security networks which constitute the basis for NATO's core tasks, and a means for increasing the resilience and protection of the Alliance.

3. Updating the current international law framework to address the new challenges

Despite the existence of a broad legal arsenal that can be deployed, at any given time, to the fight against cybercrime and to the protection of the States' CIIs from cyber threats, the legal classification of a cyber attack against an information system as a use of force or as an armed attack is problematic. The difficulty in applying the traditional rules of international humanitarian law to categorize cyber attacks stems from a number of factors. The most important of them is the failure to estimate properly the impact of a cyber attack and to determine the identity, or the political motivations of an attacker, until long after the event has occurred.

In an attempt to address these issues, the international group of experts proceeded, to the creation of the Manual on the International Law Applicable to Cyber Warfare or the so-called "Tallinn Manual" aiming at the examination of the extent to which the existing legal norms are applicable to this "new" form of warfare. This manual is not legally binding, but it should not be underestimated in terms of its function as a significant consultative document. Up to now, the "Tallinn Manual" is the most complete task for the use of international law rules (jus ad bellum and jus in bello) to interpret cyber warfare. More important than being a useful compilation of rules, it includes commentary reflecting the different views on some of the tricky issues raised by the introduction of cyber warfare.

Yet, in spite of the noticeable progress, at an international level, toward the updating of international law rules to effectively address this "new" form of warfare, there is still confusion regarding the degree of the application of international law rules to cyber warfare. Namely, it has not yet been clarified in which cases do cyber attacks constitute a "threat or use of force" so that the prohibition of Article 2(4) of the UN Charter can apply, neither is it clear in which cases these aggressions can be treated as an "armed attack", making it possible for a UN Member State to respond by exercising its legitimate right of self-defense under Article 51 of the UN Charter.

In particular, Rule 10 of the Tallinn Manual does not specify in which cases cyber operations can be considered as attacks that rise to the level of a "use of force", thus calling for the application of the prohibition of Article 2(4) of the UN Charter. Nevertheless, Rule 11 of the Tallinn Manual states that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (Schmitt, 2013). This provision is consistent with the approach that all cyber-attacks whose purpose is to directly cause either death or injury to human beings or damage to tangible goods, should undoubtedly be characterized as a use of armed force and thus be prohibited. It is, therefore, understood that for a cyber operation to be characterized as a "use of force", a parallel result logic is being used, meaning that an effort is being made to identify cyber operations that are equivalent in terms of their results to other actions, kinetic or not, that would be described, in conventional terms, as "uses of force".

But what about the cyber-attacks that do not cause death, injury or physical damage directly, but rather indirectly? How should these acts be characterized? The majority of the international law specialists consider that Article 2(4) can be used to cover nearly any type of "use of force" that is not approved by the Charter, as the phrase "other manner" entails all possible categories including cyber-attacks.

Based on the same logic, and following Article 51 of the UN Charter, Rule 13 of the Tallinn Manual states that:

> […]a State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects (Schmitt, 2013).

However, in this case also, it is not clear in which cases cyber-attacks meet the scale and effects requirements so that they can be regarded, classified and handled as an "armed attack", allowing a UN Member State to respond by exercising its legitimate right of self-defense, under Article 51 of the UN Charter. So, it can be understood that, in both Rule 11 and Rule 13 of the Tallinn Manual, the term "scale and effects" is a shorthand term that refers to those quantitative and qualitative criteria that should be analyzed for someone to be able to determine whether a cyber operation qualifies as a "use of force" or "an armed attack".

Thus, the law is unclear as to the characterization and evaluation of a number of cyber-attacks, especially in the case of "use of force", whose impact is not immediately visible. Moreover, there is currently no institutional framework for the evaluation of the "use of force" and "armed attack" concepts in cyberspace. Taking these facts into consideration, the International Group of Experts adopted, in general, the Schmitt's consequence-based approach (Schmitt, 1999), that aims to identify, in an objective way, the likelihood of classifying a cyber operation as a "use of force". Its focus is to recognize the impact of cyber attacks and equate it to the corresponding impact caused by other actions (non-kinetic or kinetic), a type of impact that the international community would describe as "use of force". A number of non-exclusive criteria (factors), based on a case-by-case assessment, would help to evaluate the aforementioned impact and draw a parallel between conventional operations that verge on being characterized as "uses of force", and corresponding cyber operations that meet the "scale and effects" requirements. These criteria (factors) are "severity" (severity of attacks), "immediacy" (the speed with which consequences manifest themselves), "directness" (the causal

relation between a cyber-attack and its consequences), "invasiveness" (the degree to which a cyber operation interferes with the targeted systems), "measurability of the effects", "military character of the cyber operation", "extent of State involvement" and "presumptive legality" (acts not expressly prohibited by international law).

Nevertheless, it should be kept in mind that these factors cannot be considered as formal legal criteria. However, taking for granted the total absence of an institutional framework for the evaluation of the "use of force" concept in cyberspace, these factors could be used in areas where there is uncertainty or disagreement in an number of legal analyses, and for making available a means for addressing all issues having to do with "use of force". From a legal point of view, the difficulty, in applying the traditional rules of the international humanitarian law to cyberspace, stems from a number of factors. The most important ones are limitations in jurisdiction and the failure of "attribution".

4. Limitations in jurisdiction

One of the most important issues relating to cyber-attacks is the so-called "jurisdiction issue". The open architecture of the internet, which allows billions of users around the world to interact with each other and the number of services offered on a global basis (by servers/internet service provider which may be located on the other side of the planet), complicates the issue of jurisdiction for crimes taking place in cyberspace.

As Kassner (2009) suggested in a draft paper prepared for the Council of Europe, the jurisdiction issue complicates the use of a nation's cybercrime law to prosecute violations that occur over the internet. According to Public International Law, the main and most common principle – which is also applicable to cybercrime (CETS 185, 23.11.2001, Council of Europe, 2009) – is the "territoriality principle", which denotes that a sovereign State has the authority to prosecute criminal acts that are committed within its borders. However, according to Kaspersen, the internet environment is different in the sense that it is usually possible to gather on-line electronic evidence that is physically located in a computer system in one territory but that is available (retrievable by means of software) to the law enforcement authorities of another territory (of another State). In principle, public international law does not permit extraterritorial jurisdiction to gather such (evidentiary) material. Limitations are stricter in this case than concerning the assertion of extraterritorial jurisdiction to regulate. The State concerned should be requested to render mutual assistance to provide for the material needed. Despite dedicated regulation – such as the Cybercrime Convention and the Directive 2013/40/EU – intended to increase the speed of procedures of mutual assistance, this may nevertheless not always ensure the availability of the evidentiary material. These arguments relate to the practical difficulty of law enforcement in the case of private actions and are directly linked to the cyber crime jurisdiction issue.

But what if the situation under consideration concerns an act that is generated or is motivated by a State, where the attacker has to be identified as a State actor, that is, as an actor committing an armed attack and not just a criminal act? Under International Law, States may bear responsibility for cyber operations that their agents carry out or for which the States can alternatively be held accountable by the virtue of the law of State responsibility. In some cases also, the actions of non-State actors may be attributed to the States. However, there is no official document (an agreement or a treaty) indicating the judicial mechanism to be used in those cases that a State is behind a cyber-attack. There are only a couple of bilateral agreements (such as the Mutual Legal

Assistance Treaty – "MLAT") between Estonia and Russia, the utility of which is doubtful, as it proved out in practice (despite earlier promises, Russia refused to provide assistance to Estonia under the MLAT, when such a need arose). In essence, the cyber-attack actor bears no consequences for his actions. The only official, but non-binding, document that exists, aiming to shade a light on cyber warfare jurisdiction issues is the Rule 2 of the Tallinn Manual which states:

> Without prejudice to applicable international obligations, a State may exercise its jurisdiction:
>
> over persons engaged in cyber activities on its territory;
>
> over cyber infrastructure located on its territory; and
>
> extraterritorially, in accordance with international law.

The territoriality criterion, however, is not always safe, as the use of ICTs allows the assaulter, by taking advantage of the multiple internet service providers or the existing cloud-based services, to hide his territorial (as well as his physical) identity by creating replications and dynamic relocations of data or by spoofing the geo-coordinates of the computing devices. Moreover, there is always the possibility of an IT device and/or system to become the instrument of a cyber-attack without its user's/owner's knowledge. In this case, the device can become a zombie device (through the implantation of special software on it) and participate in cyber-attacks while its user is completely unaware of the fact.

So, while the leading actors are usually national-State actors, the activities of non-State actors, including, cybercriminals and terrorist groups, create confusion and misperception as to the actual cyber warfare "players". In essence, cyberspace conflicts allow for the combination of crime, espionage and military action in ways that often make it quite difficult – if not impossible – to distinguish them.

In the two most striking cases, namely, Estonia and Georgia, Russia, the territory of which was identified as the starting point of the cyber-attacks, refused to provide any help to these countries in their efforts to detect and punish the offenders despite of the fact that there was a binding agreement that required it to do so. Hence, the issue of jurisdiction is complicated and difficult to address. Concisely, the variety of jurisdictional bases in international law and the technical difficulties to identify the attacker constrict the effective confrontation of cyber operations.

5. The attribution problem

Probably the most crucial problem arising with respect to cyber operations and to the way they are developed, is the technical complexity of determining the perpetrators and of positively identifying the key actor of cyber operations, resulting, thus, in major difficulties to handle the issue of "attribution". This is due to the fact that the process of decoding and identifying the location of the system that originated the attack is lengthy and expensive. Determining perpetrator's identity and motivation becomes even more challenging in cases of attacks involving intermediaries who may or may not be willing participants in the attacks. In such cases, determining motivation seems difficult, mainly due to the complex architecture and geography of cyberspace. The identification of the perpetrator's motivation, although extremely challenging, is necessary for making a distinction between cybercrime, cyber terrorism and cyber warfare, given the fact that the actors behind an attack may range from criminal actors to nation States. So,

effective attribution is a precondition for determining whether the actor is a criminal, a terrorist or even a State actor posing a potentially greater national security threat (Finklea and Theohary, 2015).

Successful attribution, while depending largely on the available forensic evidence, is a lot more than that. The process of matching an offender to an offence is an extremely challenging one in any domain, let alone cyberspace – and it calls for the minimization of uncertainty in terms of tactics, operations and strategy. Attribution is a multi-layered process, and it requires a range of skills in a number of levels. It is a slow process that necessitates careful management, good leadership, stress-testing, prudent communication and the ability to recognize limitations and challenges. In terms of tactics, the crucial thing is to appreciate the incident primarily in its technical aspects. With regard to operations, the key goal must be to understand both the profile of the attacker and the architecture of the attack. And as far as strategy is concerned, the key issues include the identification of the perpetrator of an attack, the assessment of the consequences of that attack, the significance of the impact of the attack in the State and the decision of appropriate response. Throughout this process, a critical parameter should be the identification of a government or organization, and not of individuals, as the key actor of an attack. Undoubtedly, the process of attribution is a techno-political one that depends largely on what is at stake in terms of politics (Rid and Buchanan, 2014).

So, whenever a State is engaging in a cyber operation and its actions cannot be justified under the self-defense doctrine or do not have the UN Security Council authorization, it can be claimed that this State violates Article 2(4) of the UN Charter and the prohibition on the use of force. Respectively, a State can be held responsible for cyber warfare operations that rise to the level of unlawful use of force, when these operations are launched by its agents. Thus, for a violation to result in State responsibility, it must be attributable to a State. But in which cases can a State be held accountable for the actions of individuals or groups? Clearly, a State can be held legally responsible for actions taken by their entities or governmental organizations. However, in the case of non-State actors, such as private individuals, organized groups and terrorist organizations, a State can be held legally responsible only if it can be proven without doubt that these non-State actors were acting under the instructions or the control of the State (Schmitt, 2014).

Within the cyber warfare framework, then, States can be held responsible for violating the prohibition on the use of force when it can be proven that they have either instructed private individuals or groups to carry out the operations or when it can be confirmed that they are heavily involved in them through involvement of their entities or government organs. A decision on that can be made only on a case-by-case basis through the examination of the extent and nature of the relationship of the State with the actor/actors and on its involvement in the operations under consideration.

For example, in the Nicaragua case, the International Court of Justice considered it imperative to address the required degree of control for attribution, by examining whether the effective control criterion was met, allowing thus for holding a State responsible for violations committed by non-State actors in relation to the use of force prohibition. It is noteworthy to consider though that, although the tribunal rejected the claim of effective control, the technical legal issue taken into consideration to reach that decision was the nature of the armed conflict and not the State responsibility. Then again, in the Tadic case, the International Criminal Tribunal for the Former Yugoslavia

addressed the issue under consideration in a different way. It held that the authority exercised by the Government of the Federal Republic of Yugoslavia over the Bosnia Serb armed groups:

> […]required by international law for considering the armed conflict to be international was overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations (Schmitt, 2011).

Generally speaking, it can be alleged that in those cases where the effective control criterion is not met, the State may not bear direct responsibility for private acts, but rather an indirect one, meaning that it can be held responsible for tolerating the private action in question or for not undertaking any action to prevent it. To deal and possibly eliminate this phenomenon, it has been suggested that the States bear an international obligation on the ground of the principles of international law both to prevent non-State actors, acting from within their territory, from committing cyber-attacks; and to offer their support to the States that become victims of the attacks. Moreover, in case of no compliance with this obligation, it has been recommended for the victim-States of the cyber-attacks to have the legal right to respond by retaliating, even if it cannot be proven that there is a "causal link" between non-State actors who carried out the attack and the Government's "tolerance". This measure, which allows the victim-States to protect themselves from cyber-attacks originated from within the territory of a hostile State, is called "Active Cyber Defense" (Gaycken, 2010). In such cases, there is an urge to establish meaningful accountability for improper actions taken by the adversaries or for negligence on their behalf, affecting the confidentiality, integrity and availability of CIIs of the State-target of the attack. Establishing accountability for activities in and through cyberspace is now at least as important as attribution (Shanahan, 2014).

Many different technical approaches have been developed in an attempt to address the attribution problem. Each of these techniques, which can be used individually or in combination, can apply to many different network protocols. Yet, an analysis of all these techniques will show that they can only be considered under the greater regulatory context of different legal jurisdictions (Mudrinich, 2012).

In addition, any proposals for a public, personally identifiable packet-level mechanism, intended to contribute to the transition of internet from a model of online anonymity to a new model of "pseudonymity" (through converting IPv4 addresses to IPv6 ones and assigning these new addresses to a unique individual after having that individuals' identity authenticated in some verifiable way) should be treated with caution, as many questions are raised relating both to the users' safety and to the protection of privacy. Privacy has emerged as a concern of modern societies aiming to ensure liberty and creativity. The ability to control the release of personal information constitutes a critical factor for the establishment of acceptable levels of trust in a society. International principles of privacy are reflected in Article 12 of the UN Universal Declaration of Human Rights. Moreover, the EU has implemented a comprehensive legal framework on data protection and privacy consisting of a number of official documents such as the Data Protection Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data", the Directive 2002/58/EC "concerning the processing of personal data and the protection of privacy in the electronic communications" and the Privacy Enhancing Technologies (PETs) Communication [COM 228/2007; European Commission,

2007 "on Promoting Data Protection by PETs"]. So, the emergence of a system, contradicting with the current European and international legal framework, that would turn Internet into a State surveillance device, restricting users' freedom and privacy, would constitute a direct threat to their privacy.

Conclusively, the process of attribution is a multi-layered one that requires both the employment of technical means and the adoption of legal and policy tools. The technologies implemented so far to deal with it are rather incomplete in nature and, thus, according to the assessment of effective attribution, their effectiveness is questionable. The difficulty in applying these techniques stems mainly from the existence of legal constraints in establishing meaningful accountability for cyber warfare acts and in implementing the existing legal framework to deal with them, while simultaneously respecting citizen's privacy and civil liberties.

6. Conclusions

Cyber conflict constitutes a new and challenging problem. For the time being, there are many difficulties, from a technical and institutional perspective, in applying international law rules in cyber operations. In fact, the international community of States needs something more than bilateral agreements which do not bring about any sanctions in case of non-compliance. Despite the fact that some States have adopted measures of a binding nature at the organizational level (creation of a national cyber security strategy by determination of CII) to reduce the effects of cyber-attacks, these measures have a limited scope. Moreover, there are no multilateral agreements or international treaties providing a straightforward definition as to what "a cyber-attack" should entail, and as to the sanctions (economic or other) it should induce. In short, there is a lack in universal agreements regarding the process of monitoring, processing and effective sharing of the information required to track and trace assaulters (Lewis, 2009).

In cyber warfare, the activities of key actors (States) can often not be easily distinguished from the activities of non-State actors (such as cybercriminals and terrorists groups), rendering the terrain of cyber conflict complicated. The combination of anonymity and parallel action from both State and non-State actors and the difficulty in distinguishing military from criminal actions makes the management of this type of conflicts complicated and the implementation of international humanitarian law rather problematic.

The objective facts of every cyber operation incident are quite difficult to identify; thus, it cannot be claimed with certainty that the key criteria of both State involvement and gravity of effect are met. In addition, uncertainty regarding attribution along with the absence of a common understanding creates the risk of instability and misperception. Consequently, from a strategic point of view, the classification of cyber conflicts becomes quite challenging as a result of both the multi-layered nature and the multi-jurisdictional character of the attribution problem. Future work will provide a basis for the creation of a method that will attempt, through the adoption of specific evaluative criteria, to categorize and rank cyber operations in terms of their intensity and seriousness.

References

Berson, T. and Denning, D. (2011), "Cyber warfare", *IEEE Security & Privacy*, Vol. 9 No. 5, pp. 13-15.

Blank, S. (2008), "Web war I: is Europe's first information war a new kind of war?", *Taylon & Francis Online Journal*, Vol. 3 No. 2, pp. 227-247.

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

Council of Europe (2009), "Cybercrime and Internet Jurisdiction", Convention on Cybercrime, European Treaty Series 185, Project on Cybercrime, 23.11.2001, Council of Europe, Budapest.

European Commission (2007), "On promoting data protection by privacy enhancing technologies (PETs) (Communication) COM", 228 final.

European Commission (2009), "On critical information infrastructure protection, protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (Communication) COM", 149 final, Brussels, 30. 03.09.

European Commission (2013), "Cyber security Strategy of the European Union: an open safe and secure cyberspace", Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, JOIN, 1 Final, Brussels, 7.2.2013.

Farwell, J. and Rohozinski, R. (2011), "Stuxnet and the future of cyber war", *IISS, Survival: Global Politics and Strategy*, Vol. 53 No. 1, pp. 23-40.

Finklea, K. and Theohary, C. (2015), "Cybercrime: conceptual issues for congress and US Law Enforcement", Congressional Research Service Report, available at: www.fas.org/sgp/crs/misc/R42547.pdf (accessed 18 May 2015).

Gaycken, S. (2010), "The necessity of (some) certainty – a critical remark concerning Matthew Sklerov's concept of 'active defense'", *Journal of Military and Strategic Studies*, Vol. 12 No. 2, available at: www.jmss.org/jmss/index.php/jmss/article/view/293/304 (accessed 12 February 2013).

Kassner, M. (2009), "Ghostnet: why it's a big deal", available at: www.techrepublic.com/blog/it-security/ghostnet-why-its-a-big-deal/1339/ (accessed 2 October 2013).

Mudrinich, E. (2012), "Cyber 3.0: the department of defense strategy for operating in cyberspace and the attribution problem", *The Air Force Law Review*, Vol. 68, pp. 167-205.

O'Connell, M. (2012), "Cyber security without cyber war", *Journal of Conflict & Security Law*, Vol. 17 No. 2, pp. 187-209.

Pipyros, K., Mitrou, L., Gritzalis, D. and Apostolopoulos, T. (2014), "A cyber attack evaluation methodology", *Proceeding of the 13th European Conference on Cyber Warfare and Security*, *Greece*, pp. 264-270.

Roberts, P. (2012), "Leading US banks targeted in DDoS attacks", available at: http://nakedsecurity.sophos.com/2012/09/27/banks-targeted-ddos-attacks/ (accessed 2 October 2013).

Sang-Hun, Ch. (2013), "Computer networks in South Korea are paralyzed in cyber attacks", available at: www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=0 (accessed 2 October 2013).

Schmitt, M. (1999), "Computer network attack and the use of force in international law: thoughts on a normative framework", *Columbia Journal of Transnational Law*, Vol. 37, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800 (accessed 2 October 2013).

Schmitt, M. (2011), "Cyber operations and the jus ad bellum revisited", *56 Villanova Law Review,* pp. 569-606, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2184850 (accessed 2 April 2015).

Schmitt, M. (2014), "Proxy wars in cyberspace: the evolving international law of attribution", *Fletcher Security Review*, Vol. 1 No. 2.

Schmitt, M. (2013), *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, available at: http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf (accessed 2 July 2013).

Shanahan, J. (2014), "Achieving accountability in cyberspace: revolution or evolution?", *Joint Force Quarterly, National Defence University,* No. 73, pp. 20-25.

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A. and Vihul, L. (2008), *Cyber Attacks Against Georgia: Legal Lessons Identified*, CCD COE Publications.

Tikk, E., Kaska, K. and Vihul, L. (2010), *International Cyber Incidents: Legal Considerations*, CCD COE Publications.

United Nations (1948), "Universal declaration of human rights", available at: www.un.org/en/documents/udhr/ (accessed 2 July 2014).

Virvilis, N. and Gritzalis, D. (2013), "The big four – what we did wrong in advanced persistent threat detection?", *Proceeding of the 8th International Conference on Availability, Reliability and Security*, Springer, pp. 248-254.

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

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

Zetter, K. (2010), "Google hack attack was ultra sophisticated", New Details Show, available at: www.wired.com/threatlevel/2010/01/operation-aurora/#ixzz0deHCunGn (accessed 2 October 2013).

Further reading

Boampong, M. (2013), "Creating an internationally recognized code on cyber warfare", Harlem MUN, available at: http://web.hmun.nl/wp-content/uploads/2013/02/Creating-an-internationally-recognized-code-on-cyber-warfare.pdf (accessed 20 May 2013).

Bumgarner, J. and Borg, S. (2009), "Overview by the US-CCU of the cyber campaign against Georgia in August 2008", available at: www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (accessed 22 May 2013).

Cornish, P., Hughes, R. and Livingstone, D. (2009), "Cyberspace and the National security of the United Kingdom", Chatham House Report, Royal Institute of International Affairs, London.

Council Directive (EC) (95/46/EC), of the European Parliament and of the Council of 8 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities No L 281/31.

Council Directive (EC) (2002/58/EC), of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (Directive on privacy and electronic communications), Official Journal of the European Communities L 201/37.

Council Directive (EC) (2013/40/EU), of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union L 218/8.

European Commission (2006), "On a European Programme for Critical Infrastructure Protection" (Communication) COM, 786 final, OJ C126.

European Commission (2006), "On Fighting spam, spyware and malicious software (Communication) COM", 688 final.

European Commission (2013), "EU Cybersecurity plan to protect open internet and online freedom and opportunity", available at: http://europa.eu/rapid/press-release_IP-13-94_en.htm (accessed 27 April 2013).

Hathaway, O., Crootof, R., Levitz, Ph., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012), "The law of cyber-attack", *California Law Review*, Vol. 100 No. 4, pp. 817-886.

ISO 27001 Security (2013), "ISO/IEC 27001: 2013 Information technology – security techniques – information security management systems – requirements", available at: www.iso27001security.com/html/27001.html (accessed 4 October 2013).

Lynn, W. (2010), "Defending a new domain: the pentagon's cyberstrategy", Foreign Affairs, available at: www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed 10 April 2013).

Morningstar, C. and Farmer, F.R. (2003), "The lessons of Lucasfilm's habitat", in Wardrip-Fruin, N. and Montfort, N. (Eds), *The New Media Reader*, The MIT Press, Cambridge, pp. 664-677.

Nowak, A. (2013), "*Cyberspace as a New Quality of Hazards, in National Defence University*", *Scientific Quarterly*, Vol. 3 No. 92.

Obama, B. (2009), "Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure", available at: www.projectcywd.org/resources/items/show/127 (accessed 6 July 2013).

Owens, W., Dam, K. and Herbert, S. (2009), *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, The National Academies Press, Washington, DC, available at: www3.nd.edu/~cpence/eewt/Owens2009.pdf (accessed 8 July 2013).

The Economist (2010), "Cyber war: war in the fifth domain", *The Economist*, available at: www.economist.com/node/16478792 (accessed 8 April 2013).

UK Office of Cyber Security and UK Cyber Security Operations Centre (2009), "Cyber security strategy for the United Kingdom", available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (accessed2 April 2012).

Corresponding author
Dimitris Gritzalis can be contacted at: dgrit@aueb.gr