9 Potential Role of International Law in the Field of IT Warfare

Tamás Lattmann[*]

Attacks on IT devices that are currently dominating our present days are becoming a major threat, so legal remedies need to be developed in order to deal with this growing menace. While the internal legal environment of states has more or less developed to ensure the necessary standards, the international regulation of these issues is still incomplete and sometimes very vague. The present analysis focuses on attacks using IT tools against public objects within interstate relations.

9.1 Objectives and Tools of IT attacks

IT attacks can serve a variety of purposes. Deleting or interrupting data stored or transmitted on IT systems, or to obtain or observe those, or to use those for misinformation or deceive the other party. The purpose can also be to cause actual damage, such as paralyzing a hostile logistics or communication network, resulting in serious problems in the system of another country. This outcome is not necessarily achievable only by affecting the public network, but also by disruption of a more sensitive private IT structure (such as stock exchange transactions or electronic service providers) and may also result in damage. It is a special and perhaps simplest but at the same time the most spectacular goal when the attack aims to cause a "propaganda" effect, i.e. deface, when the websites on a network can be replaced with often funny or offensive content created by the attacker, but that does not usually mean serious structural intervention. All in all, the purpose of IT attacks can be either political or military, or the support of other (e.g. military) activities.

The IT tools at hand to achieve the above goals can be varied. So far the tools used in IT attacks usually make use of the features of a networked computer system or the potential unique failures or disabilities of systems and applications running on individual machines.

The most commonly used method on the Internet is the so-called denial of service, or overload attack (hereinafter referred to as DoS), designed to disrupt, and possibly paralyze an IT system that serves a specific online service or structure. The point is that a

* PhD, senior researcher at the Institute of International Relations (IIR) Prague, and associate professor of National University of Public Service (NKE), Budapest.

target device providing a particular IT service (such as a web or an internal server) will not be able to serve the larger amount of requests it receives. The widespread version of this method is the so-called Distributed Denial of Service (hereinafter referred to as DDoS), in which requests are executed in a coordinated manner by multiple devices, possibly even if their operators do not know about it (so-called zombie networks). For computers without Internet access, various viruses, worms, and Trojan programs pose a threat that can be used for many purposes after they have been sent to target machines: obtaining, forwarding information, and providing access to the target machines and systems for their creator.

9.2 Analysis of Recent Major IT Attacks

In May 2007, an IT attack wave with the most serious effects was inflicted on Estonia. According to the analysis, DDoS attacks from Russia have affected the entire infrastructure, paralyzing the Parliament, ministries, and Internet sites handling major banks and media. Since Estonia was a leader among European countries during that period in the application of IT tools in the administrative sector, the disruption caused by the attacks caused serious damage and raised considerable concerns about IT security.

The prelude to the attack was a debate of a concrete political nature, because the local government of Tallinn had angered both the Russian minority in the country and the neighbouring Russia by deciding to remove a Soviet monument of the Second World War. As a consequence, the event was accompanied by the visible public support of Russia, and computer applications quickly became available, by downloading and installing, so that anyone could "become a part of the operation" by making their own computer as a tool of the attack. On the other side, of course there was serious indignation, with both Tallinn and the Estonian public were talking about aggression, and NATO was trying to handle the delicate situation with visible nervousness. Lastly, although the case was not considered as a real armed attack, nevertheless the political event caused such a furore that Tallinn's ambition to become the headquarters of the organization's future Cyber Defence Centre was confirmed. Perhaps, thanks to this attack, this happened soon after this.[1]

At the same time, armed conflict became intertwined with the IT attacks that took place during the South Ossetian war in August 2008. In addition to the actual fighting disputes between Georgian and Russian troops, overwhelming attacks were made against a number of Georgian government websites, such as the website of president and the

1 *NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE)*. Its establishment has been on the agenda since 2003 in Estonia. It was established on May 14, 2008 and received full NATO accreditation on October 28, 2008. For more information about the organization, please visit <https://www.ccdcoe.org/> (01/08/2017).

national bank. There is no credible information on what actual attacks have reached the Georgian military infrastructure and with what kind of success, but there is no reason to suspect that such an attack would have not taken place.

The third and most interesting IT attack was carried out in 2010, this time not in an overload format, but in the form of the installed worm virus named Stuxnet. This was triggered in certain Iranian nuclear facilities in their individual control systems which are generally blocked from the internet, and has caused considerable damage in the short term. Analysing the impact soon led to the conclusion that it should be treated as a deliberate, targeted attack with a state background. The virus was discovered a year later as a variant by the Data and System Security Laboratory of Budapest University of Technology and Economics, which was named as Duqu,[2] and shortly before that, the Iranian authorities reported another viral attack by a virus named Stars, but as the technical information related to it was not shared with the professional community, reservations about its use were held for a considerable time afterwards.[3]

The state background behind Stuxnet is supported by the fact that the software itself was very complex and sophisticated, with a targeted differentiation in its activity with respect to a predetermined control system. An analysis of the relationship between the supplier of control software in Iranian installations and Israel further reinforced the idea that using the virus meant intentional interuption of the nuclear program of the Persian state, and Israel did not hide its clear objectives on this issue.

By analysing the above cases, we can distinguish three possible application forms of IT attacks.

In the Russian-Estonian case, although such an act was serious and increased existing political tension, it was not a realistic threat for the use of armed force. Although the world has seen a conflict that erupted during a football match (the so-called "football war" in July 1969 between El Salvador and Honduras. Although the real cause of the war was certainly not the violent acts against the spectators during the qualifying matches between the two states during the 1970 World Cup in June 1969, it has become the direct cause), the demolition of a memorial obviously does not involve such a risk, and in such a situation there is no justification for such a drastic tool. In such a case, cyberattacks may be useful in handling political tensions instead of recourse to force, but still it cannot be regarded being legitimate under current international law.

IT attacks during the Georgian-Russian war, accompanying the ongoing armed conflict can be considered being acceptable harmful acts to a hostile state. They can be regarded as legitimate under international law if they affect legitimate military objects (le-

2 Bencsáth, Boldizsár – Pék, Gábor – Buttyán, Levente – Félegyházi, Márk: *Duqu: A Stuxnet-like malware found in the wild.V0.93 (14 / Oct / 2011)*. Technical Report by Laboratory of Cryptography and System Security (CrySyS). Available online: <www.crysys.hu/publications/files/bencsathPBF11duqu.pdf> (01.08.2017).

3 *Experts sceptical on new Iran "cyber attack" claim*. Reuters, May 5, 2011. Available online: <www.reuters.com/article/2011/05/05/iran-cyber-idAFLDE74417H20110505> (01.08.2017).

gitimate military targets) under the laws of warfare. In such a situation, IT tools and solutions can be treated as legitimate weapons.

The attack on Iranian facilities was, in my opinion, the first case where an IT attack has occurred as a real alternative to the use of armed force. With regard to the Iranian nuclear program, it is clear from the state declarations so far, that the Israeli government was putting itself to a legitimate self-defence position (even if preventive one), therefore it has refrained from the use of force not for legal, but for other reasons, such as political or military considerations. It is a fact that a military operation is complicated, risky and difficult to implement, while also being questionable in effect and politically unpredictable. Consequently, an understandable decision is the choice of IT tools which are capable of causing serious damages, but with more security, while additionally, it brings up a new dimension for the existing conflict: it creates mistrust towards its proprietary software running the standardized tools, generating unpredictability and causing serious uncertainty on the other side. For such a kind of attack – with the follow-up knowledge of the results – it is almost certain that the Iranian party was not prepared.

Due to the advantages outlined above, it is almost certain that IT attacks are becoming more and more realistic alternative to the use of actual armed forces among foreign policy tools. Of course, I do not claim that they will become exclusive, as in some cases these tools are inadequate, but their significance is growing rapidly, which is also evidenced by the fact that states are developing their skills with a rapid pace.[4] Additionally, a series of scandals emerged related to the United States' eavesdropping activities during 2013, which gave an extra boost to them, not even separately mentioning the scandals regarding the 2016 US presidential elections.

9.3 The Question of the Nature and Legal Classification of IT Attacks

If an IT attack is carried out without the existence of an actual armed conflict, i.e. without military activities and with no state background, it is undoubtedly a criminal offense under current provisions of states' domestic legal systems.[5] This qualification is also confirmed by international law, as the so far developed international rules are in line with the substantive content of these internal norms and, on the other hand, they include the possibility of international criminal cooperation on the basis of these.[6]

4 For more on the European situation, see e.g.: *Across Europe, Nations Mold Cyber Defenses*. DefenseNews, July 9, 2013. Available online: <www.defensenews.com/article/20130709/DEFREG01/307090008/> (01/08/2017); For more information on other states: Shackelford, Scott J.: *Estonia Three Years Later*: *Progress Report on Combating Cyber Attacks*. In: Journal of Internet Law, Vol. 13. No. 8. (2010) p. 22.

5 See e.g. *Act C of 2012 on the Criminal Code*. Within this, the Code of Criminal Procedure Act XLIII., such acts are shown in chapter 6, but there are also a number of other offenses related to these regulations, see e.g. Section 287, Section 314, Section 375.

6 The most important international treaty agreed on this topic can be considered as the convention against cybercrime adopted by the Council of Europe. *Convention on Cybercrime*. CETS No. 185. In Hungarian: *Act*

But this interpretation may change if such acts are carried out with a state background or by the institutions for the purpose of serving some political goals. The acts of the persons involved in the operations can continue to be classified as above, but if they are attributable to a state, it also becomes the responsibility of the state in which the criminal liability of the participating individuals may be not recognised. See for example, the military personnel of a military blockade by one state against another one cannot be held criminally liable for it, only because the blockade itself may happen to be illegal under international law. Within the system of international law today, the *ius ad bellum* provisions based on the UN Charter and relevant judicial practice help to determine whether a state uses force legally against another state, and it would be a mistake to declare that an IT attack has to be considered as an "armed attack", and most of the interpretations have rejected it so far, or leave this possibility open with caution.[7]

The situation is different in the case of an armed conflict, as IT tools and solutions are available during ongoing hostilities for serving the military objectives of the state concerned. The goals that are being pursued include collecting hostile military data, misleading enemy military leadership, psychological warfare, disrupting or even actually attacking IT tools (for example weapons with DoS or DDoS tools described above, or with installed viruses). For these acts, *ius in bello* has to be applied to the full range of international law in warfare, since the norms of international humanitarian law (IHL), based on the 1949 Geneva Conventions, apply to all "armed conflicts" under their common Article 2.

What if there is no armed conflict between two states, but is there an IT attack? Could it lead to an "armed conflict" under international law, meaning the outbreak of an international legally-controlled "cyber war" and what consequences would it have?

If we accept that an IT attack can qualify to become an "armed attack" in an international legal sense, a number of questions arise.

Under the current system of international law, an armed attack raises the right to exercise self-defence, which makes it possible to use force – which leads to the question

---

LXXIX of 2004 Act in Budapest by the Council of Europe, which is the Convention on Computational Crime made on 23 November 2001 in Budapest. The importance of the Convention is demonstrated by the fact that, although under the Council of Europe, Australia, Japan and the United States have also become parties.

7 The cautious approach related to this topic is well illustrated by Stéphane Abrial, head of NATO Allied Transformation Command (NATO ATC), published in 2011: Abrial, Stéphane: *NATO Builds Its Cyberdefenses*. The New York Times, February 27, 2011. Available online: <www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=0> (01/08/2017). The Guidelines issued by the NATO CCD COE in 2012 state that such acts may, if appropriate, be integrated into the concept of aggression and trigger the practice of self-defense. Klimburg, Alexander (ed.): *National Cyber Security Framework Manual*. NATO CCD COE Publication, Tallinn, 2012. pp. 169-170. See *inter alia*: Buchan, Russel: *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?* In: Journal of Conflict and Security Law, Volume 17, Issue 2, pp. 212-227; Schmitt, Michael: *Classification of Cyber Conflict*. In: Journal of Conflict and Security Law, Volume 17, Issue 2, pp. 245-260.

of the legitimate toolbox of self-defence against IT operations. Obviously, it is legitimate for a state to use passive defence systems (anytime, not only during an armed conflict), as the purpose of those is to prevent an attack. However, if this happens, would IT counter-attacks with the same means become lawful? Or what is a more delicate issue, can actual military attacks be lawful against the infrastructure and tools used for IT operations?

9.4 International Legal Difficulties in IT Warfare

Difficulties arise from two factors: on the one hand, the complex nature of the subject matter of regulation and, on the other hand, the shortcomings of this regulation regime.

When analysing the problems of IT warfare, we must first conclude that the so-called "virtual battlefield" unfortunately is not purely military. Of course, there are dedicated military systems, but a very large part of the data traffic takes place on the civilian network – hence, most of the potential attacks will be directed against civilian or at least dual-purpose objects (whether IT or real, physically).

There are currently no mandatory, laws of war provisions applicable explicitly to IT warfare. There are several reasons for this deficiency. On the one hand, during the codification of our existing set of norms of international humanitarian law, IT warfare was not a reality in its present form. In 1949, when the Geneva Conventions or, in 1977, when the two Additional Protocols were adopted, the states becoming party did not have to deal with this issue. As a result, their contractual will has not extended to this specific situation, so in the case of any questions not covered by the basic principles of IHL (and its customary norms), it is hard to argue for any legal binding power.

Another major problem is the lack of "conceivable" space as an element. What is "cyberspace" and how can we handle it as a regulatory area? Our entire modern international legal system rests on states which are exercising sovereignty over their territories, and as a result, both the legal regime governing the use of force and of IHL are inseparable from the question of the territory. Yet, in the area of IT warfare, we can hardly build on territoriality: while physical battlefields have some kind of lines and state boundaries, they are difficult to interpret in cyberspace, which can lead to many problems.

Additionally, it is difficult to decide what constitutes a legitimate military target and who qualifies for a legitimate combatant, and what countermeasures against the latter do we consider being permissible by the states. A related problem is the difficulty of dealing with possible violations – for example, in the actual "physical" warfare, the unlawful nature of the act of a civilian person directly engaging in hostilities is easily recognizable on the location in the absence of the criteria established by the Geneva Conventions, and criminal action against that person can be ensured within the legal framework of the same conventions. But this is difficult to imagine from a distance of hundreds or even thousands of kilometres.

9.5 Attempt to Regulate

How can we overcome the problem missing legal provisions somehow? Based on the principles of IHL, we are able to set up analogies with appropriate and possibly even extensive interpretation of the existing rules that can be used to define a corpus juris used in a "cyber war". For example, Additional Protocol I of 1977 contains a number of warfare standards that are appropriate to apply in case of IT attacks.

A remarkable experiment on this topic is the Tallinn Manual, originally prepared in 2013 by NATO CCD COE, which attempts to display these rules systematically.[8] This work is an interpretation and analysis of experts, compiled by the authors invited by the organization, and was intended to create a collection of rules to serve as a basis for the possible creation of an international legally binding regime, using existing law of war standards and practices. During the work, they have included all the existing warfare standards that can be applicable for IT operations as well.

For example, the Additional Protocol defines the principle of distinction during warfare, which dictates that, during hostilities, parties to the conflict are obliged to direct their military operations against the military objects of the adverse party.[9] There is no doubt about the customary legal binding power of this norm, and there is no possible argument to deviate from it in any way, even in the case of use of IT tools – another question is that the practical application of the aforementioned is not easy in cyberspace.[10] Nevertheless, the Tallinn Handbook represents the 31st rule in the same way as for IT operations.[11]

The protocol also clarifies the concept of "attack", which should be an "act of violence",[12] which can be conducted "in whatever territory"[13] according to the wording of the Protocol. This, in my opinion, may include cyber-attacks if we accept broader interpretations of "violence" and "whatever" terms. I find it even possible contrary to the fact, that in the next paragraph, the wording of the Protocol refers to "land, air or sea warfare",[14] omitting the IT warfare, indicating that contracting states were actually thinking about the physical territory when drafting the Protocol. The 30th rule of Tallinn Handbook, bypassing these criteria, as an IT attack, defines IT operations that can reasonably cause injury or death or damage or destruction of material goods.[15]

8 Schmitt, Michael N. (ed.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.
9 *Additional Protocol I.* Article 48.
10 For the customary power, see Articles 7, 146. and 147 rules of the customary study of the International Committee of the Red Cross. Henckaerts, Jean-Marie and Doswald-Beck, Louise: *Customary International Humanitarian Law*. Vol. 1, ICRC and Cambridge University Press, 2009, pp. 25, 519, 523.
11 *Tallinn Manual.* op. cit., p. 95.
12 *Additional Protocol I.* Article 49.
13 Ibid. Section 2.
14 Ibid. Section 3.
15 *Tallinn Manual.* op. cit., p. 92.

The Additional Protocol properly lays down the protection of civilian property and the definition of so-called "military targets".[16] They are also suitable for IT operations. The rules of 32 to 40 of the Tallinn Handbook deal with these issues, essentially creating a regulatory regime parallel to the provisions of the Protocol and the customary international humanitarian law.[17]

Similar solutions can be found in the case of precautions during hostilities, regarding to special legal protection for special objects and in many other sub-fields of IHL. Overall, we can conclude that, as it is generally the case for laws of war or IHL in case of all types of armed conflicts, they are considered being legally binding in the case of IT operations and IT warfare as well.

The Tallin project has not slowed down ever since. The next version of the volume has been publiched in the February of 2017, with extensions and additional analysis.[18]

9.6 Active Individual Participation in IT Operations

In the area of humanitarian international law, civilian individual participation in hostilities has become one of the most burning issues of the recent period, namely the engagement of those who are not entitled to it under the rules of war. This problem is a difficult task for the armed forces of states and for IHL, it is no coincidence that in 2009 a comprehensive guide was published by the International Committee of the Red Cross.[19]

Related to IT operations, this problem is exaggerated, because in an IT operation, the willingness of the civilians to participate is much greater than in "normal" hostilities with actual weapons. The obvious reason for this is the minor sense of danger, as an individual often conducts this activity in his home, in a safe environment, and he does not have to fear from falling bombs or military assault. Additionally, as this is a simple activity, the average user often needs to do nothing else than just installing a destination application and then settling down satisfied, with the sense of he has "done something". During the Russian-Estonian "cyber war" described above, a problem that has already been mentioned was visible in a very spectacular way: on the Russian internet community interfaces, programs were made easily available for users so that they could use them to "set their own machines into battle" with DDoS attacks against Estonian systems. This is complemented by the fact that the technical equipment required for this is really easily accessible to everyone: weapons and ammunition are not easy to obtain, but anyone can access to IT tools through the right commercial, or the illegal online channels.

16 *Additional Protocol I.* 51-52. Article.
17 *Tallinn Manual.* op. cit. pp. 97-118.
18 N. Schmitt, Michael (ed.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd. ed.)*. Cambridge University Press, 2017.
19 Melzer, Nils: *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. ICRC, 2009.

The authors of the Tallinn Handbook specifically addressed this problem and introduced Rule 35 with the customary law of the law of war and based on the analysis of the Red Cross,[20] according to which civilians lose their protection and immunity if they get directly involved in the hostilities.[21] According to the authors, they can legitimately be attacked by using both IT and other legitimate methods,[22] but the manual does not clarify legitimacy.

One shortcoming and an open-ended question is that the investigation has not resolved the problem of "passive", i.e., unintentional but still direct participation. It is possible that someone becomes involved in negligence, for example, by simply neglecting the protection of his own computing devices, and his computer becomes an actor for such an operation as a zombie. It is a legitimate argument that in this case the person cannot be regarded as an active participant in the absence of his intention[23] but at the same time the attacked party cannot decide about the device whether he intentionally or negligently participates in the attack against him – and under certain circumstances that party will not even strive for this. This problem points to one of the major shortcomings of our modern IT society itself, namely the conscious and responsible use of computers, or more specifically, the lack of it. It should be made clear to the users that – even in a way comparable to driving – that the use of computer technology can be a hazardous operation, which means responsibility. But the scope of this responsibility has not yet been determined by the law.

9.7 Conclusion

The present study does not deal with all emerging issues and it is currently focused on questions and fundamental points.

Solutions in the area of international law seem to be capable of addressing the problems arising from today's information society. However, the problems and shortcomings are becoming more and more acute, for which some international legislation is inevitable, even in the near future. For now, expert analyses and studies are preparing this, but when it will be realized in the form of actual international treaties, is still an open question.

20 Ibid. pp. 46-47.
21 *Tallinn Manual.* op. cit., pp. 101-102.
22 Ibid. p. 102. 3. bek. (Translation and highlighting of the author).
23 The same conclusion is drawn according to the interpretation of the Red Cross. Melzer, Nils: op. cit., p. 60.