# (New) Cyber Exploitation and (Old) International Humanitarian Law

**Longobardo, M.**

This is a copy of an article published in ZaöRV/HJIL 77 (2017), p. 809-834.

http://www.zaoerv.de/77_2017/vol77.cfm

# (New) Cyber Exploitation and (Old) International Humanitarian Law

*Marco Longobardo*[*]



## Abstract

Cyber exploitation is a new means of intelligence gathering. It refers to unauthorised access to computers, computer systems, or networks, in order to gain information, without affecting the functionality of the accessed system or deleting the data contained or in transit therein. States employ cyber exploitation both in peacetime and in wartime since cyber exploitation often

[*] Research Fellow (Public International Law) at Westminster University, and Adjunct Professor (International Law and EU Law) at the University of Messina; Ph.D. (International Law and EU Law) from the University of Rome "Sapienza". I wish to thank *Marcella Distefano*, *Giulio Bartolini*, and *Marco Roscini* with whom I discussed this topic on a number of occasions. I presented some ideas embodied in this article at the conference "La protezione dei dati personali ed informatici nell'era della sorveglianza globale", University of Messina, 7.11.2015, and at the seminar "Cyber Exploitation and International Humanitarian Law", University of Westminster, 26.5.2016; many thanks to all the participants to these events for their useful comments. All the usual disclaimers apply. All internet references were last accessed on 15.5.2017 when the paper was completed. Email <m.longobardo1@westminster.ac.uk>.

proves relevant both in order to plan and launch an attack and in order to gain information for defensive purposes.

Since international humanitarian law is the law that regulates the conduct of the hostilities, it is necessary to test the applicability of its rules to cyber exploitation. Cyber exploitation proves particularly problematic because it is an extremely recent phenomenon, while international humanitarian law rules were mainly codified in 1907, 1949 and 1977, when cyber warfare had not yet been envisaged. Accordingly, the application of these old provisions to such a new phenomenon requires an in depth analysis.

To this end, this paper first examines the international humanitarian law rules regarding intelligence collection in wartime, with particular regard given to espionage. This paper goes on to verify whether these old rules are applicable and relevant to the case of cyber exploitation. Finally, this paper examines the applicability of the rules regarding direct participation of civilians in hostilities to instances involving cyber exploitation.

This paper concludes postulating that international humanitarian law considers cyber exploitation to be a lawful activity since these rules do not prohibit intelligence gathering. However, this paper further demonstrates that specific international humanitarian law rules are not applicable to cyber exploitation, apart from very marginal and unpractical cases.

> Oh friends! hath no Achaian here such trust
> In his own prowess, as to venture forth
> Among yon haughty Trojans? He, perchance,
> Might on the borders of their host surprise
> Some wandering adversary, or might learn
> Their consultations, whether they propose
> Here to abide in prospect of the fleet,
> Or, satiate with success against the Greeks
> So signal, meditate retreat to Troy.
> These tidings gain'd, should he at last return
> Secure, his recompense will be renown
> Extensive as the heavens, and fair reward.[1]

[1] *Homer*, Iliad, X, 240 et seq., English translation available at <archive.org>.

# I. Introduction

The way in which hostilities and warfare are conducted changes constantly, evolving very rapidly. Men and women have tried to improve their capacity to kill other men and women seemingly with the same perseverance as natural predators in the wilderness strives to become faster than their prey. The rule at the basis of the entire evolutionary model is that even preys evolve, and thus, the predators will ultimately never be able to prevail completely. However, they will try to evolve further, and the evolution of both prey and predator will continue.[2]

The same phenomenon can be observed in the evolution of the activity of intelligence gathering, one of the oldest human activities connected with the art of warfare, going back further than the times of *Homer*. Since the dawn of civilisation as we know it, powers have been exploring new ways to gather information about their enemies in times of armed conflict, but their efforts have been matched by the equal struggles of other powers to develop more sophisticated defences against enemy intelligence activity. As with wildlife, this balance between two opposite forces is at the basis of the frenzied evolution of intelligence gathering techniques and technologies.[3]

However, the evolution of the instruments through which mankind steals its enemies' secrets has not been equally matched by a similar evolution of the international law rules regarding intelligence gathering in wartime. The relevant rules are embodied in the international humanitarian law conventions, which were adopted between 1899 and 1977. Frankly, these rules are quite outdated compared to the technological revolution that has radically changed the way information is collected in wartime since the end of the twentieth century, continuing through the beginning of the new millennium.

This paper focuses on a specific means of intelligence collection, cyber exploitation, and on the applicability of international humanitarian law to this new phenomenon. The paper begins by defining what cyber exploitation encompasses. After an examination of the international humanitarian law rules regarding the collection of intelligence in wartime and specifically

[2] It should be superfluous to mention here the masterpiece of *C. Darwin*, The Origins of Species by Means of Natural Selection, 1859.

[3] For an overview of this process, see *F. Calvi/O. Schmidt*, Intelligences secrètes: annales de l'espionnage, 1988; *A. N. Shulsky/G. Schmitt*, Silent Warfare: Understanding the World of Intelligence, 3rd ed. 2002; *J. Keegan*, Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Quaeda, 2003.

regarding espionage, the paper moves on to verify whether these old rules are applicable and relevant for cyber exploitation. Moreover, the paper analyses the applicability of the rules on direct participation of civilians in the hostilities to cyber exploitation. The paper concludes by positing that, even though international humanitarian law is not completely silent regarding intelligence gathering activity through this means, the old international humanitarian law rules are not entirely adequate to regulate this new phenomenon of cyber exploitation.

## II. Intelligence Collection in Wartime: An Overview

Intelligence collection in wartime is a practice as old as war itself, and is often nicknamed the second oldest profession.[4] Acquiring information in times of armed conflict is crucial. An attacking army needs to know the position of the enemy, their strengths, the number of troops presiding over military objectives, the intentions of the enemy commanders, and other similar circumstances that, if known, could impact the success of offensive and defensive operations. This information is considered so critical that states usually cloak the entire war process in secrecy in order to prevent the enemy from gaining relevant information.[5] Generally, the activity of collecting information is called intelligence gathering,[6] and it can be performed both in times of peace and war.

The most striking difference between peacetime and wartime intelligence collection is that, according to a number of authoritative publicists, international law neither prohibits nor allows peacetime intelligence collection,[7]

---

[4] *P. Knightley*, The Second Oldest Profession: Spies and Spying in the Twentieth Century, 1980.

[5] See *O. Ben-Naftali/R. Peled*, How Much Secrecy Does Warfare Need?, in: A. Bianchi/A. Peters (eds.), Transparency in International Law, 2013, 321 et seq.

[6] Other definitions of intelligence encompass other activities as well. For instance, on the basis of some domestic legislation, some publicists consider that extraterritorial covert military operations fall into the definition of intelligence (see e.g. *L. Salvadego*, La nuova disciplina italiana sulle operazioni di "intelligence di contrasto" all'estero, Riv. Dir. Int. 99 (2016), 1187 et seq.).

[7] See *R. A. Falk*, Foreword, in: R. J. Stanger (ed.), Essays on Espionage and International Law, 1962, i et seq., v; *S. Chesterman*, The Spy Who Came from the Cold War: Intelligence and International Law, Mich. J. Int'l L. Michigan Journal 27 (2006), 1071 et seq.; *G. Sulmasy/J. Yoo*, Counterintuitive: Intelligence Collection and International Law, Mich. J. Int'l L. 28 (2007), 635 et seq. For recent overviews of this topic, see *I. Navarrete*, L'espionnage en temps de paix en droit international public, Can. Yb. Int'l L. 63 (2016), 1 et seq.; *K. Kitti-*

while international humanitarian law clearly considers intelligence collection in wartime to be lawful. According to Art. 24 of the 1907 Hague Regulations (HR), "[r]uses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible".[8] This rule is embodied in a number of international instruments regarding the law of war,[9] and it is part of customary international law. Accordingly, a state involved in intelligence gathering during an armed conflict does not breach international humanitarian law, but rather it exercises a prerogative that is connected with its freedom to choose the means and method of warfare.

Moreover, an attacking state is compelled to gather certain information in order to verify the nature of the objective of the attack and its consequences pursuant to Art. 57(2)(a)(i) of the First Additional Protocol (AP I).[10] One can therefore conclude that intelligence collection in wartime is an activity that states can lawfully undertake for the success of a military operation; at the same time, an attacking state must perform intelligence collection in order to implement the principles of distinction and proportionality.

Intelligence collection covers a number of different activities, developed since the ancient times for as long as new technological devices and techniques have been being devised. One can classify intelligence collection on the basis of different criteria, based on the methods employed (human intelligence, communication intelligence, financial intelligence)[11], or the object

---

*chaisaree*, Public International Law of Cyberspace, 2017, 233 et seq. For the view that states have the right to collect intelligence information, see *A. Lubin*, Espionage as a Sovereign Right Under International Law and Its Limits, ILSA Quarterly 24 (2016), 22 et seq.

[8] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18.10.1907 (HR).

[9] Project of an International Declaration concerning the Laws and Customs of War, Brussels, 27.8.1874 (Brussels Declaration), available at <https://ihl-databases.icrc.org>, Art. 14; HPCR Manual on International Law Applicable to Air and Missile Warfare, Bern, 15.5.2009 (HPCR Manual), available at <ihlresearch.org>, Rule 119. See also Instructions for the Government of Armies of the United States in the Field (Lieber Code), 24.4.1863, available at <www.icrc.org>, Art. 101, which is the first codification of the law of armed conflict, albeit in the form of a domestic military manual.

[10] Protocol Additional to the Geneva Conventions of 12.8.1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8.6.1977 (API) <www.icrc.org>. On this topic, see *M. Longobardo*, L'obbligo di verificare l'obiettivo e le conseguenze di un attacco ai sensi del diritto internazionale umanitario e nuove forme di intelligence: profili di responsabilità internazionale, in: A. Spagnolo/S. Saluzzo (eds.), La responsabilità degli Stati e delle organizzazioni internazionali: nuove fattispecie e problemi di attribuzione e di accertamento, 2017, forthcoming, available at <papers.ssrn.com>.

[11] See *A. Sambei*, Intelligence Cooperation versus Evidence Collection and Dissemination, in: L. van den Herik/N. Schrijver (eds.), Counter-Terrorism Strategies in a Fragmented

and scope of the activity itself (strategic intelligence, tactical intelligence, operation intelligence)[12], or its scale (mass surveillance or targeted surveillance). Despite the fact that all these categories are useful for an understanding of the complexities of intelligence collection and its adaptability to different exigencies, the only means of intelligence collection specifically examined by international humanitarian law is espionage, which is regulated by a number of international law conventions pertaining to the law of armed conflict. Other than in the case of espionage, international humanitarian law merely considers the genus "intelligence" to be lawful, not paying any attention to the specific way in which it is undertaken, at least as long as it does not constitute an act of perfidy prohibited by Art. 37 AP I.

## III. The Practice of Cyber Exploitation

Traditionally, war has been combatted in the physical realms of land, sea, air, and – in recent times – space. In recent decades, a new intangible battlefield – cyberspace – has become increasingly relevant.[13] In this realm, technology allows states to conduct war-like operations that are commonly defined as cyber operations. Even if there is no general consensus on the exact definition of cyber operations, for practical reasons this paper relies on the definition recently embodied in the 2016 United States (US) Military Manual, according to which cyber operations are

Legal Order, 2013, 212 et seq., 216 et seq. Other authors suggest different classifications (see e.g. *W. Gracido/J. Pirc*, Cybercrime and Espionage: An Analysis of Subversive Multivector Threats, 2011, 96 et seq.).

12 See *W. Gracido/J. Pirc* (note 11), 91 et seq.

13 The literature on cyberspace as battlefield is particularly vast. See, among many others, *H. Harrison Dinniss*, Cyber Warfare and the Laws of War, 2012; *M. N. Schmitt* (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013 (Tallinn Manual); *L. Baudin*, Les cyber-attaques dans les conflits armés: qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire, 2014; *M. Roscini*, Cyber Operations and the Use of Force in International Law, 2014; *Y. Radziwill*, Cyber-Attacks and the Exploitable Imperfections of International Law, 2015; *C.-J. Woltag*, Cyber Warfare: Military Cross-Border Computer Network Operations under International Law, 2015; *K. Kittichaisaree* (note 7), 201 et seq.; *M. N. Schmitt* (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed. 2017 (Tallinn Manual 2.0). See also the papers published in *R. Buchan/N. Tsagourias* (eds.), Symposium: Cyber War and International Law, Journal of Conflict and Security Law 17 (2012), 183 et seq.; *R. Buchan/N. Tsagourias* (eds.), Special Issue: Non-state Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence, Journal of Conflict and Security Law 21 (2016), 377 et seq.

> "those operations that involve '[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace'. Cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace."[14]

Normally, cyber operations are divided into two main categories: cyber-attacks and cyber exploitation. A cyber-attack "is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[15] In the view of the US Department of Defense, cyber exploitation (or computer network exploitation) is an "[e]nabling operation[ ] and intelligence collection to gather data from target or adversary automated information systems or networks".[16] Accordingly, the main difference between cyber-attacks and cyber exploitation operations is in the nature of the payload to be executed: in cases of cyber exploitation, the computer or system targeted is not disrupted or damaged, and the data transient therein are not altered, corrupted or deleted.[17] Even though cyber-attacks and cyber exploitation are often conducted jointly and with similar means, they are different phenomena that must be kept distinct.

Cyber exploitation may be performed both in times of peace and in times of war. With regard to recent peacetime practice,[18] for instance it can be recalled that Georgia recently affirmed that Russian security agencies had collected confidential information by infiltrating malware in some Georgian security servers.[19]

---

[14] US Department of Defense, Law of War Manual (Updated December 2016), 16.1.2 (references omitted). See also the definitions embodied in Tallinn Manual 2.0 (note 13), 258, and in ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, ICRC Doc 31IC/11/5.1.2, October 2011, 36.

[15] Rule 92 in Tallinn Manual 2.0 (note 13), 106.

[16] See US Department of Defense, Joint Terminology for Cyberspace Operations, 4, para. 5.

[17] See *H. S. Lin*, Offensive Cyber Operations and the Use of Force, Journal of National Security Law and Policy 4 (2010), 63 et seq., 64; *M. Roscini* (note 13), 16.

[18] For an overview of this practice in peacetime and valuable remarks on its legal implications, see *H. P. Aust*, Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht, AVR 52 (2014), 375 et seq.; *R. Buchan*, Cyber Espionage and International Law, in: N. Tsagourias/R. Buchan (eds.), Research Handbook on International Law and Cyberspace, 2015, 168 et seq.

[19] See Georgian Ministry of Justice, Cyber Espionage Against Georgian Government, available at <dea.gov.ge>. Moreover, it has been reported that the Italian Ministry of Foreign Affairs was targeted by operations of cyber exploitation in 2016 (see *S. Kirchgaessner*, Russia

As to recent wartime practice, it has been reported that both the Syrian government and the opposing groups are involved in cyber exploitation activities,[20] while, in 2014, Hamas claimed to have violated Israeli governmental systems and to have stolen some data.[21] Moreover, in 2015, a Kosovo citizen was arrested in Malaysia under suspicion of having stolen US service members' data on behalf of the Islamic State of Iraq and Syria (ISIS).[22] In addition, the relevance of these kinds of cyber operations during armed conflict is evident in a number of military manuals and doctrines, all of which emphasise the role of confidential information exploited through cyberspace in relation to different aspects of the conduct of hostilities.[23]

Consequently, because of the present and future importance of cyber exploitation to the manner in which States conduct hostilities, determining whether international humanitarian law regulates these cyber exploitation operations is crucial.

---

Suspected over Hacking Attack on Italian Foreign Ministry, The Guardian, 10.2.2017, available at <www.theguardian.com).

[20] See *J. Sahalni*, In Syria, the Cyberwar Intensifies, 20.2.2013, available at <www.oiip.ac.at>.

[21] See Hamas "Hacks into" Israeli Defence Computers and Leak Video Footage, International Business Times, 14.12.2014, available at <www.ibtimes.co.uk>.

[22] See U.S. Accuses Hacker of Stealing Military Members' Data and Giving It to ISIS, The Washington Post, 16.10.2015, available at <www.washingtonpost.com>.

[23] See U.S. Department of the Army, Targeting, ATP 3-0, FM 3-60, May 2015, Section B-29: "[…] Documents and pocket litter, as well as information found on computers and cell phones, can provide clues that analysts need to evaluate enemy organizations, capabilities, and intentions. The threat's network becomes known a little more clearly by reading his email, financial records, media, and servers. Target and document exploitation help build the picture of the threat as a system of systems."

See also Republica de Colombia, Manual de Doctrina Básica Aérea y Espacial, 4th ed. 2013, 86: "Ciber-inteligencia: Son operaciones realizadas en el ciberespacio encaminadas a recolectar, procesar, explotar y difundir información para el planeamiento y ejecución de operaciones Aéreas, Espaciales y Ciberespaciales."

# IV. Cyber Exploitation as a Modern Kind of Espionage in Times of War

## 1. The Regime of Espionage under International Humanitarian Law

### a) The Definition of Espionage and Spies

International humanitarian law conventions, non-binding private codifications, and military manuals generally address espionage in a coherent way, so that today, one can easily conclude that the regulation of espionage is the same both in treaty and customary international humanitarian law.[24]

Espionage falls into the definition of ruses of war not amounting to perfidy pursuant to Art. 24 HR. Consequently, espionage in times of war is a lawful method of war, as recognized by national case law.[25]

Espionage may be performed either by members of the enemy armed force or by civilians. According to the HR and a number of non-binding private codifications, spies are "individuals" or "persons".[26] Such a classification implies that both soldiers and civilians can be considered to be spies.[27] This conclusion is confirmed by Art. 5 of the Fourth Geneva Convention (IV GC) which regulates the guarantees pertaining to "individual protected person[s] … definitely suspected of or engaged in activities hostile to the security of the State" and "individual protected person[s] …detained as a spy or saboteur" in the occupied territory.[28] Accordingly, the fact that Art. 46(1) AP I refers to "member of the armed forces of a Party to the conflict … engaging in espionage" should not be considered as a reformulation

[24] See e.g. *E. David*, Principes de droit des conflits armés, 4th ed. 2008, 489; *W. H. Boothby*, The Law of Targeting, 2012, 277.

[25] *Flesche* case (Holland, Special Court of Cassation, 1949) [1949] 16 AD 266 et seq., 271 et seq. See also U.K. Ministry of Defence, The Joint Service Manual of the Law of Armed Conflict, 2004, section 4.9.3; Australia, Law of Armed Conflict, ADDP 06.4, 2006, section 7.18; US Department of Defense (note 14), section 4.17.4.

[26] See HR, Art. 29; Lieber Code, Art. 88; Brussels Declaration, Art. 19; Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Drafted by a Commission of Jurists at the Hague, December 1922-February 1923 (Hague Rules Air Warfare), available at <www.icrc.org>, Art. 27; HPCR Manual, Rule 118.

[27] See *Flesche* case (note 25), 271.

[28] Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12.8.1949 (IV GC), Art. 5.

of the definition of a spy.[29] The possibility of considering also civilians to be spies in light of the AP I is confirmed by the incipit of Art. 46(1) itself, according to which this provision is without prejudice to rules embodied in the IV GC.[30]

Spies are defined according to a three-fold test. First, espionage requires an activity of information collection and transmission. Spies collect information that is relevant for the conduct of the armed conflict and transmit or attempt to transmit this information to one of the parties of the conflict.[31] If an individual accidentally or unwillingly discovers relevant information, they is not a spy.[32] Equally, if the information is not linked to the armed conflict or the individual does not want to deliver it to one of the parties of the conflict, then they should not be considered a spy.[33]

Second, spies act clandestinely or under false pretence. Consequently, members of armed forces have to act in disguise (e.g. without their uniform or other distinctive emblems) in order to be qualified as spies; whereas, any individual – military or civilian – who carries out their activity openly should not be considered a spy.[34] If the clandestine character of the activity is not present, the activity of intelligence gathering may not be considered espionage. For instance, members of the armed forces openly collecting information relevant for an armed conflict fall into the definition of military reconnaissance, which is a lawful kind of intelligence gathering that is inherently different from espionage.[35]

Finally, international humanitarian law considers only individuals who gather information in certain areas to be spies. In this respect, conventional international humanitarian law shows a progressive evolution: according to the Lieber Code, only individuals "within or lurking about the lines of the

---

29 See *K. Ipsen*, Combatants and Non-Combatants, in: D. Fleck (ed.), The Handbook of International Humanitarian Law, 3rd ed. 2013, 79 et seq., 108; *E. Crawford/A. Pert*, International Humanitarian Law, 2015, 98.

30 AP I, Art. 46(1): "Notwithstanding any other provision of the Conventions or of this Protocol …".

31 Lieber Code, Art. 88; Brussels Declaration, Art. 19; HR, Art. 29; Hague Rules Air Warfare, Art. 27; AP I, Art. 46(2); HPCR Manual, Rule 118.

32 Brussels Declaration, Art. 22; HR, Art. 29.

33 See *G. Balladore Pallieri*, Diritto bellico, 2nd ed. 1954, 223.

34 Lieber Code, Art. 88; Brussels Declaration, Art. 19 and Art. 22; HR, Art. 29; Hague Rules Air Warfare, Art. 27; AP I, Art. 46(2) and Art. 46(3); HPCR Manual, Rule 120.

35 On this topic, see generally *O. J. Lissitzyn*, Electronic Reconnaissance from the High Seas and International Law, International Law Studies 61 (1970), 563 et seq.; *C. Hollweg*, Military Reconnaissance, in: R. Bernhardt (ed.), EPIL, Vol. III, 1982, 279 et seq.; *D. Stephens/T. Skousgaard*, Military Reconnaissance, in: R. Wolfrum (ed.), MPEPIL online ed., 2009, available at <opil.ouplaw.com>.

captor" are spies;[36] pursuant to the Brussels Declaration, spies are those individuals who operate in "the districts occupied by the enemy";[37] the 1899 and 1907 Hague Regulations refer to "the zone of operations of a belligerent",[38] and a similar criterion is embodied in the Hague Rules on the Air Warfare;[39] the IV GC, more broadly, considers to be spies those who collect information "... in the territory of a Party to the conflict ... [or] in occupied territory ..."[40], while the AP I refers to "the territory controlled by an adverse Party".[41] This last geographical qualification is the one most in line with contemporary customary law.[42]

In brief, international humanitarian law only considers someone a spy if that person is present in a territory controlled by a belligerent, gathering information relevant for the conflict through clandestine means and/or under disguise, and intending to transmit that information to the enemy.[43]

### b) The Penal Prosecution of Spies

After having defined who is a spy and what espionage is international humanitarian law prescribes that spies, if captured, are not entitled to the status of prisoners of war.[44] This means that spies are subject to the domestic criminal law of the state that captures them. However, since espionage is not a violation of international humanitarian law, spies should not be prosecuted as war criminals.

---

36 Lieber Code, Art. 83.

37 Brussels Declaration, Art. 19.

38 HR, Art. 29.

39 Hague Rules Air Warfare, Art. 27: "… within belligerent jurisdiction or in the zone of operations of a belligerent …".

40 IV GC, Art. 5.

41 AP I, Art. 46(2). See also HPCR Manual, Rule 118.

42 See *Y. Dinstein*, The Conduct of Hostilities under the Law of International Armed Conflict, 3rd ed. 2016, 280 et seq.

43 This conclusion is confirmed by a number of military manuals. See, among the most recent ones, section UK Ministry of Defence, Joint Service Manual of the Law of Armed Conflict (JSP 383, 2004), 4.9; German Ministry of Defense, Law of Armed Conflict – Manual – Joint Service Regulation (ZDv) 15/2, 1.5.2013, section 345; US Department of Defense (note 14), section 4.17.2.

44 See HR, Art. 31; AP I, Art. 46(1); *J.-M. Henckaerts/L. Doswald-Beck* (eds.), Customary International Humanitarian Law, Vol. I, 2005, (ICRC Customary IHL), Rule 107; HPCR Manual, Rule 121. See also *Ex parte Quirin et al.* (US Supreme Court), AD 10 (1941-1942), 564 et seq., 571.

International humanitarian law provides some guarantees to the captured spy. In this regard, one can register an important evolution. At the origins of the codification of the law of armed conflict, the Lieber Code provided that a spy should be executed by hanging, notwithstanding their gender.[45] Subsequent conventions have alleviated the treatment of spies, which can be punished only after a fair trial.[46] Moreover, if the spy is a protected person under the IV GC, the individual has the right to all the guarantees provided by the convention itself, unless they would be prejudicial to the security of the state.[47] However, if a spy is detained in occupied territory, they can be denied rights of communication if absolute military security so requires.[48] On the other hand, they must be treated with humanity, and in case of trial, shall not be deprived of the rights of fair and regular trial.[49] Finally, one has to note that today it is well established that both international human rights law and international humanitarian law are applicable during armed conflict.[50] Although this is not the occasion to discuss the interplay between international humanitarian law and international human rights law,[51] suffice it to say that the captured spy must be treated in conformity with the relevant international human rights standards, which are also relevant for the interpretation of international humanitarian law provisions (such as those regarding the right of a "fair trial").[52]

The possibility for a state to threat an individual as a spy is limited with respect to the time of its capture. According to a rule codified in every instrument dealing with espionage, an individual may not be punished as a

45 Lieber Code, Art. 88(2), Art. 101, and Art. 102.

46 HR, Art. 30. An identical provision is embodied in the ICRC Customary IHL, Rule 107.

47 IV GC, Art. 5(1) and (3).

48 IV GC, Art. 5(2).

49 IV GC, Art. 5(3).

50 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion), ICJ Rep. 1996, 226 et seq., para. 25; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion), ICJ Rep. 2004, 126 et seq., para. 106 (*Wall* opinion); *Armed Activities on the Territory of the Congo* (*DRC v. Uganda*) (Judgment), ICJ Rep. 2005, 168 et seq., para. 216.

51 See generally the essays collected in *P. Eden/M Haploid* (eds.), Symposium: The Relationship between International Humanitarian Law and International Human Rights Law, Journal of Conflict and Security Law 14 (2009), 441 et seq.; *R. Arnold/N. Quénivet* (eds.), International Humanitarian Law and Human Rights Law: Towards a New Merger in International Law, 2008; *R. Kolb/G. Gaggioli* (eds.), Research Handbook on Human Rights and Humanitarian Law, 2013.

52 See *Y. Arai-Takahashi*, Fair Trial Guarantees in Occupied Territory — The Interplay between International Humanitarian Law and Human Rights Law, in: R. Arnold/N. Quénivet (note 51), 449 et seq.

spy if they has returned to their army or the territory controlled by their party.[53] It has been suggested that this rule applies only to spies that belong to an armed force, and, therefore, it would be inapplicable to civilians since they do not belong to any army and they are not entitled to the status of prisoners of war.[54] This rule may be justified on different grounds: it has been suggested that such hard punishment of spies is a deterrent that becomes moot if the spies, returned to their party, have delivered the collected information.[55] Moreover, some have argued that it is a consequence of the fact that spies are unlawful combatants rather than war criminals, and thus they can be punished only while they are actively carrying out their activity.[56] Notwithstanding the legal justification behind this rule, it reflects a well-established state practice and body of case law developed during the two World Wars that is part of customary international law today.[57]

## 2. The Application of the Rules on Espionage to Cyber Exploitation

After having described the rules on espionage, it is necessary to try to apply them to cyber exploitation. To this end, it is worthwhile to note that no international humanitarian law convention deals with cyber exploitation; this is due to the fact that at the time of the drafting, this phenomenon did not yet exist. In the absence of a specific convention on cyber operations,[58] it is necessary to try to apply the existing rule to new phenomena such as

[53] Lieber Code, Art. 104; Brussels Declarations, Art. 21; HR, Art. 31; API, Art. 46(4); HPCR Manual, Rule 122.

[54] See *Flesche* case (note 25), 272; US Department of Defense (note 14), section 4.17.5.1; *Y. Dinstein* (note 42), 279. Contra, see *F. Lafouasse*, L'espionnage en droit international, A.F.D.I. 47 (2001), 63 et seq., 98 et seq.; *L. Salvadego* (note 6), 1192.

[55] See *M. C. Ciciriello*, Spionaggio (diritto internazionale), in: Enciclopedia Giuridica, Vol. XXX, 1993, 1 et seq., 4.

[56] See *G. Balladore Pallieri* (note 33), 224; *Y. Dinstein* (note 42), 279.

[57] See the practice analysed by *G. Balladore Pallieri* (note 33), 224 et seq.

[58] Some argue that such a convention should be adopted. See e.g. *D. Brown*, A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflicts, Harv. Int'l. L.J. 47 (2006), 179 et seq. For an overview of the ongoing debate, see *R. Liivoja*, Technological Change and the Evolution of the Law of War, Int' l Rev. of the Red Cross 97 (2015), 1159 et seq., 1160 et seq.

cyber exploitation.[59] To this end, the Tallinn Manuals provide extremely useful guidance notwithstanding their non-binding character.[60]

First, one has to consider that cyber exploitation may be conducted by members of armed forces or can be outsourced to civilian agencies. Agencies such as the US Central Intelligence Agency are among the most prominent actors in the intelligence arena and are made up by civilians.[61] Potentially, both civilian and military operators who are responsible for cyber exploitation could be considered spies.

Second, cyber exploitation meets the criterion of the willingness to gather information that is relevant for the hostilities in order to transmit said information to a party of the conflict.[62]

Third, cyber exploitation is *per se* a clandestine method of information gathering since the programs employed are designed to collect information in secrecy.[63] Accordingly, if the operator is a civilian, the intelligence operation is conducted clandestinely irrespectively of any other elements thanks

---

[59] See *M. Roscini* (note 13), 280 et seq.; *N. Tsagourias*, The Legal Status of Cyberspace, in: N. Tsagourias/R. Buchan (note 18), 13 et seq.

[60] On the value of the so-called private codifications of international customary law, such as the Tallinn Manual, see *T. Treves*, International Customary Law, in: R. Bernard (note 35), paras. 61-62; *S. Sivakumaran*, The Influence of Teachings of Publicists on the Development of International Law, ICLQ 66 (2017), 1 et seq., 7 et seq. For some critical remarks on the content of the Tallinn Manual, see *D. Fleck*, Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual, Journal of Conflict and Security Law 18 (2013), 331 et seq.; *O. Kessler/W. Werner*, Expertise, Uncertainty, and International Law, a Study of the Tallinn Manual on Cyberwarfare, LJIL 26 (2013) 793 et seq.; *W. Heintschel von Heinegg*, The Tallinn Manual and International Cyber Security Law, Yearbook International Humanitarian Law 15 (2012), 3 et seq.; *R. Liivoja/T. McCormack*, Law in the Virtual Battlespace: The Tallin Manual and the Jus in Bello, Yearbook International Humanitarian Law 15 (2012), 15 et seq., 45 et seq.

[61] Congressional Research Service, Special Operations Forces (SOF) and CIA Paramilitary Operations: Issues for Congress, CRS Report RS22017, 4.1.2005, 2.

[62] Republica de Colombia (note 23), 86; US Department of the Army (note 23), Section B-29.

[63] See Tallinn Manual 2.0 (note 13), 410.

"'Clandestinely' refers to activities undertaken secretly or secretively, as with a cyber espionage operation designed to conceal the identity of the persons involved or the fact that it has occurred. An act of cyber information collection is 'under false pretenses' when so conducted as to create the impression that the individual concerned is entitled to access the information in question. In the cyber domain, it often consists of an individual masquerading as a legitimate user by employing the user's permissions to access targeted systems and data."

See also *W. A. Owens/K. W. Dam/H. S. Lin*, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 2009, 81 et seq.: "The primary technical requirement of a cyberexploitation is that the delivery and execution of its payload must be accomplished quietly and undetectably – secrecy is often far less important when cyberattack is the mission."

to the inherent clandestine character of the means employed for cyber exploitation. On the other hand, if the operator is a member of the armed force, the problem is more convoluted: it has been argued that, since it is not practically feasible to design military Internet Protocol (IP) addresses in order to implement the principle of distinction,[64] one has to consider irrelevant the fact that the operator wears a uniform because "in the high-tech battlespace there is no practical need for such distinguishers".[65] However, this argument is not completely convincing since it conflicts with the aforementioned clear provisions regarding the fact that a member wearing its uniform is not a spy par definition. Respect for the principle of distinction and the role of uniforms and emblems in cyber operations are extremely complex issues due to the interplay between private and public actors on the one hand, and private and public infrastructures on the other.[66] However, in the absence of a contrary practice, it is critical to qualify as espionage cyber exploitation conducted by operators in uniform.

Fourth, espionage requires the physical presence of the individual in the territory controlled by the enemy. This requirement of physical presence appears to be the main hindrance to considering cyber exploitation a form of espionage. The advantage of cyber exploitation is that it allows belligerents to gather information far from the actual place where the hostilities are conducted, from a remote and safe position that is situated normally within the territory of the state that launches the cyber exploitation. Accordingly, operators responsible for cyber exploitation are unlikely to ever be present in the territory controlled by the enemy; not only would it be extremely risky for the operators, but it would also frustrate the main advantage of cyber exploitation – that is the possibility of gathering information far from the theatre of the armed conflict.

Other scholars have suggested that the requirement of the physical presence of the operator in the territory controlled by the enemy could be interpreted in a looser way. According to one author, the cyber exploitation agent can be considered physically present in the enemy territory since their programs infiltrate systems and networks that are located in that territory.[67]

---

64 *H. Harrison Dinniss* (note 13), 146 et seq.

65 *H. Harrison Dinniss* (note 13), 147 et seq. (with reference to distinction in cyber-attacks). See also 158 (with reference to espionage).

66 For more on this, see *K. Bannelier-Christakis*, Is the Principle of Distinction Still Relevant in Cyberwarfare?, in: N. Tsagourias/R. Buchan (note 18), 343 et seq.

67 See *H. Harrison Dinniss* (note 13), 158 et seq. See also *H. Harrison Dinniss*, Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Law of War, in: D. Saxon (ed.), Inter-

Although it is true that international law allows that an activity originating from the territory of one state may be considered to have occurred in another state because of how its consequences impact the other territory,[68] this assumption does not regard the localisation of the agent – which is the criterion that international humanitarian law looks at with respect to espionage. Actually, it is not possible to consider that the agent is present in the territory in which the targeted system is located since the malware employed for cyber exploitation is no more a part of the operator than an intercontinental missile is a component of the agent who launched it. Moreover, the fact that a belligerent in its territory employs the targeted system does not mean that material components of that system are located in its territory. In general, defining territoriality in the realm of cyberspace is not so easy nor is it as immediate as in the physical realm.[69] Accordingly, the absolute requirement of the physical presence of the operator[70] is not satisfied by considering the location of the targeted systems and the effects of the operations.

In addition, one cannot consider that the presence of the agent is no longer necessary thanks to an evolutionary interpretation of the relevant international humanitarian law provisions in light of subsequent state practice.[71] Simply, there is no state practice indicating this shift; on the contrary,

national Humanitarian Law and the Changing Technology of War, 2012, 251 et seq., 264 et seq.

[68] See generally *A. Cassese*, International Criminal Law, 2003, 278; *C. Ryngaert*, Jurisdiction in International Law, 2008, 75-76.

[69] For an overview of this issue, see *D. Midson*, Geography, Territory and Sovereignty in Cyber Warfare, in: H. Nasu/R. McLaughlin (eds.), New Technologies and the Law of Armed Conflict, 2014, 75 et seq. More generally, on the relationship between the internet and territory, see *A. Oddenino*, La governance di Internet fra autoregolazione, sovranità statale e diritto internazionale, 2008.

[70] Publicists have confirmed that this requirement is essential for the existence of an act of espionage even in recent times, when cyber exploitation was a known phenomenon. See e.g. *W. H. Boothby* (note 24), 277; *Y. Dinstein* (note 42), 277.

[71] Evolutionary interpretation is based on Art. 31(3) of the 1969 Vienna Convention on the Law of Treaties. On evolutionary interpretation of treaties, see generally *M. Fitzmaurice*, Dynamic (Evolutive) Interpretation of Treaties, Hague Y.B. Int'l. L., Part I, 21 (2008), 101 et seq., Part II, 22 (2009), 3 et seq.; *J. Arato*, Subsequent Practice and Evolutive Interpretation: Techniques of Treaty Interpretation over Time and Their Diverse Consequences, The Law and Practice of International Courts and Tribunals 9 (2010), 443 et seq.; *P.-M. Dupuy*, Evolutionary Interpretation of Treaties: Between Memory and Prophecy, in: E. Cannizzaro (ed.), The Law of Treaties beyond the Vienna Convention, 2011, 123 et seq.; *G. Distefano*, L'interprétation évolutive de la norme internationale, R.G.D.I.P. 115 (2011), 373 et seq.; *G. Nolte* (ed.), Treaties and Subsequent Practice, 2013; *E. Bjorge*, The Evolutionary Interpretation of Treaties, 2014.

recent military manuals have restated this requirement.[72] Consequently, there is no case law supporting that the relevant provisions may be interpreted differently due to subsequent practice.

One has to note the view according to which, in certain circumstances, international humanitarian law may be applied by analogy pursuant to the so-called *Martens* Clause in order to fill gaps that are due to evolution of the law of armed conflict not envisaged by the drafters of the conventions.[73] However, such an operation is permitted only in order to amplify individual guarantees. By contrast, applying the rules on espionage to individuals falling outside the definition of spies would result in their subsequent deprivation of some basic guarantees due to the inapplicability of the prisoner of war status to spies.

In conclusion, it is unlikely that cyber exploitation itself amounts to espionage. However, it is possible that an individual could have to perform cyber exploitation from within enemy territory due to the structure of the targeted system. Certain systems can be accessed only if the operator is physically close to the target. For instance, it has been reported that a Universal Serial Bus (USB) flash drive was first employed in order to spread the malware *Stuxnet* into the targeted systems of some Iranian nuclear plants.[74] In the case of *Stuxnet*, the cyber operations amounted to a cyber-attack, but it is possible that exploiting information transient or located in close computer systems and networks would require a similar physical contiguity between the operator and the target. In this case, if the agent is within the territory controlled by the enemy and the other requirements of espionage are met, the activity of cyber exploitation could be labelled as cyber espionage and the rules on espionage would be applicable.[75]

---

72 See e.g. German Ministry of Defense (note 43), section 345; US Department of Defense (note 14), section 4.17.2.2.

73 This position was famously advocated by *A. Cassese*, The Martens Clause: Half a Loaf of Simply Pie in the Sky?, EJIL 11 (2000), 187 et seq., 189 et seq. and 212 et seq.

74 On *Stuxnet*, see generally *A. Matrosov/E. Rodionov/D. Harley/J. Malcho*, Stuxnet Under the Microscope, Revision 1.31, 8, available at <go.eset.com>. For an analysis of the main legal issues regarding this episode, see *J. Richardson*, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, John Marshall Journal of Computer and Information Law 29 (2011), 1 et seq.

75 See Rule 66 and the accompanying commentary in Tallinn Manual (note 13), 192 et seq., and Rule 89 and the accompanying commentary in Tallinn Manual 2.0 (note 13), 409 et seq.

However, in most cases, rules on espionage are not applicable to cyber exploitation due to the lack of the physical presence of the agent in the territory controlled by the enemy.[76]

## V. Cyber Exploitation as Direct Participation of Civilians in the Hostilities

### 1. A Brief Introduction to the Direct Participation of Civilians in the Hostilities

Although cyber exploitation falls into the definition of espionage only in marginal cases, it is necessary to evaluate whether it can constitute direct participation of civilians in the hostilities. Obviously, this rule may be applicable only when the agent responsible for cyber exploitation is a civilian.

International humanitarian law is built on the pivotal principle of distinction between civilians and combatants, and between civilian objects and military objects.[77] Civilians and civilian objects are immune from attacks, they should not be directly targeted, belligerents have to constantly verify that their military operations are not launched against them, and unavoidable civilian casualties are lawful only if not excessive in relation to the planned military advantage.[78] However, the protection afforded to civilians is not absolute. Civilians are immune from attacks as long as they do not participate directly in hostilities.[79] According to Art. 51(3) AP I, "[c]ivilians shall enjoy the protection afforded by [AP I], unless and for such time as

[76] See Tallinn Manual (note 13), 193; *L. Doswald-Beck*, Some Thoughts on Computer Network Attack and the International Law of Armed Conflict, in: M. N. Schmitt/B. T. O'Donnell (eds.), Computer Network Attack and International Law, 2002, 163 et seq., 172; *M. Roscini* (note 13), 240; *D. Turns*, Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict and Security Law 17 (2012) 279 et seq., 290.

[77] See *Legality of the Threat or Use of Nuclear Weapons* (note 50), paras. 78-79. On this topic, see generally *N. Melzer*, The Principle of Distinction Between Civilians and Combatants, in: A. Clapham/P. Gaeta (eds.), The Oxford Handbook of International Law in Armed Conflict, 2014, 296 et seq.

[78] On the protection of civilians during armed conflict — a topic too vast to be explored in this occasion — see generally *N. Ronzitti*, Civilian Population in Armed Conflict, in: R. Wolfrum (note 35); *Y. Dinstein* (note 42), 139 et seq.

[79] On this topic, see generally *G. Bartolini*, The Participation of Civilians in Hostilities, in: M. Matheson/D. Momtaz (eds.), Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts, 2010, 321 et seq.; *E. Crawford*, Identifying the Enemy: Civilian Participation in Armed Conflict, 2015; Y. Disntein (note 42), 174 et seq.

they take a direct part in hostilities". This provision was adopted unanimously and no reservation has been made. It is part of international customary law,[80] as demonstrated by the case law of the Israel Supreme Court,[81] which is extremely relevant since Israel is not party to AP I.[82] This rule is considered to be relevant also in relation to cyber operations.[83]

The main issue regarding Art. 51(3) AP I is that its application is quite problematic due to a lack of clarity on its elements. The term "hostilities" connotes more than mere military attacks; accordingly, it also encompasses conduct that does not quite reach the definition of an attack pursuant to Art. 49(1) AP I.[84] Obviously, if a civilian performs an attack against a belligerent, their conduct is considered direct participation in the hostilities. However, many other activities are not *per se* harmful, and one has to analyse on a case-by-case basis whether they fall into the definition of direct participation of civilians in the hostilities. In theory, there are two possible, albeit extreme, solutions: considering only fighting activities to be covered by this rule, or considering that every activity related to the war effort removes civilian immunity from attacks.

Official documents such as military manuals are not particularly useful in dispelling doubts over which activities fall into the category of direct participation of civilians, since very often they just restate the AP I provision, or the scant available lists are discordant.[85] In order to clarify the content of this rule, in 2009, the International Committee of the Red Cross published an Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Interpretive Guidance). Al-

---

80 ICRC Customary IHL, Rule 6.

81 *Israel Supreme Court: Public Committee Against Torture in Israel v. Israel* (*Targeted Killings* case), International Legal Materials 46 (2007), 375 et seq., para. 30. See US Department of Defense (note 14), section 5.8.

82 On the issue of the customary status of rules embodied in treaty not ratified by a relevant number of states, see *North Sea Continental Shelf* (*Federal Republic of Germany v. Denmark — Federal Republic of Germany v. Netherlands*) (Judgment), ICJ Rep. 1969, 3 et seq., paras. 76-77.

83 See generally Tallinn Manual 2.0 (note 13), Rule 97; *M. Roscini* (note 13), 202 et seq. More specifically, this issue was addressed by *S. Watts*, Combatant Status and Computer Network Attack. Va. J. Int'l L. 50 (2010), 391 et seq.; *I. Kilovaty*, ICRC, NATO, and the U.S. — Direct Participation in Hacktivities — Targeting Private Contractors and Civilians in Cyberspace under International Humanitarian Law. Duke Law & Technology Review 15 (2016), 1 et seq.

84 See *C. Pilloud/Y. Sandoz/C. Swinarski/B. Zimmermann* (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 1987, para. 1943.

85 See the references collected in ICRC Customary IHL, Vol. II, 108 et seq.

though the Guidance is a non-binding instrument,[86] it provides a useful analysis of state practice and *opinio juris*, and may help in the interpretation and practical application of the rule.

According to the Interpretive Guidance, conduct performed by a civilian is a kind of direct participation in the hostilities if it meets three cumulative criteria:

> "1. the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm); 2. there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation); 3. the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus)."[87]

Since these criteria are in line with the scant state practice, case law, and academic opinions available,[88] attempting to apply them to cyber exploitation may provide valuable insight.

## 2. Direct Participation of Civilians in the Hostilities and Cyber Exploitation

### a) Intelligence Gathering as Direct Participation

Intelligence gathering activity performed by civilians may be considered a form of participation in the hostilities, since this last term also encompasses conduct that is not an attack. The main issue is whether intelligence gathering is a form of direct or indirect participation.

---

[86] *N. Melzer* (ed.), Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Adopted by the Assembly of the International Committee of the Red Cross on 26.2.2009, Int' l Rev. of the Red Cross 90 (2008), 991 et seq. (Interpretive Guidance). For some remarks on them, see *D. Akande*, Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities, ICLQ 59 (2010), 180 et seq.; *K. Watkin*, Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities Interpretive Guidance", N. Y. U. J. Int' l L. & Pol. 42 (2010), 641 et seq.

[87] Interpretive Guidance (note 86), 995 et seq.

[88] Inter-American Court of Human Rights, Third Report on Human Rights Situation in Colombia, OEA/Ser.L/V/II.102, Doc. 9, rev 1, 26.2.1998, Chapter IV, para. 53; *Targeted Killings* case (note 81), para. 37 et seq. See also *G. Bartolini* (note 79), 321 et seq., 352 et seq.

Case law and state practice appear partially discordant. According to Israel – which is not party to the AP I – intelligence gathering is always considered to be direct participation in the hostilities. This is the opinion of the Supreme Court of Israel,[89] confirmed also by the practice related to the armed operations conducted in the Strip of Gaza.[90] The rule is also embodied in some less recent US military manuals.[91]

However, the opinion of the International Committee of the Red Cross appears to take the opposite stance, at least in its Commentary to the Two Additional Protocols, in which intelligence gathering – albeit if conducted by children – seems to be always considered a form of indirect participation in the hostilities, thus falling outside the scope of Art. 51 (3) AP I.[92]

The case law of the International Criminal Tribunal for the former Yugoslavia enlists intelligence gathering in both the lists of direct and indirect forms of participation of civilians in the hostilities. According to the decision in the *Strugar* case:

> "Examples of active or direct participation include: … transmitting military information for the immediate use of a belligerent … Examples of indirect participation include: … gathering and transmitting military information."[93]

This last approach, far from being contradictory, is the most correct. The International Criminal Tribunal for the former Yugoslavia makes a distinction between the mere activity of gathering and transmitting military information – which is a form of indirect participation – and the transmission of military information that is employed for the immediate use of the belligerent. In this last case, there is a genuine causal link between the intelligence activity and harm to the enemy; this link is considered the pivotal criterion for establishing whether a conduct constitutes direct participation of civilians in the hostilities. Interestingly, the 2016 US military manual adopts an approach more cautious than in the past and embodies a similar consideration, with practical examples of gathering and transmitting information that

89 *Targeted Killings* case (note 81), para. 35.

90 See Israel Ministry of Foreign Affairs, Operation Pillar of Defense – IDF Updates, 22.11.2012, available at <mfa.gov.il>: "The IDF also surgically targeted a Hamas intelligence operations center on 7th floor of a media building in Gaza City. Reporters in the building were unharmed."

91 US Air Force, The Commander's Handbook, Pamphlet 110 et seq., 1980, section 2-8.

92 See *C. Pilloud/Y. Sandoz/C. Swinarski/B. Zimmermann* (note 84), para. 3187. See also *L. Salvadego* (note 6), 1191, according to which civilians involved in espionage are not deprived of their immunity from attack for the time they perform acts of espionage.

93 See ICTY, *The Prosecutor v. Strugar*, IT-01-42-A, 17.7.2008, para. 177.

are relevant for the immediate use of belligerents.[94] This approach is embodied in the Tallinn Manual 2.0 as well.[95]

Accordingly, intelligence activity may be considered a form of both direct and indirect participation; it depends on whether concretely the activity performed meets the requirements of the threshold of harm, direct causation, and the belligerent nexus. This analysis must be performed case-by-case.

### b) Why Direct Participation of Civilians Is Not a Practical Answer to Cyber Exploitation

In light of the analysis conducted above, cyber exploitation may be considered a form of direct participation of civilians in the hostilities if it is performed by civilians, and if it directly causes harm to the enemy in order to support a party of an armed conflict. This conclusion is also supported by the Interpretive Guidance and by the Tallinn Manuals, even if these last documents intermingle cyber exploitation with cyber-attacks[96] – an opinion this author does not share.[97] Accordingly, if all these requirements are satisfied, the operators responsible for cyber exploitation may be targeted.

There is also a tentative state practice in support of this view, even if the information available is incomplete and should be handled with care. It has been reported that the US, which typically considers intelligence gathering to be a form of direct participation in the hostilities, has targeted hackers

---

[94] See US Department of Defense (note 14), section 5.8.3.1:
"Examples of Taking a Direct Part in Hostilities. The following acts are generally considered taking a direct part in hostilities that would deprive civilians who perform them of protection from being made the object of attack. These examples are illustrative and not exhaustive: … [P]roviding or relaying information of immediate use in combat operations, such as: acting as an artillery spotter or member of a ground observer corps or otherwise relaying information to be used to direct an airstrike, mortar attack, or ambush; and acting as a guide or lookout for combatants conducting military operations."

[95] Tallinn Manual 2.0 (note 13), 430.

[96] See Interpretive Guidance (note 86), 1017-1018; Tallinn Manual (note 13), 194; Tallinn Manual 2.0 (note 13), 412.

[97] On the need to make a distinction between these two kinds of cyber operations, see *H. Lin*, Cyber Conflict and International Humanitarian Law, Int' l Rev. of the Red Cross 94 (2012), 515 et seq., 518 et seq.; *A. Wortham*, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal 64 (2012), 643 et seq., 646 et seq.; *M. Roscini* (note 13), 16 et seq.

affiliated with the Islamic State.[98] As aforementioned, cyber operators affiliated with the Islamic State have been accused of having stolen US cyber-data, thereby performing cyber exploitation.[99] However, the present author has no sufficient information in order to assess whether the targeted hackers have been attacked because of their activity of cyber exploitation – if any – or because of other activities they have performed through the cyberspace, such as cyber-attacks and propaganda.[100]

In addition, the German Military manual explicitly considers that people who "engage in electronic warfare or computer network operations" lose their protection as civilians.[101] This suggests that all cyber operations – both cyber-attacks and cyber exploitation – are considered direct participation in the hostilities. However, the lack of any definition of cyber operation in the German manual suggests a cautious approach when making such an inference.

However, even assuming that the US is targeting individuals responsible for cyber exploitation and that Germany considers them to be civilians directly participating in hostilities, the application of the rule of the direct participation in hostilities is highly impractical in these cases. Indeed, this rule aims to allow states to identify and target civilians who act as combatants. However, in cyberspace it is extremely difficult to identify the responsibility for each cyber operation – both cyber-attacks and cyber exploitation. The distance between the operator and the target, the cyberspace itself that enables identification of IP addresses but not physical individuals at the keyboards, and the fact that cyber exploitation is a process performed by a number of individuals with different tasks (programmers, operators, analysts), makes the identification of the target almost impossible.[102]

Moreover, civilians who are not physically present within the territory of a state party to the conflict may still launch cyber operations such as cyber exploitation. In this case, even if they would meet the criteria to be considered civilians who participate directly in the hostilities, their targeting is ra-

98 See US Department of Defense, Department of Defense Press Briefing by Col. *Warren* via Teleconference from Baghdad, Iraq, 29.12.2015, available at <www.defense.gov>.

99 See Section III.

100 According to the US Department of Defense (note 98): "[O]ur one high-value target who was killed … was a hacker. He kind of led some of their hacking programs. He also facilitated development of weapons and *some of their surveillance techniques*." (emphasis added).

101 German Ministry of Defense (note 43) section 1120.

102 On this issue, see *H. Harrison Dinniss*, Participants (note 67), 271 et seq.; *D. Turns* (note 76), 279 et seq., 289 et seq.; *E. Crawford*, Virtual Battleground: Direct Participation in Cyber Warfare, I/S: A Journal of Law and Policy for the Information Society 9 (2013), 1 et seq., 13 et seq.

ther unpractical.[103] For instance, in the aforementioned case of the Kosovo citizens arrested in Malaysia under the suspicion of having stolen US classified data on behalf of the Islamic State, a US military action against them would have been a patent violation of Malaysia sovereignty (and, likely, an act of aggression). Furthermore, even in the case of the consent of Malaysia to such an operation, there may be serious concerns regarding Malaysia's respect for its human rights obligation to protect individuals under its jurisdiction. Consequently, targeting such an individual who dwells outside the belligerents' territory is rather unfeasible. The most correct approach is just charging the suspect under the domestic law of the state of residence – which is exactly what happened in the case of the alleged Kosovo hackers.

Moreover, according to Art. 51 (3) AP I, civilians may be targeted only for the time they take part into the hostilities.[104] Cyber operations in general, and specifically cyber exploitation, are conducted very quickly with regard to the targeting of the enemy network with malware;[105] then, the program may steal data for a long period of time, without any human activity. Which element should be considered relevant for the application of the rule on direct participation – a rule that is applicable only for the time the civilian directly participates in the hostilities? During the elaboration of the Tallinn Manuals, it was suggested that civilian operators were targetable for the time of the operation and the time in which the program was in function.[106] However, the majority of the convened experts rejected this view.[107] Accordingly, the only answer appears to be that only the human action is relevant since, as aforementioned, the malware *per se* is not a component of the human operator.[108] Consequently, it appears incredibly unlikely that a belligerent discovers the intrusion in one of its systems immediately, identifies the operator responsible at once, and immediately launches an attack

103 See *F. Delrue*, Civilian Direct Participation in Cyber Hostilities, IDP. Revista de Internet, Derecho y Política 19 (2014), para. 4, available at <journal-of-conflictology.uoc.edu>.

104 The provisions states: "…or such time as they take a direct part in hostilities." Its interpretation is controversial. For more on this, see *W. H. Boothby*, "And for such Time as": The Time Dimension to Direct Participation in Hostilities, N. Y. U. J. Int' l L. & Pol. 42 (2010), 741 et seq.

105 See *J. M. Prescott*, Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States?, in: C. Czosseck/R. Ottis/K. Ziollkowski (eds.), Proceedings of the 2012 4th International Conference on Cyber Conflict, 2012, 251 et seq., 258 et seq.

106 Tallinn Manual 2.0 (note 13), 431.

107 Tallinn Manual 2.0 (note 13), 431.

108 See Section IV. 2.

against it while the intrusion – the relevant activity – is still being performed.[109]

In conclusion, even if cyber exploitation may be seen as direct participation of civilians in the hostilities, this qualification has very scant practical relevance.

## VI. Conclusion

In this author's opinion, only one international humanitarian law rule is clearly applicable to cyber exploitation: the fact that it is a legitimate means of information gathering in times of war pursuant to Art. 24 HR.

Rules on espionage are applicable only in the case of cyber espionage, a marginal occurrence since the use of cyber capabilities in order to collect data was developed also in order to avoid risks due to proximity with the enemy.

Although the rule of direct participation of civilians in the hostilities may be applied to cyber exploitation from a theoretical point of view, in practice, it seems highly difficult for the targeted belligerent to identify and attack the civilian responsible for cyber exploitation while that civilian is still performing that operation.

Finally, other international humanitarian law rules apply to the operators of cyber exploitation; e.g., if this individual is a member of the enemy armed forces, they may be targeted. However, this possibility is not linked to the activity performed, but rather to their belonging to the enemy army.

However, the fact that international humanitarian law does not specifically address cyber exploitation is not a source of concern. International humanitarian law never presumed to regulate every activity performed during and linked to an armed conflict. As affirmed by the International Court of Justice in its *Wall* opinion, certain conduct is regulated by international humanitarian law, while other conduct is regulated by international humanitarian law and other branches of international law, and yet another type of conduct is regulated by other branches of international law.[110] In the case of cyber exploitation, branches such as international human rights law, diplomatic law, the law of the sea, and international space law may play a more important role. This final suggestion paves the way for further analysis and

[109] The temporal issue is considered more relevant in cyber intelligence operation rather than in cyber-attacks by *I. Kilovaty* (note 83), 28.

[110] See *Wall* opinion (note 50), para. 106. See also *DRC v. Uganda* (note 50), para 2016.

research since the effects of the war on treaties is far from being a settled issue in international law, as demonstrated by the work of the International Law Commission.[111] For instance, a thorough analysis of the applicability of the right to privacy during armed conflict could provide some answers to the legality of cyber exploitation.

[111] See International Law Commission, Draft Articles on the Effects of Armed Conflicts on Treaties, (2011), available at <legal.un.org>. On this topic, see generally *M. K. Prescott*, How War Affects Treaties between Belligerents: A Case Study of the Gulf War, Emory International Law Review 7 (1993), 197 et seq.; *M. Mancini*, Stato di guerra e conflitto armato nel diritto internazionale, 2009, 257 et seq.; *A. Pronto*, The Effect of War on Law — What Happens to Their Treaties When States Go to War?, Cambridge Journal of International and Comparative Law 2 (2013), 227 et seq.