

JOURNAL OF LAW AND CYBER WARFARE

- I. Counterterrorism Measures via Internet Intermediaries: A First Amendment & National Security Dilemma.....1
Mohamed H. Aziz
- II. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks.....23
Elizabeth Mavropoulou
- III. Legal Implications of Vulnerability Disclosure in International Conflict.....93
Thomas Cross
- IV. Virtual Crimes, Actual Threats: Deterring National Security Offenses Committed Through Cyberspace.....108
Asaf Wiener

Editor-in-Chief

Daniel B. Garrie, *Partner, Law & Forensics*

Senior Associate Editors

Michael Mann
Samantha Tucker
Radhika Tiwari
Tarique Collins

Junior Associate Editors

Jennifer Chan
Barry Dynkin
Anthony Ford
Geoffrey Kalender
Zachary Levy
Mary Beth Winningham

Editorial Board

Christopher Burgess <i>Founder & CEO, Prevendra</i>	Robert Clark <i>Cyber Attorney, Army Cyber Institute</i>
Jean-Claude Knebel <i>Consul General of Luxembourg to New York</i>	Robert Bair <i>Lieutenant Commander, United States Navy</i>
Jack Dever <i>Director, Business Intelligence Unit, General Electric</i>	Deborah Housen-Couriel <i>Special Counsel, Zeichner Ellman & Krause</i>
Dr. Larry Ponemon <i>Chairman, Ponemon Institute</i>	William Spernow <i>Chief of Security, Virus Inspector</i>
Jeremy Kroll <i>CEO, K2 Intelligence</i>	Eric Jensen <i>Law Professor, BYU</i>
John Dever <i>General Counsel of Defense Firm</i>	Uma Chandrashekhar <i>Global Information Security and Privacy Leader at Edwards Life Sciences</i>
Major Reserve, US Army	Vincent Scott <i>GBS-ITS Cybersecurity, Proctor & Gamble Company</i>
Dr. Joseph Weiss <i>Managing Partner, Applied Control Solutions</i>	Rhea Siers <i>Senior Associate at the GWU Cyber Security Initiative</i>
Shane Reeves <i>Associate Law Professor, US Military Academy, West Point</i>	Richard Borden <i>Chief Privacy Lawyer, Department of Trust and Clearing Corproartion</i>
Mitchell Silber <i>Executive Managing Director, K2 Intelligence</i>	Professor Michael Schmitt <i>Director, Stockton Study of International Law at the US Naval War College</i>
Noah Bledstein <i>IT Data Privacy Leader at GE Healthcare</i>	
Retired Major U.S. Airforce	

Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks

Elizabeth Mavropoulou

ABSTRACT

The conduct of hostilities via cyberspace poses many issues regarding the application of international humanitarian law. Cyberspace should be considered as a sui generis battlefield when it comes to the study of the applicable law. The present contribution aims to identify some of the key issues arising from the application of the law of targeting to cyber operations in the context of an armed conflict, focusing exclusively on the application of the principle of distinction. The principle of distinction - the cornerstone on which humanitarian law stands - today is shrouded in uncertainty in the context of cyber operations. The key threshold of attack, the definition of military objective and the targeting of dual-use cyber infrastructures and digital data are some key issues that need to be further developed in the context of cyber operations. Finally, with regard to targetable individuals, the status of cyber combatants, cyber levée en masse and the notion of direct participation in cyber hostilities, are underdeveloped legal

concepts and need particular interpretation in the context of cyber operations. The complete lack of international jurisprudence and the embryonic state practice on the emerging field of cyber warfare call for the principle of distinction and the relevant provisions of lex lata to be assessed on a humanitarian basis and re-conceptualized in light of the warfare reality.

I. THE VIRTUAL BATTLEFIELD OF CYBERSPACE

A few years ago, cyber warfare would seem fictional and ambitious for a research topic. Yet today, as it remains ambitious, it is all but fictional. Sophisticated cyber weapons exist. The famous Stuxnet virus that allegedly targeted the Iranian uranium enrichment facilities in Natanz in June 2010 was a seminal event in cyber warfare, demonstrating the capabilities of such weapons. Experts agree that Stuxnet was a highly sophisticated computer virus that was distributed through thousands of computer systems around the world, before targeting Natanz facilities where it destroyed more than 900 gas centrifuges. Surprisingly, there has been no collateral damage reported to civilian systems. In the final analysis, Stuxnet deliberately infected but caused no harm to any other system than its intended military target.¹ In fact, the virus self-destructed when the system infected did not fit into the programmed

¹ John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 7, 34 (2011), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888.

target profile.² In this sense, Stuxnet manifestly proves the extraordinary capabilities of cyber weapons on delicacy, accuracy and precision. Technological advances in the domain of cyberspace and the ever-increasing use of cyber weapons by the military raise significant issues related to the law of armed conflict.³ Targeting via cyber space appeals more than ever to states. Computer network attacks or cyber attacks⁴ can be remotely authorized, saving states from the high cost of conventional military operations and obscuring the origin of the attack.

Cyberspace should be considered a *sui generis* battlefield when it comes to the study of the applicable law. Despite what has been written, state practice is still embryonic in the field of cyber operations and the existing principles of *lex lata* are blurred rendering thus the application of the law a demanding task. However, until future state practice crystallizes the applicable law, one could reach some tentative conclusions on the application of international humanitarian law to cyberspace for the time being.

The conduct of hostilities via cyberspace raises a number of issues regarding the application of international humanitarian law. The inherent interconnectivity of the Internet is what fundamentally differentiates cyberspace from other battlefields. Civilian and military infrastructure are

² *Id.* at 34.

³ The law of armed conflict is also known as international humanitarian law, a term founded by the International Committee of the Red Cross (“ICRC”). In this paper, the terms international humanitarian law, law of armed conflict and the equivalent Latin term *jus in bello* are used interchangeably and with the same meaning.

⁴ Both terms have the same meaning in the present paper and will be used interchangeably.

not only closely interrelated and interconnected, but as some scholars contend, they are one and the same thing.⁵ This assertion can lead to conclusions that pose significant obstacles in the application of the basic rule of targeting, namely the principle of distinction. If every component of cyberspace is a dual use object, serving at the same time military and civilian purposes, the classification of the object according to the principle of distinction can be excessively problematic.⁶ On the other side of the river, the classification of individuals as combatants or civilians is not always clear given the ever-increasing phenomenon of civilianization of the military and participation of civilians in cyber hostilities.

The present contribution aims to identify some of the key issues arising from the application of the law of targeting to cyber operations, focusing exclusively on the application of the principle of distinction. Hence, a crucial assumption is made for the purposes of our analysis: it is assumed that an armed conflict is already established under international humanitarian law, triggering the application of the Geneva Conventions and their Additional Protocols under the *jus in bello* regime. Therefore, issues related to *jus ad bellum*, the branch of international law that regulates the use of force by states under the UN Charter are beyond the scope of this research.

Against this fundamental background, the analysis will proceed in three major parts. The first chapter will address the preliminary legal threshold

⁵ Robin Geiss & Henning Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISR. L. REV. 381, 386 (2012), available at <http://eprints.gla.ac.uk/78067/1/78067.pdf>.

⁶ *Id.* at 383.

of whether cyber operations constitute an attack, as defined in Article 49 of Additional Protocol I.⁷ Provided that a cyber operation, in the context of an ongoing armed conflict, qualifies for an attack under the Protocol, then the law of targeting applies. The second chapter will apply the principle of distinction with respect to military objectives focusing on what can be legitimately targeted. The analogical application to cyber operations with regard to objects will be assessed on the basis of the humanitarian concerns covered by law. In particular, the chapter will examine what can be lawfully attacked under the normative rules of targeting in the context of a cyber attack, pointing out the key issues on the application of the principle of distinction to cyber operations. The third chapter will address the principle of distinction with regard to individuals. It will examine who can be lawfully attacked by cyber operations in the context of both international and non-international armed conflict. Each type of conflict poses various challenges to the application of the principle regarding “cyber” combatants and civilians taking direct part in cyber hostilities. Upon completion of the principle’s assessment, the research demonstrates that upholding the distinction principle becomes more challenging in cyber warfare than in other types of warfare. There are issues to be further reconceptualised and reassessed in light of cyber reality. Reconceptualization can be achieved through interpretation in light of the object and

⁷ Protocol Additional to the Geneva Conventions of 12th August 1949, Relating to the Protections of Victims of International Armed Conflicts (Protocol I), art. 49 (1977), available at <https://www.icrc.org/applic/ihl/ihl.nsf/INTRO/470> [hereinafter Additional Protocol I].

purpose of the humanitarian treaties as well as in light of the new cyber reality.

II. CYBER OPERATIONS AND THE KEY THRESHOLD OF ATTACK UNDER ARTICLE 49 OF ADDITIONAL PROTOCOL I

Having established an armed conflict as the starting point of our analysis, it is now time to examine the key threshold of attack. The law of targeting governs a certain type of conduct and in particular applies only to military operations that amount to attacks.⁸ In framing that conduct, the necessary starting point is the definition of attack contained in Article 49 of Additional Protocol I, which for the most part reflects customary law.⁹ Attacks as defined therein are “*all acts of violence against the adversary, whether in offence or in defense.*” Two main theories have been developed in the legal discourse on the interpretation of “*acts of violence*” in the context of cyber operations. Each theory will be dealt separately as the analysis develops. The common ground is that both theories acknowledge attack as a term of art, having specific meaning and establishing a key threshold under international humanitarian law.¹⁰

⁸ Emphasis will be added throughout this chapter, as the word “attack” is a definitional term establishing a key threshold under international humanitarian law.

⁹ JEAN MARIE HECKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, VOLUME I: RULES OF THE INT’L COMM. OF THE RED CROSS 29-32 (2009), available at http://www.academia.edu/4032273/Customary_International_Humanitarian_Law_v.1_Rules_ICRC [hereinafter ICRC Customary International Humanitarian Law Rules].

¹⁰ Michael N. Schmitt, “*Attack*” as a Term of Art in

Traditionally, the meaning of “*acts of violence*” has been understood as denoting physical force. This authoritative interpretation comes from the Commentary of Bothe, Partsch and Solf - all three involved in the Protocol’s drafting proceedings. The interpretation of the term attack requiring physical force, reasonably excludes psychological operations as well as “*dissemination of propaganda, embargoes or other non-physical means of psychological, political or economic warfare.*”¹¹ A similar approach has been adopted by the Official Commentary of the International Committee of the Red Cross (“ICRC”), which understands “*acts of violence*” as “*combat action.*”¹² Hence, cyber operations that do not result in acts of violence, such as those aimed at intelligence gathering or cyber espionage are excluded from the definition of Article 49 under the traditional approach.

Insofar as certain cyber operations do not necessarily and directly release violent physical

International Law: The Cyber Operations Context in 2012 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 284 (C. Czosseck, et al. eds., 2012), available at https://ccdcoe.org/cycon/2012/proceedings/d3r1s1_schmitt.pdf [hereinafter Schmitt, “*Attack*” as a Term of Art].

¹¹ MICHAEL BOTHE ET AL., NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949 289 (1982), available at http://books.google.com/books?id=9C1OrmFbA4kC&pg=PR7&source=gbs_selected_pages&cad=2#v=onepage&q&f=false.

¹² INT’L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 para. 1880 (Yves Sandoz et al. eds., 1987), available at http://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf [hereinafter ICRC Commentary of Additional Protocols].

forces, but can nevertheless cause serious damage, it is worthwhile to consider reinterpreting the definition of attack. On this basis, the first approach on the notion of attack understands the term “*acts of violence*” as those acts entailing violent consequences. This consequence-based or effects-based approach, primarily taken forward by Professor Schmitt for reasons of conformity and compliance with the humanitarian concerns of the Protocol, sets aside the “*instrumentality-based*” definition of attack that reads as “*acts of violence*” and promotes a consequence-based interpretation in an attempt to operationalize the term.¹³ This position seems to be further endorsed by the Protocol’s own wording. According to Schmitt, the Protocol itself operationalizes the principle of distinction in terms of consequences and results.¹⁴ For instance, the Protocol prohibits attacks on dams and dykes, as well as on other “*works or installations containing dangerous forces*” that might result in “*severe losses among the civilian population*”¹⁵ or might result in “*widespread, long-term and severe damage*” to the natural environment.¹⁶ Finally, the principle of proportionality itself assesses the final legitimacy of an attack in terms of results by prohibiting “*incidental loss of civilian life, injury to civilians or damage to the civilian objects, or a combination thereof, which would be excessive to the concrete and direct military advantage anticipated.*”¹⁷

¹³ Schmitt, “*Attack*” as a Term of Art, *supra* note 10, at 290.

¹⁴ *Id.* at 289; Michael N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 INT’L L. STUDIES 89, 93 (2011) [hereinafter Schmitt, *Key Issues*].

¹⁵ Additional Protocol I, *supra* note 7, at art. 56(1).

¹⁶ Additional Protocol I, *supra* note 7, at art. 55(1).

¹⁷ Additional Protocol I, *supra* note 7, at art. 51(5)(b).

Inductively applying the above to cyber operations, a definition of cyber attack would likely be, pursuant to the consequence-based approach, the following: “*cyber attacks are those cyber operations that result, or could result, if unsuccessful, in death or injury to individuals or destruction or damage to objects.*”¹⁸ Under this definition adopted by the recently published Tallinn Manual Applicable to the International Law on Cyber Warfare,¹⁹ contaminating a water pipe that provides civilians with potable water by means of a computer network attack would qualify for an attack, as the contamination would result in death or illness.²⁰ Likewise, opening the floodgates of a dam in a similar way would result in physical harm to the civilian population. In addition, starving a civilian population to death or terrorizing it by causing physical or mental suffering would again qualify as an attack.²¹

So far the above scenarios are commonly accepted as attacks, as their effects on the civilian population are obvious and indubitable. However, complex cyber scenarios involve those operations whose effects do not entail directly violent consequences under the sense of Article 49 Additional Protocol I but cause serious disruption to the functionality of the targeted object.

¹⁸ Schmitt, “*Attack*” as a Term of Art, *supra* note 10, at 291.

¹⁹ TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013), available at <https://ccdcoe.org/research.html> [hereinafter Tallinn Manual].

²⁰ Schmitt, “*Attack*” as a Term of Art, *supra* note 10, at 291.

²¹ Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84 INT’L REV. OF THE RED CROSS 365, 377 (2002) [hereinafter Schmitt, *Wired Warfare*].

The Tallinn Manual has adopted the element of “functionality” as the criterion according to which some disruptive cyber operations may qualify for attacks in the sense of *jus in bello*. Under the Tallinn approach, destruction or damage to an object pursuant to the theory of consequences should render the physical component completely non-functional “*unless repairable*.”²² Pursuant to the Manual, if restoration of functionality requires the replacement of physical components, then those disruptive cyber operations reach the key threshold of attack.²³ Dinstein on the meaning of attacks, in conformity with Schmitt and his effects-based approach endorses as well the doctrine of kinetic equivalence for cyber operations and disqualifies from the notion of attack, *inter alia*, “*the breaking through a computer’s firewall...or...the mere disruption of communication*.”²⁴

The difficulty with the effects-based approach is in determining how disruptive cyber operations have to be in order to reach the threshold of the Protocol. Certainly, the mere disruption of communications in times of conflict does not reach the threshold of Article 49, however, by adopting a *stricto sensu* definition of attack pursuant to the consequences-based approach, all disruptive cyber operations that do not render the target completely irreparable are left unregulated and thus permissible under the law. Indeed, the effects-based approach limits the notion of attack so as to exclude those

²² Tallin Manual, *supra* note 19, at 93.

²³ *Id.*

²⁴ Yoram Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 17 J. OF CONFLICT AND SEC. L. 261, 264 (2012) [hereinafter Dinstein, *Principle of Distinction*] (emphasis added).

operations that result in severe and disruptive non-physical harm. Cyber operations have the advantage of being able to deprive an object of its functionality without causing any outright physical harm to the object. Consequently and pursuant to the effects-based approach, the distributed denial of service (“DDoS”) cyber operations conducted in 2008 against Georgian official governmental and ministerial websites, would fall below the key threshold of attack, as no outright physical consequences to the civilian population were noted.

The kinetic equivalence theory has been criticized for having an under-inclusive definition of attack predicated on the occurrence of physical effects on the targeted object.²⁵ However, certain cyber operations, such as rendering the information systems of financial and capital markets inoperable but not irreparable, can have a profound impact on a state’s economy and infrastructure without causing any physical harm.²⁶ This is where the Dörmann’s approach on the notion of attack enters the discussion. The legal adviser of the ICRC, Dr. Knut Dörmann, aiming to respond to below-threshold cyber operations, expands the notion of based on the definition of “military objective” contained in Article 52 (2) of Additional Protocol I, ending up creating a rather over-inclusive approach on the notion of attack. As Dörmann explains, in the same

²⁵ Marco Roscini, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 180 (2014).

²⁶ John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield – Distinction and Proportionality on the Cyber Battlefield*, 29 J. MARSHALL J. INFO. TECH. & PRIVACY L. 1, 17-18 (2011), available at <http://repository.jmls.edu/cgi/viewcontent.cgi?article=1697&context=jitpl>.

section of the Protocol and in particular in the definition of military objective, one of the potential results of an attack is the object's "*neutralization*."²⁷ In the context of cyber operations and under Dörmann's approach, a denial-of-service cyber attack via a cyber worm or virus that would merely disable the object or disrupt its functionality - without requiring the replacement of physical components as the Tallinn Manual requires - should qualify for an attack in the sense of the Protocol.²⁸

The weakness of this argument, as Schmitt points out, is that the notion of "military objective" does not come into play before the threshold of attack is itself primarily satisfied.²⁹ First, one has to establish the key threshold of attack and then enter the law of targeting principles, as the law of targeting applies only to cyber operations that qualify for attacks in the first place. Away from the reasoning of each argumentation, the crux issue in question remains the severe disruptive impact of certain cyber operations on otherwise protected persons and objects.

Other scholars have also supported the extension of the notion of attack to cyber operations that might not lead to physical harm directly but result in the malfunction of essential cyber infrastructures to the civilian population.³⁰ The

²⁷ See Additional Protocol I, *supra* note 7, at art. 52 (2) (defining "military objective").

²⁸ Knut Dörmann, APPLICABILITY OF ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 4 (2004), *available at* https://www.icrc.org/eng/assets/files/other/applicabilityofihlto_cna.pdf.

²⁹ Schmitt, *Key Issues*, *supra* note 14, at 95.

³⁰ Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the Tallinn Manual*, 18 J. OF CONFLICT AND SEC. L. 331, 341 (2013).

massive distributed denial of services attacks (“DDoS”), directed against Estonia during the conflict with Russia in May 2007, targeted, *inter alia*, websites of the political leadership, newspapers, telecommunications and broadcasters causing more than the mere disruption of civilian systems. The effects could have been life threatening, according to cyber experts, with the emergency lines for ambulances and fire service being out of action for more than an hour.³¹ Were there enough conclusive evidence for those cyber operations to be attributed to Russia, the DDoS was a clear example of disrupted cyber operations directed against civilians that rose to the level of attack.³² In light of the Estonian example, it can be safely supported that the expansion of the notion of attack might be compelling in some cases. Likewise, given the ever-increasing cyber-centric nature of so many modern societies and their dependence on computer networks, it could be similarly contended that targeting massive financial assets in stock, capital and trading markets via distributed denial-of-service attacks could result in temporary but severe malfunction of the market’s system that could have quintessential impact on the civilian population. Other remaining or potential borderline cases have to be seen in future state practice and should be assessed on a case-by-case basis.

³¹ Newly Nasty: Defenses Against Cyber Warfare are Still Rudimentary, *The Economist*, (May 24, 2007), *available at* <http://www.economist.com/node/9228757>.

³² Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1429 (2008).

Most significantly, the problem with the two approaches is that neither of them can respond to the unique threat posed by cyber operations. The first fails to respond to below-threshold cyber operations and the second stretches the notion of attack so much as to include in it even the mere disruption of civilian cyber infrastructure.³³ However, mere inconvenience to civilians should be excluded from the notion because in times of crisis and conflict harassment of the civilian quality of life forms an integral part of hostilities and is outweighed by the demands of military necessity.³⁴ It is widely accepted that the principle of distinction and the law of targeting applies only to attacks and not in general to the conduct of hostilities. This is why the Protocol, excludes civilians from being “*the object of attack*.”³⁵ This creates the following normative lacuna; cyber operations by nature expand the possibilities of civilians or civilian objects to be “targeted” but not “attacked” under the international humanitarian law connotation.³⁶ In the context of an armed conflict, it is impossible to ensure a normal life for the civilian population as in times of peace.³⁷ Hence, it still remains open for further consideration whether below-threshold cyber operations - i.e. cyber operations that do not result in injury or death to persons or damage to objects or severe malfunction to systems - would be permissible against otherwise protected persons and objects under international humanitarian law.³⁸

³³ Schmitt, *Key Issues*, *supra* note 14, at 95.

³⁴ Schmitt, *Wired Warfare*, *supra* note 21, at 377.

³⁵ Additional Protocol I, *supra* note 7, at art. 51 (2).

³⁶ Schmitt, *Wired Warfare*, *supra* note 21, at 378-379.

³⁷ Roscini, *supra* note 25, at 181.

³⁸ Fleck, *supra* note 30, at 341; Erki Kodar, *Applying the Law*

Unfortunately, the Tallinn Manual Experts did not achieve consensus on the matter either. It is an issue to be further considered but the author's tentative conclusion is that protected persons and objects under international humanitarian law shall never be the target of any hostilities that go beyond those of mere inconvenience.

III. LEGITIMATE OBJECTIVES UNDER THE LAW OF TARGETING

The principle of distinction forms the cornerstone on which international humanitarian law stands. It has been characterized by the International Court of Justice as one of the cardinal principles of customary international humanitarian law, the other being the principle of unnecessary suffering.³⁹ By nature, war is brutal, in particular for the civilian population that is often seriously affected by the conflict and the dictates of military necessity. The Geneva Conventions and their Protocols were concluded so as to minimize the brutality of warfare by setting the limits and restrictions to the conduct of hostilities. As the analysis enters the law of targeting, it will first begin by examining *what* can be attacked under the law by applying the principle of distinction analogically to cyber operations.⁴⁰

of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I, 15 ENDC Proceedings 107, 117 (2012).

³⁹ Int'l Ct. of Just., *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* 257 (1996), available at <http://www.icj-cij.org/docket/files/95/7495.pdf> [hereinafter ICJ, Nuclear Weapons].

⁴⁰ Emphasis added.

Cyber attacks resulting in physical harm to objects or persons, i.e. the destruction of military barracks via a computer network attack, is a relatively common scenario with no particular issues in relation to the application of the distinction principle. The legitimacy or illegitimacy of such an attack would be assessed on the same basis as in an equivalent kinetic scenario. However, as cyber attacks can be severely disruptive without causing any physical harm or any physical manifestation to the real world and as the majority of the cyber domain is used for both civilian and military purposes, there are fundamental issues arising on the analysis of a cyber attack's compliance with the principle of distinction. As some scholars argue, high tech belligerent parties in future cyber conflicts, may target exclusively the enemy's cyber domain so as to gain control over it and degrade or destroy its cyber assets.⁴¹ Hence, issues of targeting dual use cyber assets as well as digital data *per se* dominate the present legal discourse and are going to be addressed in the following section.

A. Definition of Military Objective

The customary principle of distinction, reflected in Article 48 of Additional Protocol I, indicates to the parties to a conflict what a legitimate targetable objective is. Referred to as the "Basic Rule," belligerents shall "*at all times distinguish between the civilian population and combatants and between the civilian objects and military objectives and accordingly shall direct their operations only*

⁴¹ Geiss and Lahmann, *supra* note 5, at 384.

against military objectives.”⁴² Thus, cyber warfare is subject to the principle of distinction as any other type of warfare and should respect the civilian population and civilian objects accordingly. The classification of conflict is irrelevant with respect to targetable objectives as the customary principle of distinction applies to all types of conflict irrespective of their classification under the law.

A military objective is the only legitimate target of attack under the principle of distinction.⁴³ A civilian object, according to the Protocol, is any object that does not qualify as a military objective and, because of its status as civilian, is generally protected from attack and shall never be the object of reprisals.⁴⁴ The Protocol defines military objectives as “those objects which by their nature, location purpose and use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”⁴⁵ Thus there are two important elements of the definition that have to be met: the object shall make an “*effective contribution*” to the military action and the attack of it shall offer a “*definitive military advantage*.”⁴⁶

The effective contribution to military action is that contribution which is closely and obviously linked to military operations.⁴⁷ The nexus between

⁴² Additional Protocol I, *supra* note 7, at art. 48.

⁴³ Additional Protocol I, *supra* note 7, at art. 52 (2).

⁴⁴ Additional Protocol I, *supra* note 7, at art. 52 (1).

⁴⁵ *Id.*

⁴⁶ Emphasis added.

⁴⁷ Louise Doswald-Beck, *Some Thoughts on Computer Network Attacks and the International Law of Armed Conflict*, 76 INT’L L. STUD. 163, 166-167 (2002).

“effective contribution” and “military operations” has been interpreted differently by the United States, despite the nature of the definition as customary.⁴⁸ Even though the United States is not a party to the Protocol, it has publicly endorsed the definition as that of customary law, but with a broader reading. The United States also considers certain “war-fighting” or “war-sustaining” targets such as economic targets to be covered by the Protocol’s definition, in particular when such targets “[i]ndirectly but effectively support the enemy’s capability.”⁴⁹ This expansive interpretation of the “effective contribution” element to war-sustaining targets is farfetched and inconsistent with the Protocol. An expanded notion of “military objective” can muddy the waters of the distinction principle even more in the context of cyber warfare and can lead belligerents to more violations of international humanitarian law.⁵⁰ The U.S. concept of military objective interpreted in the cyber context allows for “[a]ny of the adversary’s information functions that have a bearing on his capability to fight to qualify as a legitimate target.”⁵¹ As discussed above, disruptive cyber operations directed against non-military targets such as financial stock markets, banking systems and others offer the possibility to belligerents to attack otherwise protected objects under *jus in bello* when at the same time they indirectly impede or disable military targets,

⁴⁸ ICRC Customary International Humanitarian Law Rules, *supra* note 9, at 29.

⁴⁹ U.S. DEPARTMENT OF THE NAVY, THE COMMANDER’S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 8.1.1 (2007); Koddar, *supra* note 38, at 118.

⁵⁰ Kelsey, *supra* note 32, at 1440.

⁵¹ Roscini, *supra* note 25, at 186.

avoiding at the same time the political cost associated with civilian casualties that conventional means of warfare would entail.⁵² Reasonably so, scholars are quite skeptical on cyber means in general that open the door for more violations of the law of targeting principles and put the principle of distinction under fire.⁵³ It is worth noting that the issue of striking economic targets is becoming more and more appealing to cyber targeteers. However, war-sustaining targets are not included in the Protocol's customary definition and alternative interpretations reflect, according to the author, *lex ferenda*.

The definition also provides useful guidance on the “effectiveness” of the contribution by advertent to the “nature,” “location,” “purpose” and “use” of the objects. The ICRC Commentary on Article 52 (2) of Additional Protocol I aims to elucidate that guideline. According to the Commentary, the “nature” refers to the inherent character of the object, while “purpose” is concerned with the intended future use of it.⁵⁴ In the cyber context, military objectives by nature can be computer networks that are inherently military, such as command and control networks exclusively transmitting military data, forming a part of weapons systems.⁵⁵ As Dinstein notes, there is no fixed borderline between civilian objects and military objectives.⁵⁶ This is *a fortiori* the case in the cyber

⁵² Kelsey, *supra* note 32, at 1440; Koddar, *supra* note 38, at 117.

⁵³ Kelsey, *supra* note 32, at 1440.

⁵⁴ ICRC Commentary of Additional Protocols, *supra* note 12, at para. 2020, 2022.

⁵⁵ Roscini, *supra* note 25, at 184.

⁵⁶ Yoram Dinstein, *Legitimate Military Objectives under the Current Jus in Bello*, 78 INT'L L. STUD. 139, 144 (2002) [hereinafter Dinstein, *Legitimate Military Objectives*].

domain, especially in relation to the use of an object. Not only there is no fixed borderline but also the inherent structure of cyber space provides no foolproof segregation of private, military and civilian networks.⁵⁷ The analysis will address the dual-use targets in the context of cyber operations upon completion of the analysis of the military objective definition.⁵⁸

The definition of military objective also requires that there be a definite military advantage to be gained. The advantage has to be definite and concrete.⁵⁹ Potential and indeterminate advantages are not acceptable; neither are political ones.⁶⁰ The advantage also must be, according to Boothby, “militarily necessary.”⁶¹ It is often difficult to identify the military advantage anticipated for a given attack, especially in the cyber context where measuring the effects of a cyber operation can be challenging.⁶² Before executing an attack, the attacker should carefully and reasonably evaluate the object’s qualification in the context of the principle distinction as well as the proportionality of the attack.⁶³ Both assessments bear the risk of failure or mistake, due to misleading intelligence. However, as

⁵⁷ Koddar, *supra* note 38, at 115.

⁵⁸ *See infra* Chapter III B.

⁵⁹ Robert Kolb & Richard Hyde, An introduction to the International Law of Armed Conflict 131 (2008).

⁶⁰ YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 93 (2nd ed. 2010) [hereinafter Dinstein, *Conduct of Hostilities*]; ICRC Commentary of Additional Protocols, *supra* note 12, at para. 2024.

⁶¹ WILLIAM H. BOOTHBY, THE LAW OF TARGETING 103 (2012).

⁶² Roscini, *supra* note 25, at 188.

⁶³ Additional Protocol I, *supra* note 7, at art. 57.

long as there is a reasonable expectation that the intended results will occur and provided that the attacker has taken the necessary precautions, there should be no legal consequences if *a posteriori* advantage was not effectively gained.⁶⁴

The second requirement of the definition of military objective is frequently ignored. It is often the case, when assessing the status of an object, for an attacker to mainly focus on the element of “effective contribution” due to the “nature,” “location,” “use” and “purpose” of the object and overlook the second element of “definite military advantage.” The Commentary of Air and Missile Warfare, for instance, reads as follows: “[i]n practical terms, compliance with the first criterion will generally result in the advantage required of the second.”⁶⁵ Such a conclusion is inconsistent with the Protocol. The evaluation-test on the military status of an object is twofold and the two requirements are equivalent. In the cyber domain especially, where the military uses the same cyber infrastructure as the civilian population for its military action, the second requirement of the definition becomes even more autonomous and one should be cautious with such sweeping conclusions.⁶⁶ Cyberspace is relatively resilient compared to other targets. In the case of an attack against a cyber infrastructure such as communication networks, the data flow is so flexible

⁶⁴ *Id.*

⁶⁵ PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 49 (Version 2.1 2010), *available at* <http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf>.

⁶⁶ Geiss and Lahmann, *supra* note 5, at 388.

that even if certain communication paths are destroyed by the cyber attack, the data packages will have various other possible paths to follow so as to reach the intended destination.⁶⁷ In this case, the partial destruction of the network might effectively contribute to military action but will hardly offer a definite advantage in the end. Only if all possible or at least the major communication paths are destroyed, might an advantage effectively be gained and this is without prejudice to future real-life scenarios.

Finally, the Protocol adds a “situational relevance” criterion to the definition of military objective.⁶⁸ The provisions of the definition are qualified by the phrase “under the circumstances ruling at the time,” significantly restricting the scope of the definition, which could otherwise take on uncontrollable dimensions and can be intentionally misused by states.⁶⁹ In practical terms, any attack has to be always assessed on a case-by-case basis and under a temporal framework that consists of the initial planning of the attack until the final execution, as each case’s circumstances are unique. Additionally, its final legitimacy ought to be additionally assessed on a proportionality basis. Compliance to proportionality dictates that the incidental civilian damage or loss should not be excessive in relation to the concrete and direct military advantage anticipated.⁷⁰

B. Dual-Use Targets

⁶⁷ *Id.*

⁶⁸ Additional Protocol I, *supra* note 7, at art. 52 (2).

⁶⁹ Geiss and Lahmann, *supra* note 5, at 387.

⁷⁰ Additional Protocol I, *supra* note 7, at art. 57 (2) (a) (iii).

The definition of military objective applied to cyber operations can render many components of the civilian cyber infrastructure military objectives by use. The concept of dual use targets is not new to the law of armed conflict. Dual use targets are those targets that serve both military and civilian purposes. The fundamental difference in cyber warfare lies in the *sui generis* nature of cyber space, namely the “systemic interconnectivity of civilian and military infrastructure.”⁷¹ Satellites, routers, cables, servers and even computers are all dual use cyber facilities.⁷² When it comes to decide on the military nature of an ordinary computer, it is rather the use of its software on which a decision falls upon (if used for deciphering codes, transmitting malicious data packages, etc.) rather than its hardware. Nevertheless, the latter can also constitute a legitimate military target if it is being used as storage of military data.⁷³

The interconnectivity of computer systems presents a fundamental and unprecedented challenge in applying the principle of distinction to cyber operations.⁷⁴ As Geiss and Lahmann note, “every component of the cyber infrastructure, every bit of memory capacity has a military potential.”⁷⁵ A clear example on the interconnectivity is the journey of military code.⁷⁶ When a military code is transmitted via cyber space, it splits up into different data packages, which then typically travel through a wide variety of civilian systems (as civilian systems form

⁷¹ Geiss and Lahmann, *supra* note 5, at 381.

⁷² Geiss and Lahmann, *supra* note 5, at 386.

⁷³ Dinstein, *Principle of Distinction*, *supra* note 24, at 263.

⁷⁴ *Id.*

⁷⁵ *Id.* at 383.

⁷⁶ *Id.* at 385.

the majority of cyberspace).⁷⁷ Hence, the civilian communication channels as well as some hardware components (servers, routers, satellites) could qualify under the first half of the definition as military objectives by use. Simply put, the systemic interconnectivity renders the whole cyber domain a potential dual-use target, at least in theory.⁷⁸ However, the view that the whole cyber domain can be a military objective by use is somewhat farfetched and one-sided. Even if the whole cyber infrastructure of a belligerent state potentially qualifies as a military objective by use, it is still difficult to prove that the object's contribution is not only effective to the military action but also closely linked to hostilities, as the definition requires. Finally, it is highly unlikely that the cyber domain as a whole could effectively contribute to the war effort offering at the same time a definite military advantage. The same conclusion is also reached by the Tallinn Experts.⁷⁹

Under the law of targeting, an object cannot simultaneously have civilian and military status. In the case of a dual use object acknowledged as a military objective under the Protocol's definition, the civilian use of the object would have to be assessed under the proportionality assessment.⁸⁰ This happens because the object effectively contributes to military action and its destruction or neutralization would offer the concrete and direct military advantage anticipated by the belligerent targeteer so that its civilian use is outweighed. Consequently, its civilian function is neutralized, as the object has become a

⁷⁷ *Id.*

⁷⁸ Geiss and Lahmann, *supra* note 5, at 390.

⁷⁹ Tallin Manual, *supra* note 19, at Rule 39 para. 5.

⁸⁰ Roscini, *supra* note 25, at 185.

military objective under the principle of distinction.⁸¹ Furthermore, as the dual use concept is not an innovation of cyber warfare, the Protocol provides a remarkable assumption for *lex scripta*. In case of doubt on the object's military status, "[i]t shall be presumed not to be so used."⁸² Certainly, the presumption can be rebutted by additional intelligence on the target. *A contrario* to the first two paragraphs of the definition and to the counter-provisions related to protected persons, the third paragraph of Article 52 does not form part of the customary international humanitarian law according to the ICRC Customary International Humanitarian Law Study, as it has not been included in the Rules.⁸³ The Tallinn Experts could not achieve unanimous consensus on the customary nature of this provision either. Therefore, the Tallinn Manual calls upon the attacker to decide upon the object's status only after a careful assessment.⁸⁴ However, the Experts were cautious to highlight that the presumption of paragraph 3 applies exclusively in respect to the "effective contribution" element and not in any other elements of the definition.⁸⁵ The author's personal view is in favor of the protected object in case of doubt and the abortion of the cyber attack accordingly, a view that probably will not find much support among military circles. The latter often tend to overlook the civilian function of dual-use targets and stress the effective contribution of the target to military action as well as the advantage

⁸¹ Tallinn Manual, *supra* note 19, at Rule 39 para. 2.

⁸² Additional Protocol I, *supra* note 7, at art. 52 (3).

⁸³ ICRC Customary International Humanitarian Law Rules, *supra* note 9.

⁸⁴ Tallinn Manual, *supra* note 19, at Rule 39 para. 2,3.

⁸⁵ Tallinn Manual, *supra* note 19, at Rule 39 para. 4.

anticipated in terms of military necessity. From a proportionality perspective, the damage of the object is likely to be found proportionate to the military advantage.

C. Digital Data As “Objects” Under The Law Of Targeting

An issue with cyber operations that still remains unsettled under the law of targeting is the status of intangible objects such as electronic or digital data. The majority of legal experts hold the view that data should not generally be considered as objects under the law of targeting and in particular under the definition of military objective, except in two cases.⁸⁶ According to Schmitt, the first case refers to data that are directly transferable into tangible objects, giving the example of banking account data transferable into money via ATMs and the second refers to data that have intrinsic value such as digital art.⁸⁷ However, a minority of the Tallinn Experts was of the opinion that data *per se* should be considered as objects at least for the purposes of targeting.⁸⁸ Otherwise, the minority argued, important civilian data could be left out of the regulatory reach of the law of armed conflict.

The view that excludes data from the notion of “object” draws its basis from the “ordinary meaning” of the word object as well as from the ICRC Official Commentary of the Protocol.⁸⁹ Under

⁸⁶ Schmitt, *Key Issues*, *supra* note 14, at 96; Tallinn Manual, *supra* note 19, at Rule 38.

⁸⁷ Schmitt, *Key Issues*, *supra* note 14, at 96.

⁸⁸ Tallin Manual, *supra* note 19, at Rule 38 para. 5.

⁸⁹ ICRC Commentary of Additional Protocols, *supra* note 12, at para. 2008.

the Protocol's Commentary, the word object refers to something, which is "tangible" and "visible."⁹⁰ Despite the Commentary's authoritative character and its invaluable contribution to the law of armed conflict, "tangible" and "visible" are not part of the Protocol's own wording. This *prima facie* interpretation seems outdated in the light of current cyber warfare reality. Back in the Protocol's drafting days, the concept of digital data could not have been envisaged by the Drafters, because the technology was not in widespread use. However, the fact that they were not included in the original concept does not mean that the Drafters intentionally excluded them, as they could have not been envisaged in the first place.⁹¹ The Commentators used the adjectives "tangible" and "visible" in order to exclude abstract concepts such as "objective" and "aim" from the notion of object.⁹² Moreover, a treaty has to be always interpreted in light of modern realities and pursuant to its object and purpose.⁹³ Excluding electronic data from the definition of object may not be the best way to protect civilians when it comes to cyber warfare.

The main argument of the majority of scholarship is that loss of non-tangible objects such

⁹⁰ "It is clear that in both English and French the word means something that is visible and tangible." ICRC Commentary of Additional Protocols, *supra* note 12, at para. 2008.

⁹¹ Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252, 267-268 (2013).

⁹² *Id.*

⁹³ Vienna Convention on the Law of Treaties, art. 31 para. 1., May 23, 1969, available at <https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf> [hereinafter Vienna Convention].

as electronic data does not entail analogue consequences to the real world. Nowadays, it is possible to destroy millions of vital (civilian) data without any physical consequences on the computers in which they are stored.⁹⁴ In such cases, in order to assess whether the loss of electronic data reaches the threshold of attack, one has to prove damage. Therefore, scholars have put forward the “potential restoration capability” test.⁹⁵ This test disqualifies digital data from the notion of objects for there is no damage occurred as long as the lost data are retrievable. However, one should question the relevance of “back up data” criterion.

Another view permits for irretrievable data to classify as objects under the law of targeting.⁹⁶ The classification under the principle of distinction of electronic data would then depend on whether the data could be restored.⁹⁷ The “potential restoration capability” test, however, could wind up excluding from the definition of object many physical structures that have traditionally been considered objects because the damage done to them can be repaired. As electronic data could be potentially restored, buildings could be potentially rebuilt. While the analogy is not perfect, in both cases the restoration of damage can bear significant costs, which we may want the law of armed conflict to address. Finally, as for targeting data, the verification of back up data could be included within the duty of the attacker to take precautions reinforcing thus the argument in favor of data as objects.⁹⁸

⁹⁴ Lubell, *supra* note 92, at 267.

⁹⁵ *Id.* at 268.

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.*

In summary, updated interpretations on the notion of object do not reflect *lex ferenda* as the Tallinn Experts argue.⁹⁹ Irrespective of the view one will chose to endorse in the end, interpretation of the Protocol's provision in light of cyber reality supports the existing body of international humanitarian law. By resisting new interpretations, the existing rules might be obsolete or misapplied.¹⁰⁰ Cyber reality calls for reconsideration of the notion of objects that will allow electronic data to be subject to the principle of distinction as contemporary targets. Otherwise, digital data will be left out of the regulatory reach of the law of armed conflict, in a normative lacuna. Future cyber conflicts and state practice will help guide interpretation of the rules and will further crystallize the notion of digital data and their status under the law of targeting.¹⁰¹

D. The Internet As Network Of Communication

In recent conflicts, insurgents in non-international armed conflicts have been using social network sites, such as Facebook, Twitter and YouTube, for purposes of the conflict, such as raising funds for weapons and supplies and promoting the fight to the world.¹⁰² The concept of disseminating propaganda through communication networks is not new to international law of armed conflict. In order

⁹⁹ Tallinn Manual, *supra* note 19, at Rule 38 para. 5.

¹⁰⁰ *Id.* at 270.

¹⁰¹ Lubell, *supra* note 92, at 272.

¹⁰² *The Role of Social Media in the Syrian Civil War* by Media-Measurement, MediaMeasurement (April 26, 2015), <http://www.mediameasurement.com/the-role-of-social-media-in-the-syrian-civil-war/>.

to determine whether or not the Internet as means of communication qualifies *per se* as a military objective under the law of targeting, it should be examined whether the two requirements of Article 52 (2), namely the effective contribution to military action and the definite military advantage are cumulatively met.

Historically, telecommunication infrastructures have been the target of attacks, as they were used by the military for military purposes. One of the indicative cases was the aerial bombardment of Serbia's Radio-Television headquarters in Belgrade ("RTS"), during the NATO Kosovo Campaign.¹⁰³ The attack was made on the basis that the Milosevic regime was using the network for military purposes such as control mechanism and dissemination of propaganda. The International Criminal Tribunal for the former Yugoslavia's ("ICTY") Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia acknowledged the legitimacy of the attack on the basis that it was aimed at disabling military command and control systems as well as destroying the apparatus that kept Milosevic Regime in power.¹⁰⁴ A similar attack against Al-Jazeera Kabul Office during Operation Enduring Freedom in 2001 was conducted and justified on the grounds of

¹⁰³ Also known under the name "Operation Allied Force."

¹⁰⁴ International Criminal Tribunal for the former Yugoslavia (ICTY) Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia para. 75 (2000), *available at* <http://www.icty.org/sid/10052> [hereinafter ICTY Final Report].

halting military propaganda by the Taliban.¹⁰⁵ In more recent conflicts like that of Libya in 2011, telecommunication networks were legitimately targeted because they formed part of military networks.¹⁰⁶

In any case, the Internet as communication network, in order to be able to constitute a legitimate object of attack, should effectively contribute to military action and its attack should offer a definite military advantage under the circumstances ruling at the time. It has been observed that an effective contribution of the Internet to the military action by means of propaganda or by undermining the civilian morale would not justify an attack because the mere disruption of its operations for the aforementioned reasons would be highly unlikely offering the necessary “definite military advantage.”¹⁰⁷ However, as already addressed above, in future cyber conflicts, the Internet *per se*, as network of communication might be a valuable cyber asset to gain control over in order to degrade the enemy’s cyber capabilities. In this hypothetical scenario, provided that the Internet would form part of the enemy’s military communication system and provided that the disruption of all its major communication paths would paralyze the enemy’s command and control structures, offering a definite military advantage under the circumstances ruling at the time, it could then qualify as a legitimate military objective under the law of targeting.¹⁰⁸ As already explained, the more communication paths are disrupted the more

¹⁰⁵ Robert Cryer, *The Fine Art of Friendship: Jus in Bello in Afghanistan*, 7 J. OF CONFLICT & SEC. L. 55 (2002).

¹⁰⁶ See Roscini, *supra* note 25, at 190, for further detail

¹⁰⁷ ICTY Final Report, *supra* note 105, at para 55.

¹⁰⁸ Roscini, *supra* note 25, at 190.

likely is to gain a definite military advantage due to the Internet's inherent resilience. However, as the Internet is a dual use cyber asset any further repercussions to its civilian function should be in conformity with the principle of proportionality; which requires that the total disruption of all communications should proportionate to the advantage gained if not the *ultimum refugium* to the attacker who would have to explore previously alternative options. Consequently, the Internet as means of communication could under certain occasions qualify for legitimate military objective *per se* under the law of targeting. Nevertheless, it is worth noting that there is no general rule and each scenario should be studied *in concreto*.

IV. TARGETING INDIVIDUALS CONDUCTING CYBER OPERATIONS

This chapter addresses the classification of persons as combatants or civilians under the principle of distinction. Determining the status of persons is of crucial legal significance since the most important legal consequences are those related to targeting.¹⁰⁹ Under the law of targeting and in the context of international armed conflicts there are only two mutually exclusive categories related to the status of individuals: “combatants” and “civilians.” Scholars have argued that civilians taking direct part in hostilities and combatants who have failed to comply with the laws of war in international armed conflicts are deemed, as a result of their behavior, “unlawful” or “unprivileged” combatants.¹¹⁰

¹⁰⁹ Vijay M. Padmanabhan, *Cyber Warriors and Jus in Bello*, 89 INT'L L. STUD. 288, 289 (2013).

¹¹⁰ Dinstein, *Conduct of Hostilities*, *supra* note 60, at 130.

However, the term “unlawful” does not introduce a third category along with civilians and combatants but is used in a descriptive manner and refers to the rights and duties of civilians and combatants upon capture by the enemy, according to the law of detention in international armed conflicts. Hence, their status remains always civilian. Issues of the law of detention, however, are excluded by the present analysis.

The analysis will first address the definition of civilians. As this definition is negatively formulated under the law of targeting, it will then turn to the definition of combatants in international and non-international armed conflict accordingly. It should be clarified that, in terms of law, there is neither “combatant” nor “prisoner of war (‘POW’)” status in the context of non-international armed conflicts. However, scholars sometimes use the notion of combatant for the purposes of the principle of distinction, even in the context of non-international armed conflicts, in its generic sense and as an indicator of those individuals that directly participate in hostilities.¹¹¹ The Manual on the Law of Non-International Armed Conflict when referring to individuals, members of armed forces, dissident armed forces or organized armed groups or those who directly participate in hostilities uses the term “fighters” for reasons of avoiding semantic confusion.¹¹² Irrespective of the descriptive word used each time, these individuals are not entitled to combatant immunity and are not combatants in the

¹¹¹ Roscini, *supra* note 25, at 192.

¹¹² INTERNATIONAL INSTITUTE OF HUMANITARIAN LAW, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY 4 (Michael N. Schmitt et al. eds., 2006).

legal term of art, as the rules of “privileged” or “unprivileged” combatancy are not applicable in non-international armed conflicts. In the present study, individual members of non-state armed groups conducting cyber operations in non-international armed conflicts will be termed as individuals assuming a “continuous combat function,” pursuant to the terminology adopted in the ICRC’s Interpretive Guidance on the Notion of Direct Participation in Hostilities (“Guidance”).¹¹³

A. Civilians

The definition of civilians is negatively formulated in Article 50 (1) of Additional Protocol I. Pursuant to the Protocol, a civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Geneva Convention and in Article 43 of Additional Protocol I. According to the ICRC Guidance, the concept of civilian in international armed conflict consists of “[a]ll persons who are neither members of the armed forces of a party to the conflict nor participants in a levée en masse and who do not take a direct part in hostilities.”¹¹⁴ Furthermore the Protocol provides that “the civilian population as such, as well as individual civilians shall not be the object of attack.”¹¹⁵ Civilians are

¹¹³ See *infra* Chapter IV 3 for the notion of continuous combat function in non-international armed conflict.

¹¹⁴ Nils Melzer, INT’L COMM. OF THE RED CROSS INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 20 (2009) [hereinafter ICRC Interpretive Guidance].

¹¹⁵ Additional Protocol I, *supra* note 7, at art. 51 (2).

generally immune from attack “[u]nless and for such times as they take a direct part in hostilities.”¹¹⁶ In the context of an armed conflict not of an international character, the Guidance defines civilians as those “[p]ersons who are not members of the state’s armed forces or non-state organized armed groups of a party to the conflict.”¹¹⁷ Hence, under the law of targeting and pursuant to the principle of distinction, legitimate targetable individuals with regard to international armed conflicts are combatants and civilians taking direct part in hostilities and with regard to non-international armed conflicts are individual members of state’s armed forces or individuals of non-state armed groups assuming a “continuous combat function” as well as civilians taking direct part in hostilities. The notion of combatant in international armed conflicts as well as the notion of continuous combat function in non-international armed conflicts will be addressed next.

B. Combatants In International Armed Conflicts

Article 43 (2) of Additional Protocol I provides for the definition of combatants in terms of membership in the armed forces; “[m]embers of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.”¹¹⁸ The 1907 Hague Regulations, in contrary, differentiate the term combatants and defines it in terms of conduct, with an exception to

¹¹⁶ Additional Protocol I, *supra* note 7, at art. 51 (3).

¹¹⁷ ICRC Interpretive Guidance, *supra* note 115, at 27.

¹¹⁸ Additional Protocol I, *supra* note 7, at art. 43 (2).

the religious and medical personnel.¹¹⁹ The Protocol's definition largely assimilates regular and irregular armed forces.¹²⁰ The ICRC Study on Customary International Humanitarian Law defines armed forces in the context of an international armed conflict as "all organized armed forces, groups and units which are under command responsible to that party for the conduct of its subordinates."¹²¹ Article 43 and 44 has been among the most controversial provisions of the Protocol with regard to the definition of combatants. The controversial character of many of the Protocol's provisions is claimed to be the reason why many states have abstained from ratifying the Protocol.¹²²

From the combination of the chapeau of Article 4 A (2) of Third Geneva Convention and Article 50 Additional Protocol I combatants, are all members of the armed forces of a belligerent party, both regular and irregular forces *de facto* incorporated, including members of militias and volunteer corps belonging to a party to the conflict as well as *levée en masse*.¹²³ The analysis will first look at the regular and irregular armed forces of a state and then proceed to members of militia and other

¹¹⁹ The Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land Article 3 (1907), available at <https://www.icrc.org/applic/ihl/ihl.nsf/0/1d1726425f6955aec125641e0038bfd6>.

¹²⁰ Additional Protocol I, *supra* note 7, at art. 43.

¹²¹ ICRC Customary International Humanitarian Law Rules, *supra* note 9, at 14.

¹²² Heather Harisson-Dinniss, *Cyber Warfare and the Laws of War*, in Cambridge Studies in International and Comparative Law 140 (2014).

¹²³ Dinstein, *Conduct of Hostilities*, *supra* note 60, at 33.

volunteer corps. Lastly, it will examine the notion of *levée en masse* in the cyber context.

1. Members Of A Belligerent State's Armed Forces Conducting Cyber Operations, Including Irregular Armed Forces *De Facto* Incorporated

States that have developed cyber technologies in war typically have also formally incorporated active cyber units into their armed forces or are believed to have done so. One indicative example is the cyber sub-unit of the United States Strategic Command known as USCYBERCOM.¹²⁴ Those that conduct cyber operations in these units are combatants pursuant to the Protocol's definition, as they form part of the regular armed forces of the state and as such are legitimate military objectives targetable at all times during a conflict. Scholars have suggested the incorporation of the specialized personnel conducting computer network attacks into the armed forces as a potential solution to the problem of distinguishing combatants and civilians for the purposes of the principle of distinction.¹²⁵ Upon incorporation into the armed forces, such personnel will be considered as combatants as it will form part of the military. Combatants under the Protocol are not only the members of the regular armed forces of a belligerent party, but also the members of irregular armed forces, namely paramilitary and law enforcement units provided that have been *de facto* incorporated to the armed forces

¹²⁴ Roscini, *supra* note 25, at 193.

¹²⁵ Doswald-Beck, *supra* note 47, at 172.

of a party.¹²⁶ The case, however, of paramilitary law enforcement units de facto incorporated into the armed forces does not seem to apply in a pure cyber conflict scenario.

2. Militias and Volunteer Groups “Belonging To A Belligerent Party” Conducting Cyber Operations

Another subcategory of combatants in the context of an international armed conflict is volunteer corps or militias “belonging to a party to the conflict.”¹²⁷ Firstly, the words “militias” or “volunteer corps” imply that the group is armed and has sufficient organization similar to that of regular armed forces, otherwise the group is a collective of civilians taking direct part in hostilities.¹²⁸ So far there is no armed group sufficiently organized existing only online.¹²⁹ Future scenarios may involve organized armed groups that also conduct cyber operations, but it may be difficult for such a group to meet the qualifications of a militia or volunteer group such that they are considered combatants. The famous Anonymous for instance is neither “armed” nor “sufficiently organized” but qualifies perhaps as a group of civilian “hactivists.”

“Belonging to a party to the conflict” is an important requirement for militias and other volunteer corps to qualify for armed forces when the

¹²⁶ Additional Protocol I, *supra* note 7, at art. 44 (3).

¹²⁷ Third Geneva Convention Relative to the Treatment of Prisoners of War, art. 4 (2), August 12, 1949 [hereinafter Third Geneva Convention].

¹²⁸ Roscini, *supra* note 25, at 195.

¹²⁹ *Id.*

former do not form part of the state's regular or irregular forces but are under the control of a belligerent party.¹³⁰ The degree of control in order for a state to be responsible over the conduct of an organized armed group is yet unsettled under the law and has evoked much controversy among scholars.¹³¹ According to the ICRC Guidance, the criterion of "belonging to a party to the conflict" requires "[a]t least a de facto relationship between an organized armed group and a party to the conflict" and if not explicit "[a] tacit agreement or a conclusive behavior."¹³² Moreover, the Guidance contends that should a group's conduct is attributable to one of the belligerent parties under the law of state responsibility then the requirement is undoubtedly satisfied.¹³³ However, this is not often the case, as states frequently use non-state actors to launch cyber operations on their behalf so as to deny any contribution to or responsibility for the attack. Furthermore, cyber operations raise particular issues regarding state attribution, as their identification is often difficult. However, the "belonging to a party to the conflict" requirement is a requirement of the law of targeting, a branch of international humanitarian law that stands regardless of the rules on international state responsibility.¹³⁴ Therefore, it should be interpreted according to the ordinary meaning of the provision and in light of the purpose

¹³⁰ This requirement follows from the combination of art. 13 (2) of the First and Second Geneva Convention, art. 4 (A) (2) of the Third Geneva Convention, and art. 50 (1) of Additional Protocol I. *See also* ICRC Interpretive Guidance, *supra* note 115, at 23.

¹³¹ ICRC Interpretive Guidance, *supra* note 115, at 23.

¹³² *Id.*

¹³³ *Id.*

¹³⁴ Roscini, *supra* note 25, at 196.

and object of the Protocol.¹³⁵ One of the basic positions in this respect is the effective control test elaborated by the ICJ in Nicaragua Judgment.¹³⁶ The Court used the “effective control” test as an attribution standard in order to establish the U.S. control over the Contras’ particular actions and for the purposes of state responsibility. The effective control standard as the Court noted in the Genocide Judgment requires the issue of “[s]pecific instructions... in respect of each act allegedly committed by the group.”¹³⁷ Hence, the “effective control” standard focuses on the particular acts committed by an organized armed group and not on the group *per se*. Consequently, the effective control might seem irrelevant or inappropriate for the purposes of the law of targeting that requires the group *per se* to belong to a state party to the conflict in order for its members to qualify as combatants. Another famous test established by the International Criminal Tribunal for the Former Yugoslavia (“ICTY”) in the Tadic Case is the “overall control” test.¹³⁸ The “overall control” test delimitates the attribution standard to the overall control over a

¹³⁵ Vienna Convention, *supra* note 94, at art. 31 para. 1.

¹³⁶ Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 115 (June 27), available at <http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5> [hereinafter ICJ Nicaragua Judgment].

¹³⁷ Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro) 2007 I.C.J. 43, 400 (Feb. 26), available at <http://www.icj-cij.org/docket/files/91/13685.pdf> [hereinafter ICJ Genocide Judgment].

¹³⁸ Prosecutor v. Tadic, IT-94-A, para. 141 (1999), available at <http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>.

military organized armed group and not over the specific acts committed by the group, being thus less restrictive than the counterpart test elaborated by the ICJ.¹³⁹ Following the overall control test, the ICTY in Tadic supported that:

[i]n order for irregulars to qualify as lawful combatants, it appears that international rules and State practice therefore require control over them by a Party to an international armed conflict and, by the same token, a relationship of dependence and allegiance of these irregulars *vis-à-vis* that Party to the conflict. These then may be regarded as the ingredients of the term “belonging to a Party to the conflict.”¹⁴⁰

Adopting the “overall control” standard the Court went on and concluded that the FRY authorities had sufficient overall control over the Bosnian Serb armed forces “[g]oing beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations.”¹⁴¹ On the contrary, with regard to individuals, members of any other group that is not “militarily” organized, the ICTY retains the “effective control” test and requires the existence of specific instructions over particular acts or the retroactive endorsement of those actions by the party to the conflict.¹⁴² However, it should be mentioned that the ICTY developed the “overall control” test for the purposes of defining an internationalized armed

¹³⁹ *Id.* at para. 145.

¹⁴⁰ *Id.* at para. 94.

¹⁴¹ *Id.* at para. 145.

¹⁴² *Id.* at para. 118.

conflict and not for establishing attribution criteria.¹⁴³

Between the two positions, the ICTY “overall control” test seems at first place to be closer to the ordinary meaning of the “belonging to a party requirement,” as it focuses on the actor rather than the act. A third position that has been developed regarding attribution standard over the acts of a group is the “complete dependence test” in the ICJ Genocide Judgment.¹⁴⁴ The “complete dependence” test requires a great degree of state control over the persons, groups or entities and was developed by the Court for the purposes of state responsibility. Pursuant to this test, for persons to belong to a party to the conflict, it must be proven that “[t]he persons, groups or entities act in ‘complete dependence’ on the State, of which they are ultimately merely the instrument.”¹⁴⁵ The proof essentially under this standard is that militias or volunteer corps are *de facto* organs of a state party to the conflict. Therefore, this even stricter “complete dependency standard” established by the ICJ in the Genocide Judgment, focusing on the nexus between the militia and the belligerent party, according to some scholars, is closer to the provision’s ordinary meaning that requires a bond between the individuals, members of the organized armed groups and the belligerent party.¹⁴⁶

The “belonging to a party requirement” interpreted in the context of cyber attacks over instrumentalized militias or volunteer corps could prove challenging to apply. The “complete

¹⁴³ *Id.* at para 138.

¹⁴⁴ ICJ Genocide Judgment, *supra* note 138, at para. 392-393.

¹⁴⁵ *Id.* at para. 392.

¹⁴⁶ Roscini, *supra* note 25, at 196.

dependence” test might seem more consonant to the Protocol’s “belonging to a party requirement,” however, it sets a relatively high threshold of control and effectively of combatant status. If, for instance, the groups that conducted the large scale distributed denial of service (“DDoS”) attacks against Georgia in the conflict between Russia and Georgia over South Ossetia had been under the “complete dependence” control of the Kremlin and the cyber operations had amounted to cyber attacks under the key threshold of Article 49 of Additional Protocol I, then the individual members of those groups would perhaps have qualified for the status of combatants under the law of targeting.

It is imperative, however, to fill the interpretation gap on the necessary degree of control so as to establish a nexus between militias and volunteer groups conducting cyber operations and belligerent parties. The standards of control so far developed by international courts were elaborated in context of conventional means of warfare. Cyber means, however, call for reconsideration of the applicable control test. Adopting the stricter test of “complete dependence” control could risk establishing eventually a very high threshold on combatant status under the law of targeting. Not only cyber operations pose unique issues of identification and attribution but proving complete dependence of individuals actors conducting cyber operations on behalf of a party to a conflict could prove extremely difficult.

According to Article 4 A (2), which is generally the more widely accepted definition of combatants and prisoners of war (“POW”) status,¹⁴⁷

¹⁴⁷ Harisson-Dinniss, *supra* note 123, at 140.

members of militias and volunteer corps i.e. partisans, organized resistance movements, shall belong to a party to the conflict in order to qualify as a combatant and obtain POW status and shall fulfill the following four additional conditions: (a) being under the person's responsible command for his subordinates; (b) have a distinctive sign recognizable at a distance; (c) carry arms openly; and (d) conduct their operations in accordance with the law and customs of war.¹⁴⁸ From a first reading, it is obvious that the Protocol's definition of POW status has eliminated the second and fourth requirements. Non-compliance with the laws and customs of war, as well as the lack of a distinguishing sign recognizable at distance, does not deprive the combatant of his entitlement for a POW status insofar as he carries arms openly pursuant to the Protocols requirements.¹⁴⁹ As the ICRC notes, it would not be sensible to place irregular armed forces under the protective regime granted under the status of civilian only because they failed in fulfilling the requirements of identification.¹⁵⁰ It should be stressed, however, that the requirements of Article 4 A of the Third Geneva Convention set the constitutive requirements for privileged combatancy, namely when combatants are entitled to a POW status. Consequently, for the purposes of the conduct of hostilities and the law of targeting, failing to prove one of the requirements set forth in the Third Geneva Convention, a combatant is not losing his status as such.¹⁵¹

¹⁴⁸ Third Geneva Convention, *supra* note 128, at art. 4 (A) (2).

¹⁴⁹ Additional Protocol I, *supra* note 7, at art. 44 (3).

¹⁵⁰ *Id.*

¹⁵¹ ICRC Interpretive Guidance, *supra* note 115, at 22.

Applying the first condition of the “responsible command of person for his subordinates” in the cyber context, individual cases of independent hackers based on the territory of a belligerent party who wish to engage in war out of personal sympathy or hatred against the enemy without the party’s authorization or consent are immediately excluded from the definition of combatant.¹⁵² In the case, for instance, of the conflict between the U.S. and Afghanistan, there were U.S. based hackers wishing to join the conflict by conducting cyber operations against Afghanistan, a behavior that the U.S. publicly condemned.¹⁵³ Cyber actors such as these would not qualify as combatants under this first condition.

The second and third requirements, though eliminated by the Protocol’s definition are issues directly related to the distinction principle. Combatants should be able to be distinguished at a distance by having a fixed distinctive sign and should always carry arms openly.¹⁵⁴ One challenge in the cyber context is that computer network attacks are characterized by anonymity.¹⁵⁵ It is highly unlikely to identify the user of a particular computer so as to decide upon his status. Lacking any proximity to the battlefield, computer attacks are covert operations by

¹⁵² Padmanabhan, *supra* note 110, at 296.

¹⁵³ David F. Gallagher, *Hackers; Government Tells Vigilantes Their ‘Help’ Isn’t Necessary*, N.Y. TIMES, Feb., 20, 2003, available at <http://www.nytimes.com/2003/02/20/technology/hackers-government-tells-vigilantes-their-help-isn-t-necessary.html?module=Search&mabReward=relbias%3Aw>.

¹⁵⁴ Third Geneva Convention, *supra* note 128, at art. 4 (A) (2) (b), (c).

¹⁵⁵ Harisson-Dinniss, *supra* note 123, at 145.

nature, rendering these two requirements of the law less significant or even obsolete.

However, as the principle of distinction remains of quintessential significance for the law of targeting, the issue should be dealt with caution. There has been put forward a technical approach suggesting the establishment of a “class” of designated military Internet Protocol (“IP”) addresses only from which computer networks attacks can be launched.¹⁵⁶ In this way, the computer with which a cyber operation is launched will be marked as a designated military IP address. Alternatively, the electronic marking of a computer could be achieved by the creation of “universally recognized electronic identifiers” that will recognize the status of persons in compliance with the Geneva Conventions.¹⁵⁷ Such a scenario, to the extent that it is technically feasible, seems not to be the case for the next couple of years, as states would perhaps oppose such a proposal for reasons of tactics. In addition, even if states approve such a measure, the belligerent parties will perhaps abuse the identifiers in times of conflicts.¹⁵⁸

The problem with electronic marking of computers conducting cyber attacks and is that sometimes tracing back an attack to the originated computer is impossible either due to technological incapacities or for reasons of time economy.¹⁵⁹ As

¹⁵⁶ *Id.* at 146.

¹⁵⁷ Davis Brown, *A Proposal of an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT’L L.J. 196 (2006).

¹⁵⁸ *Id.*

¹⁵⁹ Harisson-Dinniss, *supra* note 123, at 147; Padmanabhan, *supra* note 110, at 291.

discussed earlier,¹⁶⁰ the majority of computer network attacks such as malicious codes follow various third party intermediary servers, each of them having its own identifiable IP address, and communication paths, until they reach their target.¹⁶¹ Hence, tracing back the attack to the originated computer can be impossible either for technological incapacities, certain cyber operations are indeed untraceable or for reasons of time economy.¹⁶²

In the end, the Protocol provides for certain types of warfare where armed combatants cannot distinguish themselves to be exempted from the obligation of having a distinctive sign recognizable at distance while maintaining their status as combatants as long as they carry arms openly.¹⁶³ However, this provision is irrelevant with respect to targeting and becomes relevant on law of detention issues in case of international armed conflicts. The principle of distinction is interested solely to the status of each individual conducting cyber operations under the law as a combatant or as civilian.¹⁶⁴ All the additional requirements of Article 4 A of the Convention are there to ensure the rights and duties of persons upon capture by the enemy.

Finally the requirement that combatants comply with the laws and customs of wars when conducting cyber operations is as important as it is in every type of warfare. Perhaps, it is a fortiori the case with respect to cyber warfare, as cyber operations might tempt combatants to violate more often the

¹⁶⁰ See *infra* Chapter III on dual-use targets.

¹⁶¹ Padmanabhan, *supra* note 110, at 291.

¹⁶² Harisson-Dinniss, *supra* note 123, at 147; Padmanabhan, *supra* note 110, at 291.

¹⁶³ Additional Protocol I, *supra* note 7, at art. 44 (3).

¹⁶⁴ Roscini, *supra* note 25, at 198.

principle of distinction because of cyber means non-lethal potential. Consequently, the element of complying with the laws and customs of war becomes of crucial importance under the principle of distinction.

In summary, all members of the regular or irregular armed forces of a belligerent party as well as organized armed groups, namely militia and volunteer corps belonging to a party to the conflict under the conditions outlined above are combatants for the law of targeting and as such are targetable at all times during the conflict.

3. Cyber Levée En Masse

The notion of *levée en masse* arises exclusively in the context of an international armed conflict and is defined in Article 2 of the 1907 Hague Regulations. Persons can qualify as combatants under *levée en masse* when “the inhabitants of a non-occupied territory, who on the approach of the enemy, spontaneously take up arms to resist the invading troops, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.”¹⁶⁵ Hence, participants in *levée en masse* are combatants and are accorded a POW status upon capture. The crucial element of the notion of *levée en masse* is to “spontaneously take up arms.” Applied to cyber attacks, the existence of a cyber *levée en masse* that “spontaneously” and exclusively conduct cyber operations upon approach of the invading force seems highly problematic and impractical given the nature of cyber operations. Scholars have found the

¹⁶⁵ Third Geneva Convention, *supra* note 128, at art. 4 (A) (6).

existing provision ill-suited and outdated with regard to cyber attacks calling for a reconceptualization of this “anachronistic” notion.¹⁶⁶ *Levée en masse* is by nature an emergency uprising, a temporary mobilization of the inhabitants of a territory that comes together to defend the nation.¹⁶⁷ Hence, a cyber *levée en masse* is only feasible upon response to a traditional territory invasion by conventional force where at the same time the participants might conduct *inter alia* and cyber operations.¹⁶⁸ The notion seems unworkable in the context of participants who mobilize themselves against the enemy by “openly,” “spontaneously” and exclusively conducting cyber operations. The elements of “unoccupied territory,” as well as “spontaneously take up arms openly” simply do not conform to the realities of cyber warfare, as cyber attacks are by nature covert and anonymous and geographical limitations such as territory are not factors in the borderless cyber domain.¹⁶⁹

The main driving force behind the provision is the protection of the civilian population. Participants in *levée en masse* are combatants under the law of targeting as long as they carry arms openly and comply with the laws and customs of war. The condition of “carrying arms openly” is for the purposes of distinguishing between civilians, regular or irregular armed forces and participants in a *levée*

¹⁶⁶ David Wallace & Shane R. Reeves, *The Law of Armed Conflict's “Wicked” Problem: Levée en Masse in Cyber Warfare*, 89 INT’L L. STUD. 649, 661 (2013).

¹⁶⁷ INT’L COMM. OF THE RED CROSS, COMMENTARY OF THE THIRD GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 68 (Jean Pictet ed., 1960), available at http://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-III.pdf.

¹⁶⁸ Wallace, *supra* note 167, at 658.

¹⁶⁹ *Id.* at 660.

en masse. The main argument behind reconceptualizing the notion of *levée en masse* to cyber operations is the likelihood of indiscriminate targeting of the civilian population and as a result the violation of the principle of distinction.¹⁷⁰

The Tallinn Manual, although acknowledging the problematic nature of the notion in the cyber context, prefers to preserve the concept in its narrow sense requiring the physical invasion of a national territory in the case where a large majority of the territory's population spontaneously mounts cyber operations against the invading force.¹⁷¹ The experts did not achieve consensus whether or not the majority of a *levée en masse* mounting cyber operations could solely consist of the cyber-capable members of the population. The Tallinn Manual's approach has been criticized by some scholars who strongly contest that it is untenable to maintain such an unworkable anachronism for the principle of distinction at time where cyber realities call for reconceptualization of the notion.¹⁷² One of the recommendations made in their study is to eliminate the category of *levée en masse* in cyber conflicts and require all assemblages of cyber participants to comply with the requirements set for militias and other volunteer corps defined in Article 4 A (2) of the Third Geneva Convention as well as modify the existing criteria of irregular troop combatant category so as to conform with the cyber reality.¹⁷³ Other scholars, such as Brown, are in favor of extinguishing the notion completely in the cyber

¹⁷⁰ *Id.* at 661.

¹⁷¹ Tallinn Manual, *supra* note 19, at Rule 27 para. 3-5.

¹⁷² Wallace, *supra* note 167, at 665.

¹⁷³ Wallace, *supra* note 167, at 665.

context for the purposes of the distinction principle.¹⁷⁴

The concept of cyber *levée en masse* should indeed be re-conceptualized in light of cyber reality. Cyber domain, as a man-made virtual domain differs fundamentally from the conventional battlefields. In the end, if reconceptualization proves not feasible then the notion should be abolished.

*C. Non-International Armed Conflicts And
The Notion Of “Continuous Combat
Function”*

The International Committee of the Red Cross in its Interpretive Guidance on the Notion of Direct Participation in Hostilities (“Guidance”) developed the notion of “continuous combat function” in order to define the armed forces of non-state parties to a non-international armed conflict. For the purposes of the Guidance, armed forces of non-state parties are termed “organized armed groups,” whereas the Additional Protocol II uses the terms “dissident armed forces” and “other organized armed groups.”¹⁷⁵ As the concept of combatant does not legally exist in non-international armed conflicts, there is no such status for individuals taking direct part in hostilities on behalf of non-state parties to the conflict. Under the legal framework regulating non-international armed conflict, civilians are *prima facie* immune from attack, unless and for such times as

¹⁷⁴ See for a detailed analysis in favor of the abolishment of the provision, Brown, *supra* note 158, at 190. See also David Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 17 J. CONFLICT AND SEC. L. 293 (2012).

¹⁷⁵ ICRC Interpretive Guidance, *supra* note 115, at 20.

they direct participate in hostilities.¹⁷⁶ The categories of civilians, state armed forces and organized groups are mutually exclusive.¹⁷⁷ Lacking a definition of individuals taking direct part in hostilities on behalf of a non-state party, the ICRC uses the notion of continuous combat function to define the armed forces of a non-state party to a conflict on a membership of strictly functional sense and in terms of conduct.¹⁷⁸ Similar to the definition of combatant in the Hague Regulations,¹⁷⁹ members of organized armed groups are those who assume a continuous combat function by taking a direct part in hostilities.¹⁸⁰ Individuals who indirectly participate in hostilities, such as those accompanying or supporting an organized armed group, are not members of the group under the connotation of international humanitarian law and thus remain civilians.¹⁸¹ In practice, the application of the principle of distinction depends each time on reasonably available information.¹⁸² Thus, the

¹⁷⁶ Protocol Additional to the Geneva Conventions of 12th August 1949, and relating to the Protections of Victims of International Armed Conflicts (Protocol II), art. 13 (1977), *available at*

<https://www.icrc.org/ihl/INTRO/475?OpenDocument> [hereinafter Additional Protocol II].

¹⁷⁷ ICRC Interpretive Guidance, *supra* note 115, at 28. The legal framework regulating non-international armed conflict is art. 3 of Geneva Conventions I-IV, as well as Additional Protocol II.

¹⁷⁸ ICRC Interpretive Guidance, *supra* note 115, at 33.

¹⁷⁹ “Who does combat is a combatant.” Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land art. 3 (1907).

¹⁸⁰ ICRC Interpretive Guidance, *supra* note 115, at 33.

¹⁸¹ *Id.* at 34.

¹⁸² *Id.* at 35.

Guidance provides useful indicators of a “continuous combat function” expression such as the carrying of uniforms, distinctive signs or certain weapons and in some other cases on the basis of conclusive behavior.¹⁸³ Conclusive behavior according to the Guidance is such behavior that the individual conducts in support of hostilities in a continuous faction rather than in a spontaneous, sporadic and temporary one. Individuals assuming a continuous combat function are legitimate military objectives and therefore targetable for as long as the combat function lasts. Disengagement from the group by declaration or conclusive behavior and re-integration into civilian life excludes those individuals from the definition of military objectives.¹⁸⁴

The issue in question is whether and how the notion of continuous combat function applies to individuals conducting cyber operations on behalf of an organized armed group and what issues in particular arise from such application given the *sui generis* nature of cyber domain. Obviously, external distinctive indicators such as “uniforms” and “arms” will not suffice for the assumption of continuous combat function like they do in traditional warfare. Cyber operations are remotely and anonymously authorized via civilian IP addresses and cyber warriors are unlikely to wear uniforms as in most cases they are not incorporated in to the states’ armed forces. Closer to the nature of cyber operations would be an assumption of a continuous combat function based on conclusive behavior, i.e. individual membership in an organized armed group that collectively conducts cyber attacks against the

¹⁸³ *Id.* at 35.

¹⁸⁴ *Id.* at 34.

state. As combat function equals to direct participation in hostilities on behalf of the group, cyber operations for strategic intelligence and propaganda are excluded from the notion.¹⁸⁵ However, cyber operations that form an integral preparatory part of a cyber attack such as cyber espionage for target acquisition are clearly considered a continuous combat function.¹⁸⁶ It should be stressed that cyber espionage other than target acquisition, i.e. for strategic intelligence is ruled out from the notion of combat function according to the Guidance on the grounds that it is does not qualify for direct participation in hostilities in the first place.¹⁸⁷

Assessing the notion from the angle of the distinction principle, in practice it is not always easy to distinguish between civilians, individuals taking direct part in hostilities as part of their continuous combat function and civilians taking direct part in hostilities out of personal will. The temporal scope of the notion has been criticized as favoring the individual members of organized armed groups who qualify as military objectives only for as long as their combat function lasts, in contrast to members of state armed forces that are targetable at all times.¹⁸⁸ In the cyber context, the notion of continuous combat function remains under-developed and conclusions are to be made only without prejudice to further clarification in the context of cyber operations by future scholarship or state practice.

¹⁸⁵ *Id.* at 34, 35.

¹⁸⁶ Roscini, *supra* note 25, at 201.

¹⁸⁷ ICRC Interpretive Guidance, *supra* note 115, at 35.

¹⁸⁸ *Id.* at 202.

D. Civilians Taking Direct Part In Cyber Hostilities

One of the main purposes of international humanitarian law is the protection of civilians and this is primarily served through the principle of distinction. Civilians are generally immune from attack “[u]nless and for such time as they take direct part in hostilities.”¹⁸⁹ In other words, civilians taking direct part in hostilities are legitimate targets of attack for as long as their direct participation lasts. Questions regarding who is considered to be a civilian directly participating in hostilities have assumed increased importance in the cyber context due to the paramount involvement of civilians in cyber warfare. The majority of cyber operations are outsourced to civilian cyber experts. This is because cyber operations require specialized knowledge and technical expertise that military personnel typically do not possess and the tools required are not part of the standard inventory of the armed forces of all states.¹⁹⁰ Moreover, training the military forces on conducting cyber operations is simply not cost effective.¹⁹¹ With an exception of cyber units incorporated to the regular armed forces such as the USCYBERCOM, in most cases civilians are those who are responsible for the conduct of cyber attacks.

¹⁸⁹ Additional Protocol I, *supra* note 7, at art. 51 (3).

¹⁹⁰ Michael N. Schmitt, *Direct Participation in Hostilities and 21st Century Armed Conflict*, in CRISIS MANAGEMENT AND HUMANITARIAN PROTECTION: Festschrift für Dieter Fleck 505, 527 (Fischer et al. eds., BWV 2004), available at http://www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/schmitt_direct_participation_in_hostilities.pdf [hereinafter Schmitt, *Direct Participation*].

¹⁹¹ *Id.*

Bizarre as it might be, treaty international humanitarian law does not include a definition of what conduct does amount to “direct participation in hostilities.”¹⁹² The Commentary of Additional Protocol I does not offer much on the interpretation of the notion either.¹⁹³ In order to fill in this gap, the International Committee of the Red Cross (“ICRC”) issued an Interpretive Guidance on the Notion of Direct Participation in Hostilities, following a series of experts’ consultations, in which important guidelines are offered with regard to both international and non-international armed conflicts. The notion’s deconstruction and re-interpretation in the context of cyber operations is seminal for the application of the principle of distinction. For the purposes of the deconstruction and assessment of the notion of direct participation in hostilities to cyber operations, the classification of conflict is irrelevant as both Additional Protocols use the same concept of direct participation.¹⁹⁴ Hence, everything said in this part is equally applicable to both international and non-international armed conflicts.¹⁹⁵ Furthermore, the provision of Article 51 (3) reflects customary law according to the ICRC Customary International Humanitarian Law Study as well as according to the Israeli Supreme Court.¹⁹⁶ For the illustration of this

¹⁹² ICRC Interpretive Guidance, *supra* note 115, at 41.

¹⁹³ The Protocol’s Commentary on Article 51 (3) rather limits the notion of direct participation in hostilities as “acts of war which by nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces.” ICRC Commentary of Additional Protocols, *supra* note 12, at para. 1944.

¹⁹⁴ Additional Protocol I, *supra* note 7, at art. 51 (3); Additional Protocol II, *supra* note 177, at art. 13 (3).

¹⁹⁵ ICRC Interpretive Guidance, *supra* note 115, at 44.

¹⁹⁶ ICRC Customary International Humanitarian Law Rules,

rather obscure notion, the ICRC Guidance is used as a starting point. The first element of the concept is that of “hostilities.” The Guidance restricts the element of “hostilities” to specific hostile acts.¹⁹⁷ On the second element, “direct participation,” the Guidance identified three constitutive elements that have to be cumulatively met: (1) threshold of harm; (2) direct causation; and (3) belligerent nexus.

1. Threshold of Harm

The notion of harm according to the ICRC Guidance consists of “a specific act that is 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.”¹⁹⁸ The objective likelihood of harm suffices and is not necessary for the harm to be materialized as long as it is reasonably expected to result under the circumstances ruling at the time.¹⁹⁹ Conducting computer network attacks (“CNA”), computer network exploitation (“CNE”) as well as the transmission of tactical targeting intelligence satisfies the required threshold of harm, according to the Guidance, as it adversely affects the enemy’s military operations or military capacity.²⁰⁰ However, absent any physical consequences arising from the targeting of protected persons and objects, the

supra note 9, at 19, 20; HCJ 769/02 The Public Committee Against Torture in Israel v. Government of Israel para. 30 (2006).

¹⁹⁷ ICRC Interpretive Guidance, *supra* note 115, at 45.

¹⁹⁸ *Id.* at 47.

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 48.

Guidance disqualifies acts such as the interruption of electricity, water, food supplies, or the manipulation of computer networks from the required degree of harm, despite the serious impact upon the public health, security or commerce.²⁰¹ This position seen from the angle of cyber operations seems to contradict the previous position of the ICRC regarding the key threshold of attack as defined in Article 49 and thoroughly addressed in the first chapter of this study. A cyber attack directed against vital civilian cyber infrastructure, i.e. water supply networks, and aimed at their neutralization that resulted in serious malfunction of the computer networks, risking thus the civilian population's public health, would satisfy the required degree of harm, as materialization of the harm is not necessary and, provided the elements of "direct causation" and "belligerent nexus" are additionally satisfied, a civilian conducting the cyber operation would lose his protection under the law. This less restrictive approach on the notion of harm is more consonant to the *sui generis* interconnectivity of civilian and military infrastructure as it takes into account the cyber-centric character of modern societies where incapacitation of civilian infrastructure with no physical consequences may still cause a considerable degree of harm to civilian population.²⁰²

²⁰¹ *Id.*

²⁰² Nils Melzer, *Cyber Warfare and International Law* 28-29 (2011), available at <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>. It should be stressed however, that Melzer's view qualifying as harm the mere inconvenience or harassment of civilian population arbitrarily expands the notion of harm. See also John Ricou Heaton, *Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces*, 57 A.F. L. REV. 201 (2005). Heaton expands the

2. Direct Causation

The element of “direct causation” is satisfied when the occurrence of the harm in question is brought about “within one casual step.”²⁰³ There has to be a direct casual link between the act and the resulting harm, namely “the harm in question should be the result of that specific act or from a coordinated military operation of which that act constitutes an integral part.”²⁰⁴ Hence, indirect harm is excluded from the notion of direct participation in hostilities.

However, the direct causal link does not have to be connected through an uninterrupted casual chain of events.²⁰⁵ On the contrary, even if the chain of events is interrupted, the direct link between the act and its consequences might still be sufficient.²⁰⁶ This is key to the application of the “direct causation” requirement to cyber operations where the desired and important effects of cyber attacks are often secondary.²⁰⁷ The stage of planning cyber operations always includes chains of causality; for example, if the planner does X, Y happens, and if Y happens, it causes Z to happen, which in turn causes A to happen.²⁰⁸ These causal links vary from computer actions and results to human perceptions or reactions and the combination thereof will result to the anticipated outcome.²⁰⁹

notion of harm to damage of crucial information installed in computer networks.

²⁰³ ICRC Interpretive Guidance, *supra* note 115, at 53.

²⁰⁴ *Id.* at 51.

²⁰⁵ *Id.* at 54.

²⁰⁶ *Id.* at 54.

²⁰⁷ Turns, *supra* note 175, at 288.

²⁰⁸ *Id.*

²⁰⁹ *Id.*

However, the Guidance applies the notion of “direct causation” exclusively to the primary consequences and explicitly indicates that indirect effects do not suffice, as the resulting harm must be objectively likely.²¹⁰ Consequently, a cyber attack is unlikely to ever meet the “direct causation” requirement for the notion of direct participation in hostilities, since the crucial effects of cyber attacks often occur over several causal steps.²¹¹ Accepting this approach, however, leads to a rather unfair conclusion that all civilians who engage in cyber attacks with secondary or tertiary harmful effects retain their civilian status and their immunity against direct attack. In terms of proximity to the battlefield and the element of direct causation, civilians who remotely execute cyber operations are directly participating in hostilities, as geographical proximity is irrelevant to the causal proximity, which the element of direct causation refers to.²¹² Examples where direct causation is absent are activities such as the training and recruitment of hackers or civilians providing technical maintenance to the information systems. This is because the link between the harm to be resulted from the harm and the civilians’ contribution remains indirect.²¹³ Nevertheless, when people are specifically recruited and trained for the execution of a predetermined act, then training and recruitment activities constitute integral part of this act and therefore equal to direct participation in hostilities.²¹⁴ Regarding the malware developers and designers, the Guidance considers civilian scientists

²¹⁰ ICRC Interpretive Guidance, *supra* note 115, at 53, 54.

²¹¹ Turns, *supra* note 175, at 288.

²¹² ICRC Interpretive Guidance, *supra* note 115, at 55.

²¹³ *Id.* at 53.

²¹⁴ *Id.*

and weapon experts generally protected from attack with the exemption of civilian expertise of very exceptional and potentially decisive value for the outcome of the armed conflict.²¹⁵ To reinforce this argument, the example given during the experts meetings was the case of nuclear weapons experts of the Second World War.²¹⁶

Applying this in the cyber context, malware designers and developers possess and exclusively provide the exceptional expertise needed for the harm to occur, being thus the *condicio sine qua non* of the outcome. Therefore, under this exception civilian expertise of very exceptional and potentially decisive value for the outcome the contribution of malware designers equals to direct participation in hostilities, even though the required harm might occur further down the chain of events when the malicious program finally activates. Hence, malware designers lose their protection against direct attack due to their direct participation in hostilities. Pursuant to the Guidance, the interruption of the causality by intermediary events does not deprive the direct causation between the act and the harm.²¹⁷ Thus under this approach, the act of writing a malicious program can qualify as directly causing harm despite the separation in time between the act and the harm caused. Additionally, the design of particular malicious software to be used against the adversary might also be considered a preparatory measure of a certain attack and as such constitute an integral part of it.²¹⁸

²¹⁵ *Id.*

²¹⁶ *Id.*

²¹⁷ *Id.* at 54.

²¹⁸ *Id.* at 66.

Civilians who engage in cyber operations can be seen as falling into three main categories: those who write or design the malicious programs (programmers, cyber scientists, already addressed above); those who actually operate the computer programs in a cyber warfare scenario (operators); and those who act as service administrators and provide technical assistance and maintenance (webmasters).²¹⁹ The second category includes those who actually operate the systems. If operation is understood as execution of an attack, then the answer is relatively clear. The civilian, executor of a cyber attack who enters the necessary set of commands loses his protection against direct attack as he satisfies all three requirements.²²⁰ Treatment of the last category of webmasters or service operators remains to be seen. Perhaps they could qualify for the civilian personnel accompanying the armed forces, being thus immune from attack “[u]nless they are used to commit, outside their humanitarian function, acts harmful to the enemy.”²²¹

Moreover, the direct causation is satisfied also when a specific act does not on its own reach the required threshold of harm but constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm.²²² Applied to the cyber context collective cyber operations qualifying for direct participation in hostilities would include “the marking and identification of targets,” “the analysis and transmission of tactical intelligence to attacking forces,” and “the instructions or assistance

²¹⁹ Turns, *supra* note 175, at 289.

²²⁰ *Id.* at 295.

²²¹ Additional Protocol I, *supra* note 7, at art. 13 (1).

²²² ICRC Interpretive Guidance, *supra* note 115, at 55.

given to troops for the execution of a specific military (cyber) operation.”²²³

In summary, the requirement of direct causation applied to the cyber context raises issues of concern in particular regarding the secondary, also known as “knock on,” effects of cyber attacks and their often “indirect” causality with respect to the resulting harm.

3. Belligerent Nexus

The “belligerent nexus” requirement refers to the objective purpose of a specific act, the objective intent for which it is specifically designed. In particular the act should be closely linked to the hostilities and should aim to “[d]irectly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.”²²⁴ The notion of objective purpose should be distinguished from subjective intent, hostile intent or the state of mind of a person such as the *mens rea* requirement in criminal law.²²⁵ It is the element of the purpose of the act that must be objectively designed to directly cause harm. Hence, civilians forced to directly participate in hostilities still lose their protection against direct attack.²²⁶ An exemption to the loss of immunity is when civilians are unaware of their role in direct participation in hostilities for they are instrumentalized by a belligerent party in a military operation.²²⁷ In this context, they remain civilians under the law of targeting. In the cyber context, such

²²³ *Id.* at 55.

²²⁴ *Id.* at 58.

²²⁵ *Id.* at 59.

²²⁶ *Id.* at 60.

²²⁷ *Id.*

a scenario occurs when a robot network, mainly known as “botnet” is specifically designed to mount distributed denial of service attacks (“DDos”) via hijacked civilian computers that might result in violent physical consequences and cause harm.²²⁸ The civilians, owners of the computers, are completely unaware of the botnets and their purpose of attack. Consequently, as they lack any manifestation of act, they retain their civilian status under the law of targeting and any attack directed against them shall be taken into account in the proportionality assessment.²²⁹

All in all, there is no exhaustive list of examples of direct participation in cyber hostilities by civilians. The deconstruction of the notion provides some illustrative examples but not an exhaustive list. All three requirements applied together in conjunction constitute a relatively high threshold for the notion of direct participation in hostilities in the cyber context.²³⁰ Absent international jurisprudence on the matter, clarification of the concept is left upon academic scholarship and future state practice.

4. The Temporal Framework of Direct Participation in Hostilities; “For Such Time As”

Civilians are generally immune from attack unless and for such time as they directly participate in hostilities. The use of the word “unless” introduces an exception to the general immunity accorded to civilian population in times when the latter conducts

²²⁸ Roscini, *supra* note 25, at 210.

²²⁹ Roscini, *supra* note 25, at 211.

²³⁰ Turns, *supra* note 175, at 296.

hostile acts against the adversary that directly cause military harm or harm against other protected objects or persons. The loss of protection against direct attack is temporal and lasts from the beginning until the end of participation. Moreover, preparatory acts to the execution of a specific act as well as the timeframe between the deployment to and return from the execution constitute an integral part of that act and therefore fall under the scope of “such time as.”²³¹ In order for preparatory measures to constitute an integral part of a specific hostile act there is no need for geographical or temporal proximity to the execution of that act.²³² Consequently, neither intervals between the preparatory measure and the execution of the attack nor great geographical distance deprive the preparatory measure of its “direct participation” character.

The Guidance explicitly refers to computer network attacks in the context of remotely authorized attacks and restricts the duration of direct participation in hostilities to the “immediate execution of the act and preparatory measures forming an integral part of that act.”²³³ With regards to the “execution” of cyber attacks with long-delayed effects such as logic bombs, questions arise on the duration of the “execution” stage. The Tallinn Experts took the position that the duration period would run from commencement planning on how to emplace the logic bomb through activation upon command by that individual.²³⁴ Hence, the duration starts upon emplacement and finishes upon activation through command by that individual

²³¹ ICRC Interpretive Guidance, *supra* note 115, at 66.

²³² *Id.*

²³³ *Id.* at 68.

²³⁴ Tallinn Manual, *supra* note 19, at Rule 35 para. 8.

regardless the time of the effects or damage occurrence.²³⁵ Activation may potentially occur upon lapse of a predetermined period or upon the performance of a particular action by the target system.²³⁶ A more restrictive approach should be preferred focusing on the specific act as such and not on its subsequent effects. This stricter approach on the temporal framework of direct participation to cyber operations is preferable for two reasons. First, a civilian who is responsible for the installation of a malware that is due to activate in the next couple of months is no longer posing any military threat by the time of the malware's activation.²³⁷ An opposite view is inconsistent with the law, as it treats the civilian as a military objective targetable at all times, even when he completely detaches or disengages himself from the hostilities and punishes him for crimes committed in the past.²³⁸ Critics have argued that the temporal suspension of protection allows the civilian to engage in repeated hostilities with relative immunity creating a "revolving door" trend.²³⁹ On the other hand, the launching of a cyber operation may only last for a couple of minutes or even seconds and as there is no deployment concept due to the remote execution character of cyber operations.²⁴⁰ Considering these issues, Schmitt suggests on

²³⁵ Roscini, *supra* note 25, at 209.

²³⁶ *Id.*

²³⁷ ICRC Interpretive Guidance, *supra* note 115, at 70.

²³⁸ This view was also supported by Judge Barak in the judgment on targeted killings. See HCJ 769/02 Public Committee Against Torture in Israel v. Government of Israel para. 39 (2006), *available at* http://elyon1.court.gov.il/Files_ENG/02/690/007/A34/02007690.A34.pdf.

²³⁹ Schmitt, *Key Issues*, *supra* note 14, at 102.

²⁴⁰ *Id.*

repeated cyber operations “[t]he only reasonable interpretation of ‘for such time as’ is that it encompasses the entire period during the cyber participant engaging in repeated cyber operations.”²⁴¹ However, this view opposes the Guidance interpretation that treats each act separately in terms of the notion’s analysis.²⁴² As for whether a specific preparatory measure forms an integral part of a specific act or not, an answer should be given on a case-by-case basis.

In broad strokes, a definite answer for the issue of the “for such time as” requirement does not seem to exist in abstract terms and is dependent on a multitude of constantly changing situational factors that must be treated with the utmost care.²⁴³ Target acquisition cyber operations are accepted as forming an integral part of specific cyber attacks provided that the same person who conducted the target acquisition operations conducts also the cyber attacks, engaging in this way in repeated cyber operations.²⁴⁴ If his participation is solely limited to the preparatory measure of target acquisition, as soon as he completes the act, he is no longer targetable for direct attack. The issue here is that there will be individuals in future cyber conflicts who will participate only at a preparatory stage of an attack and whose targeting will be impossible, unless they are attacked when engaging in the preparatory cyber operation to an attack.²⁴⁵

²⁴¹ *Id.*

²⁴² ICRC Interpretive Guidance, *supra* note 115, at 45.

²⁴³ *Id.* at 68.

²⁴⁴ *Id.* at 66.

²⁴⁵ *Id.* at 65.

Summing up, the notion of direct participation in hostilities applied in the cyber context brings about issues of great importance. The deconstruction of the notion and the analysis of its components calls, at least for now, for a more restrictive, even conservative, application of the notion to cyber operations. The three constitutive elements applied in conjunction, as well as the temporal loss of protection, are met with considerable disagreement. Grey cases lie between the extremes and should be interpreted liberally in favor of finding direct participation in hostilities and protect the individual.²⁴⁶ It is submitted that final decisions on the status of civilians directly participating in cyber hostilities shall be made with utmost care, having taken all feasible precautions and in case of doubt, an attack shall be suspended or cancelled complying with the Protocol's humanitarian concerns.²⁴⁷

V. CONCLUDING REMARKS

Upholding the distinction principle certainly becomes more challenging in cyber warfare than in other types of warfare. As there is complete lack of international jurisprudence on cyber warfare, all conclusions on the applicability of the distinction principle to cyber operations are restricted to academic scholarship, speculation and embryonic state practice. Against this background, this analysis has so far illustrated the issues to be further considered and reassessed in the context of cyber warfare. There is a need for general

²⁴⁶ Schmitt, *Direct Participation*, supra note 191, at 509.

²⁴⁷ Additional Protocol I, supra note 7, at art. 57 (2).

reconceptualization of the principle of distinction in the cyber context. Reconceptualization can be achieved through interpretation in light of the object and purpose of the humanitarian treaties as well as in light of the new cyber reality. Regarding the key threshold of attack under the *jus in bello*, consideration should be given as to how below-threshold cyber operations are to be addressed. It should be stressed that reinterpreting the existing notions in light of warfare's reality does not render the existing law insufficient. On the contrary reinterpretation under the *lex lata* will prevent the provisions from becoming obsolete. Furthermore the dual use *sui generis* nature of cyber targets due to the systematic interconnectivity of civilian and military infrastructure, the resilience of cyber domain and the reconceptualization of the notion of objects so as to address digital data are issues unsettled under the law. Any concrete conclusion on the status of an object should be made following a careful assessment. The same applies with regard to individuals' classification under the law of targeting where the distinction principle is met with even more uncertainty. With regard to the classification of individuals, the requirements for the definition of cyber combatants need to be further reassessed, whereas it remains to be seen whether the concept of cyber *levée en masse* is still a workable notion in terms of law. In addition, the notions of "continuous combat function" and "direct participation in cyber hostilities" need further development.

At least for now, it is too early to put forward efforts for a new treaty body by advocating in favor of *lex ferenda*. *Lex lata* provides the basic regulation on targeting in the cyber domain. State practice and international jurisprudence should first take the lead

on interpretation of the existing legal framework and assess whether the humanitarian concerns served by it are satisfied or undermined in the interconnected domain of cyber space. Alternatively by introducing new laws every time a new type of warfare emerges, we run the risk of always remaining one war behind.