International Institute of Humanitarian Law

International Institute of Humanitarian Law
Institut International de Droit Humanitaire
Istituto Internazionale di Diritto Umanitario

Weapons and the International Rule of Law

STUDI

Politica

FrancoAngeli

International Institute of Humanitarian Law
Institut International de Droit Humanitaire
Istituto Internazionale di Diritto Umanitario

Weapons and the International Rule of Law

39th Round Table on Current Issues
of International Humanitarian Law
(Sanremo, 8th-10th September 2016)

Editor Baldwin De Vidts

Associated Editor Gian Luca Beruto

FrancoAngeli

Dr. Baldwin De Vidts has served in various legal functions within FPS Foreign Affairs of Belgium and SHAPE, acting also as the Legal Adviser to the Secretary General of the North Atlantic Treaty Organization.

Mr. Gian Luca Beruto holds a Master's degree in International Political Science and is currently Assistant to the Secretary-General of the International Institute of Humanitarian Law.

The International Institute of Humanitarian Law would like to thank
Ms Shirley Morren, librarian of the Institute, and Mr. Marco Basile,
who were both involved in the painstaking task of proofreading and editing.

Stampa: Geca Industrie Grafiche, Via Monferrato 54, 20098 San Giuliano Milanese.

Table of Contents

Weapons and the International Rule of Law

The 39th Round Table on current issues of International Humanitarian Law (IHL), held in Sanremo, gathered together international experts, representatives of governments and international organizations, academics and military officers to engage in open and fruitful discussions on the complex issues of weapons and international rule of law.

The Round Table provided an important opportunity to address the crucial topic of the protection of civilians which, now more than ever, constitutes a critical and delicate issue in today's international and non-international armed conflicts.

Non-state actors, urban warfare, weapons smuggling and autonomous armaments are some of the issues currently at stake. Considering the multiple transformations characterising the contemporary international scenario, it is an extremely difficult task for all the actors to implement IHL in this specific area.

The proceedings of this Round Table, in line with the Sanremo Institute's tradition, aim to further develop and contribute to the ongoing debate on these issues.

The **International Institute of Humanitarian Law** is an independent, non-profit humanitarian organization founded in 1970. Its headquarters are situated in Villa Ormond, Sanremo (Italy). Its main objective is the promotion and dissemination of international humanitarian law, human rights, refugee law and migration law. Thanks to its longstanding experience and its internationally acknowledged academic standards, the International Institute of Humanitarian Law is considered to be a centre of excellence and has developed close co-operation with the most important international organizations.

FrancoAngeli
La passione per le conoscenze

€ 33,00 (u)

ISBN 978-88-917-5342-7

To what degree do the difficulties in tracing the author of the attack and assessing the extent of the effects remain a challenge for addressing the legal issues raised by "cyber-weapons"?

Marco ROSCINI
Professor of International Law, University of Westminster, London

As the US Department of Defense has noted, there is no internationally agreed definition of what a 'cyber weapon' is.[1] There is agreement, however, that at least certain cyber capabilities can constitute a weapon. Certain states have expressly qualified cyber capabilities as weapons and many also have active operational cyber weapons development programs in place.[2] In April 2013, for instance, the US Air Force upgraded six cyber capabilities to 'weapon' status,[3] and the new US Law of War Manual expressly provides for a legal review of weapons that employ cyber capabilities, although it cautions that not all cyber capabilities are necessarily weapons or weapon systems.[4]

For the purposes of this paper, I will consider cyber capabilities as weapons when they are designed, intended or used to cause injury or damage to an adverse party in an armed conflict.[5] Cyber weapons include a

[1] US Department of Defense, 'Cyberspace Policy Report', November 2011, p. 2.

[2] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), p. 170.

[3] Andrea Shalal-Esa, 'Six U.S. Air Force cyber capabilities designated "weapons"', Reuters, 8 April 2013, www.reuters.com/article/net-us-cyber-airforce-weapons-idUSBRE93801B20130409.

[4] US Department of Defense, Law of War Manual, June 2015, p. 1008. See also US Air Force Instruction 51-402, as updated in July 2011, which requires a legal review of cyber capabilities used in cyber operations. The review includes establishing at a minimum: '3.1.1. Whether there is a specific rule of law, whether by treaty obligation of the United States or accepted by the United States as customary international law, prohibiting or restricting the use of the weapon or cyber capability in question. 3.1.2. If there is no express prohibition, the following questions are considered: 3.1.2.1. Whether the weapon or cyber capability is calculated to cause superfluous injury, in violation of Article 23(e) of the Annex to Hague Convention IV; and 3.1.2.2. Whether the weapon or cyber capability is capable of being directed against a specific military objective and, if not, is of a nature to cause an effect on military objectives and civilians or civilian objects without distinction' ('Legal Reviews of Weapons and Cyber Capabilities', US Air Force Instruction 51-402, 27 July 2011, p. 3 http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf).

[5] See William H. Boothby, 'Methods and Means of Cyber Warfare', 89 *International Law Studies* (2013), p. 390.

delivery system, a navigation system and a payload.[6] The delivery system could go from e-mails to malicious links in websites, hacking, counterfeit hardware and software. System vulnerabilities are the main navigation systems that provide entry points for the payload by enabling unauthorized access to the system. The payload is the component that causes damage: if the code, however sophisticated, is designed solely for the purpose of infiltrating a computer and stealing information, as in the cases of Duqu and Flame, it would not be a 'weapon', as it is neither intended nor capable of causing damage.[7]

The problems with attributing the use of cyber weapons are proverbial. Anonymity is in fact one of the greatest advantages of cyberspace. This has important consequences for the application of the law of armed conflict. If we cannot identify and attribute the cyber attacks with sufficient certainty to states, for instance, we will not be able to apply the law of *international* armed conflict to them. A belligerent may also be encouraged to use cyber weapons in a way not consistent with the law of armed conflict because there is a good chance that it will be able to hide under the invisibility cloak of plausible deniability.

Two situations must be distinguished: the *identification* of the source of the attack, which is essentially a technical matter, and the *attribution* of the attack to a state or non-state actor, which is a legal exercise. The two situations are different and should not be confused. The identification problem is not unique to cyberspace, it is only more difficult. An IP address identifies the origin and the destination of the data: with the cooperation of the Internet Service Provider (ISP) through which the system corresponding to the IP address is connected to the internet, it could be associated with a person, group or state. The IP address, however, can be 'spoofed', or the corresponding computer system could only be a 'stepping stone' for an attacker located elsewhere.[8] Hiding behind botnets (i.e. hijacked computers) is also a good way of anonymizing cyber operations.

If the assumption is that the origin of cyber attacks can never be identified, the law of armed conflict (and any other international law) clearly becomes very difficult to apply. But the case for identification is not as hopeless as is too frequently described: sufficient evidence can be found

---

[6] Fred Schreier, 'On Cyber Warfare', DCAF Horizon 2015 Working Paper no. 7, pp. 66-67, www.dcaf.ch/Publications/On-Cyberwarfare.

[7] Thomas Rid and Peter McBurney, 'Cyber-Weapons', *RUSI Journal* 157 (February/March 2012), p. 11.

[8] Scott J. Shackelford and Richard B. Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', 42 *Georgetown Journal of International Law* (2011), p. 982.

thanks to technical means, e.g. traceback tools, together with information from other sources, such as human sources and communications intercepts.[9] Furthermore, as has been observed, 'international law does not require States to be correct; it only requires them to be reasonable when arriving at, and acting on, their conclusions'.[10] Further developments in computer technology and internet regulations are also likely to make identification easier in the future.[11] I should caution that advocating for reducing or removing anonymity in cyberspace, and on the internet in particular, is a double-edged sword: it would lead to identifying not only the authors of malicious cyber attacks, but also, say, pro-democratic hacktivists who use social media to protest against autocratic regimes.

Assuming that the authors of a cyber operation are eventually identified, the problem arises as to whether their conduct can be attributed to a state under the law of state responsibility: it is one thing to say that the hack came from IPs in Russia and another is to say that Russia is responsible for it. As already noted, if identification is essentially a technical matter, attribution is a legal exercise. Although it is not entirely implausible that a special regime of international responsibility could develop as a consequence of the peculiar features of cyber operations, in the present lack of any indications in that sense such conclusion would certainly be premature.[12] The applicable rules are, therefore, those contained in Chapter II of Part One of the 2001 International Law Commission (ILC)'s Articles on the Responsibility of States for Internationally Wrongful Acts, which substantially reflect customary international law. I cannot see any insurmountable problems with applying these rules in cyberspace that require the rethinking of these rules. With cyber weapons, the real problem

---

[9] Michael Schmitt, 'Normative Voids and Asymmetry in Cyberspace', *Just Security*, 29 December 2014, www.justsecurity.org/18685/normative-voids-asymmetry-cyberspace/; William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: The National Academies Press, 2009), pp. 138-141.

[10] Schmitt. 'Normative Voids'.

[11] In a previous Round Table, Nils Melzer observed that, 'in the early days of air warfare, hostile airplanes could be detected only once they were near enough to be visible and audible. But then the radar was invented and solved the problem – until the stealth fighter came along' (Nils Melzer, 'Towards a Code of Conduct for Cyber Space', in Wolff Heintschel von Heinegg (ed.), *International Humanitarian Law and New Weapons Technologies* (Milano: FrancoAngeli, 2012), p. 172).

[12] Article 55 of the ILC Articles provides that '[t]hese articles do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a State are governed by special rules of international law'. Read the text of the Articles in *Yearbook of the International Law Commission*, 2001, vol. II, Part Two, pp. 26-30.

is one of finding sufficient evidence, not of changing and even less lowering, the standards of attribution under the law of state responsibility. As the ICJ in the *Nicaragua* Judgment highlighted well before the advent of cyber technologies, 'the problem is not… the legal process of imputing the act to a particular State… but the prior process of tracing material proof of the identity of the perpetrator.'[13]

There are increasing calls to deal with this cyber attribution problem by making a state responsible for all cyber attacks that emerge from within its borders, even if the attacks are not sponsored by that state. This view is inconsistent with the current law of state responsibility: the ILC Articles on state responsibility provide that a state is responsible for the conduct of individuals or groups that are not organs only when they are 'in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct' (Article 8). At least one commentator has suggested that, due to the inherently clandestine nature of cyber activities and the technical difficulty of identifying the authors, the looser *Tadić* test should be preferred to the *Nicaragua* test to attribute the use of cyber weapons under the law of state responsibility.[14] This view is untenable: indeed, it is exactly because of the identification problems characterizing cyber weapons and the potential for a false flag that the 'effective control' test is preferable, as it would prevent states from being frivolously or maliciously accused of cyber operations. Clear support for the application of the effective control test to cyber operations can be found in the speech given by the then US State Department's Legal Advisor, Harold Koh, at the US CYBERCOM in 2012, where he claims that states are internationally responsible for cyber acts undertaken through 'proxy actors' when they 'act on the State's instructions or under its direction or control.'[15] Azerbaijan also denounced cyber attacks conducted by a group of hackers called the 'Armenian Cyber Army' under the 'direction and control' of Armenia.[16]

Let us now move to the problem of assessing the effects of cyber weapons. First, while it is true that cyber weapons can produce effects practically immediately, operationally they are much slower: targets need to be identified, access to the target system needs to be gained and

---

[13] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, Judgment, 27 June 1986, ICJ Reports 1986, para. 57.

[14] Scott J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27 *Berkeley Journal of International Law* (2009), p. 235.

[15] CarrieLyn D Guymon (ed.), *Digest of United States Practice in International Law*, 2012, p. 596.

[16] Letter dated 6 September 2012 from the Chargé d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, 7 September 2012, UN Doc A/66/897–S/2012/687, p. 1.

vulnerabilities identified, the payload has to be developed and deployed.[17] The belligerents, then, have plenty of opportunities to assess the possible effects, consult a military lawyer and consider the legality of the operation. In fact, it is believed that several planned cyber attacks (like those by NATO on Serbia's air defences and by the United States on Libya's air defence system) were cancelled because of the concerns about their collateral effects.[18] Speed of effects, then, could hamper retaliation, but does not necessarily prevent compliance with the law of armed conflict by the attacker.

It has also been said that, because malware may spread uncontrollably, its effects are difficult to assess and, therefore, cyber weapons are by definition inconsistent with the principle of distinction. But this is not necessarily true. It all depends on how the malware is designed and on the characteristics of the targeted system. Malware can be designed to spread indiscriminately: for instance, malware that disrupts the air traffic control system may not be able to distinguish between civilian and military aircraft. But malware could also be introduced into a closed military network,[19] or be written so as to negatively affect exclusively certain systems, as was the case of Stuxnet. The same considerations apply to the principle of proportionality: proportionate cyber attacks are possible if the software is written with this purpose in mind and the targeted system is sufficiently known. While Stuxnet was promiscuous, for instance, it made itself inert if the specific Siemens software used at Iran's Natanz uranium enrichment plant was not found on infected computers, and contained safeguards to prevent each infected computer from spreading the worm to more than three others, before self-destructing on 24 June 2012.[20] In addition, it caused no more than inconvenience to infected computers other than the Natanz operating system, as the worm did not self-replicate indefinitely so as to slow down computer functions.[21]

---

[17] Herbert S. Lin, 'The Technology of Offensive Cyber Operations', in *Technological Challenges to the Humanitarian Legal Framework*, 11th Bruges Colloquium, 21-22 October 2010, p. 38, www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf.

[18] Jeffrey T.G. Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', 106 *Michigan Law Review* (2007-08), pp. 1434-1435; Rid and McBurney, 'Cyber-Weapons', p. 6.

[19] Commentary to Rule 43, in *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), p. 146.

[20] Jeremy Richmond, 'Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?', 35 *Fordham International Law Journal* (2011-2012), p. 856.

[21] Richmond, 'Evolving Battlefields', p. 861.

Of course, targeteers will almost inevitably have to be assisted by cyber engineers when assessing the possible effects of cyber weapons and making decisions with regard to a cyber attack, unless they are trained cyber experts themselves.[22] Collecting information about the architecture of the attacked network (network mapping) or operating system (footprinting) through cyber exploitation or traditional intelligence gathering will be of decisive importance in this context, as the effects of a cyber weapon greatly depend on the characteristics of the targeted systems. It should also be recalled that the duty to take precautions in attack and against the effects of an attack extends to cyberspace.[23]

My conclusion is that the difficulties related to the attribution of the use of cyber weapons and their effects are not an impossible challenge for existing rules of the law of armed conflict. At the same time, I do not want to give the impression that I am downplaying the problems – that indeed exist – arising from the application in the cyber context of rules adopted well before the Information Age. These provisions need now to be re-interpreted in an evolutionary way so as to take into account the dependency of today's societies on computers, computer systems and networks. As recalled by the former President of the Israeli Supreme Court, Aharon Barak, in another context, 'new reality at times requires new interpretation. Rules developed against the background of a reality which has changed must take on a dynamic interpretation which adapts them, in the framework of accepted interpretational rules, to the new reality.'[24] The arguments in favour of evolutionary interpretation apply even more strongly to the law of armed conflict: the forward-looking character of this law is demonstrated by the inclusion in Additional Protocol I of Article 36 on the study, development, acquisition or adoption of a new weapon, means, or method of warfare, and of the Martens Clause. The debate on how the existing law of armed conflict applies in cyberspace, then, needs to continue.

---

[22] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), pp. 206-207.

[23] US Law of War Manual, p. 1006. See Roscini, *Cyber Operations*, pp. 232-239.

[24] *Public Committee Against Torture in Israel et al. v. The Government of Israel et al.*, Israel's Supreme Court, HCJ 769/02, 11 December 2005, para. 28 (Barak). Vice President Rivlin also stated that 'international law must adapt itself to the era in which we are living' (ibid., para. 2 (Rivlin)).