Applying the *ius in bello* in the cyber domain: Navigating between *lex lata* and *lex ferenda*

Emanuele Sommario[*]

In the 1983 movie *War Games*, the leading character is a young hacker who unwittingly accesses a United States military supercomputer programmed to predict the possible outcomes of nuclear war, and then proceeds to start his favourite game: *Global Thermonuclear War*. What we know, but the computer geek does not, is that the US military, hoping to eliminate the unpredictable 'human element' in the event of an actual war, has given the computer total control over the launching of nuclear warheads. The film describes the protagonist's race against time to reverse the computer's resolve to start World War III. What was considered science fiction some 30 years back – the possibility of being able to hack into a military computer system to start an armed conflict - has now become a realistic scenario.

The military use of cyberspace is not a hypothetical possibility anymore, but rather an existing fact. Several states have already included cyber warfare in their military doctrine and established specific units that are designed to engage in cyber hostilities. In a recent study by the United Nations Institute for Disarmament Research (UNIDIR), more than 30 states are described as having adopted specific measures to include cyber warfare in their military plans and structures.[1] Such a trend is surely destined to increase, as are the technological developments in

[*] Assistant Professor of International Law, Scuola Superiore Sant'Anna.

[1] See Center for Strategic and International Studies, 'Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization' (UNIDIR, 2011) available at: <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>.

the area of information technology and the reliance of states and private actors on computer networks. Cyberspace has effectively become a new domain, which offers huge benefits to everyone who is able to exploit it, but whose pervasive influence on our lives also turns it into a significant source of threats and vulnerabilities.

When such threats may degenerate into an armed conflict, the exercise for international lawyers becomes that of assessing whether the existing legal framework – developed at a time when the cyber domain did not yet exist and was presumably not even thought of – offers adequate rules to protect states and individuals from the menaces of cyber warfare.

This is the task that Marco Roscini takes on in his book *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014), where he surveys the laws governing the resort to force and the conduct of hostilities as they relate to computer network attacks (CNAs), with the aim 'to provide a systematic and coherent analysis of the international law applicable to military cyber operations'.[2] Given the pivotal importance the topic has assumed in contemporary legal debate, it comes as no surprise that a significant number of books and studies have already dealt with it.[3] This, on one hand, has prevented the author from breaking new ground on at least some of the matters covered in the book as they had already been explored in existing literature. On the other hand, Roscini makes excellent use of the wealth of scholarly material available, also reviewing contributions in languages other than

[2] M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP, 2014) 42.

[3] Important contributions include H Dinniss, *Cyber Warfare and the Laws of War* (CUP, 2012) and, more recently, Y Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (Brill, 2015). Also notable are the collections of essays edited by MN Schmitt in the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013) and by N Tsagourias and R Buchan in their recent *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015). The same two authors had already edited a special issue of the *Journal of Conflict and Security Law* (vol 19, 2012) entirely devoted to the application of *jus ad bellum/jus in bello* to cyber war. A special edition of the *Air Force Law Review* (vol 64, 2009) has also grappled with the same topic, as has the special issue of the *Israel Yearbook on Human Rights* (vol 43, 2013), edited by Y Dinstein and F Domb. The individual contributions on various aspects of cyber warfare that feature in international journals and reviews are almost countless.

English, and providing balanced and often innovative solutions in adapting traditional international law rules to the new cyber realm.

The book is composed of five chapters, preceded by a foreword by Yoram Dinstein. Chapter 1 sets the stage for the subsequent legal analysis. It provides an account of the threat that cyber operations pose to international security, as well as an introduction to computer terminology. Roscini is able to illustrate technicalities in a language that non-specialists will understand, without however oversimplifying the relevant concepts. Most importantly, he explains his contention that 'existing treaty and customary norms can be extended to cyber operations by means of interpretation even though the relevant treaties and custom do not expressly contemplate them'.[4] His argument is convincingly based on state practice, ie on the fact that most states clearly consider cyber-attacks as being potential threats to international peace and security, and – at least when they occur in the framework of an ongoing armed conflict – as subjected to the regulatory regime of International Humanitarian Law (IHL). The author also sets aside the argument that the law should not be applied to CNAs because the Geneva Conventions were drafted significantly before the technology to launch such attacks was available. According to Roscini,[5] the forward-looking disposition of IHL can be clearly inferred from the inclusion of the so-called Martens Clause in all major *jus in bello* treaties, which states that, in the presence of legal gaps, 'civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience'.[6] In addition, Article 36 of Additional Protocol I (AP I) requires states to review new weapons, means and methods of warfare for compatibility with the Protocol and with other rules of international law applicable to the parties to the treaty. Hence, if one accepts that cyber operations do constitute a means and methods of combat, it flows that

[4] Roscini (n 2) 19.
[5] ibid 22, 29.
[6] Art 1(2), Additional Protocol I to the 1949 Geneva Conventions on the Protection of Victims of International Armed Conflicts (adopted 8 June 1977) 1125 UNTS 3.

the laws of armed conflict are applicable to CNAs, despite the fact that their technology is new.[7]

Chapter 2 of the book deals with the applicability of contemporary *jus ad bellum* to CNAs, while Chapters 3 and 4 deal respectively with the applicability of IHL to cyber operations and with the way in which its rules can be adapted to respond to the challenges of such modern methods of warfare. The fifth and final Chapter considers the obligations of neutral and belligerent states under the law of neutrality in the cyber domain. The present piece briefly looks at some of the arguments Roscini puts forward when he assesses whether and how the *jus in bello* is able to effectively regulate cyber attacks.

The starting point for his analysis is that the special characteristics of cyber weapons raise some new ethical and legal problems, which prompt questions on whether existing rules are sufficiently accurate to handle the unprecedented challenges raised by cyber operations. Is it enough to reinterpret established legal tenets in a progressive and teleological fashion? Or is there perhaps a need for a new standard-setting exercise to regulate at least certain aspects of cyber warfare? Roscini clearly supports the first option, and the book abounds with examples where evolutive interpretations of IHL provisions are convincingly put forward. According to the author, international law is 'well equipped to face [the] challenges posed by cyber warfare'. [8]

While many of his conclusions are to be welcomed as they appear to strike a fair balance between state interests and the obligation to safeguard civilians and civilian objects, it should not be forgotten that international law offers specific directions when it comes to treaty interpretation. It is true that the general rules included in the Vienna Convention on the Law of Treaties recognize subsequent agreements and subsequent practice of the parties as important means of interpretation (Vienna Convention, Article 31(3) (a) and (b)). Yet a difference must be traced between subsequent practice in the application of a treaty *which establishes the agreement of the parties regarding its interpretation* and

[7] See also the famous passage of the Nuclear Weapons Advisory Opinion, where the International Court of Justice held that the Geneva Conventions and Additional Protocols apply 'to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future': *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion, 8 July 1996) [1996] ICJ Rep, para 86.

[8] Roscini (n 2) 280.

other subsequent practice which does not necessarily reflect an agreement on interpretation.[9] The latter might still be relevant in determining the meaning to be given to specific treaty language, yet it is not as conclusive as the former when it comes to interpreting a treaty in an evolutive way. This is even more the case if one considers the high number of state parties to the Geneva Conventions and its Additional Protocols, as it might be difficult to assess the practice of numerous states, deciding how to appraise any inconsistencies in that practice, how to interpret any silence or inaction, and how to define which types of practice are relevant, especially considering the secretive nature of cyber operations.[10] Therefore, one is left to wonder if the practice referred to in Roscini's book is in all cases quantitatively and qualitatively sufficient to substantiate novel interpretations of IHL treaties, or rather should be used to support the idea that customary rules are crystallizing in certain areas.

Roscini himself appears to leave the door open to the development of new general rules pertaining to CNAs, as 'it cannot be excluded that customary international law rules specific to cyber warfare might be in the process of forming and eventually ripen'.[11] Yet even in this respect, caution is warranted. Because of the secrecy that still surrounds state conduct in the cyber domain and the inherent difficulties in attributing responsibility for cyber attacks, publicly available and legally relevant state practice remains scarce. The author in fact readily accepts that times may be premature to identify fully fledged customary rules pertaining to CNAs, and looks at military manuals and policy documents as indicators of 'trends of the direction towards which customary international law is starting to develop in this area'.[12]

In Chapter 3, the book offers a very convincing analysis of how IHL applies to cyber operations, whether conducted in isolation or in the

[9] See G Nolte, 'First report on subsequent agreements and subsequent practice in relation to treaty interpretation' UN Doc A/CN.4/660 (19 march 2013) 29.

[10] See SD Murphy, 'The Relevance of Subsequent Agreement and Subsequent Practice for the Interpretation of Treaties', in G Nolte (ed), *Treaties and Subsequent Practice* (OUP, 2013) 92-93.

[11] Roscini (n 2) 25.

[12] ibid 30. For a first attempt to look at relevant state practice see T Keber and NR Przemyslaw, 'Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis' (2011) 49 Archiv des Völkerrechts 399.

framework of an ongoing traditional armed conflict. Different sections are devoted to international armed conflicts (including situations of belligerent occupation), to non-international armed conflicts (NIACs), and to situations of *internal disturbances*, that do not amount to an armed conflict and fall within the scope of domestic law and international human rights law. One aspect on which perhaps some further analysis by legal scholars would be warranted concerns the features that an armed confrontation needs to possess in order to be qualified as a NIAC.

Roscini sets out from the definition developed by the International Criminal Tribunal for the former Yugoslavia (ICTY) Appeals Chamber in the *Tadić* decision, which defines a NIAC as 'protracted armed violence between governmental authorities and *organized* armed groups or between such groups within a State'.[13] When assessing the level of organization required, the author reviews the case of a private firm that conducts cyber-attacks for financial gain, concluding that – in the presence of the required level of organization – its motivations are 'irrelevant' for the qualification of conflict.[14] This assumption is, in effect, not uncontroversial. While it is true that the qualification as an organized armed group is based on objective criteria so as to avoid giving prominence to subjective factors such as the group's motivation, the law is not completely 'blind' in that respect. The ICTY maintains that such entities should be characterized by

> 'the existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; its ability to plan, coordinate and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and use military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords.'[15]

[13] ICTY, *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeals on Jurisdiction) IT-94-1 (2 October 1995) para 70 (emphasis added).

[14] Roscini (n 2) 156.

[15] ICTY, *Prosecutor v Haradinaj et al* (Judgement, Trial Chamber) IT–04–84 (3 April 2008) para 60.

By requiring an objectively verifiable military strategy or capacity to carry out military operations, the definition appears to exclude entities that rely exclusively on terrorist or other perfidious methods, whose main activity is to assert their egoistic interests through an arbitrary use of violence.[16] Indeed, states do not seem to be at all keen to categorize clashes with militarily organized criminal groups as NIACs.[17] One would imagine that such an attitude would persist even *vis-à-vis* a group of hackers, although it is recognized that cyber-gangs can cause extensive damage to civilians and civilian infrastructure while pursuing their criminal aims. More generally, while it is true that these indicators 'are not binding, not exhaustive and not cumulative, and none of them is more important than the others',[18] it is also rather clear that the list was drawn with kinetic attacks in mind. Hence, non-state actors fighting the incumbent government by exclusively carrying out cyber attacks would probably face problems in being acknowledged as sufficiently organized for the purposes of triggering the application of IHL.

Chapter 4 focuses on a series of important legal issues connected to the use of cyber technology in military operations. Questions under review include the legality of cyber weapons as such; the notion of *direct participation in hostilities* in the cyber domain; the application of the rules on targeting to CNAs (including the ones defining the proportionality of an attack); how cyber operations not resulting in loss of life or injury to persons (and hence not amounting to 'attacks') are regulated by IHL; and what the law says about undertaking cyber attacks as belligerent reprisals.

One of the most debated issues, of course, concerns the application of the principle of proportionality in cyber attacks, ie the balancing between the concrete and direct military advantage that is anticipated from the attack and the expected loss of civilian life and damage to ci-

[16] See P Hauck, S Peterke, 'Organized Crime and Gang Violence in National and International Law' (2010) 92 Intl Rev Red Cross 407, 433. Emily Crawford, for instance, submits that 'for policy reasons, in the case of organized crime groups, the motives of the parties should be taken into consideration if IHL is to be the *lex specialis*': E Crawford, *Identifying the Enemy: Civilian Participation in Armed Conflict* (OUP, 2015) 186.

[17] C Bergal, 'The Mexican Drug War: The Case for a Non-International Armed Conflict Classification' (2011) 34 Fordham Intl L J 1042, 1076-80.

[18] Roscini (n 2) 155.

vilian property that might be caused. Roscini introduces a useful conceptualisation of the effects of cyber attacks, [19] dividing them into primary effects (those on the attacked computer, computer system or network), secondary effects (those on the infrastructure operated by the attacked system or network), and tertiary effects (those on the persons affected by the destruction or incapacitation of the attacked system or infrastructure). This distinction is resorted to also in his description of the proportionality equation, where he stresses that all three types of effects must be taken into account in assessing the level of acceptable incidental damage.[20] The collateral damage that should be balanced against the military advantage is only the one that is *expected*, ie damage that is 'a reasonably likely or foreseeable consequence of the operation on the basis of the information available at the time of the attack'.[21] However, in a context in which military and civilian networks are often interconnected, damage to civilian objects might be extremely difficult to predict. As Schmitt argues, 'the problem of knock-on effects looms much larger in computer network attacks than in kinetic attacks owing to the interconnectivity of computers'.[22] Due to the inherent features of cyber weapons, an attacking actor might not be able to regulate the amount of force applied and the cyber-strike might have a destructive effect on unintended targets. Thus, a higher degree of uncertainty seems to be intrinsic to CNAs, as the predictability of its end results heavily relies on the specific (often hard-to-obtain) knowledge of the target's configuration at the moment of the attack. Roscini himself recognizes that – when called to assess and balance the expected incidental damage and the anticipated military advantage – the cyber context presents unique difficulties, which make any *ex ante* evaluation 'an esoteric prediction'.[23] Yet he concludes that, by adopting precautions in the planning and launching of the attack as required by IHL, even cyber attacks can be brought in line with the principle of proportionality. Ironically, the first precautionary measure which Article 57 of AP I imposes on those who plan an attack is to verify that the objectives to be attacked

[19] ibid 52-53.
[20] ibid 220.
[21] ibid 221.
[22] MN Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' (2000) 84 Intl Rev Red Cross 365, 393.
[23] Roscini (n 2) 228.

are military objectives within the meaning of IHL. Given the fact that virtually the entire cyber infrastructure (computers, cables, satellites, etc.) is used for both civilian and military communications (ie all of these items are so-called dual-use objects) its classification as a 'military objective' might be an all-to-easy task.[24] In a context in which much of a nation's everyday activities rely on cyber infrastructure, it is not overly difficult for an enemy State to destroy all (or much of) it by arguing that such computers or servers are (also) used to transmit military communications. While the attacking party would still have to comply with the rules on proportionality, this scenario poses great concern for the protection of the civilian population.[25]

At times, moreover, the attempt to adjust traditional *jus in bello* to the reality of cyber operations appears to considerably stretch the meaning of its rules, suggesting that, while IHL remains applicable, it probably does not adapt perfectly to cyber attacks. The notion of *levée en masse* seems to well illustrate this point.[26] It is difficult to see how civilians who conduct CNAs in response to a foreign invasion can obtain prisoner of war (POW) status in case of capture if – for this purpose – the law requires them to 'carry arms openly'. Civilian laptops, servers or pieces of software do not necessarily fit the definition of *arms* envisaged by the drafters of IHL treaties.[27] Therefore, participants in a cyber *levée en masse* would on one hand be considered as capable of launching *attacks* as defined by AP I, but would in all likelihood fall short of the requirements necessary to enjoy combatant privileges. The impression, thus, is that certain IHL provisions do not conform to the realities of

[24] This is even more the case since authoritative doctrine states that 'status as a civilian object and military objective cannot coexist; an object is either one or the other', and that even a limited military use of an otherwise civilian object turns it into a military objective, *Tallinn Manual* (n 3) 134.

[25] C Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 Intl Rev Red Cross 533, 564.

[26] Art 4.A.6 of the Third Geneva Convention defines *levée en masse* as a spontaneous uprising by '[i]nhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.' All those falling under such definition are entitled to POW status if captured.

[27] The *Tallinn Manual* even notes that the 'requirement to carry arms openly has little application in the cyber context' (n 3) 100.

cyber warfare, which raises the question of whether an *ad hoc* treaty would assist in solving some of the outstanding legal conundrums.

This is particularly true in the cyber domain when conventional IHL does not fully keep up with the protective aims it is meant to achieve.[28] In the end, some important legal questions are better settled not by scholars but by the states that will themselves be governed by the solution. Even where traditional *jus in bello* does offer some guidelines, a distinct and more focused legal instrument would help in clarifying and strengthening the rules. Indeed, the presence of general norms outlawing the use of certain means of warfare has not prevented states form adopting specific treaties aimed at limiting, forbidding the use or preventing the development of certain types of weapons.[29] Clearly, such an exercise is all the more important if one considers the potential (intended but also unintended) effects of cyber attacks.[30] Also, more legal precision would probably assist military and civilian personnel in planning and implementing operations in the cyber domain, and may somewhat alleviate their fear of the consequences of violating the law of armed conflict.[31]

While the adoption of a new binding instrument would – in the present author's view – contribute to increase the level of legal protection bestowed on civilians and civilian objects, it needs to be recognized that it is currently a rather unlikely prospect given the difficulty of treaty promulgation in this area.[32] This is why Roscini's volume is all the more

[28] See DB Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 Lewis and Clark L Rev 1023.

[29] For instance, the 1972 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction was adopted notwithstanding the fact that poisons had long been banned in customary international law, see D Brown, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (2006) 47 Harvard Intl L J 179, 183.

[30] In 2009, President Obama described computer network attacks as a 'weapon of mass disruption'. The White House, 'Remarks by the President on Securing our Nation's Cyber infrastructure' (Office of the Press Secretary, 29 May 2009) <www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.

[31] See Brown (n 27) ibid.

[32] For instance, in 2009, the Russian Federation unsuccessfully lobbied for a treaty 'to ban states from secretly embedding malicious codes or circuitry that could be later activated from a distance in the event of war', see C Wilson, 'Cyber Security and Cyber

a welcome addition to existing literature in the field. The way in which the author uses concrete cases of cyber operations as practical, real-world examples of the types of attacks which have taken place – and his subsequent legal assessment – make this volume a much valued navigation tool, useful to appraise the current state of legal development in the area. The detail and breadth of information found in all of the chapters is remarkable, and the book will quickly become a required reading for anyone who wishes to contribute in a qualified manner to the debate on cyber warfare.

Weapons: Is Nonproliferation Possible?' in M Martellini (ed) *Cyber Security Deterrence and IT Protection for Critical Infrastructures* (Springer, 2013) 11, 18.