Cyber Operations and the Use of Force in International Law

MARCO ROSCINI

The Leverhulme Trust

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

First Edition published in 2014

Impression: 1

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2013953298

ISBN 978–0–19–965501–4

Printed and bound in Great Britain by
CPI Group (UK) Ltd, Croydon, CR0 4YY

1

Identifying the Problem and the Applicable Law

I. The Emergence of the Cyber Threat to International Security

Modern societies have become increasingly dependent on computers, computer systems, and networks, with vital services now relying on the internet.[1] This 'digital revolution' has involved not only civilian infrastructures, but also the armed forces: as *The Economist* noted in a famous article, '[b]ombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centres; even the ordinary foot-soldier is being wired up'.[2] Digitalization, however, is a double-edged sword: as the US Deputy Secretary of Defense has emphasized, '[i]n the 21st Century, bits and bytes can be as threatening as bullets and bombs'.[3] In fact, the more digitally reliant a state is, the more vulnerable to cyber attacks: if computer networks become the society's 'nerve system', incapacitating them may mean paralysing the country.[4]

Cyber security is likely to acquire increasing importance in the next few years.[5] The threat no longer comes exclusively from the proverbial teenage hacker, but also from ideologically motivated individuals ('hacktivists'), states, and criminal

[1] While a computer is '[a] device that processes data', a computer system is '[o]ne or more interconnected computers with associated software and peripheral devices' (*Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), p 258). A computer network links two or more computers or computer systems (also known as 'network nodes') to exchange data by using wired, wireless, or mixed technology.

[2] 'War in the fifth domain', *The Economist*, 1 July 2010, <http://www.economist.com/node/16478792>. The US *National Strategy to Secure Cyberspace* acknowledges that '[b]y 2003, our economy and national security became fully dependent upon information technology and the information infrastructure' (*The National Strategy to Secure Cyberspace*, February 2003, p 6, <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf>).

[3] *Remarks on the Department of Defense Cyber Strategy, As Delivered by Deputy Secretary of Defense William J. Lynn, III*, 14 July 2011, <http://www.defense.gov/speeches/speech.aspx?speechid=1593>.

[4] The 2010 US *National Security Strategy* recalls that '[t]he very technologies that empower us to lead and create also empower those who would disrupt and destroy' (*National Security Strategy*, May 2010, p 27, <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>).

[5] As noted by the US National Strategy to Secure Cyberspace in 2003, 'the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving' (*The National Strategy to Secure Cyberspace*, p 6). The views, however, are not unanimous: see Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

and terrorist organizations: cyber technologies and expertise are relatively easy and cheap to acquire, which allows weaker states and even non-state actors to potentially cause considerable damage to countries with superior conventional military power.[6] Indeed, cyber operations may not only be used for industrial espionage or intelligence collection, but also to delete, alter, or corrupt software and data resident in computers, with possible negative repercussions on the functionality of computer-operated physical infrastructures. Even though extreme scenarios have not occurred yet, a cyber operation could go as far as to disable power generators, cut off the military command, control, and communication systems, cause trains to derail and aeroplanes to crash, nuclear reactors to melt down, pipelines to explode, weapons to malfunction, banking systems to cripple. Geographical distance and frontiers also become irrelevant in the cyber context, as a target could be hit on the other side of the world in a matter of seconds. The advent of cloud computing, with software and data stored in remote servers instead of resident computers, further complicates the matter and increases potential security risks: breaking the defences of the remote server means having access to the information of all users.[7]

It is, therefore, hardly surprising that cyber threats have become a concern of the international community, with the UN General Assembly adopting a series of annual resolutions on information security since 1998 emphasizing that 'the dissemination and use of information technologies and means affect the interests of the entire international community',[8] that 'the criminal misuse of information technologies may have a grave impact on all States'[9] and that these technologies 'can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security'.[10] The resolutions called for the views of the UN member states on information security and established three Groups of

[6] As noted in the Australian *Cyber Security Strategy*, '[t]he distinction between traditional threat actors—hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services—is increasingly blurred' (Australian Government, *Cyber Security Strategy*, 2009, p 3, <http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>). It does not seem, however, that 'terrorist' groups have been particularly active so far in conducting cyber operations, with the possible exception of Al-Qaeda: see Gregory J Rattray and Jason Healey, 'Non-State Actors and Cyber Conflict', in *America's Cyber Future. Security and Prosperity in the Information Age*, edited by Kristin M Lord and Travis Sharp (Center for a New American Security, June 2011), Vol II, p 72, <http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf>; Richard Garnett and Paul Clarke, 'Cyberterrorism: A New Challenge for International Law', in *Enforcing International Law Norms Against Terrorism*, edited by Andrea Bianchi (Oxford and Portland: Hart, 2004), p 467; Susan W Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), p 43.

[7] Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR), *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, Doc XXXIV, no 4, 7 July 2010, p 47.

[8] See eg the Preambles to GA Resolutions 55/28 of 20 November 2000; 56/19 of 29 November 2001; 59/61 of 3 December 2004; 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 5 December 2007; 63/37 of 2 December 2008; 64/25 of 2 December 2009; 65/41 of 8 December 2010; 66/24 of 2 December 2011; 67/27 of 3 December 2012.

[9] See eg the Preambles to GA Resolutions 55/63 of 4 December 2000; 56/121 of 19 December 2001.

[10] See eg the Preambles to GA Resolutions 58/32 of 8 December 2003; 59/61 of 3 December 2004; 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 5 December 2007; 63/37 of 2 December 2008; 64/25 of 2 December 2009; 65/41 of 8 December 2010; 66/24 of 2 December 2011; 67/27 of 3 December 2012.

Governmental Experts (GGE) that examined threats in cyberspace and discussed cooperative measures to address them.[11] The General Assembly also endorsed the holding of the World Summit on the Information Society, that took place, in two phases, in Geneva in 2003 and Tunis in 2005.[12] It is not only the United Nations, however, that has become concerned with cyber security. The 2010 Organization for the Security and Cooperation in Europe (OSCE)'s Astana Commemorative Declaration also mentioned cyber threats as one of the 'emerging transnational threats'.[13] NATO's New *Strategic Concept*, adopted in November 2010, recognizes the new security environment and emphasizes that, if 'the threat of a conventional attack against NATO territory is low', '[c]yber attacks are becoming more frequent, more organized and more costly in the damage that they inflict [and] can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability'.[14] In September 2011, China, the Russian Federation, Tajikistan, and Uzbekistan submitted a draft resolution to the UN General Assembly on an international Code of Conduct for Information Security.[15] The United Kingdom's *National Security Strategy*, published in October 2010, highlights that cyber attacks by states and non-state actors are one of the four high-priority risks for the UK's national security.[16] In particular, the document claims that '[a]ctivity in cyberspace will continue to evolve as a direct national security and economic threat, as it is refined as a means of espionage and crime, and continues to grow as a terrorist enabler, as well as a military weapon for use by states and possibly others'.[17] The United Kingdom also adopted a Cyber Security Strategy, as did several other states and international organizations.[18] The United States has been a particularly prolific issuer of documents on cyber security issues: apart from commissioning a study on information operations as early as 1999,[19] the Department of Defense (DoD) adopted a partly declassified *National Military Strategy for Cyberspace Operations* (2006)[20]

[11] While the first Group, established in 2004, did not produce a substantial report, the second, created in 2009, issued a report in 2010 (UN Doc A/65/201, 30 July 2010). A third Group met between 2012 and 2013 and also adopted a final report containing a set of recommendations (UN Doc A/68/98, 24 June 2013).

[12] For the documents adopted at the Summit, see <http://www.itu.int/wsis/index.html>.

[13] OSCE, *Astana Commemorative Declaration—Towards a Security Community*, SUM.DOC/1/10/Corr.1, 3 December 2010, para 9, <http://www.osce.org/cio/74985?download=true>.

[14] NATO, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, November 2010, paras 7, 12, <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

[15] UN Doc A/66/359, 14 September 2011.

[16] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010, pp 29–30, <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy>.

[17] *A Strong Britain*, p 29.

[18] See the documents on the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)'s website: <http://www.ccdcoe.org/328.html>.

[19] US Department of Defense, *An Assessment of International Legal Issues in Information Operations*, May 1999, <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>.

[20] Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, December 2006, <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_joint Operations/ 07-F-2105 doc1.pdf>.

and a *Strategy for Operating in Cyberspace* (2011).[21] The Air Force published the pioneering *Cornerstones of Information Warfare* in 1997[22] and subsequently a comprehensive doctrine of cyber operations.[23] The Joint Chiefs of Staff also released, among others, a *Joint Doctrine for Information Operations*,[24] while the Bush and Obama Presidencies adopted a *National Strategy to Secure Cyberspace* in 2003[25] and a *Cyberspace Policy Review* in 2009,[26] followed by the adoption of an *International Strategy for Cyberspace* in 2011, respectively.[27]

If 'cyber crime', ie the offences against the confidentiality, integrity, and availability of computer data and systems committed by individuals or private entities for personal gain,[28] is essentially a domestic law matter, cyber activities conducted by states against other states fall under the remit of international law. The applicable legal paradigm, then, depends first and foremost on whether or not the operation is attributable to a subject of international law. Several states have in fact been the object of cyber attacks of which other states were suspected. As early as June 1982, a logic bomb installed in the computer control system of a Soviet gas pipeline by the US Central Intelligence Agency (CIA) allegedly caused a major explosion in Siberia.[29] Predictably, however, there was no official confirmation of the incident by either the United States or the Soviet Union and it is still uncertain whether the attack actually occurred. Fast forward 25 years and, in 2007, a three-week Distributed Denial of Service (DDoS) attack targeted Estonia, one of the most wired countries in the world, shutting down government websites first and then extending to newspapers, TV stations, banks, and other targets.[30] The attack, which, at least in its second phase, involved more than one million computers based in

[21] *Department of Defense Strategy for Operating in Cyberspace*, July 2011, <http://www.defense.gov/news/d20110714cyber.pdf>.

[22] US Department of the Air Force, *Cornerstones of Information Warfare*, 17 April 1997, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA323807>.

[23] *Cyberspace Operations*, Air Force Doctrine Document 3-12, 15 July 2010, p 49, <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-060.pdf>.

[24] White House, *Information Operations*, Joint Publication 3-13, 27 November 2012, <http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf> ('Joint Doctrine for Information Operations'). Previous versions dated to 1998 and 2006.

[25] *The National Strategy to Secure Cyberspace*.

[26] *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009, <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[27] *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*, May 2011, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. On the international law aspects of the Strategy, see David P Fidler, 'International Law and the Future of Cyberspace: The Obama Administration's *International Strategy for Cyberspace*', *ASIL Insights*, Vol 15, issue 15 (8 June 2011), <http://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration%E2%80%99s>.

[28] The language is borrowed from Chapter II, Section 1, Title 1 of the 2001 Budapest Convention on Cyber Crime. The text of the Convention is in *International Legal Materials* 41 (2002), pp 282 ff.

[29] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), p 6.

[30] On DDoS attacks, see below, Section II, p 18 of this Chapter. For the facts of the case, see Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents. Legal Considerations* (CCDCOE, 2010), pp 18 ff, <http://www.ccdcoe.org/publications/books/legalconsiderations.pdf>.

over 100 countries hijacked and linked through the use of botnets, followed the decision of the Estonian government to remove a Soviet war memorial from Tallinn's city centre and, overall, lasted almost a month. The attack caused some limited economic and communication disruption, but no material damage, injuries, or loss of life.[31] Websites were also defaced and their content replaced with pro-Russia propaganda. Because of the political context in which the operation occurred and the fact that Russian Internet Protocol (IP) addresses were involved, fingers were pointed at Russia, which, however, firmly denied any involvement. In addition to Estonia, cyber operations also hit, among others, Azerbaijan,[32] Kyrgyzstan,[33] Lithuania,[34] Montenegro,[35] South Korea,[36] Switzerland,[37] Taiwan,[38] the United Kingdom,[39] and the United States.[40] In August 2012, a virus, dubbed 'Shamoon' from a word contained in its computer code, destroyed the data of about 30,000 company computers of Saudi Aramco, the world's largest oil producer, and, according to Saudi Arabia, targeted the country's economy with the purpose of stopping pumping oil into domestic and international markets.[41] The deleted data were replaced with a burning American flag.

[31] Sean M Watts, 'Low-Intensity Computer Network Attack and Self-Defense', *International Law Studies* 87 (2011), p 70.

[32] 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, UN Doc A/66/897–S/2012/687.

[33] 'The fog of cyberwar', *The Guardian, Technology Supplement*, 5 February 2009, p 1; Fred Schreier, *On Cyber Warfare*, DCAF Horizon 2015 Working Paper no 7, p 113, <http://www.dcaf.ch/Publications/On-Cyberwarfare>, 7 September 2012.

[34] In June 2008, after the Lithuanian Parliament adopted a law prohibiting the public display of Soviet symbols, political and private websites were defaced and their content replaced with pro-Soviet propaganda (Tikk, Kaska, and Vihul, *International Cyber Incidents*, pp 63 ff).

[35] A cyber attack forced the shutdown of more than 150 websites, including the postal service and several banks' websites in March 2010. The attack apparently originated in Kosovo ('Cyber-attack shut 150 Montenegrin websites', *The Sydney Morning Herald*, 12 March 2010, <http://news.smh.com.au/breaking-news-technology/cyberattack-shut-150-montenegrin-websites-20100312-q1xo.html>).

[36] Matthew Weaver, 'Cyber attackers target South Korea and US', *The Guardian*, 8 July 2009, <http://www.guardian.co.uk/world/2009/jul/08/south-korea-cyber-attack>; Schreier, *On Cyber Warfare*, p 114.

[37] Michael Barkoviak, 'Swiss Ministry Suffers Cyber Attack', *Daily Tech*, 28 October 2009, <http://www.dailytech.com/Swiss+Ministry+Suffers+Cyber+Attack/article16629.htm>.

[38] Susan W Brenner, '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare', *Journal of Criminal Law and Criminology* 97 (2006–07), p 402.

[39] Jonathan Richards, 'Thousands of cyber attacks each day on key utilities', *The Times*, 23 August 2008, <http://www.thetimes.co.uk/tto/news/uk/crime/article1874881.ece>. According to the *Annual Report 2009–2010* of the UK Intelligence and Security Committee, the greatest threat of electronic attacks to the United Kingdom comes from states, in particular from Russia and China (Intelligence and Security Committee, *Annual Report 2009–2010*, March 2010), p 16, <http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61295/isc-annualreport0910.pdf>.

[40] See, for instance, the 2003 'Titan Rain' operation, that infiltrated governmental computer networks in the United States for four years through the installation of back door programs to steal information (Scott J Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', *Berkeley Journal of International Law* 27 (2009), p 204). See also the other incidents reported in Schreier, *On Cyber Warfare*, pp 107, 114.

[41] 'Saudi Aramco says cyber attack targeted kingdom's economy', *Al Arabiya News*, 9 December 2012, <http://www.alarabiya.net/articles/2012/12/09/254162.html>. Oil production, however, remained uninterrupted.

But what has been epitomized as a 'game changer' was first discovered in September 2010, when it was reported that a computer worm, dubbed Stuxnet, had attacked Iran's industrial infrastructure with the alleged ultimate purpose of sabotaging the gas centrifuges at the Natanz uranium enrichment facility, one of the sites where the Islamic Republic is developing a nuclear programme.[42] Even though an earlier version had already been released in 2007,[43] the worm—which presumably infiltrated the Natanz system, which is not usually connected to the internet for security reasons, through laptops and USB drives—mainly operated in three waves between June 2009 and May 2010.[44] Unlike other worms, Stuxnet did not limit itself to self-replicate, but also contained a 'weaponized' payload, designed to give instructions to other programs[45] and (if one excludes the above-mentioned almost legendary case of the Siberian pipeline) is, in fact, the first and so far only known use of malicious software designed to cause material damage by attacking the Supervisory Control and Data Acquisition (SCADA) system of a national critical infrastructure (NCI).[46] Stuxnet had two components: one designed to force a change in the centrifuges' rotor speed, inducing excessive vibrations or distortions, and one that recorded the normal operations of the plant and then sent them back to plant operators to make it look as if everything was functioning normally.[47] Although the exact consequences of the incident are still the object of debate in 2010, the International Atomic Energy Agency (IAEA) reported that Iran stopped feeding uranium into a significant number of gas centrifuges at Natanz.[48] In October 2011, another worm, dubbed DuQu, was discovered: its code had striking similarities with Stuxnet although its payload was not designed to cause physical damage, but to obtain information that could be used to attack industrial control systems.[49] Malware, known as

[42] For a comprehensive technical analysis of Stuxnet, see Symantec's Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32 Stuxnet Dossier*, version 1.4, February 2011, <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Iran claims that its uranium enrichment programme is for purely civilian purposes.

[43] Ivanka Barzashka, 'Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme', *RUSI Journal* 158, no 2 (April 2013), pp 50, 55.

[44] It was also reported that, in December 2012, the worm reappeared and targeted companies in southern Iran ('US general warns over Iranian cyber-soldiers', *BBC News Technology*, 18 January 2013, <http://www.bbc.co.uk/news/technology-21075781>).

[45] Jeremy Richmond, 'Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?', *Fordham International Law Journal* 35 (2012), p 849.

[46] SCADA systems are computer-controlled industrial control systems that monitor and control industrial processes of physical infrastructures. On NCIs, see Chapter 2, Section II.1.2.

[47] William J Broad, John Markoff, and David E Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *The New York Times*, 15 January 2011, <http://www.cfr.org/iran/nyt-israeli-test-worm-called-crucial-iran-nuclear-delay/p23850>.

[48] William J Broad, 'Report Suggests Problems with Iran's Nuclear Effort', *The New York Times*, 23 November 2010, <http://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html>. It is, however, unconfirmed whether this was due to Stuxnet or to technical malfunctions inherent to the equipment used (Katharina Ziolkowski, *Stuxnet—Legal Considerations* (CCDCOE, 2012), p 5; Barzashka, 'Are Cyber-Weapons Effective?', p 52).

[49] Symantec, *W32.DuQu—The Precursor to the Next Stuxnet*, 23 November 2011, <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>. For a discussion of the legal aspects of DuQu, see David P Fidler,

Flame, was also found in May 2012 to have penetrated the computers of senior Iranian officials with the alleged goal of stealing sensitive data. Disguised as a routine Microsoft update, Flame collected intelligence from a variety of sources and sent it back to its controllers, but, unlike Stuxnet, did not cause material damage.[50] It is entirely possible that DuQu and Flame worked together with Stuxnet for the same purpose: slowing down Iran's nuclear programme, which is allegedly aimed at developing nuclear weapons. Although the evidence is at best circumstantial,[51] the sophistication of Flame and DuQu and, in the case of Stuxnet, also its consequences on the Natanz facility have raised claims that states could be behind the incidents, in particular Israel and the United States: it has been reported that cyber efforts to disrupt the Iranian nuclear programme, codenamed 'Operation Olympic Games', were started in 2006 by the Bush Administration with Israel's cooperation and were expanded by President Barack Obama.[52]

Cyber operations have also been used in connection with a military operation or an armed conflict. It appears, for instance, that, during Operation Allied Force in 1999, the United States considered launching a cyber attack against Yugoslavia's air defence command network to disrupt its ability to target NATO aircraft, but eventually cancelled the plan because of doubts on its legality and of the risks for civilian aviation.[53] Pro-Serbian hackering groups such as the 'Black Hand', however, attacked NATO internet infrastructure during the armed conflict: although it is unknown whether their actions were attributable to Yugoslavia, their stated goal was to disrupt NATO's military operations.[54] In the second Chechen war (1999–2000), Russia disabled the insurgents' websites in order to prevent them from delivering anti-Russian propaganda: the Chechen insurgents are in fact considered pioneers in the use of the internet as a war propaganda tool.[55] It also seems that the 2007 bombing by Israel of a nuclear facility in Syria (codenamed 'Operation Orchard') was preceded by a cyber attack that neutralized ground radars and anti-aircraft batteries.[56] The cyber operations against Georgia of July–August 2008, that occurred before and during the armed conflict with the Russian

'Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think', *International Journal of Critical Infrastructure Protection* 5 (2012), pp 28–9.

[50] Ellen Nakashima, Greg Miller and Julie Tate, 'U.S., Israel developed Flame computer virus to slow down Iranian nuclear efforts, officials say', *The Washington Post*, 19 June 2012, <http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware>.

[51] On the standard of evidence required for attribution of cyber operations amounting to a use of force, see below, Chapter 2, Section III.6.

[52] David E Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *The New York Times*, 1 June 2012, <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0>.

[53] Jeffrey TG Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', *Michigan Law Review* 106 (2008), pp 1434–5.

[54] Schreier, *On Cyber Warfare*, p 108.

[55] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (CCDCOE, November 2008), p 5. On the use of the internet by armed groups for propaganda and communication purposes, see Wael Adhami, 'The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfare', *International Review of the Red Cross* 89 (2007), pp 867–70.

[56] Harrison Dinniss, *Cyber Warfare*, p 7; Schreier, *On Cyber Warfare*, pp 110–11.

Federation, caused the governmental websites to go off-line and slowed down internet services.[57] In particular, immediately before and after Russian troops entered the secessionist Georgian province of South Ossetia, several governmental websites were defaced and their content replaced with anti-Georgian propaganda, while DDoS attacks crippled the Caucasian nation's ability to disseminate information. Georgia accused the Russian Federation of carrying out the cyber attacks,[58] but Russia denied its involvement and claimed that the attacks were the responsibility of private citizens that voluntarily decided to take action. The cyber operations were mentioned in the 2009 Report of the Independent Fact-Finding Mission on the Conflict in Georgia, which, however, did not reach any conclusion on their attribution or legality but noted that '[i]f these attacks were directed by a government or governments, it is likely that this form of warfare was used for the first time in an inter-state armed conflict'.[59] Since 2000, the 'cyber war' in the Middle East has accompanied traditional hostilities. In October 2000, after the kidnapping of three Israeli soldiers, a Hezbollah website was defaced and its content replaced with Israel's flags and a sound file with the Israeli national anthem. Pro-Israeli hackers also attacked the official websites of military and political organizations such as the Palestinian National Authority, Hamas, and Iran. In response, hackers hit Israeli political, economic and military targets, including the Bank of Israel and the Tel Aviv Stock Exchange, as well as telecommunications, media, and universities.[60] In 2006, in the midst of another crisis between Israel and Gaza, some 700 Israeli internet domains were shut down by hackers.[61] Unusually severe cyber operations also targeted several of Israel's governmental websites during the 2008–09 Operation Cast Lead in the Gaza Strip, mainly for defacement purposes.[62] Israeli governmental and defence-related websites were also attacked by 'Anonymous' and other hackering groups in response to Israel's air raids and internet disruption in Gaza during the 2012 Operation Pillar of Defense.[63] Israel's chief information officer was quoted as saying that '[t]he war is taking place on three fronts. The first is physical, the second is on the world of social networks and the third is cyber'.[64]

[57] See the facts of the case and their legal anaylsis in Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, *Cyber Attacks Against Georgia*, pp 4 ff. For the technical aspects of the cyber operations against Georgia, see *Russia/Georgia Cyber War—Findings and Analysis*, Project Grey Goose: Phase I Report, 17 October 2008, <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>.

[58] *National Security Concept of Georgia*, 2011, p 9, <http://www.nsc.gov.ge/files/files/National%20Security%20Concept.pdf>.

[59] *Report of the Independent Fact-Finding Mission on the Conflict in Georgia*, September 2009, Vol II, pp 217–19, <http://www.ceiig.ch/Report.html>.

[60] Kenneth Geers, 'Cyberspace and the changing nature of warfare', *SC Magazine*, 28 August 2008, <http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/#>.

[61] Geers, 'Cyberspace'.

[62] Stefan Kirchner, 'Distributed Denial-of-Service Attacks Under Public International Law: State Responsibility in Cyberwar', *The IUP Journal of Cyber Law* 8, no 3–4 (2009), p 14.

[63] Maya Epstein, 'The Fight for Public Opinion and Warfare on the Web', *Haaretz*, 19 November 2012, <http://www.haaretz.com/news/features/the-fight-for-public-opinion-and-warfare-on-the-web.premium-1.478993>.

[64] 'Mass cyber-war on Israel over Gaza raids', *Aljazeera*, 19 November 2012, <http://www.aljazeera.com/news/middleeast/2012/11/201211197311174613 7.html>. On the use of new media to influence public opinion in the Palestinian–Israeli conflict, see Diana Allan and Curtis Brown, 'The *Mavi Marmara* at the Frontlines of Web 2.0', *Journal of Palestine Studies* 40 (2010), pp 63 ff.

During the 2011 armed conflict in Libya, the United States considered the use of cyber operations to disrupt Ghaddafi's air defence systems, although it eventually backed down.[65] Finally, the Syrian government has apparently used cyber operations through the self-styled 'Syrian Electronic Army' as part of its counterinsurgency campaign, while the opposition forces and 'Anonymous' have engaged in defacement operations against the Assad regime.[66]

The above list of incidents is by no means intended to be exhaustive but should sufficiently explain why the armed forces have become increasingly concerned with cyber security to the point that 'cyberspace', defined by the US DoD as '[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers',[67] is now considered a fifth domain of warfare in addition to land, sea, air, and space.[68] As the 2010 Report of the GGE found, there is 'increased reporting that States are developing information and communications technologies as instruments of warfare and intelligence, and for political purposes'.[69] The Vision of the Polish Armed Forces 2030 expressly states that '[a]part from traditional geo-spaces, such as land, sea, air (including outer space), spheres unprovided with geographical parameters, immeasurable and unlimited, such as virtual cyberspace or information sphere, will be used as a battleground'.[70] This new battlefield 'will have no classical, linear nature, there will be no points of contact between fighting units nor delimitation lines. The future battlefield will be space in

[65] Thomas Rid and Peter McBurney, 'Cyber-Weapons', *RUSI Journal* 157, no 1 (February 2012), p 6.

[66] Justin Salhani, 'In Syria, the Cyberwar Intensifies', *Defense News*, 18 January 2013, <http://www.defensenews.com/article/20130118/C4ISR01/301180018/In-Syria-Cyberwar-Intensifies>.

[67] US DoD, *Dictionary of Military and Associated Terms*, Joint Publication 1–02, 8 November 2010 (As Amended Through 15 July 2013), p 70, <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Cyberspace, then, goes beyond the internet and includes all networked digital activities. A slightly different definition is contained in the 2006 US *National Military Strategy for Cyberspace Operations* and in the *Joint Terminology for Cyberspace Operations*: 'a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures' (US, *The National Military Strategy for Cyberspace Operations*, p 3; Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, *Joint Terminology for Cyberspace Operations*, November 2010, p 7, <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>).

[68] 'War in the fifth domain'. Unlike the traditional domains of warfare, however, cyberspace is man-made and has no specific boundaries. See the UNIDIR report on certain states that have included cyber warfare in their doctrine: Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare—Preliminary Assessment of National Doctrine and Organization* (UNIDIR, 2011), <http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>.

[69] UN Doc A/65/201, 30 July 2010, p 2. The Report was endorsed by the General Assembly in Resolution 65/41 of 8 December 2010.

[70] Ministry of National Defence, *Vision of the Polish Armed Forces 2030*, May 2008, p 13, <http://www.wp.mil.pl/pliki/File/vision_of_paf_2030.pdf>.

which combat operations and other actions of different nature and intensity will simultaneously take place.'[71]

The increasing militarization of cyberspace is reflected not only in the incorporation of cyber operations in military doctrines, but also in the creation of cyber units within national armies. Colombia has, for instance, established the Armed Forces Joint Cyber Command, which is mandated with preventing and countering cyber operations affecting national values and interests.[72] More famously, the United States has set up a military Cyber Command (a sub-unit of the Strategic Command).[73] China has also apparently created cyberspace battalions and regiments,[74] while North Korea's Unit 121, which at least partly operates from China because of the limited number of internet connections in North Korea, is believed to be responsible for disabling South Korea's military command, control, and communication networks.[75] Other states, including Argentina, Belgium, Brazil, Canada, Denmark, France, Germany, India, Iran, Israel, Japan, the Netherlands, South Korea, Switzerland, and the United Kingdom, have also either established military cyber units or plan to do so in the near future.[76]

II. The Taxonomy of Military Cyber Operations: Definitions and Classification

There are no consistent terminology or widely accepted definitions in this area. As is clear from its title, this book generally prefers to refer to 'cyber operations' instead of 'cyber war' to avoid using outdated notions and superficial and misleading analogies.[77] The expression 'cyber warfare' is also narrower than 'cyber operations'

[71] *Vision of the Polish Armed Forces*, p 13.

[72] UN Doc A/67/167, 23 July 2012, p 5.

[73] See the US Cyber Command's website: <http://www.arcyber.army.mil>.

[74] Sean M Condron, 'Getting It Right: Protecting American Critical Infrastructure in Cyberspace', *Harvard Journal of Law and Technology* 20 (2007), p 405; Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence', *Stanford Journal of International Law* 38 (2002), p 212; Sean Watts, 'Combatant Status and Computer Network Attack', *Virginia Journal of International Law* 50 (2010), p 405; Alexander Klimburg, 'Mobilising Cyber Power', *Survival* 53, no 1 (February–March 2011), p 45.

[75] Richard A Clarke and Robert K Knake, *Cyber War. The Next Threat to National Security and What to Do About It* (New York: Harpercollins, 2010), pp 27–8.

[76] John Goetz, Marcel Rosenbach, and Alexander Szandar, 'War of the Future: National Defense in Cyberspace', *Der Spiegel*, 11 February 2009, <http://www.spiegel.de/international/germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html>; Elad Benari, 'Israel to Establish Cyber Warfare Administration', Israel National News, 13 January 2012, <http://www.israelnationalnews.com/News/News.aspx/151713>; 'UK to create new cyber defence force', BBC News, 29 September 2013, <http://www.bbc.co.uk/news/uk-24321717>; Dutch Government Response to the AIV/CAVV Report on Cyber Warfare, <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf>, pp 3–4; Ziolkowski, *Stuxnet*, pp 51–2; Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare*, p 4; Li Zhang, 'A Chinese Perspective on Cyber War', *International Review of the Red Cross* 94 (2012), p 805.

[77] See eg Michael Rundle, '"Anonymous" Hackers Declare Cyberwar on North Korea, Claim Internal Mail System Hacked', *The Huffington Post*, 4 April 2013, <http://www.huffingtonpost.co.uk/2013/04/04/anonymous-hackers-declare-war-north-korea_n_3012451.html>. As has been

and technically refers only to the conduct of hostilities in armed conflict using cyber technologies: it will therefore only be employed in the Chapters dealing with the law of armed conflict.[78]

In military doctrine, states' 'cyber operations' fall within the broader category of information operations.[79] 'Information operations' have been defined as the 'integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own'.[80] What characterizes cyber operations and makes them unique, however, is that information can also be used to inflict disruption or damage on an adversary.[81] The US DoD *Dictionary of Military and Associated Terms* defines 'cyberspace operations' as '[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace'.[82] The *Tallinn Manual on the International Law Applicable to Cyber Warfare*, published in 2013 by a Group of Experts at the invitation of NATO's CCDCOE,[83] slightly modifies this language and defines cyber operations as 'the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace'.[84] More descriptively, the International Committee of the Red Cross (ICRC)'s definition refers to 'operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system.'[85] All the above definitions suggest that cyberspace

observed, '[r]hetoric that uses a terminology of war, like "cyber war" or "cyber attack," can create situations in which a State has fewer obstacles to an aggressive response to a non-State actor's cyber threats or cyber conduct, stretching or overstepping the relevant legal boundaries' (Laurie R Blank, 'International Law and Cyber Threats from Non-State Actors', *International Law Studies* 89 (2013), p 437). The 'ideology of militarism' applied to cyberspace is also criticized by Mary Ellen O'Connell, 'Cyber Security without Cyber War', *Journal of Conflict and Security Law* 17 (2012), pp 191 ff.

[78] See Chapters 3, 4, and 5 of the present book.

[79] According to the *Oxford English Dictionary*, 'cyber' means 'relating to information technology, the Internet, and virtual reality' (*The Oxford Compact English Dictionary* (Oxford: Oxford University Press, 2003), p 268).

[80] US, *National Military Strategy for Cyberspace Operations*, p GL–2. The updated version of the Joint Doctrine for Information Operations (2012) describes them as the 'integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own' (Joint Doctrine for Information Operations, p GL-3).

[81] Daniel J Ryan, Maeve Dion, Eneken Tikk, and Julie JCH Ryan, 'International Cyberlaw: A Normative Approach', *Georgetown Journal of International Law* 42 (2011), p 1179.

[82] US DoD, *Dictionary of Military and Associated Terms*, p 70. See also *Joint Terminology for Cyberspace Operations*, p 8; and Joint Doctrine for Information Operations, p II–9.

[83] The CCDCOE is a think-tank based in Tallinn that was created after the 2008 DDoS attacks against the Baltic state. It is not integrated into NATO's structure or funded by it. On the Manual, see Section III.3 of this Chapter.

[84] Tallinn Manual, p 258.

[85] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, ICRC Doc 31IC/11/5.1.2, October 2011, p 36, <http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf>.

can be at the same time the target and the medium through which an attack is delivered.[86]

The 1999 US DoD's *Assessment of International Legal Issues in Information Operations*, the 2006 US *National Military Strategy for Cyberspace Operations* and the *Manual on International Law Applicable to Air and Missile Warfare*, adopted by the Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University in 2009, do not refer to 'cyber operations' but to 'computer network' operations (CNO). In strict linguistic terms, this latter notion is ambiguous, as it may lead to the erroneous belief that only computer networks are the targets of a cyber operation, while they may also include individual and specific computers within a network, as well as websites.[87] Furthermore, cyber operations can be conducted not only remotely through networks, but also through local installation of malware by agents that have physical access to the system. More recent documents, such as the 2010 US *International Strategy for Cyberspace*, the 2011 US DoD's *Strategy for Operating in Cyberspace*, the 2012 US Presidential Policy Directive 20 and the 2013 *Tallinn Manual on Cyber Warfare* drop the use of 'CNO' and refer to 'cyberspace operations' (the first two) and 'cyber operations' (the latter two).[88] The expressions CNO and its offshoots were eventually approved for removal also from the DoD *Dictionary of Military and Associated Terms* and do not appear in the 2012 version of the *Joint Doctrine for Information Operations*.[89]

There are different classifications of cyber operations in the US documents. In 2006, the US DoD distinguished CNO in computer network attacks (CNA), computer network defense (CND), and 'related computer network exploitation enabling operations' (CNE).[90] CNE was defined as '[e]nabling operations and intelligence collection to gather data from target or adversary automated information systems or networks'.[91] The *Joint Terminology for Cyberspace Operations* adds that CNE must occur 'through the use of computer networks'.[92] More

[86] Robin Geiss and Henning Lahmann, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space', *Israel Law Review* 45 (2012), p 384.

[87] HPCR, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge; Cambridge University press, 2013) 21.

[88] But see NATO's 2013 *Glossary of Terms and Definitions*, that reintroduces the distinction between CNA and CNE (p 2–C–11). The *Glossary* qualifies a CNA as a type of 'cyber attack' without, however, defining this expression.

[89] Joint Doctrine for Information Operations, p GL–3.

[90] US *National Military Strategy for Cyberspace Operations*, p GL–1. An alternative classification is contained in Germany's *Cyber Security Strategy*, which defines a 'cyber attack' as 'an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security'. It includes cyber espionage, ie an attack against the confidentiality of systems conducted by foreign intelligence services, and cyber sabotage, that prejudices the integrity and availability of IT systems (Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011, p 16, <http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile>). Referring at the same time to the author and the purpose of the action as classification criteria, the Italian Comitato parlamentare per la sicurezza della Repubblica distinguishes between cyber crime, cyber terrorism, cyber espionage, and cyber war (COPASIR, *Relazione sulle possibili implicazioni*, p 17).

[91] US *National Military Strategy for Cyberspace Operations*, p GL–1.

[92] *Joint Terminology for Cyberspace Operations*, p 4.

vaguely, NATO's Glossary of Terms defines CNE as '[a]ction taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage'.[93]

The US *National Military Strategy for Cyberspace Operations* defines CNAs as '[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'.[94] A very similar definition appears in NATO's Glossary of Terms and Definitions.[95] This often cited definition distinguishes between two types of CNA, those targeting the computer or computer network and those targeting the *information* contained in the computer or computer network. As such, it may include kinetic or electronic attacks on the physical components of the cyber infrastructure.[96] The HPCR Manual adjusts the DoD's definition of CNA to also cover operations that 'manipulate' computer information and that aim 'to gain control over the computer or computer network'.[97] While both the DoD and HPCR definitions focus on the computers and computer systems as targets and do not indicate by what means (cyber, electronic or kinetic) the attack must be conducted,[98] the 2010 *Joint Terminology for Cyberspace Operations* more accurately defines CNAs as 'actions . . . taken *through the use of computer networks* to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves'.[99] CNA, then, is narrower than 'cyber attack', which can be conducted not only through computer networks, but also through close access to the system, and whose intended effects 'are not necessarily limited to the targeted computer system or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 [command and control] capability'.[100]

As to CND, the US *National Military Strategy for Cyberspace Operations* defines it as '[a]ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks'.[101]

[93] NATO's Glossary of Terms and Definitions, p 2–C–11.

[94] US *National Military Strategy for Cyberspace Operations*, p GL–1. The definition is criticized by Dinstein, who argues that '[h]ad [it been] legally binding—or had it factually mirrored the whole gamut of the technological capabilities of the computer—the likelihood of a CNA ever constituting a full-fledged armed attack would be scant' (Yoram Dinstein, 'Computer Network Attacks and Self-Defense', *International Law Studies* 76 (2002), p 102).

[95] NATO's Glossary of Terms and Definitions, p 2–C–11.

[96] 'Cyber infrastructure' includes 'communications, storage, and computing resources upon which information systems operate' (Tallinn Manual, p 258).

[97] Rule 1(m), HPCR Manual, p 20. On the Manual, see Jordan J Paust, 'A Critical Appraisal of the Air and Missile Warfare Manual', *Texas International Law Journal* 47 (2012), pp 277 ff.

[98] Daniel T Kuehl, 'Information Operations, Information Warfare, and Computer Network Attack—Their Relationship to National Security in the Information Age', *International Law Studies 76* (2002), pp 44–5.

[99] *Joint Terminology for Cyberspace Operations*, p 3 (emphasis added).

[100] *Joint Terminology for Cyberspace Operations*, p 5.

[101] US *National Military Strategy for Cyberspace Operations*, p GL–1. NATO's Glossary of Terms only distinguishes between CNAs and CNE and does not include CND.

CND employs information assurance capabilities, intelligence, counterintelligence, law enforcement, and also military capabilities, and includes both active and passive cyber defences:[102] while the latter consist of defending the networks through the use of firewalls, honeypots, encryption, routers, intrusion detection and prevention devices, numerical identifiers for communication between genuine users, anti-virus systems, and other tools which do not involve coercion or unauthorized intrusion into computer systems, the former are in kind responses to a previous cyber attack and are in fact attacks themselves.[103] Active defences capabilities, which can range from benign to aggressive, can work in an automated manner or be operated manually, and their details are often classified.[104]

In addition to referring to CNE, whose definition is identical to that of the 2006 National Military Strategy apart from the added specification that they must be conducted 'through the use of computer networks',[105] the US Air Force's *Doctrine for Cyberspace Operations*, adopted in July 2010 and updated in 2011, drops the expression CND and refers to 'cyberspace defense', defined as '[t]he passive, active and dynamic employment of capabilities to respond to imminent or on-going actions against AF [Air Force] or AF-protected networks, AF's portion of the Global Information Grid (GIG) or expeditionary communications assigned to the AF'.[106] It also introduces the concept of 'cyberspace force application', ie '[c]ombat operations in, through, and from cyberspace to achieve military objectives and influence the course and outcome of conflict by taking decisive actions against approved targets'.[107] Counter cyberspace operations are distinguished in offensive and defensive: the former, that replace CNAs, are defined as '[t]he operational planning and employment of capabilities to disrupt, deny, degrade, divert, neutralize or destroy an adversary's use of cyberspace capability or other data and information infrastructures to conduct activities or freedom of action', while the latter correspond to active defences.[108]

In November 2010, the US Joint Chiefs of Staff developed a terminology for cyberspace operations common to all US military forces. The document defines 'cyber warfare' as '[a]n armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict'.[109] Cyber warfare is divided in

[102] US *National Military Strategy for Cyberspace Operations*, p GL–1.

[103] Matthew J Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent', *Military Law Review* 201 (2009), pp 21–6.

[104] Active cyber defence involves 'launching a pre-emptive, preventive, or cyber counter-operation against the source', while passive cyber defence does not involve a counter-operation against the source but uses tools like firewalls, honeypots, anti-virus software, and the like (Tallinn Manual, pp 257, 261). See a categorization of active defences in Richard E Overill, 'Reacting to Cyber-intrusions: The Technical, Legal and Ethical Dimensions', *Journal of Financial Crime* 11 (2003), pp 163–4.

[105] *US Air Force, Cyberspace Operations*, p 49.

[106] *US Air Force, Cyberspace Operations*, p 50.

[107] *US Air Force, Cyberspace Operations*, p 50.

[108] *US Air Force, Cyberspace Operations*, pp 52 and 50, respectively.

[109] *Joint Terminology for Cyberspace Operations*, p 8.

cyber attack, cyber defence and cyber enabling operations. Cyber enabling operations presumably correspond to CNE. Cyber attack is defined as '[a] hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions'.[110] Cyber attacks are different from CNAs in that 'the action meets use-of-force levels or is specifically intended to disrupt, deny, degrade, manipulate, and/or destroy adversary computer systems or data'.[111] Cyber attacks are also different from Offensive Counter-Cyber (OCC) operations as they can affect non-cyber systems and are not necessarily associated with imminent or ongoing hostilities.[112] Cyber defence is '[t]he integrated application of DOD or US Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyse and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable US freedom of action'.[113] It includes Proactive Net Operations, Defensive Counter Cyber and Defensive Countermeasures. 'Countermeasures' is not used in a legal sense, but indicates merely technical devices and techniques that fall below the use of force threshold.[114]

The US DoD *Dictionary of Military and Associated Terms* uses an alternative classification and distinguishes 'cyberspace operations' according to their purpose in defensive cyberspace operations (DCO), ie '[p]assive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems' and offensive cyberspace operations (OCO), which are those 'intended to project power by the application of force in or through cyberspace'.[115] Defensive cyberspace operation response action (DCO-RA) are a type of DCO that involve '[d]eliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems'.[116] Cyber counterintelligence includes '[m]easures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions'.[117]

Finally, the leaked 2012 US Presidential Policy Directive 20 distinguishes 'cyber operations' in Cyber Collection (CC) and 'Cyber Effects' Operations (CEO). The former, which basically correspond to CNE, are '[o]perations and related programs or activities conducted by or on behalf of the United States Government, in or through cyberspace, for the primary purpose of collecting intelligence—including information that can be used for future operations—from computers, information

[110] *Joint Terminology for Cyberspace Operations*, p 5.
[111] *Joint Terminology for Cyberspace Operations*, p 6.
[112] *Joint Terminology for Cyberspace Operations*, p 13.
[113] *Joint Terminology for Cyberspace Operations*, p 6
[114] *Joint Terminology for Cyberspace Operations*, pp 4–5.
[115] US DoD, *Dictionary of Military and Associated Terms*, pp 75, 204.
[116] US DoD, *Dictionary of Military and Associated Terms*, p 75.
[117] US DoD, *Dictionary of Military and Associated Terms*, pp 69–70.

or communications systems, or networks with the intent to remain undetected'.[118] The latter's aim is to achieve a 'cyber effect', defined as '[t]he manipulation, disruption, denial, degradation, or destruction of computers, information or communication systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon'.[119] CEO are further distinguished into Defensive Cyber Effects Operations (DCEO) and Offensive Cyber Effects Operations (OCEO) depending on whether they are conducted in offence or in defence.[120] DCEO include Nonintrusive Defensive Countermeasures (NDCM), which do not entail unauthorized access to computer systems and networks and only produce minimum cyber effects to mitigate threats, but not Network Defense, ie programs, activities and tools for protection of computer systems and networks that do not require unauthorized access to them.[121]

In spite of the multiplicity of terms employed, what all the classifications above have in common is ultimately the main distinction between cyber exploitation and cyber attack. Cyber exploitation is hereby intended as referring to the unauthorized access to computers, computer systems, or networks, in order to exfiltrate information, but without affecting the functionality of the accessed system or amending/deleting the data resident therein. As has been observed, '[t]he primary technical difference between cyber attack and cyberexploitation is in the nature of the payload to be executed—a cyber attack payload is destructive whereas a cyberexploitation payload acquires information non-destructively'.[122] Although they are often labelled in the press as 'cyber attacks', then, cyber exploitation operations are different as they do not affect the system's operation. They focus on intelligence collection, surveillance, and reconnaissance rather than on system disruption and can be preliminary to a kinetic or cyber attack that they aim to enable, for instance by mapping the architecture of the network or operating system to be attacked or by identifying previously unknown vulnerabilities.[123] Stealing security data or intellectual property from governments and corporations could also be an aim in itself and is a major threat to national security and commerce.[124] 'Trapdoors' and

[118] US, Presidential Policy Directive/PPD–20, October 2012, p 2, <http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text>.

[119] US, Presidential Policy Directive 20, p 2.

[120] Presidential Policy Directive 20, p 3.

[121] US, Presidential Policy Directive 20, pp 2–3.

[122] Herbert S Lin, 'Offensive Cyber Operations and the Use of Force', *Journal of National Security Law and Policy* 4 (2010), p 64.

[123] Intelligence is 'any information concerning enemy forces and activities, as well as information necessary to facilitate one's own operations'. Surveillance is 'the systematic observation of areas, places, persons, or things, by visual, aural, electronic, photographic, or other means'. Reconnaissance is 'a single mission undertaken to obtain—by visual observation or other detection methods—specific information about the activities and resources of an enemy' (HPCR Manual, pp 320–1). See also *Joint Terminology for Cyberspace Operations*, p 11, according to which intelligence, surveillance and reconnaissance are '[a]n activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations'.

[124] As has been noted, 'the cyber context changes the scale and consequences of theft and espionage to a degree that can result in harm to the country at least as severe as a physical attack' (Jack Goldsmith, 'How Cyber Changes the Laws of War', 24 *European Journal of International Law* (2013), p 133).

'sniffers' are particularly useful tools to conduct this type of operations: the former allow an external user to access software at any time without the computer's owner being aware of it, while the latter are programs executed from a remote computer that intercept and record data passing over a network in order to steal user IDs and passwords.

On the other hand, cyber attacks are those cyber operations, whether in offence or in defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer system, or network. As will be seen,[125] a 'cyber attack' might be an 'armed attack' in the sense of Article 51 of the UN Charter or an 'attack' under Article 49(1) of Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of War, but care should be taken not to see these expressions as coterminous. In a military context, cyber attacks could be standalone operations, or used in conjunction with a subsequent kinetic or cyber operation that they aim to enable or facilitate, or be employed in armed conflict. A cyber attack can go from relatively innocuous psychological operations, such as website defacement, to acts that cause havoc in military campaigns by generating misinformation, or even acts resulting in major disruption of services and, material damage to property and loss of lives. In all cases, a cyber 'attack' involves an *action*, in offence or in defence, that is delivered in or through cyberspace, although not necessarily via a network, and could target either information systems or infrastructure control systems.[126] The former contain information but do not operate physical infrastructures, hence an attack on them causes loss or corruption of data but does not result in loss of functionality or material damage. The latter, of which a common type is SCADA systems, operate infrastructures: if corrupted, the consequence may be malfunctions or even physical damage.[127] For security

In the Moonlight Maze and Titan Rain operations, for instance, Russian and Chinese hackers stole sensitive information from the US DoD and Army's computers (Arie J Schaap, 'Cyber Warfare Operations: Development and Use Under International Law', *Air Force Law Review* 64 (2009), pp 141–2). As a consequence of the cyber intrusions allegedly originating from China, the US government adopted a new strategy to combat intellectual property theft (White House, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, February 2013) <http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>, on which see David P Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies', *ASIL Insights*, Vol 17, issue 10 (20 March 2013) <http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>).

[125] See Chapter 2, Section III.1 and Chapter 4, Section III.1.1.

[126] John Ricou Heaton, 'Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces', *Air Force Law Review* 57 (2005), p 161. While syntactic attacks target the operating system, ie the instructions contained in a software program, semantic attacks alter or delete information stored in a computer system to mislead those that rely on that information (for instance, geographical coordinates in navigation systems). Mixed attacks combine the two (Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?', *Goettingen Journal of International Law* 1 (2009), pp 378–9).

[127] Ricou Heaton, 'Civilians at War', p 161.

reasons, SCADAs are normally 'air gapped' from the internet and the attack can only be delivered from within the closed network or through local installation of malware by agents that have close access to the system.

The most used methods to conduct a cyber attack are the corruption of hardware ('chipping')[128] or software, or flooding the system with so much information to cause its collapse. Popular software tools designed to interfere with the normal functioning of a computer are Trojan horses, logic bombs, viruses, and worms, which can be installed in a computer through chipping, hacking, via a portable storage device, or by inadvertently downloading them from a website or an email attachment.[129] A virus is a self-replicating program that usually attaches itself to a legitimate program on the target computer, modifying it and subsequently affecting other programs and, if the computer is connected to a network, potentially other computers as well. A virus will normally carry a payload, which is the code that corrupts or deletes computer data on the affected computer. A worm replicates itself in its entirety into other computers but, unlike viruses, does not usually modify other programs: it captures the addresses of the target computer and resends messages throughout the system so to cause a general slowdown of the system and potentially a crash. Unlike a virus, a worm can spread without human intervention.[130] Viruses and worms can be hidden in Trojan horses, an apparently innocuous code fragment that actually conceals a harmful program or allows remote access to the computer by an external user. Time and logic bombs are a type of Trojan horse designed to execute at a specific time or by certain circumstances, respectively. Denial of Service (DoS) attacks, of which 'flood attacks' are an example, are different as they do not normally penetrate into the system but aim to inundate the target with excessive calls, messages, enquiries, or requests in order to overload it and force its shut down.[131] Permanent DoS attacks are particularly serious attacks that damage the system and cause its replacement or reinstallation of hardware.[132] When the DoS attack is carried out by a large number of computers organized in botnets, it is referred to as a DDoS attack.[133]

[128] 'Chipping' involves 'integrating computer chips with built-in weaknesses or flaws' (Todd A Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter', *Case Western Journal of International Law* 30 (1998), p 572).

[129] Stephen J Cox 'Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War', *Houston Law Review* 42 (2005–06), pp 888–9.

[130] Harrison Dinniss, *Cyber Warfare*, p 296.

[131] Richard E Overill, 'Denial of Service Attacks: Threats and Methodologies', *Journal of Financial Crime* 6 (1999), p 353. Worms are a form of DoS attack to the extent that, by replicating themselves in each network node, they render the targeted system incapable of performing its normal functions (p 351). Unlike 'flood attacks', however, worms imply an intrusion into the targeted system.

[132] Schaap, 'Cyber Warfare Operations', p 135.

[133] 'Botnets' (short for 'robot networks'), which are the source of most spam, are networks of infected computers hijacked from their unaware owners by external users: linked together, such networks can be used to mount massive DDoS attacks (Stewart Baker, Shaun Waterman, and George Ivanov, *In the Crossfire—Critical Infrastructure in the Age of Cyber War*, 2009, p 6, <http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf>). The Mariposa botnet, started in 2008, was one of the world's biggest with up to 12.7 million computers controlled (Charles Arthur, 'Alleged controllers of "Mariposa" botnet arrested in Spain', *The Guardian*, 3 March 2010,

III. The Applicable Law: *Inter (Cyber) Arma Enim Silent Leges*?

Cyber operations amount to internationally wrongful acts if they are inconsistent with a primary rule of international law and are attributed to a state under the secondary rules on state responsibility.[134] The latter will be discussed in Section IV of this Chapter. As to the primary rules, there is so far only one treaty that expressly and specifically addresses cyber activities. The 2001 Budapest Convention on Cybercrime, negotiated in the framework of the Council of Europe and entered into force on 1 July 2004, requires states parties to criminalize certain cyber offences in their domestic legislation, to extend their jurisdiction to offences originating from their territory or committed by their nationals, and to provide mutual assistance in investigations and prosecutions.[135] An Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems was also adopted in 2003 and entered into force on 1 March 2006. The Convention, however, excludes from its scope of application 'conduct undertaken pursuant to lawful governmental authority'[136] and therefore does not apply to cyber operations conducted by states.

The lack of ad hoc rules does not mean that cyber operations can be conducted by states without restrictions. As pointed out by Judge Simma, the view according to which the 'absence of a legal prohibition . . . constitute[s] the presence of a legal permission'[137] reflects 'an old, tired view of international law'.[138] It is this book's contention that existing treaty and customary norms can be extended to cyber operations by means of interpretation even though the relevant treaties and customs do not expressly contemplate them. It cannot also be excluded that specific customary international law provisions are in the process of developing in relation to at least certain aspects of the conduct of cyber operations by states. These arguments will be explored in turn in the next two Sections.

<http://www.guardian.co.uk/technology/2010/mar/03/mariposa-botnet-spain>). On botnets, see 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, DC: National Academies Press, 2009), pp 92–6; Liis Vihul, Christian Czosseck, Katharina Ziolkowski, Lauri Aasmann, Ivo A Ivanov, and Sebastian Brüggemann, *Legal Implications of Countering Botnets* (CCDCOE, 2012).

[134] While primary rules are rules about conduct, secondary rules regulate the creation, modification, interpretation, validity, termination of primary rules and the consequences of their violation. The distinction between primary and secondary rules in the context of the works on state responsibility was first used by Roberto Ago, Second Report on State Responsibility—The Origin of International Responsibility, *Yearbook of the International Law Commission*, 1970, Vol II, p 179.

[135] A Committee formed of the parties to the Convention meets twice a year in plenary to consult on matters related to the Convention.

[136] Cyber Crime Convention, Explanatory Report, para 38, <http://conventions.coe.int/Treaty/EN/Reports/html/185.htm>.

[137] Julius Stone, '*Non Liquet* and the Function of Law in the International Community', *British Year Book of International Law* 35 (1959), 136. The presumption was famously asserted by the Permanent Court of International Justice (PCIJ) in *The Case of the S.S. 'Lotus' (France v Turkey)*, Judgment No 9, 1927, PCIJ, Series A, No 10, p 18.

[138] *Accordance with international law of the unilateral declaration of independence in respect of Kosovo*, Advisory Opinion, 22 July 2010, ICJ Reports 2010, Declaration of Judge Simma, para 2.

1. The applicability of existing treaties to cyber operations conducted by states

Together with customary international law, treaties are one of the two sources of international law.[139] Rules on the creation, interpretation, termination, and invalidity of treaties have been codified in the 1969 Vienna Convention on the Law of Treaties (entered into force in 1980), whose Article 2(1)(a) defines a treaty as 'an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation'.[140]

Although treaties have been concluded in all areas of international relations, those cyber operations that amount to a use of force or to acts of hostilities would fall within the provinces of international law that regulate the right of states to use force (*jus ad bellum*) and the conduct of warfare once an armed conflict has broken out (*jus in bello*, or the law of armed conflict, or international humanitarian law).[141] In the absence of ad hoc treaty regulation, the question is whether existing treaties that apply to traditional uses of force can be extended to cyber operations. The key *jus ad bellum* and *jus in bello* treaties are the 1945 Charter of the United Nations, the Hague Conventions of 1899 and 1907, the four 1949 Geneva Conventions on the Protection of Victims of War and their two 1977 Additional Protocols. It goes without saying that, for obvious historical reasons, none of the above texts refers to cyber issues. In the Advisory Opinion on the *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, however, the International Court of Justice (ICJ) found that 'an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation'.[142] The concept of 'dynamic' or evolutive, interpretation, which is also implied in Article 31(3)(b) of the Vienna Convention on the Law of Treaties,[143] was employed again by the Court in a subsequent Judgment, where it held that

> where parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered

[139] See Art 38 of the Statute of the ICJ.

[140] The text of the Convention is in UNTS, Vol 1155, pp 331 ff. On the law of treaties, see Anthony Aust, *Modern Treaty Law and Practice*, 3rd edn (Cambridge: Cambridge University Press, 2013); Malgosia Fitzmaurice and Olufemi Elias, *Contemporary Issues in the Law of Treaties* (Utrecht: Eleven Publishing, 2005).

[141] Although there are slight differences of meaning in these expressions, they will be used as synonymous.

[142] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* Advisory Opinion, 21 June 1971, ICJ Reports 1971, para 53.

[143] According to Art 31(3)(b) of the Vienna Convention, treaties shall be interpreted taking into account, inter alia, 'any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation' (text in UNTS, vol 1115, pp 331 ff). Such practice includes 'documents, arrangements, and actions that express a specific understanding of the treaty' (Matthias Herdegen, 'Interpretation in International Law', in *Max Planck Encyclopedia of Public International Law* (2012), Vol VI, p 263). See also Rudolf Bernhardt, 'Evolutive Treaty Interpretation, Especially of the European Convention on Human Rights', *German Yearbook of International Law* 42 (1999), p 15.

into for a very long period or is 'of continuing duration', the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning.[144]

An 'interpretive reorientation'[145] of existing *jus ad bellum* and *jus in bello* provisions to accommodate cyber technology finds support in the fact that many states have affirmed the application of existing laws, including the UN Charter and the law of armed conflict, to cyber operations, often without distinguishing between treaties and customary norms. In a speech at the US CYBERCOM, the then Legal Advisor of the US State Department, Harold Koh, emphasized that 'international law principles do apply in cyberspace', including (but not limited to) the *jus ad bellum* and the *jus in bello*.[146] The White House's *International Strategy for Cyberspace* explains that '[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete'.[147] When submitting its views to the UN Secretary-General on information security, the United States also declared that '[d]espite the unique attributes of information and communications technologies, existing principles of international law serve as the appropriate framework within which to identify and analyse the rules and norms of behaviour that should govern the use of cyberspace in connection with hostilities'.[148] The 2012 US National Defense Authorization Act clarified that offensive cyber operations in cyberspace are subject, inter alia, to 'the policy principles and legal regimes that the Department [of Defense] follows for kinetic capabilities, including the law of armed conflict'.[149] Other states and international organizations that have affirmed the applicability of the existing law on the use of force and the law of armed conflict to cyber operations include Australia,[150] China,[151] Cuba,[152] the European

[144] *Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)*, Judgment, 13 July 2009, ICJ Reports 2009, para 66.

[145] Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', *Yale Journal of International Law* 36 (2011), p 437. A leading commentary of the UN Charter, for instance, suggests that 'the rules on treaty interpretation and on the sources of international law do not exclude the possibility that Art 51 is reinterpreted, including on the basis of subsequent practice' (Albrecht Randelzhofer and Georg Nolte, 'Article 51', in *The Charter of the United Nations—A Commentary*, edited by Bruno Simma, Daniel-Erasmus Kahn, Georg Nolte, and Andreas Paulus, 3rd edn, Vol 2 (Oxford: Oxford University Press, 2012), p 1400).

[146] CarrieLyn D Guymon (ed), *Digest of United States Practice in International Law*, 2012, p 594.

[147] International Strategy for Cyberspace, p 9. See also US DoD, *Cyberspace Policy Report. A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934, November 2011, p 9, <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf> ('[i]nternational legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e. sea, air, land, and space), also apply to the cyberspace domain').

[148] UN Doc A/66/152, 15 July 2011, p 18.

[149] National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 5 January 2012, Section 954, p 254, <http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf>. See also US Presidential Policy Directive 20, p 4.

[150] UN Doc A/66/152, 15 July 2011, p 6.

[151] Zhang, 'A Chinese Perspective', p 4.

[152] UN Doc A/57/166/Add.1, 29 August 2002, p 3.

Union,[153] Hungary,[154] Iran,[155] Italy,[156] Mali,[157] the Netherlands,[158] Qatar,[159] the Russian Federation,[160] the United Kingdom.[161] On the basis of the views submitted by the UN member states, the 2013 Report of the GGE set up by the UN General Assembly was able to find that '[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [Information and Communications Technologies] environment'.[162]

With specific regard to international humanitarian law, the so-called Martens Clause provides, in its latest codification, that

> [i]n cases not covered by this Protocol or by other international agreements, 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.[163]

The Clause may be invoked in the interpretation of international humanitarian law treaties both to rule out that what is not expressly prohibited is permitted and as a presumption that favours humanitarian considerations whenever doubts exist on the meaning of certain provisions.[164] As such, the Clause can be used to found the extension of existing principles and rules to new weaponry so to avoid gaps in legal regulation. In its *Nuclear Weapons* Advisory Opinion, the ICJ found that the Martens Clause is 'an effective means of addressing the rapid evolution of military technology'.[165] According to the ICRC Commentary of Additional Protocol I, the Clause 'prevents the assumption that anything which is not explicitly prohibited by

[153] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013, pp 15–16, <http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667>. See also Speech by EU High Representative Catherine Ashton on Cyber security: An open, free and secure internet, Budapest, 4 October 2012, p 3, <http://europa.eu/rapid/press-release_SPEECH-12-685_en.htm>.

[154] Budapest Conference on Cyberspace, Opening Session, 4 October 2012, Welcome speech by János Martonyi, Minister of Foreign Affairs of Hungary, <http://www.cyberbudapest2012.hu/welcome-speech-by-janos-martonyi-hungarian-minister-of-foreign-affairs>.

[155] Alireza Miryousefi and Hossein Gharibi, 'View from Iran: World needs rules on cyberattacks', *The Christian Science Monitor*, 14 February 2013, <http://www.csmonitor.com/Commentary/Opinion/2013/0214/View-from-Iran-World-needs-rules-on-cyberattacks-video>.

[156] Governo italiano, *La posizione italiana sui principi fondamentali di Internet*, 17 September 2012, p 5, <http://www.governo.it/backoffice/allegati/69257-8014.pdf>.

[157] UN Doc A/64/129/Add.1, 9 September 2009, p 7.

[158] Dutch Government Response to the AIV/CAVV Report on Cyber Warfare, pp 5–6.

[159] UN Doc A/65/154, 20 July 2010, pp 9–10.

[160] *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*, 9 September 2000, p 6, <http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf> (CCDCOE's unofficial translation).

[161] UN Doc A/65/154, 20 July 2010, p 15.

[162] UN Doc A/68/98, 24 June 2013, p 8.

[163] Article 1(2) of Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of International Armed Conflicts, text in UNTS, Vol 1125, pp 3 ff.

[164] Antonio Cassese, 'The Martens Clause: Half a Loaf or Simply Pie in the Sky?', *European Journal of International Law* 11 (2000), pp 189–90, 212–13.

[165] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports 1996 ('*Nuclear Weapons*'), para 78.

the relevant treaties is therefore permitted' and proclaims 'the applicability of the principles mentioned regardless of subsequent developments of types of situation or technology'.[166] The fact that international humanitarian law treaties can extend to weapons developed after their adoption is also confirmed by the inclusion in Protocol I Additional to the Geneva Conventions of Article 36, which states that

> [i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[167]

In the ICRC's view, then, 'means and methods of warfare which resort to cyber technology are subject to IHL [international humanitarian law] just as any new weapon or delivery system has been so far when used in an armed conflict by or on behalf of a party to such conflict. If a cyber operations [*sic*] is used against an enemy in an armed conflict in order to cause damage, for example by manipulation of an air traffic control system that results in the crash of a civilian aircraft, it can hardly be disputed that such an attack is in fact a method of warfare and is subject to prohibitions under IHL'.[168] At the United Nations, the ICRC recalled 'the obligation of all parties to conflicts to respect the rules of international humanitarian law if they resort to means and methods of cyberwarfare, including the principles of distinction, proportionality and precaution'.[169] It should also be noted that the parties to a conflict can always conclude special agreements between themselves to expand their obligations under international humanitarian law.[170] Agreements may be concluded, for instance, to clarify the application of the *jus in bello* to cyber operations in a particular conflict, or to submit to special protection certain data, software and cyber infrastructure.

The problem with the extension of existing rules and principles to new scenarios such as cyber operations is that they do not take into account their uniqueness and might prove to be too general. As a product of the Westphalian order, for instance, existing rules of international law apply to and imply the existence of territory with geographical borders over which states exercise sovereignty or at least jurisdiction, while cyberspace is an apparently borderless, ever changing man-made domain. As has been observed, however, 'components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction'.[171] In fact, it should

[166] Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Dordrecht: Nijhoff, 1987), para 55.

[167] On this provision, see also Chapter 4, Section II, p 170 ff.

[168] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, pp 36–7, <http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf>.

[169] UN Doc A/C.1/66/PV.9, 11 October 2011, p 21.

[170] See Art 3(3) Common to the Geneva Conventions; Art 6 of Geneva Conventions I, II, and III; Art 7 of Geneva Convention IV. The text of the Conventions is in UNTS, Vol 75, pp 31 ff, 85 ff, 135 ff, 287 ff.

[171] Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', *International Law Studies* 89 (2013), p 126. See also Eneken Tikk, 'Ten Rules for Cyber Security',

not be forgotten that cyberspace consists of physical and syntactic (or logical) layers: the former includes the physical infrastructure through which the data travel wired or wireless, including servers, routers, satellites, cables, wires, and the computers, while the latter includes the protocols that allow data to be routed and understood, as well as the software used and the data.[172] Cyber operations can thus be seen as 'the reduction of information to electronic format and the actual movement of that information between physical elements of cyber infrastructure'.[173] The internet itself is nothing else than 'a set of inter-connected computer networks linked to state territory and, thus, is liable to the exercise of sovereign jurisdiction on a territorial basis'.[174] Cyber operations, then, can be 'territorialized' by focusing on the location of the cyber infrastructure used to conduct the operations and on where the effects occur. [175] Therefore, '[i]f a cyber action will result in kinetic or kinetic-like effect (e.g., changing the function of a physical system, or file manipulation that results in a financial loss), the target location is the physical location of the effect'.[176] In its 2013 Report, the GGE confirmed that 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.[177]

2. The role of customary international law

While treaties must be respected only by those states that have ratified them, customary rules are binding on all subjects of international law (with the exception

Survival 53 (June–July 2011), p 121 ('Information infrastructure located within a state's territory is subject to that state's territorial sovereignty'). See Rules 1–3 of the Tallinn Manual, pp 15–23.

[172] David J Betz and Tim Stevens, 'Analogical Reasoning and Cyber Security', *Security Dialogue* 44 (2013), p 151; Jonathan Zittrain, 'A Mutual Aid Treaty for the Internet', Governance Studies at Brookings, 27 January 2011, p 5, <http://www.brookings.edu/research/papers/2011/01/27-internet-treaty-zittrain>. See also Duncan B Hollis, 'Stewardship Versus Sovereignty? International Law and the Apportionment of Cyberspace', CyberDialogue 2012, March 2012, p 7, <http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hollis.pdf>; Johann-Christoph Woltag, 'Computer Network Operations Below the Level of Armed Force', ESIL Conference Paper no 1/2011, pp 16–17, <http://www.esil-sedi.eu/node/82>.

[173] Nils Melzer, *Cyberwarfare and International Law*, UNIDIR, 2011, p 5, <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=134218>.

[174] Teresa Scassa and Robert J Currie, 'New First Principles? Assessing the Internet's Challenges to Jurisdiction', *Georgetown Journal of International Law* 42 (2011), p 1079.

[175] On the exercise of the principles of territorial sovereignty and territorial jurisdiction in cyberspace, see Heintschel von Heinegg, 'Territorial Sovereignty', p 134. China has for instance claimed that 'the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded' and that 'each country has the right to manage its own cyberspace in accordance with its domestic legislation' (UN Doc A/61/161, 18 July 2006, p 4). Venezuela has also stated that 'any violation of information security is contrary to the legitimate right of States to full exercise of their sovereignty' (UN Doc A/59/116/Add.1, 28 December 2004, p 6). The United States is exploring ways to define national borders in cyberspace (Scott D Applegate, 'The Principle of Maneuver in Cyber Operations', in *2012 4th International Conference on Cyber Conflict*, edited by Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (CCDCOE, 2012), p 192).

[176] *Joint Terminology for Cyberspace Operations*, p 14.

[177] UN Doc A/68/98, 24 June 2013, p 8.

of local customs and, possibly, the case of persistent objectors).[178] There is no hierarchy between the two sources: treaties can amend or repeal a custom and vice versa, with prevalence determined by principles like *lex posterior derogat priori* and *lex specialis derogat generali* (subsequent and special laws prevail over previous and general laws). Article 38(1) of the ICJ Statute defines customary international law as 'evidence of a general practice accepted as law'. Customary international law, which is generally non-written, is then created by the convergence of two elements: practice (*usus*, or *diuturnitas*) by a sufficiently representative number of states and other subjects of international law (for instance, international organizations) and 'evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it'[179] or, at least, by social, political or economic exigencies (*opinio juris ac necessitatis*).[180]

The role of customary international law in relation to cyber operations is twofold. First, existing *jus ad bellum* and *jus in bello* customary rules extend to cyber operations amounting to a use of force or acts of hostilities, respectively, in the same way as the relevant treaty provisions do: what has been written in the previous Section, then, applies to customary norms as well. From this point of view, '[t]here is no need for State practice to develop separately as regards every concrete weapon employed in an armed attack'.[181] Secondly, it cannot be excluded that customary international law rules specific to cyber warfare might be in the process of forming and eventually ripen. In this regard, more than ten years ago D'Amato predicted that 'computer network attack will soon be the subject of an outright prohibition under customary international law'.[182] Other commentators, however, have been more sceptical and have argued that no customary international law has yet developed because the phenomenon is still too recent and there is no state practice.[183] The Introduction of the Tallinn Manual adopts a more cautious approach and explains that 'because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists'.[184] In order to verify whether these affirmations are correct, one has first to establish

[178] Tullio Treves, *Diritto internazionale* (Milano: Giuffrè, 2005), pp 233–5.

[179] *North Sea Continental Shelf (Germany v Denmark/The Netherlands)*, Judgment, 20 February 1969, ICJ Reports 1969 ('*North Sea Continental Shelf*'), para 77; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)*, Merits, Judgment, 27 June 1986, ICJ Reports 1986 ('*Nicaragua*'), para 183; *Nuclear Weapons*, para 64.

[180] Antonio Cassese, *International Law*, 2nd edn (Oxford: Oxford University Press, 2005), p 156.

[181] Yoram Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference', *International Law Studies* 89 (2013), p 280.

[182] Anthony D'Amato, 'International Law, Cybernetics, and Cyberspace', *International Law Studies 76* (2002), p 69.

[183] See Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', *Columbia Journal of Transnational Law* 37 (1998–99), p 921, who concludes that '[a] customary norm may develop over time, but it does not exist at present' as '[n]either practice, nor *opinio juris*, is in evidence'; Shackelford, 'From Nuclear War', p 219.

[184] Tallinn Manual, p 5.

what amounts to state practice.[185] If it is indeed impossible to find cyber operations clearly attributable to states, *usus* as an element of custom also includes '[v]erbal acts, and not only physical acts, of States', such as '[d]iplomatic statements (including protests), policy statements, press releases, official manuals (e.g. on military law), instructions to armed forces, comments by governments on draft treaties, legislation, decisions of national courts and executive authorities, pleadings before international tribunals, statements in international organizations and the resolutions those bodies adopt'.[186] When describing state practice, the 2005 ICRC Study of *Customary International Humanitarian Law* also lists 'military manuals, national legislation, national case-law, instructions to armed and security forces, military communiqués during war, diplomatic protests, opinions of official legal advisers, comments by governments on draft treaties, executive decisions and regulations, pleadings before international tribunals, statements in international organizations and at international conferences and government positions taken with respect to resolutions of international organizations'.[187]

Military manuals, in particular, are an important element of state practice.[188] In the *Tadić* case, the International Criminal Tribunal for the former Yugoslavia (ICTY)'s Appeals Chamber famously found that '[w]hen attempting to ascertain State practice with a view to establishing the existence of a customary rule or a general principle, it is difficult, if not impossible, to pinpoint the actual behaviour of the troops in the field for the purpose of establishing whether they in fact comply with, or disregard, certain standards of behaviour'.[189] This is because 'not only is access to the theatre of military operations normally refused to independent observers (often even to the ICRC) but information on the actual conduct of

[185] The UN International Law Commission (ILC) has included the formation and evidence of customary international law in its programme of work. In 2013, a First Report was published by the Special Rapporteur, Sir Michael Wood (UN Doc A/CN.4/663, 17 May 2013).

[186] *Statement of Principles Applicable to the Formation of General Customary International Law*, in International Law Association (ILA), Report of the Sixty-Ninth Conference (London, 2000), p 725. See also Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge: Cambridge University Press, 2005), Vol I, p xxxii; Ian Brownlie, *Principles of Public International Law*, 7th edn (Oxford: Oxford University Press, 2008), pp 6–7; Tullio Treves, 'Customary International Law', in *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press, 2012), Vol II, p 940; Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge: Cambridge University Press, 2010), p 10; Michael Wood, 'State Practice', *Max Planck Encyclopedia of Public International Law* (2012), Vol IX, p 510. As Gray maintains, interpreting state practice means looking at what states say, not necessarily at what they do (Christine Gray, *International Law and the Use of Force* (Oxford: Oxford University Press, 2008), p 418).

[187] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Vol I, p xxxviii. These documents are at the same time state practice and evidence of *opinio juris*: in fact, '[i]t is . . . often difficult or even impossible to disentangle the two elements' (ILA, *Statement of Principles*, p 718). See also Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts* (Oxford and Portland: Hart, 2008), p 52.

[188] According to Garraway, '[w]hereas international manuals seek to provide an agreed version of the law, national manuals provide evidence of state practice and *opinio juris* in relation to the states by which they are issued' (Charles Garraway, 'The Use and Abuse of Military Manuals', *Yearbook of International Humanitarian Law* 7 (2004), p 431).

[189] *Prosecutor v Tadić*, Case No IT–94–1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para 99.

hostilities is withheld by the parties to the conflict; what is worse, often recourse is had to misinformation with a view to misleading the enemy as well as public opinion and foreign Governments'.[190] These words are even more fitting in the cyber scenario. The Appeals Chamber concluded that '[i]n appraising the formation of customary rules or general principles one should… be aware that, on account of the inherent nature of this subject-matter, reliance must primarily be placed on such elements as official pronouncements of States, military manuals and judicial decisions'.[191] Even if one must be 'cautious not to infuse them with a normative character that may have been unintended by the promulgating States',[192] then, military manuals 'are directly relevant for what states, or more precisely, the armed forces as a state's organ whose practice is relevant for the purposes here discussed, actually do'.[193] Unfortunately, most military manuals have been adopted before 2000 and therefore do not expressly refer to military cyber operations. To the best of this author's knowledge, the only exceptions are the British *Manual of the Law of Armed Conflict*[194] and the US *Commander's Handbook on the Law of Naval Operations*,[195] which only contain cursory references to cyber operations.

On the other hand, a significant number of states have adopted cyber security strategies and doctrines that often contain express and extensive references to international law: as has been observed, 'legal evolution is likely to occur in significant part through defensive planning doctrine and declaratory policies issued in advance of actual cyber-attack crises'.[196] As 'official pronouncements of States', 'policy statements' and 'instructions to armed and security forces', these documents are not only helpful as an assistance in treaty interpretation, but can also be evidence of state practice and could declare, and seek to impose on those who are subject to its guidance, a certain *attitude* to the law, or an *interpretation* of the law, or an operational *intent* that relates to existing law either supportively or in

[190] *Tadić*, Decision on the Defence Motion, para 99.

[191] *Tadić*, Decision on the Defence Motion, para 99.

[192] Michael N Schmitt, 'The Law of Targeting', in *Perspectives on the ICRC Study on Customary International Humanitarian Law*, edited by Elizabeth Wilmshurst and Susan Breau (Cambridge: Cambridge University Press, 2007), p 134. See also Garraway, 'The Use and Abuse', p 440. According to Post, the position of military manuals in international law 'largely corresponds to that of national legislation, i.e., as having evidentiary value' (Harry HG Post, 'Some Curiosities in the Sources of the Law of Armed Conflict Conceived in a General International Legal Perspective', in *Diversity in Secondary Rules and the Unity of International Law*, edited by Lambertus ANM Barnhoorn and Karel C Wellen (The Hague, Boston, London: Nijhoff, 1995), p 100).

[193] Michael Bothe, 'Comments', in *International Economic Law and Armed Conflict*, edited by Harry HG Post (Dordrecht: Nijhoff, 1994), p 35. See also Yoram Dinstein, 'The Creation of Customary International Law', *Recueil des cours* 322 (2006) 2006, p 272 ('military manuals—published by the high command as binding instructions to the armed forces—constitute meaningful signposts on the road leading to custom-making'); Post, 'Some Curiosities', p 99 ('[m]ilitary manuals of the most powerful nations may certainly be said to have played (and still do play) an important role in the formative process of the customary law of armed conflict').

[194] UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (Oxford: Oxford University Press, 2004), p 118.

[195] *The Commander's Handbook on the Law of Naval Operations*, July 2007, pp 8–17, <http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/>.

[196] Matthew C Waxman, 'Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions', *International Law Studies* 89 (2013), p 116.

some problematic way'.[197] It is true that they mostly reflect policy, and not legal, considerations, but when they expressly refer to international law one cannot see why they should be denied any value: as Matthew Waxman suggests, 'legal analysis and development cannot be divorced from strategy and politics'.[198]

Finally, *usus* also includes official statements made by states, including those in debates in international fora such as the UN organs.[199] As has already been noted, for instance, the UN General Assembly invited the UN member states to submit their views on information security to the Secretary-General. '[O]pinions of official legal advisers' are also a particularly valuable example of verbal acts: a notable case is the speech on international law in cyberspace pronounced by the then US State Department's Legal Advisor, Harold Koh, at the US CYBERCOM.[200]

State practice, however, must be 'extensive and virtually uniform'.[201] True, documents and statements on the legal aspects of military cyber operations come from a relatively limited number of states, but this is not an insurmountable obstacle to the formation of a custom. As Guzman observes, '[f]or many rules of CIL [customary international law], powerful states dominate the question of state practice. The group may grow still smaller once it is recognized that only states with a stake in the issue must be considered'.[202] The ILA Report on the formation of customary international law points out that the extensive character of state practice is more a qualitative than a quantitative criterion: 'if all major interests ("specially affected States") are represented, it is not essential for a majority of States to have participated (still less a great majority, or all of them)'.[203] Specially affected states are primarily those that had the opportunity to engage in the relevant practice. The ICRC Study on *Customary International Humanitarian Law* argues, for instance, that, in relation to the legality of blinding weapons, the specially affected states include those that are developing such weapons.[204] It is, therefore, at the states that have developed military cyber capabilities that one has to mainly look at in order to establish whether any 'general practice accepted as law' has sedimented.

Furthermore, the fact that cyber operations are still a relatively new phenomenon does not necessarily prevent the formation of customary international law. The ICJ famously found 'that the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law'.[205]

[197] Alyson JK Bailes and Anna Wetter, 'Security Strategies', in *Max Planck Encyclopedia of Public International Law* (2012), Vol IX, p 87 (emphasis in original).
[198] Waxman, 'Self-Defensive force', p 110.
[199] Wood, 'State Practice', p 512.
[200] Guymon (ed), *Digest of United States Practice*, pp 593 ff.
[201] The ICJ found that 'an indispensable requirement would be that within the period in question, short though it might be, State practice…should have been both extensive and virtually uniform in the sense of the provision invoked;—and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved' (*North Sea Continental Shelf*, para 74).
[202] Andrew T Guzman, 'Saving Customary International Law', *Michigan Journal of International Law* 27 (2005–06), p 151.
[203] ILA, *Statement of Principles*, p 737.
[204] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Vol I, p xxxviii.
[205] *North Sea Continental Shelf*, para 74.

Therefore, '[s]ome customary rules have sprung up quite quickly: for instance, sovereignty over air space, and the régime of the continental shelf, because a substantial and representative quantity of State practice grew up rather rapidly in response to a new situation'.[206] The idea of fast-developing customs, or *diritto spontaneo*, was elaborated by Roberto Ago almost sixty years ago:[207] the unusual rapidity by which certain customary international law rules have crystallized allegedly occurs in periods of fundamental and unprecedented changes, for instance because of technological advances.[208] In such 'Grotian moments', *opinio juris* becomes more important than *usus*.[209] In international humanitarian law, the subordination of practice to *opinio* in relation to norms based on the laws of humanity or the dictates of public conscience may also be inferred from the above-mentioned Martens Clause.[210] The ICTY, for instance, found that the Clause 'clearly shows that principles of international humanitarian law may emerge through a customary process under the pressure of the demands of humanity or the dictates of public conscience, even when State practice is scant or inconsistent. The other element, in the form of *opinio necessitatis*, crystallising as a result of the imperatives of humanity or public conscience, may turn out to be the decisive element heralding the emergence of a general rule or principle of humanitarian law'.[211] Therefore, international humanitarian law customs may arise even in the absence of extensive and uniform operational state practice, providing that a significant number of specially affected states have expressed their legal views on the matter.[212] A not too dissimilar approach was adopted by the ICJ when it founded the customary nature of certain treaty provisions of international humanitarian law on 'elementary considerations of humanity', without accompanying this view with conclusive evidence of state practice.[213]

[206] ILA, *Statement of Principles*, p 731.

[207] Roberto Ago, 'Science juridique et droit international', *Recueil des cours* 90 (1956–II), pp 931 ff.

[208] Michael P Scharf, 'Seizing the "Grotian Moment": Accelerated Formation of Customary International Law in Times of Fundamental Change', *Cornell International Law Journal* 43 (2010), pp 444, 450.

[209] Scharf, 'Seizing', p 468.

[210] Cassese, 'The Martens Clause', p 214. See also Dieter Fleck, 'State Responsibility Consequences of Termination of or Withdrawal from Non-proliferation Treaties', in *Non-proliferation Law as a Special Regime*, edited by Daniel H Joyner and Marco Roscini (Cambridge: Cambridge University Press, 2012), p 259; Theodor Meron, 'The Martens Clause, Principles of Humanity, and Dictates of Public Conscience', *American Journal of International Law* 94 (2000), pp 87–8.

[211] *Prosecutor v Kupreskić*, Case no IT-95-16-T, Trial Chamber Judgment, 14 January 2000, para 527. See Cassese, 'The Martens Clause', p 214; Robert Kolb, 'Selected Problems in the Theory of Customary International Law', *Netherlands International Law Review* 50 (2003), p 124.

[212] Cassese, 'The Martens Clause', p 214; Meron, 'The Martens Clause', p 88. It has been argued that this applies not only to international humanitarian law, but also to the rules on the use of force, 'where the practice is difficult to weigh, as much for what is done as for what is not done' (Kolb, 'Selected Problems', p 129).

[213] See eg *Nicaragua*, para 218 (with regard to Common Art 3 of the 1949 Geneva Conventions on the Protection of Victims of War). See the comments of Giulio Bartolini, 'Armed Forces and the International Court of Justice: The Relevance of International Humanitarian Law and Human Rights Law to the Conduct of Military Operations', in *Armed Forces and International Jurisdictions*, edited by Marco Odello and Francesco Seatzu (Cambridge, Antwerp, Portland: Intersentia, 2013), pp 61–2.

It can be concluded that 'the prevailing position continues to demand fulfilment of the classic two elements of State practice and *opinio juris* [but] there is also a clear tendency not to follow the two elements as strictly as originally envisaged'.[214] In particular, and in spite of some isolated, if influential, contrary views,[215] it is now generally accepted that practice can consist not only of actions, but also of verbal acts, and that the subjective element could be decisive in the formation of customs, especially in the case of prohibitory rules of international humanitarian law.[216] Of course, stating that customary international law specific to cyber operations has already formed exclusively on the basis of cyber security strategies, a few military manuals and a limited number of unattributed cyber attacks would certainly be an exaggeration. At least some uniform operational practice, in addition to verbal acts, seems necessary to avoid natural law setbacks.[217] This, however, does not mean that verbal acts could not indicate *trends* of the direction towards which customary international law is starting to develop in this area, trends that it is useful to identify also from the perspective of a future, if still uncertain, treaty regulating cyber warfare. It is in this light that the present book will examine the above-mentioned documents.

3. The *Tallinn Manual on the International Law Applicable to Cyber Warfare*

If, therefore, existing international law applies in the cyber context, the lawyer's task is to examine the traditional norms, conceived in relation to kinetic scenarios, and identify potential difficulties in their application to different types of cyber operations. It is from this perspective that NATO's CCDCOE invited a group of experts to prepare the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, published in early 2013.[218] The Manual, that aims to identify how the *lex lata* applies to cyber operations above the level of the use of force, includes a set of 95 Rules accompanied by commentaries and does not reflect NATO doctrine or

[214] Robert Heinsch, 'Methodology of Law-Making. Customary International Law and New Military Technologies', in *International Humanitarian Law and the Changing Technology of War*, edited by Dan Saxon (Leiden: Brill, 2013), p 36.

[215] See the response of the United States to the ICRC Study, according to which 'the Study places too much emphasis on written materials, such as military manuals and other guidelines published by States, as opposed to actual operational practice by States during armed conflict' (John B Bellinger, III and William J Haynes, II, 'A US Government Response to the International Committee of the Red Cross Study *Customary International Humanitarian Law*', *International Review of the Red Cross* 89 (2007), p 445). The United States, however, does not deny that verbal acts can amount to state practice but only that they can replace operational practice, and actually recognizes that military manuals are 'important indications of State behavior and *opinio juris*' (p 445).

[216] Heinsch, 'Methodology', pp 25–6.

[217] Heinsch, 'Methodology', p 35.

[218] Tallinn Manual, p 5. The CCDCOE has also published a National Cyber Security Framework Manual, which focuses on law enforcement in peacetime (Alexander Klimburg (ed), *National Cyber Security Framework Manual* (CCDCOE, 2012), <http://ccdcoe.org/369.html>).

the official position of any state or organization.[219] It is essentially a scholarly exercise and its rules are of course not binding.[220]

The Manual has been criticized in relation to the composition of the Group of Experts, the methodology employed, its scope, and certain aspects of its contents.[221] The Group of Experts that drafted the Manual comprised international law academics, practitioners, serving or former military officials, technical experts, as well as observers from NATO, the ICRC, and the US CYBERCOM, all participating in their personal capacity. It included, however, only 'military and academic lawyers and technical experts from but a few Western states'.[222] It is indeed a fact that, of the 23 members of the Group of Experts, nine (including the Project's Director) were from the United States, while none was from states that are reportedly heavily involved in cyber operations, both as authors and targets, such as Russia, China, Iran, or Israel.[223] If this can certainly be seen as a limitation, it should not be forgotten that the members participated in the initiative in their individual capacity: even if a Russian expert had been invited, he or she would have not necessarily expressed the views of the Russian government.

As to the methodology employed, only the conclusions on which unanimity among the Group of Experts (but not the observers) was reached were translated into black-letter rules: the most controversial international law aspects of cyber operations were therefore left unresolved, although the divergent positions were noted in the Commentary.[224] Overall, it seems fair to say that the Experts were very cautious to avoid taking any risks when drafting the rules, which are often a mere restatement of existing treaty provisions with the addition of the adjective 'cyber'.[225] In addition to the relevant treaties, the sources used by the Group of Experts include the ICJ jurisprudence as well as the case law of international criminal tribunals, in particular the ICTY, and the works of the ILC. The Manual also heavily relies on the ICRC Commentaries to the Geneva Conventions and Additional Protocols and on more or less successful private codifications, such as the above-mentioned HPCR Manual, the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*,[226] and the *Manual on the Law of*

[219] Tallinn Manual, p 11. Although it took part in the drafting of the Manual, in particular, the ICRC did not endorse all the views expressed therein (Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians', *International Review of the Red Cross* 94 (2012), p 541).

[220] Tallinn Manual, p 11.

[221] Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New *Tallinn Manual*', *Journal of Conflict and Security Law* 18 (2013), pp 331 ff.

[222] Fleck, 'Searching for International Rules', p 335.

[223] See the critical comments of Rain Liivoja and Tim McCormack, 'Law in the Virtual Battlespace: The Tallinn Manual and the *Jus in Bello*', Melbourne Legal Studies Research Paper no 650, 23 July 2013, pp 4, 12, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2297159>.

[224] Tallinn Manual, pp 5–6. See the critical review of Fleck, 'Searching for International Rules', pp 336 ff.

[225] The Manual itself acknowledges that '[a]t times, the text of a Rule closely resembles that of an existing treaty norm' (Tallinn Manual, p 6).

[226] *San Remo Manual on International Law Applicable to Armed Conflicts at Sea, Prepared by a Group of International Lawyers and Naval Experts Convened by the International Institute of Humanitarian*

Non-International Armed Conflict,[227] as well as on the ICRC Study on *Customary International Humanitarian Law*, although in a 'persuasive, but not dispositive' function.[228] With regard to national sources, the Manual's Commentary essentially refers to the military manuals of only four states (Germany, Canada, the United Kingdom, and the United States) on the basis that they are considered 'especially useful', that some members of the Group of Experts participated in their drafting and that they are publicly available.[229] This very narrow selection, however, should have been more extensively justified, and in any case other manuals would have met the identified selection criteria. Finally, the Manual refers to only one cyber security strategy, the 2011 White House's *International Strategy for Cyberspace*, and overlooks the many others that have been adopted, which are often more explicit and more significant.

The Manual only briefly addresses, or does not address at all, important issues.[230] In particular, there is little analysis of how the principle of non-intervention applies to cyber operations.[231] This is particularly troublesome if one considers that the Group of Experts was not able to conclusively establish the threshold for cyber operations to be considered a use of force. There is also little discussion of cyber exploitation operations, even though they could also qualify as acts of hostilities.[232] Furthermore, the Manual does not discuss at length crucial problems such as attribution criteria and evidentiary standards.[233] On the other hand, it is not clear why Rule 24, an international criminal law provision, was included in a *jus ad bellum*/*jus in bello* codification.[234]

Only time will tell whether the Tallinn Manual will be as successful as the *San Remo Manual on Armed Conflict at Sea* in influencing state conduct. Although, as the Commentary itself acknowledges, 'any claim that every assertion in the Manual represents an incontrovertible restatement of international law would be an exaggeration',[235] the Manual is, in any case, a good starting point for further analysis and should be commended for advancing the understanding of the international law applicable to cyber warfare. The present book will therefore often refer to it.

Law. Text in Adam Roberts and Richard Guelff, *Documents on the Laws of War* (Oxford: Oxford University Press, 2000), pp 573 ff.

[227] Michael N Schmitt, Charles HB Garraway, and Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict With Commentary* (Sanremo: International Institute of Humanitarian Law, 2006), <http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf>.

[228] Tallinn Manual, p 8. [229] Tallinn Manual, p 8.

[230] Fleck, 'Searching for International Rules', pp 346 ff.

[231] See Tallinn Manual, pp 44–5. The principle of non-intervention in the cyber context is discussed below, Chapter 2, Section II.1.3.

[232] See Tallinn Manual, pp 192–5. See Chapter 4, Section IV of this book.

[233] The only references to evidence are contained in Rules 7 and 8 (Tallinn Manual, pp 34–6). See Section IV of this Chapter and Section III.6 of Chapter 2.

[234] Tallinn Manual, p 91. [235] Tallinn Manual, p 5.

IV. Identification and Attribution Problems

Well before the cyber age, in the *Nicaragua* Judgment the ICJ conceded that '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'.[236] These difficulties, however, are even more evident in the cyber context, where identifying who is behind a cyber operation presents significant technical problems. Anonymity is in fact one of the greatest advantages of cyberspace. The internet, in particular, is a decentralized system where the communications protocol divides the sent data into several packets that take different unpredictable pathways to reach their destination before being reassembled.[237] 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, may have been 'spoofed', or the corresponding computer system may only be a 'stepping stone' for an attacker located elsewhere.[238]

Nonetheless, the challenges in the identification of the attackers should not be an excuse not to tackle the international legal aspects of cyber operations. After all, identifying the authors of hostile actions is a problem also in other contexts, for instance international terrorism: as the United States declared, the ambiguities of cyberspace 'simply reflect the challenges in applying the [UN] Charter framework that already exists [*sic*] in many contexts'.[239] It is also not impossible that the author of a cyber operation is eventually identified; traditional intelligence gathering and cyber exploitation, used in support of traceback technical tools, could be helpful instruments in this sense.[240] Further developments in computer technology and internet regulations, such as the introduction of the new internet protocol IPv6, might also make identification easier.[241]

[236] *Nicaragua*, para 57.

[237] As has been effectively observed, 'the internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work' (Joel Brenner, *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), p 32).

[238] Scott J Shackelford and Richard B Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', *Georgetown Journal of International Law* 42 (2011), p 982. The 1998 'Solar Sunrise' attack that broke into the US DoD's system was for instance carried out by an Israeli teenager and Californian students through a computer based in the United Arab Emirates (Shackelford, 'From Nuclear War', p 204).

[239] UN Doc A/66/152, 15 July 2011, p 18.

[240] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', *Journal of Conflict and Security Law* 17 (2012), p 234; Owens, Dam, and Lin, *Technology*, pp 140–1; Advisory Council on International Affairs/Advisory Committee on Issues of Public International Law, *Cyber Warfare*, no 77, AIV/No 22 CAVV, December 2001, p 15, <http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf>. See the traceback technology described in Jay P Kesan and Carol M Hayes, 'Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace', *Harvard Journal of Law and Technology* 25 (2011–12), pp 482 ff. The US DoD is apparently seeking to improve attribution capabilities through behaviour-based algorithms (US DoD, *Cyberspace Policy Report*, p 4).

[241] Dinstein, 'Computer Network Attacks', p 112.

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. If identification is essentially a technical matter, attribution is a legal exercise and is 'the key to understanding the motive of an attack and consequently being able to differentiate between a criminal act and warfare in cyberspace'.[242] The above-mentioned 2013 Report of the GGE confirmed that 'States must meet their international obligations regarding internationally wrongful acts attributable to them' in the cyber context.[243] Although it is not entirely implausible that a special regime of international responsibility will develop as a consequence of the unique features of cyber operations, in the present lack of any indications in that sense such conclusion would certainly be premature.[244] The applicable rules are, therefore, those contained in Chapter II of Part One of the Articles on the Responsibility of States for Internationally Wrongful Acts, adopted by the ILC in 2001 and subsequently endorsed by the UN General Assembly ('ILC Articles'), which substantially reflect customary international law.[245]

Several scenarios can be identified. The first and easiest one is the case of 'uniformed' hackers. According to Article 4(1) of the ILC Articles, '[t]he conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State'. Article 4(2) specifies that '[a]n organ includes any person or entity which has that status in accordance with the internal law of the State'. Although details of states' military cyber capabilities are often classified, it appears that several national armies have established cyber units.[246] To the extent that they are organs of a state, their conduct is attributable to that state. This conclusion would not change if the hackers were civilian, and not military, organs. In the United Kingdom, for instance, the Global Operations and Security Control Centre (GOSCC), whose role is 'to proactively and reactively defend MoD [Ministry of Defence] networks 24/7 against cyber attack to enable agile exploitation of MoD information capabilities across all areas of the Department's operations', is formed not only of members of the military but also by MoD civilian and contractor personnel from industry partners, although only military members can be sent to operational theatres.[247] It also seems that the alleged US cyber operations against Iran were

[242] Eleanor Keymer, 'The cyber-war', *Jane's Defence Weekly* (47/39, 29 September 2010), p 22.

[243] UN Doc A/68/98, 24 June 2013, p 8.

[244] 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'.

[245] Read the text of the Articles in *Yearbook of the International Law Commission*, 2001, Vol II, Part Two, pp 26–30. On attribution to international organizations, see the Draft Articles on the Responsibility of International Organizations, adopted by the ILC in 2011, in *Yearbook of the International Law Commission*, 2011, Vol II, Part Two, pp 54 ff.

[246] See Section I of this Chapter p 10.

[247] House of Commons Defence Committee, *Defence and Cyber-Security*, Sixth Report of Session 2012–13, Vol I, 18 December 2012, p 17.

'run by intelligence agencies, though many techniques used to manipulate Iran's computer controllers would be common to a military program'.[248]

A state is responsible not only for the conduct of its *de jure* organs, but also of those individuals that are 'completely dependent' on state authorities and can thus be considered *de facto* organs, even if they do not have that status according to the internal law of the relevant state. The complete dependency test was first referred to by the ICJ in *Nicaragua* and then developed in the *Genocide* Judgment.[249] As has been observed, in this exceptional situation 'the reason why a connection between a state and a de facto organ must be intense is that the mere identity of the actor as a state organ suffices for attribution to occur'.[250]

Furthermore, the hackers could be members of parastatal entities, public, semi-public or privatized corporations empowered by internal law to exercise some degree of governmental authority on behalf of state organs:[251] in this case, their conduct will be attributed to the state 'provided the person or entity is acting in that capacity in the particular instance', as stated in Article 5 of the ILC Articles. The notion of 'governmental authority' is intentionally left undefined in Article 5 as it 'depends on the particular society, its history and traditions'.[252] It seems, however, to be a notion broad enough to include both the defence of 'national' portions of cyberspace and the conduct of intelligence gathering or offensive cyber operations by the individual or the entity. Unlike state agents under Article 8 of the ILC Articles, attribution under Article 5 does not require that the acts be committed under the 'effective control' of state authorities or within those limits, as long as internal law has delegated certain governmental functions to the individual or entity in question.[253] National Computer Emergency Response Teams (CERTs), which provide 'initial emergency response aid and triage services to the victims or potential victims of cyber operations or cyber crimes, usually in a manner that involves coordination between the private sector and government entities',[254] are an example of entities authorized to exercise governmental authority in the cyber context.[255] Another example is the Cyber Unit of the Estonian Defence League, which is 'a force of programmers, computer scientists and software engineers . . . a volunteer organization that in wartime would function under a unified

[248] David E Sanger, 'U.S. Blames China's Military Directly for Cyberattacks', *The New York Times*, 6 May 2013, <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&_r=1&>.

[249] *Nicaragua*, paras 110, 393; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Merits, Judgment, 26 February 2007, ICJ Reports 2007 ('*Genocide*'), paras 392–3. It is controversial whether *de facto* organs should be ascribed to Art 4 or Art 8 of the ILC Articles.

[250] Marko Milanović, 'State Responsibility for Acts of Non-state Actors: A Comment on Griebel and Plücken', *Leiden Journal of International Law 22* (2009), p 315.

[251] *Yearbook of the International Law Commission*, 2001, Vol II, Part Two, p 42.

[252] *Yearbook of the International Law Commission*, 2001, Vol II, Part Two, p 43.

[253] *Yearbook of the International Law Commission*, 2001, Vol II, Part Two, p 43.

[254] Tallinn Manual, p 258.

[255] Michael N Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law Journal Online* 54 (2012), p 35, <http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt>.

military command'.[256] The Cyber Unit, which protects Estonia's information infrastructure and supports broader objectives of national defence, cooperates in emergency situations with the Estonian CERT to respond to cyber attacks but does not have contractual obligations or payments from the government.[257]

The conduct of organs and of persons or entities empowered to exercise elements of the governmental authority is attributable to the relevant state even if they exceed their authority or contravene the instructions received, providing they act in their official capacity (Article 7 of the ILC Articles). In case of covert operations like cyber operations, however, '[t]he distinction between *ultra vires* and purely private conduct is particularly problematic'.[258] In such cases, it has been suggested that attribution will require that 'the state organ was acting in its *actual* (rather than *apparent*) official capacity'.[259] It is worth pointing out that if, in the case of an individual who is an organ, attribution to a state is avoided if he was acting in a purely private capacity (ie not as an organ), in the case of entities which are organs their conduct is, in practice, always attributable, even if *ultra vires*, since there is no private capacity. In the case of entities, the examination of whether they were acting in the exercise of the relevant governmental authority may be coterminous with the question of whether they were within the scope of their powers. It should also be recalled that Article 91 of the 1977 Protocol I Additional to the Geneva Conventions on the Protection of Victims of War make clear that a belligerent state 'shall be responsible for *all* acts committed by persons forming part of its armed forces', including those committed in a personal capacity, providing they are unlawful under the *jus in bello*.[260]

The hackers could also be private individuals or corporations instructed by states to conduct specific cyber operations.[261] A well-known example is the Russian Business Network (RBN), a cyber crime firm specializing in phishing, malicious code, botnet command-and-control, DDoS attacks and identity theft, which is suspected of having executed the cyber operations against Georgia on behalf of Russia.[262] The existence of Iranian hackers working for the Revolutionary Guard's

[256] Tom Gjelten, 'Volunteer Cyber Army Emerges in Estonia', NPR News, 4 January 2011, <http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation>. See also Shackelford and Andres, 'State Responsibility', p 1009.

[257] Shackelford and Andres, 'State Responsibility', p 1009.

[258] Kimberley N Trapp, *State Responsibility for International Terrorism* (Oxford: Oxford University Press, 2011), p 35.

[259] Trapp, *State Responsibility*, p 35 (emphasis in the original).

[260] Article 91 Additional Protocol I (emphasis added). The provision must be read in conjunction with Art 43 of the Protocol, that defines 'armed forces'. Article 3 of Hague Convention IV has a virtually identical formulation. See Marco Sassòli, 'State Responsibility for Violations of International Humanitarian Law', *International Review of the Red Cross* 84 (2002), pp 405–6.

[261] Jonathan A Ophardt, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', *Duke Law and Technology Review* 3 (2010), paras 12–18, <http://www.law.duke.edu/journals/dltr/articles/pdf/2010dltr003.pdf>. Such corporations are allegedly paid by governments to carry out elements of the cyber attacks (Watts, 'Combatant Status', p 411).

[262] Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, *Cyber Attacks Against Georgia*, p 11; Klimburg, 'Mobilising Cyber Power', pp 49–50; John Markoff, 'Before the Gunfire, Cyberattacks', *The New York Times*, 12 August 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

paramilitary Basij group and including 'university instructors and students, as well as clerics' has also been reported.[263] Article 8 of the ILC Articles deals with state agents and provides that '[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'. In the *Nicaragua* case, the ICJ argued that 'United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the *contras*, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself…for the purpose of attributing to the United States the acts committed by the *contras* in the course of their military or paramilitary operations in Nicaragua': what has to be proved is that 'that State had effective control of the military or paramilitary operation in the course of which the alleged violations were committed'.[264] In the *Genocide* case, the ICJ returned to the point and clarified that '[i]t must…be shown that this "effective control" was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations'.[265]

According to the ICTY, however, '[t]he degree of control may…vary according to the factual circumstances of each case'.[266] Doubting the consistency of the ICJ's effective control test in *Nicaragua* with the 'logic' of the law of state responsibility,[267] the Tribunal adopted a much less restrictive test to attribute the conduct of militarily organized armed groups to a state. Under the ICTY 'overall' control test, for the actions of such groups to engage state responsibility it is sufficient that the state '*has a role in organising, coordinating or planning the military actions* of the military group, in addition to financing, training and equipping or providing operational support to that group…regardless of any specific instructions by the controlling State concerning the commission of each of those acts'.[268] As has been noted, 'the overall control is not control over the act, but over the actor, an organized and hierarchically structured group, at a general level'.[269] Unlike the 'effective control' test, then, the *Tadić* standard focuses on the 'general influence' that a state exercises over a group, and not on specific activities, but, unlike the complete dependency test, it is much less stringent.[270] In the *Genocide* Judgment,

[263] Nasser Karimi, 'Iran's paramilitary launches cyber attacks', *The Associated Press*, 14 March 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/03/14/AR2011031401029.html?referrer=emailarticle>.

[264] *Nicaragua*, para 115. [265] *Genocide*, para 400.

[266] ICTY, *Prosecutor v Tadić*, Case No IT-94-1-A, Appeals Chamber Judgment, 15 July 1999, para 117 (emphasis omitted).

[267] *Tadić*, Appeals Chamber Judgment, paras 116 ff.

[268] *Tadić*, Appeals Chamber Judgment, para 137 (emphasis in the original). The Court added that 'if, as in *Nicaragua*, the controlling State *is not the territorial State* where the armed clashes occur or where at any rate the armed units perform their acts, more extensive and compelling evidence is required to show that the State is genuinely in control of the units or groups not merely by financing and equipping them, but also by generally directing or helping plan their actions' (para 138; emphasis in the original).

[269] Milanović, 'State Responsibility', p 317. [270] Tsagourias, 'Cyber Attacks', p 238.

the ICJ rejected overall control as an attribution standard by noting that it 'has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf'.[271]

It has been suggested that, due to the inherently clandestine nature of cyber activities and the technical difficulty of identifying the authors, the *Tadić* test should be preferred to the *Nicaragua* test when cyber operations are concerned.[272] This view mixes standard of evidence with attribution criteria[273] and cannot be shared: indeed, it is exactly because of the identification problems characterizing cyber activities and the potential for abuse of the right of self-defence that the 'effective control' test is preferable, as it would prevent states from being frivolously or maliciously accused of cyber operations. The above-mentioned view also misses an important point: the ICTY applies the overall control test only to the case of an 'organised and hierarchically structured group, such as a military unit or, in case of war or civil strife, armed bands of irregulars or rebels'.[274] For the case of a 'private individual who is engaged by a State to perform some specific illegal acts in the territory of another State (for instance, by carrying out acts of sabotage)' and of unorganized, non-military and non-hierarchical groups of individuals (which would arguably include groups such as RBN or 'Anonymous'), the ICTY retains the effective control test, ie the need to prove the issue of specific instructions concerning the commission of that illegal act or the state's public retroactive approval of the actions.[275] With specific regard to cyber operations, then, there is no substantial practical discrepancy between the ICJ and the ICTY approaches: both would probably lead in most cases to the application of the effective control test, as 'organised and hierarchically structured' cyber groups do not seem to exist yet.[276] Clear support for the application of the effective control test to cyber operations can also be found in the speech given by the then US State Department's Legal Advisor, Harold Koh, at the US CYBERCOM, 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'.[277] Azerbaijan

[271] *Genocide*, para 406.

[272] Shackelford, 'From Nuclear War', p 235; Shackelford and Andres, 'State Responsibility', pp 987–8. See also Ryan, Dion, Tikk, and Ryan, 'International Cyberlaw', p 1187.

[273] See, eg, Shackelford and Andres, 'State Responsibility', p 990.

[274] *Tadić*, Appeals Chamber Judgment, para 120 (emphasis omitted).

[275] *Tadić*, Appeals Chamber Judgment, para 118.

[276] It seems, however, that members of Al-Qaeda have conducted low-intensity cyber operations against the United States (Vijay M Padmanabhan, 'Cyber Warriors and the *Jus in Bello*', *International Law Studies* 89 (2013), p 296). Certain armed groups, such as Hamas and Hezbollah, may have also hired cyber criminals in order to conduct cyber operations (James A Lewis, 'The "Korean" Cyber Attacks and Their Implications for Cyber Conflict' (Center for Strategic and International Studies, 2009), p 8, <http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf>).

[277] Guymon (ed), *Digest of United States Practice*, p 596.

also denounced cyber attacks conducted by a group of hackers called the 'Armenian Cyber Army' under the 'direction and control' of Armenia.[278]

Hackers could be neither state organs nor state agents, but their conduct could have been incited by state authorities. In 2001, for example, after a US Navy spy plane collided with a Chinese jet fighter in the South China Sea, websites appeared offering instructions to hackers on how to incapacitate US government computers.[279] It also appears that the Russian government might have encouraged 'patriotic hackers' to conduct the 2007 cyber attacks against Estonia.[280] Russian language blogs, forums, and websites also published instructions on how to overwhelm Georgian government websites as well as a list of vulnerable Georgian websites.[281] There is no express regulation of incitement in the ILC Articles on State Responsibility.[282] Incitement would thus entail state responsibility for the incited actions only to the extent it amounts to direction and control (Article 8).[283] After inciting the actions, however, state authorities may subsequently publicly endorse them: in the *Hostages* case, the ICJ found that, although the initial attack on the US Embassy in Tehran was not attributable to Iran, the subsequent adoption of the action by the Iranian authorities as their own and the decision to perpetuate the occupation transformed the occupation and detention of the hostages into acts of the state.[284] Article 11 of the ILC Articles confirms that '[c]onduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges *and* adopts the conduct in question as its own'.[285] It is true that '[a]cknowledgement and adoption of conduct by a State might be express (as for example in the *United States Diplomatic and Consular Staff in Tehran* case), or it might be inferred from the conduct of the State in question',[286] but acknowledgement and adoption of cyber operations by a state are unlikely to occur: as already noted, cyber capabilities are the perfect tool for covert operations and one of their

[278] 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, UN Doc A/66/897–S/2012/687, 7 September 2012, p 1.

[279] Noah Weisbord, 'Conceptualizing Aggression', *Duke Journal of Comparative and International Law* 20 (2009), p 20.

[280] Catherine Lotrionte, 'Active Defense for Cyber: A Legal Framework for Covert Countermeasures', in *Inside Cyber Warfare*, edited by Jeffrey Carr, 2nd edn (Sebastopol, CA: O'Reilly, 2012), p 282.

[281] Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, *Cyber Attacks Against Georgia*, pp 9–10.

[282] Incitement, however, is dealt with in the Commentary to Part One, Chapter IV of the ILC Articles (*Yearbook of the International Law Commission,* 2001, Vol II, Part Two, p 65). When expressly provided, incitement can be an unlawful act per se (see eg Art III of the 1948 Convention on the Prevention and Punishment of the Crimes of Genocide, text in UNTS, Vol 78, pp 277 ff).

[283] See *Yearbook of the International Law Commission*, 2001, Vol II, Part Two, p 65.

[284] *US Diplomatic and Consular Staff in Tehran (US v Iran)*, Judgment, 24 May 1980, ICJ Reports 1980, para 74.

[285] Emphasis added. According to the Commentary, 'acknowledgement and adoption' should be distinguished from 'mere support or endorsement': 'as a general matter, conduct will not be attributable to a State under Article 11 where a State merely acknowledges the factual existence of conduct or expresses its verbal approval of it. . . . The language of "adoption", on the other hand, carries with it the idea that the conduct is acknowledged by the State as, in effect, its own conduct' (*Yearbook of the International Law Commission*, 2001, Vol II, Part Two, p 53).

[286] *Yearbook of the International Law Commission,* 2001, Vol II, Part Two, p 54.

main advantages is exactly that the author can hide under the invisibility cloak of plausible deniability.

Finally, it could be that the cyber operations originate from computer systems located in a certain state or from the cyber infrastructure of a state without any state involvement whatsoever, as in the case of 'hacktivists' and 'patriotic hackers' willing to support a certain political cause. In such case, the hackers' conduct could not be imputed to the state of origin, which may, however, be held responsible for not taking the necessary and reasonable measures to prevent or stop the operations (for instance, by disabling the internet access of the perpetrators or updating the country's firewall settings). In spite of what some commentators have argued,[287] then, the state's wrongful act would not be the cyber operation, but the breach of its obligation 'not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[288] It appears, for instance, that, even though no evidence was found of state organs directing the attacks, Russia at least tolerated the cyber operations against Estonia and Georgia originating from Russian hacker websites.[289] Russia also did not cooperate with Estonia in tracking down those responsible, and a request for bilateral investigation under the Mutual Legal Assistance Treaty between the two countries was rejected by the Russian Supreme Procurature.[290] Whether the state victim of a cyber operation amounting to an armed attack can invoke self-defence if the operation is attributable to non-state actors and originates from the territory of a state that is unable or unwilling to prevent or terminate it is a question that will be explored in Chapter 2.[291]

V. The Book's Scope and Purpose

In light of the above, it should be clear that existing primary and secondary rules of international law, including the law of state responsibility, the *jus ad bellum* and the *jus in bello*, do apply to cyber operations. It is, however, more controversial *when* and *how* such rules apply to events that are very different from kinetic

[287] See eg David E Graham, 'Cyber Threats and the Law of War', *Journal of National Security Law and Policy* 4 (2010), p 93; Sklerov, 'Solving the Dilemma', p 49; Ryan, Dion, Tikk, and Ryan, 'International Cyberlaw', p 1188.

[288] *Corfu Channel (United Kingdom v Albania)*, Merits, Judgment, 9 April 1949, ICJ Reports 1949, p 22. The obligation is reflected in Rule 5 of the Tallinn Manual, p 26. GA Res 55/63 of 4 December 2000 on the criminal misuse of information technologies recommends that states ensure 'that their laws and practice eliminate safe havens for those who criminally misuse information technologies' (para 1). On due diligence in the cyber context, see Chapter 2, Section III.3.

[289] Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, *Cyber Attacks Against Georgia*, p 13. Another report claims that Russia refused to intervene with regard to the hacker attacks against Georgia in 2008 (Project Grey Goose, *Russia/Georgia Cyber* War, p 8). It has been suggested that the May 2007 cyber operations against Estonia's computer networks would have not been possible without the blessing of Russian authorities (Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe', *Wired Magazine*, issue 15.09, 21 August 2007, <http://www.wired.com/politics/security/magazine/15-09/ff_estonia>).

[290] Shackelford, 'From Nuclear War', p 208; Klimburg, 'Mobilising Cyber Power', p 50.

[291] See Chapter 2, Section III.3, pp 87–88.

scenarios: the present book explores these difficulties. The next Chapter analyses the *jus ad bellum* issues arising from cyber operations, in particular whether they fall under the prohibition of the threat and use of force contained in Article 2(4) of the United Nations Charter and whether the state victim of a cyber operation may react in self-defence under Article 51 of the Charter. Chapter 3 discusses under what conditions the law of armed conflict is applicable to cyber operations without concurrent kinetic hostilities or in the context of an existing traditional armed conflict, while Chapter 4 analyses the limits that the law on the conduct of hostilities imposes on cyber operations. Finally, Chapter 5 considers the duties of neutral and belligerent states under the law of neutrality in the cyber context.

A few *caveats* on what the present book does *not* do. The book will only focus on military cyber operations: therefore, it does not touch upon questions of domestic or international law related to cyber crime and cyber terrorism. Furthermore, cyber operations above the threshold of the use of force will form the primary object of analysis, although discussion will also be conducted of certain operations falling below that threshold, whenever relevant. The application of the *jus pacis*, such as the law of the sea, aviation law, space law, or international communications law,[292] as well as of international criminal law, to cyber operations is also outside the scope of this book: this is not meant to suggest that these regimes are less relevant to cyber operations than the rules on the use of force or that they cease to apply in armed conflict, but only that they deserve specific in-depth treatment in a separate work.

The book will look at qualitative data resulting from documentary analysis of different materials, *in primis* relevant *jus ad bellum* and *jus in bello* treaty provisions and customary international law, as applied by international and national courts. Although they are not, in themselves, sources of law and with all the caution motivated by the fact that they reflect operational and policy considerations, reference will also be made to military manuals, cyber security strategies and doctrines and official statements to the extent that they can assist in interpreting existing law and amount to evidence of state practice and *opinio juris*. As to cyber attacks that have already occurred, their exact details, such as the extent of damage caused or the attribution to specific states, are still uncertain: accordingly, they will be used in this book not as precedents or incontrovertible elements of state practice, but as explanatory real-life examples of different types of cyber operations. The present book is different from the Tallinn Manual in that it does not aim to distillate black-letter rules or to merely restate the law, but rather to suggest solutions and interpretations through which existing rules can be effectively applied to regulate a relatively new and unique phenomenon such as cyber operations. The book also deals with topics neglected by the Manual and suggests solutions for those problems on which the Group of Experts could not find agreement.[293]

[292] On the application of those regimes to cyber operations, see, among others, DoD, *An Assessment*, pp 26 ff; Schaap, 'Cyber Warfare Operations', pp 161–70; Shackelford, 'From Nuclear War', pp 223–4, 227–8.

[293] Such topics include, for instance, whether merely disruptive cyber operations amount to a 'use of force', 'armed attack' or 'attack', the nature of the nexus between a cyber operation and an armed

The overall goal is to provide a systematic and coherent analysis of the international law applicable to military cyber operations that will be of use to anyone who wants or needs to understand the basic issues of the rules of international law on the use of force and the law of armed conflict. Indeed, cyber operations give the opportunity to discuss some of the most controversial aspects of contemporary international law, such as self-defence against imminent armed attacks and against attacks by non-state actors, the distinction between the use of force and the law enforcement paradigms, the geographical scope of application of the law of armed conflict, the notions of 'combatancy' and 'direct participation in hostilities', and the legal issues arising from remote and automated warfare. While it is true that, until now, nobody has died in a cyber attack,[294] someone could have died: the potentially severe humanitarian consequences of certain cyber operations sufficiently justify an investigation on how international law can deal with them, even if such consequences have luckily not occurred yet.

The law is stated as of 30 September 2013.

conflict for the operation to be governed by the law of armed conflict, the attribution and evidentiary standards required for a self-defence reaction against a cyber attack, whether data constitute 'objects', whether a cyber operation qualifying as an act of hostilities but short of 'attack' may initiate an armed conflict.

[294] David P Fidler, '*Inter Arma Silent Leges Redux*? The Law of Armed Conflict and Cyber-Conflict', in *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, edited by Derek S Reveron (Washington, DC: Georgetown University Press, 2012), p 73.