Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations

Marco Roscini

Department of Law, Faculty of Social Science and Humanities, University of Westminster

This is the final publisher version of an article published in 50(2) TEX. INT'L L.J. [233-273], (2015).

Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations

MARCO ROSCINI*

SUMMARY

* Reader in International Law, University of Westminster. I am grateful to Simon Olleson for his useful comments on a previous version of this article and to Andraz Kastelic for his research assistance. All errors and omissions remain my sole responsibility. The article is based on developments as of June 2014 and all websites were last visited during that time.

INTRODUCTION

Evidentiary problems in inter-state litigation, particularly in relation to the attribution of certain unlawful conduct, are not peculiar to cyber operations.[1] Well before the cyber age, the International Court of Justice (ICJ) in the *Nicaragua v. United States* judgment 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."[2] As the United States declared in the views on information security that it submitted to the U.N. Secretary-General, then, the ambiguities of cyberspace "simply reflect the challenges . . . that already exists [sic] in many contexts."[3] It is undeniable, however, that these challenges are particularly evident in the cyber context, where identifying who is behind a cyber operation presents significant technical problems.[4] 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."[5]

One needs only look at the three most famous cases of cyber attacks against States allegedly launched by other States to realize how thorny the problem of evidence in relation to cyber operations is.[6] It has been claimed, in particular, that the Russian Federation was behind both the 2007 Distributed Denial of Service (DDoS) attacks against Estonia and the 2008 cyber attacks against Georgia.[7] These

1. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE glossary (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL] (defining cyber operations as "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace"). Cyber operations include cyber attacks and cyber exploitation. Cyber attacks are those cyber operations, whether in offense or in defense, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; (b) partly or totally disrupting the functioning of the targeted computer, computer system, or network with any related computer-operated physical infrastructure; and/or (c) producing physical damage extrinsic to the computer, computer system, or network. Cyber exploitation refers to those operations that access other computers, computer systems, or networks, without the authorization of their owners or exceeding the limits of the authorization in order to obtain information, but without affecting the functionality of the accessed system or amending/deleting the data resident therein. For a discussion of these definitions, see MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 10–18 (2014).

2. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, para. 57 (June 27).

3. U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, 18, U.N. Doc. A/66/152 (July 15, 2011) [hereinafter *Developments in the Field of Information and Telecommunications*].

4. *Cf.* FIREEYE, DIGITAL BREAD CRUMBS: SEVEN CLUES TO IDENTIFYING WHO'S BEHIND ADVANCED CYBER ATTACKS 4 (2014), *available at* https://www.fireeye.com/resources/pdfs/digital-bread-crumbs.pdf (describing the technical difficulty in pinning down the source of a cyber attack given that "[c]ybercriminals are experts at misdirection" even in the non-State actor context).

5. JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 32 (2011); *see also Developments in the Field of Information and Telecommunications*, *supra* note 3 ("The lack of timely, high-confidence attribution and the possibility of 'spoofing' can create uncertainty and confusion for Governments, thus increasing the potential for crisis instability, misdirected responses and loss of escalation control during major cyberincidents.").

6. The three most famous cases of cyber attacks are the Distributed Denial of Services (DDoS) attacks against Estonia in 2007, the cyber attacks against Georgia in 2008, and the Stuxnet attacks against Iran discovered in 2012.

7. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia,* THE GUARDIAN, May 16, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia; Jon Swaine, *Georgia: Russia*

allegations were based on the following facts. In the Estonian case, the hackers claimed to be Russian, the tools to hack and deface were contained in Russian websites and chatrooms, and the attacks peaked on May 9 (the day Russia celebrates Victory in Europe Day in the Second World War).[8] Furthermore, although the botnets included computers based in several countries, it seems that at least certain attacks originated from Russian IP addresses, including those of State institutions.[9] According to the Estonian Defense Minister, the attacks were "unusually well-coordinated and required resources unavailable to common people."[10] The DDoS attacks also took place against the backdrop of the removal of a Russian war memorial from Tallinn's city center.[11] Finally, Russia did not cooperate with Estonia in tracking down those responsible, and the Russian Supreme Procurature rejected a request for bilateral investigation under the Mutual Legal Assistance Treaty between the two countries.[12]

The cyber attacks against Georgia started immediately before and continued throughout the armed conflict between the Caucasian State and the Russian Federation in August 2008.[13] It seems that the Russian hacker community was involved in the cyber attacks and that coordination "took place mainly in the Russian language" and in Russian or Russian-related fora.[14] As in the Estonian case, some commentators claimed that the level of coordination and preparation suggested governmental support for the cyber attacks.[15] Finally, IP addresses belonging to

'Conducting Cyber War,' THE TELEGRAPH, Aug. 11, 2008, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html. For a discussion of denial of service attacks, see ROSCINI, *supra* note 1, at 18. "Denial of Service (DoS) attacks, of which 'flood attacks' are an example . . . 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. Permanent DoS attacks are particularly serious attacks that damage the system and cause its replacement or reinstallation of hardware. When the DoS attack is carried out by a large number of computers organized in botnets, it is referred to as a DDoS attack." *Id.*

8. COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 173 box 3.4 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES].

9. *Id.*

10. *Id.* (quoting Jaak Aaviksoo, Minister of Defense of Estonia, Strategic Impact of Cyber Attacks, Address before the Royal College of Defence Studies, *available at* www.irl.ee/en/articles/strategic-impact-of-cyber-attacks.

11. U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES.

12. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,* 27 BERKELEY J. INT'L L. 192, 208 (2009); *see also* Alexander Klimburg, *Mobilising Cyber Power,* 53 SURVIVAL: GLOBAL POL. & STRATEGY 41, 49–51 (2011) (describing Russia's recent support for cyber criminals in combating internal and external threats).

13. *See* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 (describing the cyberattacks as "dress rehearsal" before the shooting began in the Russo-Georgian War).

14. ENEKEN TIKK ET AL., COOP. CYBER DEF. CTR. OF EXCELLENCE, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 75 (2010), *available at* http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

15. *Id.*

Russian state-operated companies were used to launch the DDoS attacks.[16] Russia again denied any responsibility.[17]

The third case of alleged inter-state cyber operation, and possibly the most famous of the three, is that of Stuxnet. In 2012, an article published in *The New York Times* revealed that the United States, with Israel's support, had been engaging in a cyber campaign against Iran, codenamed "Olympic Games," to disrupt the Islamic Republic's nuclear program.[18] Stuxnet, in particular, was allegedly designed to affect the gas centrifuges at the Natanz uranium enrichment facility.[19] The Stuxnet incident was the first known use of malicious software designed to produce material damage by attacking the Supervisory Control and Data Acquisition (SCADA) system of a critical national infrastructure.[20] Unlike other malware, the worm did not limit itself to self-replication, but also contained a weaponized payload designed to give instructions to other programs.[21] The allegations against the United States and Israel were based on journalistic "interviews . . . with current and former American, European and Israeli officials" and other experts, whose names are not known.[22] In a recent interview, the former U.S. National Security Agency (NSA) contractor Edward Snowden also claimed that the NSA and Israel were behind Stuxnet.[23] Symantec's researchers suggested that Stuxnet's code included references to the 1979

16. *Id.*

17. *Id.*

18. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1&.

19. William J. Broad, John Markoff, & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all. Stuxnet presumably infiltrated the Natanz system through laptops and USB drives—as, for security reasons, the system is not usually connected to the Internet—and had two components: one designed to force a change in the centrifuges' rotor speed, inducing excessive vibrations or distortions that would destroy the centrifuges, and one that recorded the normal operations of the plant and then sent them back to plant operators so to make it look as if everything were functioning normally. *See generally* HOLLY PORTEOUS, LIBRARY OF PARLIAMENT, THE STUXNET WORM: JUST ANOTHER COMPUTER ATTACK OR A GAME CHANGER? 1–2 (2010).

20. Dominic Storey, *Stuxnet–The First Worm of Many for SCADA?*, IT RESELLER (Dec. 2, 2010), http://www.itrportal.com/articles/2010/12/02/6262-stuxnet-the-first-worm-of-many-for; *see also* Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 18–20 (2012) (describing Stuxnet's unique and innovative features).

21. Jeremy Richmond, Note, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 849–50 (2012). Although the exact consequences of the incident are still the object of debate, the International Atomic Energy Agency (IAEA) reported that, in the period when Stuxnet was active, Iran stopped feeding uranium into a significant number of gas centrifuges at Natanz. *See* William J. Broad, *Report Suggests Problems with Iran's Nuclear Effort*, N.Y. TIMES, Nov. 23, 2010, http://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html (describing Iran's various problems with its nuclear reactors while Stuxnet was operational, as well as international opinion as to whether Stuxnet caused those problems). It is still unclear, however, whether this was due to Stuxnet or to technical malfunctions inherent to the equipment used. *See* Ivanka Barzashka, *Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme*, 158 RUSI J. 48, 52 (2013) (proposing alternative explanations, including faulty machine parts, for the drop in centrifuge numbers).

22. Sanger, *supra* note 18.

23. *Edward Snowden Interview: The NSA and Its Willing Helpers,* SPIEGEL ONLINE (July 8, 2013), http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html.

date of execution of a prominent Jewish Iranian businessman.[24] Other circumstantial evidence includes the fact that the worm primarily hit Iran and was specifically targeted at the Natanz nuclear facility, as the worm would activate itself only when it found the Siemens software used in that facility,[25] and the implication that the attack required resources normally unavailable to individual hackers, which is supported by evidence of the high sophistication of the attack, the use of several zero-day hacks, and the insider knowledge of the attacked system.[26] Israeli and U.S. officials have neither denied nor confirmed involvement in the operation: In response to a question about the attack on Iran, President Obama's chief strategist for combating weapons of mass destruction, Gary Samore, sardonically pointed out, "I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."[27] According to *The Daily Telegraph*, a video that was played at a retirement party for Israel Defense Forces (IDF) chief of general staff Gabi Ashkenazi included references to Stuxnet as one of Ashkenazi's operational successes.[28]

Apart from the above well-known cyber attacks, allegations of state involvement have also been made in relation to other cyber operations, including cyber exploitation activities. The U.S. Department of Defense's 2013 Report to Congress, for instance, claims that some of the 2012 cyber intrusions into U.S. government computers "appear to be attributable directly to the Chinese government and military," although it is not entirely clear on what grounds.[29] According to the controversial Mandiant Report, "the sheer number of [hacking group] APT1 IP addresses concentrated in these Shanghai ranges, coupled with Simplified Chinese keyboard layout settings on APT1's attack systems, betrays the true location and language of the operators."[30] The Report concludes that "APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors."[31] According to the Chinese Defense Ministry, however, "the report lacked 'technical proof'" linking the IP addresses used by ATP1 to a military unit of the People's Liberation Army (PLA), as the attacks employed hijacked addresses.[32] In

24. NICOLAS FALLIERE, LIAM O. MURCHU & ERIC CHIEN, SYMANTEC, W32.STUXNET DOSSIER, VERSION 1.4, at 18 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/ whitepapers/w32_stuxnet_dossier.pdf.

25. *See* Barzashka, *supra* note 21, at 50 (explaining that "more than 60 per cent of all infected IP . . . addresses were in Iran, and almost 70 per cent of these had Siemens software installed").

26. *See* Rid, *supra* note 20, at 19 (explaining that "[t]he resources and investment that went into Stuxnet could only be mustered by a cyber superpower . . . .") (internal quotation marks omitted).

27. Broad, Markoff & Sanger, *supra* note 19.

28. Christopher Williams, *Israel Video Shows Stuxnet as One of Its Successes*, TELEGRAPH, Feb. 15 2011, http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html.

29. U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, at 36 (2013), *available at* http://www.defense.gov/pubs/ 2013_china_report_final.pdf.

30. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 39 (2013) [hereinafter MANDIANT, APT1], *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

31. *Id.* at 2.

32. *China Condemns Hacking Report by US Firm Mandiant*, BBC (Feb. 20, 2013), http://www.bbc.co.uk/news/world-us-canada-21515259.

May 2014, the U.S. Department of Justice eventually brought charges against five members of the PLA for hacking into the computers of six organizations in western Pennsylvania and elsewhere in the United States to steal trade secrets, without providing much supporting evidence (if any at all) of the involvement of the defendants.[33]

In spite of the obvious crucial importance of evidentiary issues, works on inter-state cyber operations, both above and below the level of use of force, have so far focused on whether such operations are consistent with primary norms of international law and on the remedies available to the victim State under the *jus ad bellum* and the law of state responsibility. Thus, studies of these operations have almost entirely neglected a discussion of the evidence the victim State needs to produce to demonstrate, either before a judicial body or elsewhere, that an unlawful cyber operation has been conducted against it and that the attack is attributable to another State.[34] The first edition of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* also does not discuss in depth evidentiary issues in the cyber context: The only references to evidence are contained in Rules 7 and 8.[35] The present article aims to fill this gap. It will start with a brief account of the international law of evidence and will then discuss who has the burden of proof in relation to claims seeking remedies (including reparation) for damage caused by cyber operations. It will then analyze the standard of proof required in the cyber context. Finally, the possible methods of proof will be examined, distinguishing between those that are admissible and those that are inadmissible. The present article only deals with international disputes between States and will not discuss evidentiary issues in relation to cyber crime before domestic courts. It also does not look at evidence before international criminal tribunals, as the focus is on state responsibility for cyber operations and not on the criminal responsibility of individuals.[36]

33. *See* Indictment at 29–35, United States v. Wang Dong, No. 14-118 (W.D. Pa., May 1, 2014), *available at* http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf (laying out the facts and evidence related to the five defendants' overt cyber attacks).

34. *See generally* Robin Geiß & Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 621 (Katharina Ziolkowski ed., 2013) [hereinafter PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE] (explaining the problems of attribution of responsibility for cyber attacks in the context of self-defense considerations); *see also* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 984–93 (2011) (positing standards of evidence and describing the problems with evidence and attribution of cyber attacks to different sovereigns). In the context of law enforcement, the Council of Europe and European Union have drafted an Electronic Evidence Guide for cyber crime. CYBERCRIME@IPA JOINT PROJECT OF THE COUNCIL OF EUROPE AND THE EUROPEAN UNION, *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors, and Judges* (Mar. 18, 2013), *available at*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp.

35. TALLINN MANUAL r. 7–8.

36. The statutes and rules of international criminal tribunals provide for specific evidentiary rules. Rüdiger Wolfrum, *International Courts and Tribunals*, *Evidence*, *in* 5 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 552, 567–69 (Rüdiger Wolfrum ed., 2012).

I. THE INTERNATIONAL LAW OF EVIDENCE

"Evidence" is "information . . . with the view of establishing or disproving alleged facts."[37] It is different from proof in that "'proof' is the result or effect of evidence, while 'evidence' is the medium or means by which a fact is proved or disproved."[38] Evidence is normally required to provide proof of both the objective (be it an act or omission) and subjective elements of an internationally wrongful act, i.e., its attribution to a State.[39] A State invoking self-defense against cyber attacks, for instance, will have to produce evidence that demonstrates (a) that the cyber attack actually occurred, that it was directed against the State, and that its scale and effects reached the threshold of an "armed attack";[40] and (b) that it was attributable to a certain State.[41] For a State to invoke the right to take countermeasures, on the other hand, it may be sufficient to provide evidence that a cyber operation originated from a certain State and that that State did not exercise due diligence in terminating it, without necessarily having to prove attribution of the attack itself to the State.[42] In the *Nicaragua* case, the ICJ clearly explained the distinction between the objective and subjective elements from an evidentiary perspective:

> One of the Court's chief difficulties in the present case has been the determination of the facts relevant to the dispute. . . . Sometimes there is no question, in the sense that it does not appear to be disputed, that an act was done, but there are conflicting reports, or a lack of evidence, as to who did it . . . . The occurrence of the act itself may however have been shrouded in secrecy. In the latter case, the Court has had to endeavour first to establish what actually happened, before entering on the next stage of considering whether the act (if proven) was imputable to the State to which it has been attributed.[43]

The Court's observations were made against the backdrop of the secrecy that surrounded the U.S. and Nicaraguan covert operations in Central America,[44] which is also a quintessential characteristic of cyber operations.[45] In this context too, then, it is likely that evidence will be required both to establish the material elements of the wrongful act and to establish its attribution. It is still unclear, for instance, not only who is responsible for Stuxnet, but also whether the worm caused any damage and, if so, to what extent.[46] This last question is essential in order to establish whether the

37. *Id.* at 552.

38. 31A C.J.S. Evidence § 8 (1964).

39. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, para. 57 (June 27) (noting the difficulty of imputing acts to particular States).

40. *Id.* para. 195. On the distinction between "use of force" and "armed attack," see *id.* paras. 191, 195.

41. *See generally* ROSCINI, *supra* note 1, at 80–88 (discussing whether self-defense can be exercised against cyber attacks by non-state actors).

42. Geiß & Lahmann, *supra* note 34, at 635–37.

43. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 57.

44. *Id.*

45. *See* ROSCINI, *supra* note 1, at 38.

46. *See* Barzashka, *supra* note 21, at 48 (noting that no one has admitted to the Stuxnet attack and that the "evidence of the worm's impact . . . is circumstantial and inconclusive").

cyber operation amounted to a use of force and, more importantly, whether it was an armed attack entitling the victim State to self-defense.[47] As to establishing the subjective element of the internationally wrongful act, what is peculiar to cyber operations is that in fact three levels of evidence are needed to attribute a cyber operation to a State: First, the computer(s) or server(s) from which the operations originate must be located; second, the individual behind the operation needs to be identified; and third, it needs to be proved that the individual acted on behalf of a State so that his or her conduct is attributable to it.[48]

This leads us to an important specification: The standard of proof must be distinguished from the rules of attribution. The former is "the *quantum* of evidence necessary to substantiate the factual claims made by the parties."[49] The latter, on the other hand, determine the level of connection that must exist between an individual or group of individuals and a State for the conduct of the individuals to be attributed to the State at the international level.[50] The rules of attribution for the purposes of state responsibility have been codified in Part One of the Articles on the Responsibility of States for Internationally Wrongful Acts adopted by the International Law Commission (ILC), as well as having been articulated in the case law of the ICJ.[51] Evidence according to the applicable standard must be provided to demonstrate that the attribution test has been satisfied: In *Nicaragua*, for instance, the ICJ had to assess whether there was sufficient evidence that the United States had exercised "effective control" over the *contras* so that it could be held responsible for their violations of international humanitarian law.[52]

The standard of proof should also be distinguished from the burden of proof. The latter does not determine how much evidence, and of what type, is necessary to prove the alleged facts, but merely identifies the litigant that must provide that evidence.[53] In other words, the burden of proof is "the obligation on a party to show

47. See ROSCINI, *supra* note 1, at 45–63, 70–77 (describing the meaning of "use of force" and when and how a State can use self-defense).

48. *See generally id.* at 98–103.

49. James A. Green, *Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice,* 58 INT'L & COMP. L.Q. 163, 165 (2009).

50. For a discussion of the rules of attribution, see ROSCINI, *supra* note 1, at 34–40.

51. Draft Articles on Responsibilities of States for Internationally Wrongful Acts, with Commentaries, Rep. of the Int'l Law Comm'n, 53d Sess., Apr. 23–June 1, July 2–Aug. 10, 2001, pt. 1, U.N. Doc. A/56/10 (2001). For case law development, see, e.g., Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, paras. 392–93 (Feb. 26); Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 I.C.J. 14, paras. 110, 393 (June 27). For further discussion, see generally ROSCINI, *supra* note 1, at 34–40.

52. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 115. In the *Nicaragua* case the Court did not find that there was sufficient evidence to conclude that the *contras* were totally dependent on the United States so as to qualify as de facto organs. However, it found that a situation of partial dependency,

> the exact extent of which the Court cannot establish, may certainly be inferred *inter alia* from the fact that the leaders were selected by the United States. But it may also be inferred from other factors, some of which have been examined by the Court, such as the organization, training and equipping of the force, the planning of operations, the choosing of targets and the operational support provided.

Id. para. 112.

53. ANNA RIDDELL & BRENDAN PLANT, EVIDENCE BEFORE THE INTERNATIONAL COURT OF JUSTICE 81 (2009).

that they have sufficient evidence on an issue to raise it in a case."[54] The burden of proof includes not only the "burden of persuasion,"[55] but also the "burden of production," which is the burden to produce the relevant evidence before a court.[56]

Evidence may be submitted not only to an international court or tribunal, but also to political organs (for instance, to secure a favorable vote).[57] It may also be disseminated more widely for the purposes of influencing public opinion and gaining support for certain actions or inactions.[58] One could recall the evidence presented by the Reagan Administration before the U.N. Security Council to justify its 1986 strike on Tripoli as a measure of self-defense.[59] When justifying its 2001 armed operation against Afghanistan, the U.S. Permanent Representative to the United Nations referred to the fact that the U.S. government had "clear and compelling information that the Al-Qaeda organization, which is supported by the Taliban regime in Afghanistan, had a central role in the [September 11, 2001] attacks," without, however, going into further details.[60] The same language was used by the Secretary-General of the North Atlantic Treaty Organization (NATO).[61] Evidence was also famously one of the controversial aspects of the 2003 U.S. and U.K.-led intervention in Iraq.[62] More recently, in the context of the proposed intervention to react against the use of chemical weapons in Syria, President Obama stated that "attack[ing] another country without a UN [sic] mandate and without clear evidence that can be

54. *Id.*

55. *See id.* (stating that the burden of proof is the "duty of a party to persuade").

56. Markus Benzing, *Evidentiary Issues*, *in* THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY 1234, 1245 (Andreas Zimmermann et al., eds., 2012) [hereinafter THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY]. As there are no parties in advisory proceedings, there is no burden of proof in this type of proceeding. Wolfrum, *supra* note 36, at 565.

57. *See* Matthew C. Waxman, *The Use of Force Against States that* Might *Have Weapons of Mass Destruction*, 31 MICH. J. INT'L L. 1, 2–3 (2009) (discussing the George W. Bush administration's unilateral approach for decisions regarding self-defense based on evidence of weapons of mass destruction (WMDs)).

58. Whether or not States have an obligation to make evidence public is a matter of debate. It has been observed that "[i]f nations are permitted to launch unilateral attacks based on secret information gained largely by inference, processed by and known only to a few individuals and not subject to international review, then Article 2(4) of the U.N. Charter is rendered virtually meaningless." Jules Lobel, *The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan*, 24 YALE J. INT'L L. 537, 547 (1999). *See also* GEORGE P. FLETCHER & JENS DAVID OHLIN, DEFENDING HUMANITY: WHEN FORCE IS JUSTIFIED AND WHY 169 (2008) (noting that "[t]he principle of publicity is critical" because "there is no authority but the eyes of the world to assess" whether there was sufficient evidence to support a State's actions). *But see* Waxman, *supra* note 57, at 65 ("One practical problem frequently raised in response is that key information often cannot be disclosed publicly without compromising critical intelligence sources and methods.").

59. Lobel, *supra* note 58, at 549.

60. Permanent Rep. of the United States of America to the U.N., Letter dated 7 October 2001 from the Permanent Rep. of the United States of America to the United Nations addressed to the President of the Security Council, UN Doc S/2001/946 (Oct. 7, 2001).

61. Lord George Robertson, Statement by NATO Secretary General (Oct. 2, 2001), *available at* http://www.nato.int/docu/speech/2001/s011002a.htm.

62. *See generally* U.K. FOREIGN & COMMONWEALTH OFFICE, IRAQ'S WEAPONS OF MASS DESTRUCTION: THE ASSESSMENT OF THE BRITISH GOVERNMENT (2002) (summarizing evidence of the various weapons capabilities of the Iraqi government as of 2002); U.N. SCOR, 58th Year, 4701st mtg. at 2–17, U.N. Doc S/PV.4701 (Feb. 5, 2003) (transcribing Colin Powell's remarks to the Security Council regarding WMDs in Iraq).

presented" would raise questions of international law.[63] The political or judicial relevance of evidence may relate to the different phases of the same international dispute. For instance, the State invoking the right of self-defense against an armed attack by another State will normally try to justify the exercise of this right first before the international community and public opinion by providing evidence of the occurrence (or imminent occurrence) of the armed attack and of its attribution to the target State.[64] If, as in the *Nicaragua* case, a State subsequently brings the case before an international court which has jurisdiction over the case, the evidence will have to be assessed by that court in order to establish international responsibility and its consequences, and in particular whether the requirements for the exercise of self-defense were met.[65]

Investigations of cyber attacks among States are complicated by the absence of a uniform body of rules on the production of evidence in international law.[66] There is no treaty provision that regulates evidentiary issues in non-judicial contexts, and it is doubtful that international law has developed customary rules in that sense.[67] As to the production of evidence in inter-state litigation, non-criminal international courts normally determine their own standards in each case, which may considerably differ according to the nature of the court or the case under examination.[68] As it is not possible to identify uniform evidentiary rules applicable in all cases and before all international courts, this article will focus on proceedings before the ICJ. This is because the ICJ is the main U.N. judicial organ that deals, if the involved States have consented to its jurisdiction, with claims of state responsibility arising from the violation of any primary norm of international law.[69] The overall purpose is to establish whether rules on evidence may be identified that would apply to claims in inter-state judicial proceedings seeking remedies for damage caused by cyber

63. Julian Borger, *West Reviews Legal Options for Possible Syria Intervention Without UN Mandate,* GUARDIAN, Aug. 26, 2013, http://www.theguardian.com/world/2013/aug/26/united-nations-mandate-airstrikes-syria. Indeed, the Report of the U.N. Secretary-General's Investigation found "clear and convincing evidence" of the use of chemical weapons in the armed conflict. Rep. of the U.N. Mission to Investigate Allegations of the Use of Chemical Weapons in the Syrian Arab Republic on the Alleged Use of Chemical Weapons in the Ghouta Area of Damascus on 21 August 2013, U.N. Doc. A/67/997–S/2013/553, GAOR, 67th Sess., 8 (Sept. 16, 2013).

64. *See* Mary Ellen O'Connell, *Lawful Self-Defense to Terrorism*, 63 U. PITT. L. REV. 889, 895 (2002) [hereinafter O'Connell, *Lawful Self-Defense*] ("In many cases of self-defense, the facts of the attack and the responsible party are evident for all the world to see. Iraq's 1990 invasion of Kuwait is a case in point. When a less obvious event occurs, like the September 11 attacks, the [S]tate contemplating self-defense may have to provide evidence that future attacks are pending.").

65. *See*, *e.g.*, Ruth Teitelbaum, *Recent Fact-Finding Developments at the International Court of Justice*, 6 L. & PRAC. INT'L CTS. & TRIBUNALS 119, 151 (2007) (describing the International Court of Justice's (ICJ) assessment of the evidence in the *Nicaragua* case).

66. Mary Ellen O'Connell, *Evidence of Terror*, 7 J. CONFLICT & SECURITY L. 19, 21 (2002) [hereinafter O'Connell, *Evidence of Terror*].

67. *Id.*; *see also* Green, *supra* note 49, at 165 ("In general, international law does not have a clear benchmark against which the persuasiveness or reliability of evidence may be gauged for the purposes of attributing responsibility or assessing legal claims. In other words, there is no consistent standard of proof with regard to international obligations.").

68. *See* Daniel Joyce, *Fact-Finding and Evidence at the International Court of Justice: Systemic Crisis, Change or More of the Same?*, 18 FINNISH Y.B. INT'L L. 283, 286 (2007) ("The theme of flexibility dominates public international law's approach to evidence.").

69. *See*, *e.g.*, H. Vern Clemons, Comment, *The Ethos of the International Court of Justice is Dependent Upon the Statutory Authority Attributed to its Rhetoric: A Metadiscourse*, 20 FORDHAM INT'L L.J. 1479, 1486, 1490–91 (1997) (detailing modes of jurisdiction by the ICJ over States).

operations. It should be noted, however, that the conclusions reached with regard to the ICJ only apply to it and could not automatically be extended to other international courts.

Rules on the production of evidence before the ICJ are contained in the ICJ Statute, the Rules of Court (adopted in 1978), and Practice Directions for use by States appearing before the Court (first adopted in 2001 and subsequently amended).[70] In the following pages, the relevant rules on evidentiary issues contained in those documents, as well as those elaborated by the Court in its jurisprudence, will be applied to allegations related to cyber operations.

II. BURDEN OF PROOF AND CYBER OPERATIONS

The burden of proof identifies the litigant that has the onus of meeting the standard of proof by providing the necessary evidence.[71] Once the burden has been discharged according to the appropriate standard, the burden shifts to the other litigant, who has to prove the contrary.[72] Normally, the party that relies upon a certain fact is required to prove it (the principle *onus probandi incumbit actori*, derived from Roman law).[73] This general principle of law, invoked consistently by the ICJ and other international courts and tribunals,[74] "applies to the assertions of fact both by the Applicant and the Respondent."[75] The party bearing the burden of proof, therefore, is not necessarily the applicant (i.e., the State that has brought the application before the tribunal) but is rather the party "who . . . raised an issue,"[76] regardless of its procedural position.[77] For instance, the party (applicant or respondent) that relies on an exception, including self-defense, has the burden of proving the facts that are the basis for the exception.[78] It should also be recalled that the distinction between applicant and respondent may not always be clear in inter-

70. Rules of Court, arts. 38–89, 1978 I.C.J. Acts & Docs. 6; Statute of the International Court of Justice arts. 39–64, June 26, 1945, 33 U.N.T.S. 933; I.C.J. Practice Directions of the International Court of Justice, Practice Direction IX, 2007 Acts & Docs. 163.

71. Green, *supra* note 49, at 165.

72. *See* Roger B. Dworkin, *Easy Cases, Bad Law, and Burdens of Proof*, 25 VAND. L. REV. 1151, 1159 (1972) ("No one seems to have trouble understanding that the burden of producing evidence on one issue may shift from party to party as the case progresses.").

73. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 162 (Apr. 20); *see also* NATHAN D. O'MALLEY, RULES OF EVIDENCE IN INTERNATIONAL ARBITRATION: AN ANNOTATED GUIDE 203 n.34 (2012) (explaining the Roman roots of the concept).

74. Teitelbaum, *supra* note 65, at 121.

75. *Arg. v. Uru.*, 2010 I.C.J. para. 162.

76. RIDDELL & PLANT, *supra* note 53, at 89 (citing "an early indication that the Court w[ill] look carefully into which party [is] seeking to rely on certain facts, rather than relying on the traditional applicant/respondent dichotomy.").

77. According to Shabtai Rosenne, "the tendency of the Court is to separate the different issues arising in a case, treating each one separately, applying the rule *actori incumbit probatio*, requiring the party that advances a particular contention to establish it in fact and in law. The result is that each State putting forward a claim is under the general duty to establish its case, without there being any implication that such State is 'plaintiff' or 'applicant' in the sense in which internal litigation uses those terms." SHABTAI ROSENNE, THE LAW AND PRACTICE OF THE INTERNATIONAL COURT, 1920–2005, at 1200–01 (4th ed. 2006),

78. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 57 (Nov. 6); RIDDELL & PLANT, *supra* note 53, at 87.

state litigation, especially when the case is brought before an international court by special agreement between the parties.[79]

The *onus probandi incumbit actori* principle is subject to three main limitations. First, facts that are not disputed or that are agreed upon by the parties do not need to be proven.[80] Second, the Court has relieved a party from the burden of providing evidence of facts that are "notorious" or "of public knowledge."[81] In *Nicaragua*, for instance, the Court found that "since there was no secrecy about the holding of the manoeuvres [sic], the Court considers that it may treat the matter as one of public knowledge, and as such, sufficiently established."[82] As has been noted, "the notion of common or public knowledge has, over the years, expanded, given the wide availability of information on current events in the press and on the [I]nternet."[83] Companies like McAfee, Symantec, Mandiant, and Project Grey Goose, as well as think tanks like NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE), have also published reports on cyber incidents.[84] These reports essentially contain technical analysis of cyber incidents and, with the possible exception of those of the CCD COE, do not normally investigate attribution for legal purposes of those incidents in any depth (if at all).[85] The fact that cyber incidents have received extensive press coverage, as in the case of Stuxnet, may also contribute to the public knowledge character of certain facts. In *Nicaragua,* however, the ICJ warned that "[w]idespread reports of a fact may prove on closer examination to derive from a single source, and such reports, however numerous, will in such case have no greater value as evidence than the original source."[86] The ICJ has also held that the "massive body of information" available to the Court, including newspapers, radio and television reports, may be useful only when it is "wholly consistent and concordant as to the main facts and circumstances of the case."[87]

Third, the *onus probandi incumbit actori* principle only applies to facts, as opposed to the law, which does not need to be proven (*jura novit curia*).[88] It should be noted, however, that, in inter-state litigation, municipal law is a fact that must be

79. RIDDELL & PLANT, *supra* note 53, at 89.; Andrés Aguilar Mawdsley, *Evidence Before the International Court of Justice*, *in* ESSAYS IN HONOUR OF WANG TIEYA 533, 538 (Ronald St. John Macdonald ed., 1994).

80. Wolfrum, *supra* note 36, at 563.

81. *See*, *e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 92 (June 27) (accepting a newspaper report as evidence of notoriety). Judicial notice has been frequently invoked by international criminal tribunals. Teitelbaum, *supra* note 65, at 144–45.

82. *Nicar. v. U.S.,* Judgment, 1986 I.C.J. para. 92.

83. RIDDELL & PLANT, *supra* note 53, at 142–43.

84. TIKK ET AL., *supra* note 14; MANDIANT, 2014 THREAT REPORT [hereinafter MANDIANT, THREAT REPORT], *available at* http://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf; MCAFEE, MCAFEE LABS THREATS REPORT (2014), *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf; SYMANTEC CORP., INTERNET SECURITY THREAT REPORT (2014), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

85. *See generally* TIKK ET AL., *supra* note 14; MANDIANT, THREAT REPORT, *supra* note 84; MCAFEE, *supra* note 84; SYMANTEC CORP., *supra* note 84.

86. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 63.

87. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, para. 13 (May 24).

88. Wolfrum, *supra* note 36, at 556.

proven by the parties invoking it.[89] Furthermore, the ICJ has often distinguished between treaty law and customary international law, holding that the existence and scope of customary rules—especially those of a regional character—must be proven by the parties because one of their two elements, state practice, is factual.[90] A party invoking national legislation or the existence of a general or cyber-specific custom in its favor, therefore, will bear the burden of producing relevant evidence before the Court. Certain authors have suggested that shifting the burden of proof "from the investigator and accuser to the nation in which the attack software was launched" could solve the problems of identification and attribution in the cyber context.[91] In such an approach, international law would require the State where the attack originated to prove that it neither carried out the operation nor negligently allowed others to misuse its infrastructure, as opposed to requiring the accuser to prove the contrary. Similarly, it has been argued that "[t]he fact that a harmful cyber incident is conducted via the information infrastructure subject to a nation's control is *prima facie* evidence that the nation knows of the use and is responsible for the cyber incident."[92] This, however, is not correct. First, mere knowledge does not automatically entail direct attribution, but rather merely a potential violation of the due diligence duty not to allow hostile acts from one's territory.[93] What is more, the views arguing for a reversal of the burden of proof are at odds with the *jurisprudence constante* of the ICJ.[94] In the *Corfu Channel* case, the Court famously found that the exclusive control exercised by a State over its territory "neither involves *prima facie* responsibility nor shifts the burden of proof" in relation to unlawful acts perpetrated therein.[95] The Court, however, conceded that difficulties in discharging the burden of proof in such cases may allow "a more liberal recourse to inferences of fact and circumstantial evidence."[96] This point will be further explored below in Part VI.[97] In *Armed Activities (Dem. Rep. Congo v. Uganda)*, the ICJ also did not shift the burden of proving that Zaire had been in a position to stop the armed groups' actions originating from its border regions, as claimed by Uganda in its counter-claim, from Uganda to the Democratic Republic of the Congo (DRC), and therefore found that it could not "conclude that the absence of action by Zaire's Government against the rebel groups in the border area is tantamount to 'tolerating' or 'acquiescing' in their activities."[98]

89. *Id.* at 557.

90. Asylum Case (Colom. v. Perú), Judgment, 1950 I.C.J. 266, 276–77 (Nov. 20); Rights of Nationals of the United States of America in Morocco (Fr. v. U.S.), Judgment 1952 I.C.J. 176, 200 (Aug. 27).

91. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 249 (2010).

92. Daniel J. Ryan, Maeve Dion, Eneken Tikk & Julie J. C. H. Ryan, *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1185 (2011).

93. *See* Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9) ("It cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein . . . .").

94. *See id.* (stating that control by a State over its borders does not shift the burden of proof to the accused State).

95. *Id.*

96. *Id.*

97. *See infra* Part VI.

98. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 301 (Dec. 19). Judge Kooijmans wrote a separate opinion, arguing that "[i]t is for the

If one applies these findings in the cyber context, the fact that a State has exclusive "territorial" control of the cyber infrastructure from which the cyber operation originates does not per se shift the burden of proof, and it is therefore still up to the claimant to demonstrate that the territorial State is responsible for the cyber operation or that it failed to comply with its due diligence duty of vigilance, and not to the territorial State to demonstrate the contrary.[99]

Even beyond the principle of territorial control, the fact that relevant evidence is in the hands of the other party does not per se shift the burden of proof. In the *Avena* case, the ICJ held that it could not

> accept that, because such information may have been in part in the hands of Mexico, it was for Mexico to produce such information. It was for the United States to seek such information, with sufficient specificity, and to demonstrate both that this was done and that the Mexican authorities declined or failed to respond to such specific requests. . . . The Court accordingly concludes that the United States has not met its burden of proof in its attempt to show that persons of Mexican nationality were also United States nationals.[100]

The fact that cyber operations were conducted in the context of an armed conflict, as was the case of those against Georgia in 2008,[101] also does not affect the normal application of the burden of proof.[102] In *Nicaragua*, the ICJ recalled the *Corfu Channel* and *Tehran Hostages* judgments and found that "[a] situation of armed conflict is not the only one in which evidence of fact may be difficult to come by, and the Court has in the past recognized and made allowance for this . . . ."[103] Even in such circumstances, therefore, "it is the litigant seeking to establish a fact

State under a duty of vigilance to show what efforts it has made to fulfill that duty and what difficulties it has met" and concluding that the Democratic Republic of the Congo (DRC) had not provided evidence to show that it had adopted "credible measures" to prevent transborder attacks. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 306, paras. 82–83 (Dec. 19) (separate opinion of Judge Kooijmans).

99. It should not be forgotten that cyberspace consists of a physical and a syntactic (or logical) layer: 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. David J. Betz & Tim Stevens, *Analogical Reasoning and Cyber Security*, 44 SECURITY DIALOGUE 147, 151 (2013). Cyber operations can then be seen as "the reduction of information to electronic format and the actual movement of that information between physical elements of cyber infrastructure." NILS MELZER, UNIDIR RES., CYBERWARFARE AND INTERNATIONAL LAW 5 (2011), *available at* http://www.isn.ethz.ch/Digital-Library/Publications/ Detail/?lng=en&id=134218. In its 2013 Report, the Group of Governmental Experts established by the UN General Assembly 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." Rep. of the Group of Gov. Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Sec., 68th Sess., 8, U.N. Doc. A/68/98 (June 24, 2013).

100. Avena and Other Mexican Nationals (Mex. v. U.S.), Judgment, 2004 I.C.J. 12, para. 57 (Mar. 31).

101. Markoff, *supra* note 13.

102. *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

103. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1984 I.C.J. 392, para. 101 (Nov. 26).

who bears the burden of proving it . . . ."[104] In the *El Salvador/Honduras* case, the Court stated that it

> fully appreciates the difficulties experienced by El Salvador in collecting its evidence, caused by the interference with governmental action resulting from acts of violence. It cannot however apply a presumption that evidence which is unavailable would, if produced, have supported a particular party's case; still less a presumption of the existence of evidence which has not been produced.[105]

The application of the *onus probandi incumbit actori* principle is also not affected by the possible asymmetry in the position of the litigants in discharging the burden of proof due to the fact that one has acted covertly (as is virtually always the case of cyber operations).[106] As Judge Owada points out in his Separate Opinion attached to the *Oil Platforms* judgment, however, the Court should "take a more proactive stance on the issue of evidence and that of fact-finding" in such cases in order to ensure that the rules of evidence are applied in a "fair and equitable manner" to both parties.[107]

Finally, it has been argued that a reversal of the burden of proof may derive from an application of the precautionary principle based on international environmental law in cyberspace.[108] The precautionary principle entails "the duty to undertake all appropriate regulatory and other measures at an early stage, and well before the (concrete) risk of harm occurs."[109] On this view, States would have an obligation to implement measures to prevent the possible misuse of their cyber infrastructure, in particular by establishing a national cyber security framework.[110] Regardless of whether the precautionary principle, with its uncertain normativity, extends to cyberspace,[111] it still would not lead to a reversal of the burden of proof from the claimant to the State from which a cyber operation originates. In the *Pulp Mills* case, the ICJ concluded that "while a precautionary approach may be relevant in the interpretation and application of the provisions of the Statute [of the River Uruguay], it does not follow that it operates as a reversal of the burden of proof."[112]

104. *Id.*

105. Land, Island and Maritime Frontier Dispute (El Sal./Hond.: Nicar. intervening), Judgment, 1992 I.C.J. 351, para. 63 (Sept. 11).

106. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 306, para. 46 (Nov. 6); (separate opinion of Judge Owada).

107. *Id*. para. 47.

108. *See* Thilo Marauhn, *Customary Rules of International Environmental Law – Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE, *supra* note 34, at 475 (describing the precautionary approach's relationship to international environmental law).

109. Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE, *supra* note 34, at 169.

110. *Id*.

111. *See* Marauhn, *supra* note 108, at 475–76 (asserting doubt that the precautionary principle applies to cyberspace).

112. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 164 (Apr. 20).

The Court, however, did not specify whether the precautionary principle might result in at least a lowering of the standard of proof.[113]

In light of the above discussion, it can be concluded that it is unlikely that the ICJ would accept that there is a reversal of the burden of proof in the cyber context. As has been correctly argued, "suggesting a reversal of the burden of proof could easily lead to wrong and even absurd results given the possibility of routing cyber operations through numerous countries, and to the denouncing of wholly uninvolved and innocent States."[114] In the case of the 2007 DDoS campaign against Estonia, for instance, the botnets included computers located not only in Russia, but also in the United States, Europe, Canada, Brazil, Vietnam and other countries.[115] Difficulties in discharging the burden of proof, which are particularly significant in the context under examination, may, however, result in an alleviation of the standard of proof required to demonstrate a particular fact. It is to this aspect that the analysis now turns.

III. STANDARD OF PROOF AND CYBER OPERATIONS

It is well known that, while in civil law systems there are no specific standards of proof that judges have to apply because they are authorized to evaluate the evidence produced according to their personal convictions on a case-by-case basis, common law jurisdictions employ a rigid classification of standards.[116] From the most to the least stringent, these include: beyond reasonable doubt (i.e., indisputable evidence, a standard used in criminal trials), clear and convincing (or compelling) evidence (i.e., more than probable but short of indisputable), and the preponderance of evidence or balance of probabilities (i.e., more likely than not or reasonably probable, a standard normally used in civil proceedings).[117] A fourth standard is that of *prima facie* evidence—a standard that merely requires indicative proof of the correctness of the contention made.[118]

The Statute of the ICJ and the Rules of Court neither require specific standards of proof nor indicate what methods of proof the Court will consider as being probative in order to meet a certain standard.[119] The ICJ has to date avoided clearly indicating the standards of proof expected from the litigants during the proceedings.[120] It has normally referred to the applicable standard of proof in the

113. *See id.* (discussing the applicability of the precautionary principle to the burden of proof).

114. Geiß & Lahmann, *supra* note 34, at 628.

115. U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 8, at 173.

116. Marko Milanović, *State Responsibility for Genocide*, 17 EUR. J. INT'L L. 553, 594 (2006).

117. Mary Ellen O'Connell, *Rules of Evidence for the Use of Force in International Law's New Era*, 100 AM. SOC'Y INT'L L. PROC. 44, 45 (2006) [hereinafter O'Connell, *Rules of Evidence*]; Milanović, *supra* note 116, at 594; Green, *supra* note 49, at 167.

118. Green, *supra* note 49, at 166; Geiß & Lahmann, *supra* note 34, at 624.

119. *See generally* Statute of the International Court of Justice, June 26, 1945, 33 U.N.T.S. 933; Rules of Court, 1978 I.C.J. Acts & Docs. 6.

120. That approach has been criticized by judges from common law countries. *See*, *e.g.*, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 270, paras. 42–44 (Nov. 6) (separate opinion of Judge Buergenthal) (stating that the Court failed to explain a standard of proof); Oil Platforms (Iran v. U.S.), 2003 I.C.J. 225, paras. 30–39 (Nov. 6)(separate opinion of Judge Higgins) (criticizing the court for not stating a standard of proof).

judgments, but at that point it is of course too late for the parties to take it into account in pleading their cases.[121]

There is no agreement on what standard of proof the ICJ should expect from the parties in the cases before it.[122] If, because of their nature, international criminal courts use the beyond reasonable doubt standard in their proceedings,[123] the most appropriate analogy for inter-state litigation is not with criminal trials, but with certain types of civil litigation.[124] In his Dissenting Opinion in the *Corfu Channel* case, Judge Krylov suggested that "[o]ne cannot condemn a State on the basis of probabilities. To establish international responsibility, one must have clear and indisputable facts."[125] Wolfrum has argued that, while the jurisdiction of an international court over a case should be established beyond reasonable doubt, the ICJ has generally applied a standard comparable to that of preponderance of evidence used in domestic civil proceedings when deciding disputes involving state responsibility.[126] Others have maintained that such a standard only applies to cases not concerning attribution of international wrongful acts, such as border delimitations, and that when international responsibility is at stake, the standard is stricter and requires clear and convincing evidence.[127]

It is therefore difficult, and perhaps undesirable,[128] to identify a uniform standard of proof generally applicable in inter-state litigation or even a predominant one: the Court "tends to look at issues as they arise."[129] This case-by-case approach, however, does not exclude that a standard of proof may be identified having regard to the primary rules in dispute, i.e., "the substantive rules of international law through . . . which the Court will reach its decision."[130] Indeed, when the allegation is the same, it seems logical that the evidentiary standard should also be the same.[131] There are indications, for instance, that claims related to *jus ad bellum* violations, in particular in relation to the invocation of an exception to the prohibition of the use of

121. *See* Teitelbaum, *supra* note 65, at 124 ("The Court's determination of the standard of proof may be said to be made on an *ad hoc* basis, and is only revealed at the end of the process when the Court delivers its judgment."). It has been suggested that "the Court might consider whether, either prior to the submission of written pleadings, after the first round of written pleadings, or prior to the oral hearings, it should ask the parties to meet a specific burden of proof for certain claims." *Id.* at 128).

122. H.E. Judge Rosalyn Higgins, President, Int'l Court of Justice, Speech to the Sixth Committee of the General Assembly 4 (Nov. 2, 2007).

123. Wolfrum, *supra* note 36, at 569.

124. Waxman, *supra* note 57, at 59.

125. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 72 (Apr. 9) (dissenting opinion of Judge Krylov).

126. Wolfrum, *supra* note 36, at 566.

127. RIDDELL & PLANT, *supra* note 53, at 133.

128. Green, *supra* note 49, at 167.

129. Sir Arthur Watts, *Burden of Proof, and Evidence before the ECJ*, *in* IMPROVING WTO DISPUTE SETTLEMENT PROCEDURES: ISSUES AND LESSONS FROM THE PRACTICE OF OTHER INTERNATIONAL COURTS AND TRIBUNALS 289, 294 (Friedl Weiss ed., 2000).

130. ROSENNE, *supra* note 77, at 1043. In Ahmadou Sadio Diallo (Guinea v. Dem. Rep. Congo), Judgment, 2010 I.C.J. 639, para. 54 (Nov. 30), the ICJ makes a similar point with regard to the burden of proof.

131. *See* Green, *supra* note 49, at 169–71 (suggesting that one consistent standard should apply to all cases of self-defense—whatever magnitude the consequences of the violation of the prohibition of the use of force might have—both to the objective and subjective elements of the internationally wrongful act).

force in international relations, have been treated as requiring '"clear and convincing evidence."[132] In the *Nicaragua* judgment, the Court referred to "convincing evidence" of the facts on which a claim is based and to the lack of "clear evidence" of the degree of control exercised by the United States over the *contras*.[133] In the *Oil Platforms* case, the ICJ rejected evidence with regard to Iran's responsibility for mine laying that was "highly suggestive, but not conclusive," holding that "evidence indicative of Iranian responsibility for the attack on the *Sea Isle City*" was insufficient.[134] In *Dem. Rep. Congo v. Uganda*, the ICJ referred again to facts "convincingly established by the evidence," "convincing evidence," and "evidence weighty and convincing."[135] Beyond the ICJ, the Eritrea-Ethiopia Claims Commission also found that there was "clear" evidence that events in the vicinity of Badme were minor incidents and did not reach the magnitude of an armed attack.[136] The above suggests that at least clear and convincing evidence is expected for claims related to the use of force. As self-defense is an exception to the prohibition of the use of force, in particular, the standard of proof should be high enough to limit its invocation to exceptional circumstances and thus avoid abuses.[137]

If clear and convincing evidence is required at least for claims related to the use of armed force, the question arises whether there is a special, and lower, standard in the cyber context, in particular for claims of self-defense against cyber operations. Indeed, "evidentiary thresholds that might have worked well in a world of conventional threats—where capabilities could be judged with high accuracy and the costs of false negatives to peace and security were not necessarily devastating—risk exposing States to unacceptable dangers."[138] There is of course no case law in relation to claims arising out of inter-state cyber operations,[139] so possible indications in this sense have to be found elsewhere. The Project Grey Goose Report on the 2008 cyber operations against Georgia, for instance, relies on the concordance of various pieces of circumstantial evidence to suggest that the Russian government was

132. O'Connell, *Evidence of Terror*, *supra* note 66, at 22; *see also* Teitelbaum, *supra* note 65, at 125–26 (discussing an ICJ case in which the Court applied a standard "similar to" clear and convincing).

133. Green, *supra* note 49, at 172; *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, paras. 24, 29, 62, 109 (June 27) (mentioning both "convincing" and lack of "clear" evidence).

134. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, paras. 71, 61 (Nov. 6). *See also* Green, *supra* note 49, at 172–73; Teitelbaum, *supra* note 65, at 125–26 (arguing that the ICJ uses a clear and convincing standard of evidence).

135. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 72, 91, 136 (Dec. 19). Confusingly, however, in other parts of the Judgment the Court seemed to employ a *prima facie* or preponderance of evidence standard, in particular when it had to determine whether the conduct of armed groups against the DRC was attributable to Uganda. Green, *supra* note 49, at 175–76.

136. Partial Award—Jus Ad Bellum: Ethiopia's Claims 1–8 (Eth. v. Eri.), 26 R.I.A.A. 459, para. 12 (Eri. Eth. Cl. Comm. 2005); *See* O'Connell, *Rules of Evidence*, *supra* note 117117, at 45 (discussing the evidence standard decided in the Ethiopia-Eritrea Jus Ad Bellum Claim).

137. O'Connell, *Lawful Self-Defense*, *supra* note 64, at 898.

138. Waxman, *supra* note 57, at 62. The author argues that "the required degree of certainty about capability ought to vary with certainty about intent." *Id.* at 61. Transposed in the cyber context, when the likelihood that an adversary will be able and willing to use cyber weapons is higher, less evidence will be required to prove it.

139. Herbert Lin, *Cyber Conflict and International Humanitarian Law*, 94 INT'L REV. RED CROSS 515, 524 (2012).

responsible for the operations.[140] In its reply to the U.N. Secretary-General on issues related to information security, the United States claimed that "high-confidence attribution of identity to perpetrators cannot be achieved in a timely manner, if ever, and success often depends on a high degree of transnational cooperation."[141] In a Senate questionnaire fulfilled in preparation for a hearing on his nomination to head of the U.S. Cyber Command, Lieutenant General Keith Alexander argued that "some level of mitigating action" can be taken against cyber attacks "even when we are not certain who is responsible."[142] Similar words were employed by his successor, Vice Admiral Michael S. Rogers: "International law does not require that a nation know who is responsible for conducting an armed attack before using capabilities to defend themselves from that attack."[143] However, Vice Admiral Rogers also cautioned that, "from both an operational and policy perspective, it is difficult to develop an effective response without a degree of confidence in attribution."[144] Overall, the above views seem to suggest an evidentiary standard, based on circumstantial evidence, significantly lower than clear and convincing evidence and even lower than a preponderance of the evidence, on the basis that identification and attribution are more problematic in a digital environment than in the analog world.[145]

It is difficult, however, to see why the standard of proof should be lower simply because it is more difficult to reach it. The standard of proof exists not to disadvantage the claimant, but to protect the respondent against false attribution, which, thanks to tricks like IP spoofing,[146] onion routing,[147] and the use of botnets,[148] is a particularly serious risk in the cyber context. The views mentioned above are also far from being unanimously held, even within the U.S. government: The Air Force

140. *See generally* PROJECT GREY GOOSE, RUSSIA/GEORGIA CYBER WAR—FINDINGS AND ANALYSIS (PHASE I REPORT) (2008), *available at* http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.

141. *Developments in the Field of Information and Telecommunications*, *supra* note 3, at 17.

142. Advance questions for Lieutenant General Keith Alexander for Commander, USA Nominee for Commander, U.S. Cyber Command, S. Comm. Armed Servs. 12 (Apr. 15, 2010), https://epic.org/privacy/nsa/Alexander_04-15-10.pdf.

143. Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, U.S. Cyber Command, S. Comm. Armed Servs. (Mar. 11, 2014), http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

144. *Id*.

145. *See*, *e.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 93 (2010) ("Given the difficulties raised by the traditional requirement to attribute cyber attacks conclusively and directly to a state . . . there is now a growing effort to formulate acceptable alternatives to the notion of 'conclusive attribution.'"). The author seems, however, to confuse attribution criteria and standards of evidence.

146. *See* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 614–15 (2011) ("IP spoofing is a kind of hijacking technique that allows the hacking user to operate a computer while appearing as a trusted host. By thus concealing his true identity, the hacker can gain access to computer networks and network resources.").

147. *See* Christopher Riley, *The Need for Software Innovation Policy*, 5 J. TELECOMM. & HIGH TECH. L. 589, 607 (2007) ("Onion routing protects the anonymity of an Internet user by routing messages through multiple intermediate nodes. Each intermediate node hides the origin of messages in such a way that a reply message can reach the original source node, and yet no node knows more of the path of the message than the nodes immediately before and after it on the message path.").

148. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1034 n.158 (2014) ("A botnet is a set of computers that have been infected with malware and that are controlled by someone other than their users.").

Doctrine for Cyberspace Operations, for instance, States that attribution of cyber operations should be established with "sufficient confidence and verifiability."[149] A report prepared by Italy's Parliamentary Committee on the Security of the Republic goes further and requires it to be demonstrated "*in modo inequivocabile*" (unequivocally) that an armed attack by cyber means originated from a State and was undertaken on the instruction of governmental bodies.[150] The document also suggests that attribution to a State requires "«*prove*» *informatiche inconfutabili*" ("irrefutable digital «evidence»"), which, the Report concedes, is a standard that is very difficult to meet.[151] Germany also highlighted the danger of a lack of "reliable attribution" of malicious cyber activities in creating opportunities for "false flag attacks," misunderstandings, and miscalculations.[152] In relation to the DDoS attacks against Estonia, a U.K. House of Lords document lamented that "the analysis of today is really very elusive, not *conclusive* and it would still be very difficult to act on it."[153] Finally, the AIV/CAVV Report, which has been endorsed by the Dutch government,[154] requires "reliable intelligence . . . before a military response can be made to a cyber attack" and "sufficient certainty regarding the identity of the author of the attack."[155] In its response to the Report, the Dutch government argued that self-defense can be exercised against cyber attacks "only if the origin of the attack and the identity of those responsible are sufficiently certain."[156]

All in all, clear and convincing evidence seems the appropriate standard not only for claims of self-defense against traditional armed attacks, but also for those against cyber operations: a *prima facie* or preponderance of evidence standard might lead to specious claims and false or erroneous attribution, while a beyond reasonable doubt standard would be unrealistic. In the *Norwegian Loans* case, Judge Lauterpacht emphasized that "the degree of burden of proof . . . adduced ought not to be so stringent as to render the proof unduly exacting."[157] As explained by

149. U.S. AIR FORCE, CYBERSPACE OPERATIONS: AIR FORCE DOCTRINE DOCUMENT 3-12, at 10 (2010).

150. COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA, RELAZIONE SULLE POSSIBILI IMPLICAZIONI E MINACCE PER LA SICUREZZA NAZIONALE DERIVANTI DALL'UTILIZZO DELLO SPAZIO CIBERNETICO 26 (2010), *available at* http://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc_XXXIV_n_4.pdf.

151. *Id*.

152. Letter from the Permanent Mission of the Fed. Republic of Ger. to the United Nations addressed to the Office for Disarmament Affairs, Note No. 516/2012 (Nov. 5, 2012). Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INT'L L. STUD. 406, 417 (2013) ("[T]he victim State must tread carefully and seek as much clarity regarding the source of the attack as possible to avoid launching a self-defense response in the wrong direction.").

153. EUROPEAN UNION COMMITTEE, PROTECTING EUROPE AGAINST LARGE-SCALE CYBER-ATTACKS, 2009–2010, H.L. 68, at 42 (emphasis added).

154. Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 280 n.40 (2014); *Government Response to the AIP/CAVV Report on Cyber Warfare*, RIJKSOVERHEID (Apr. 26, 2012), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlageregeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf (Netherlands) [hereinafter GOV'T OF THE NETH.].

155. ADVISORY COUNCIL ON INT'L AFFAIRS & ADVISORY COMM. ON ISSUES OF PUB. INT'L LAW, CYBER WARFARE 22 (2011).

156. GOV'T OF THE NETH., *supra* note 154, at 5. The CCD COE Report on Georgia also concludes that "there is no *conclusive* proof of who is behind the DDoS attacks, even though finger pointing at Russia is prevalent by the media." TIKK ET AL., *supra* note 14, at 12 (emphasis added).

157. Certain Norwegian Loans (Fr. v. Nor.), Judgment, 1957 I.C.J. 9, 39 (July 6) (separate opinion of

Michael Schmitt, a clear and convincing standard "obliges a state to act reasonably, that is, in a fashion consistent with the normal state practice in same or similar circumstances. Reasonable States neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence."[158]

Those who criticize a clear and convincing evidence standard for the exercise of self-defense against cyber operations would rely on the fact that, due to the speed at which such operations may occur and produce their consequences, the requirement of a high level of evidence may in fact render it impossible for the victim State safely to exercise its right of self-defense. Such concerns, however, are exaggerated. Indeed, if the cyber attack was a standalone event that instantaneously produced its damaging effects, a reaction in self-defense would not be necessary. If, on the other hand, the cyber attack were continuing or formed of a series of smaller scale cyber attacks,[159] the likelihood that clear and convincing evidence could be collected would considerably increase.[160]

However, there are also indications that the most serious allegations, such as those involving international crimes, require a higher standard to discharge the burden of proof.[161] As Judge Higgins wrote in her separate opinion attached to the *Oil Platforms* Judgment, "the graver the charge the more confidence must there be in the evidence relied on . . . ."[162] In *Corfu Channel*, the Court appeared to suggest that the standard of proof is higher for charges of "exceptional gravity against a State."[163] In the *Bosnian Genocide* case, the ICJ confirmed that "claims against a State involving charges of exceptional gravity must be proved by evidence that is *fully conclusive* . . . . The same standard applies to the proof of attribution for such acts" (and accordingly applies both to the objective and subjective elements of an international crime) (emphasis added).[164] The Court also found that assistance

Judge Sir Hersch Lauterpacht).

158. Schmitt's exact verbiage calls for a "clear and compelling" standard. Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV 569, 595 (2011).

159. On the application of the doctrine of accumulation of events to cyber operations, see ROSCINI, *supra* note 1, at 108–10.

160. *See* Yoram Dinstein, Professor Emeritus, Tel Aviv University, Cyber War and International Law, Concluding Remarks at the 2012 Naval War College International Law Conference, *in* 89 INT'L L. STUD. 276, 282 (2013) (exemplifying similar reasoning in relation to the identification of the State responsible for the cyber attack).

161. *Contra* Prisoners of War–Eritrea's Claim 17 (Eth. v. Eri.), Partial Award, 26 R.I.A.A. 23, paras. 45–47 (Eri. Eth. Cl. Comm. 2003) (deciding to require clear and convincing evidence, as opposed to a higher burden of proof, because the Commission is "not a criminal tribunal").

162. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 225, para. 33 (Nov. 6) (separate opinion of Judge Higgins).

163. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 17 (Apr. 9). This interpretation of the Court's judgment, however, is not uncontroversial. *See* Andrea Gattini, *Evidentiary Issues in the ICJ's* Genocide *Judgment*, 5 J. INT'L CRIM. JUST. 889, 896 (2007) ("The Court somehow hid behind a quotation from the *Corfu Channel* case, where it had been stated that 'a charge of such exceptional gravity against a State would require a degree of certainty that has not been reached here.'").

164. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 209 (Feb. 26) (emphasis added); s*ee also U.K. v. Alb.*, 1949 I.C.J. at 17. It is not entirely clear whether the Court linked the notion of gravity to the importance of the norm allegedly breached or the magnitude of the violation. It would seem more correct to refer to the gravity as linked to the former, as, if the evidentiary standard depended on the

provided by Yugoslavia to the Bosnian Serbs had not been "established beyond any doubt."[165] Gravity is, of course, inherent in any *jus cogens* violation.[166] Claims of reparation for cyber operations qualifying as war crimes, crimes against humanity, or acts of genocide, therefore, should require fully conclusive evidence, not just evidence that is clear and convincing. As has been aptly suggested, however, "[a] higher standard of proof may only be justified if the Court is willing to balance this strict approach with a more active use of its fact-finding powers to make sure that claims for breaches of *jus cogens* norms are not doomed to fail merely on evidential grounds."[167]

In the *Bosnian Genocide* judgment, the Court also appeared to make a distinction between a violation of the prohibition of committing acts of genocide, for which evidence must be "fully conclusive," and a violation of the obligation to prevent acts of genocide, where the Court required "proof at a high level of certainty appropriate to the seriousness of the allegation,"[168] even though not necessarily fully conclusive evidence.[169] Such an approach appears justified by the different nature of the obligation breached: Indeed, presumptions and inferences necessarily play a more significant role when the wrongful act to be proved consists of an omission, as is the case of the breach of an obligation to prevent.[170] By the same token, it may be suggested that the standard of proof required to prove that a State has conducted cyber operations amounting to international crimes is higher than that required to prove that it did not exercise the necessary due diligence to stop its cyber infrastructure from being used by others to commit international crimes.

IV. METHODS OF PROOF AND CYBER OPERATIONS

What type of evidence may be relied on in order to meet the required standard of proof and establish that a cyber operation has occurred, has produced damage, and is attributable to a certain State or non-state actor? The production of evidence before the ICJ is regulated by Articles 48 to 52 of its Statute and by the Rules of Court. There is, however, no list of the methods of proof available to parties before the Court nor any indication of their different probative weight.[171] Article 48 of the ICJ Statute provides only that "[t]he Court shall . . . make all arrangements

latter, "some States could have a perverse incentive to sponsor more devastating attacks so as to raise the necessary burden of proof and potentially defeat accountability." Shackelford & Andres, *supra* note 34, at 990.

165. *Bosn. & Herz. v. Serb. & Montenegro,* 2007 I.C.J. para. 422.

166. *See* Sévrine Knuchel, *State Immunity and the Promise of* Jus Cogens, 9 NW. J. INT'L HUM. RTS. 149, 172 (2011) (describing the *Ferrini* case, which illustrates the Court's "reli[ance] on *jus cogens* not as a conflict rule, but rather as a means of highlighting the seriousness of the acts committed by the foreign State . . . .").

167. Benzing, *supra* note 56, at 1266.

168. *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. paras. 209–10.

169. Benzing, *supra* note 56, at 1266.

170. Gattini, *supra* note 163, at 899. In *Nicaragua*, the Court had already found that the fact that Nicaragua had to prove a negative (the non-supply of arms to rebels in neighboring countries) had to be borne in mind when assessing the evidence. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, para. 147 (June 27).

171. *Compare* Statute of the International Court of Justice arts. 48–52, June 26, 1945, 33 U.N.T.S. 933, *and* Rules of Court, arts. 57, 58, 62–64, 71, 1978 I.C.J. Acts & Docs. 6 (together demonstrating that there are no methods of proof for dealing with the production of evidence before the ICJ).

connected with the taking of evidence,"[172] while Article 58 of the Rules of Court confirms that "the method of handling the evidence and of examining any witnesses and experts . . . shall be settled by the Court after the views of the parties have been ascertained in accordance with Article 31 of these Rules."[173]

As a leading commentator has observed, "[t]he International Court of Justice has construed the absence of restrictive rules in its Statute to mean that a party may generally produce any evidence as a matter of right, so long as it is produced within the time limits fixed by the Court."[174] Although it is primarily the parties' responsibility to produce the evidence necessary to prove the facts alleged, the Court may also order the production of documents, call experts and witnesses, conduct site visits, and request relevant information from international organizations.[175] In *Nicaragua*, for instance, the Court found that it was "not bound to confine its consideration to the material formally submitted to it by the parties."[176] In that judgment, the ICJ also emphasized the principle of free assessment of evidence, stating that "within the limits of its Statute and Rules, [the Court] has freedom in estimating the value of the various elements of evidence . . . ."[177]

In the next pages, methods of proof that may be relevant in relation to cyber operations will be examined.

A. Documentary Evidence

Although there is no formal hierarchy between different sources, the ICJ has taken a civil law court approach and has normally given primacy to written documents over oral evidence.[178] Documentary evidence includes "all information submitted by the parties in support of the contentions contained in the pleadings other than expert and witness testimony."[179] According to Shabtai Rosenne, documentary evidence can be classified in four categories:

> published treaties included in one of the recognized international or national collections of treaty texts; official records of international organizations and of national parliaments; published and unpublished diplomatic correspondence, and communiqués and other miscellaneous materials, including books, maps, plans, charts, accounts, archival material,

172. Statute of the International Court of Justice art. 48, June 26, 1945, 33 U.N.T.S. 933.

173. Rules of the Court, art. 58, 2007 I.C.J. Acts & Docs. 91.

174. DURWARD V. SANDIFER, EVIDENCE BEFORE INTERNATIONAL TRIBUNALS 184 (rev. ed. 1975).

175. Statute of the International Court of Justice arts. 49, 50, June 26, 1945, 33 U.N.T.S. 933; Rules of Court, arts. 62, 66, 67, 69, 1978 I.C.J. Acts & Docs. 6.

176. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 30 (June 27). *See* Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933; Rules of the Court, art. 62, 2007 I.C.J. Acts & Docs. 91.

177. *Nicar. v. U.S.*, 1986 I.C.J. para. 60. *See also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 59 (Dec. 19) (explaining the Court's own considerations regarding the weight of the evidence).

178. RIDDELL & PLANT, *supra* note 53, at 232; Aguilar Mawdsley, s*upra* note 79, at 543.

179. Wolfrum, *supra* note 36, at 558.

> photographs, films, legal opinions and opinions of experts, etc.; and affidavits and declarations.[180]

Although the Court has the power to call upon the parties to produce any evidence it deems necessary or to seek such evidence itself, it has normally refrained from doing so and has relied on that spontaneously produced by the litigants.[181] All documents not "readily available" must be produced by the interested party.[182] A "publication readily available" is a document "available in the public domain . . . in any format (printed or electronic), form (physical or on-line, such as posted on the internet) or on any data medium (on paper, on digital or any other media) . . . [that] should be accessible in either of the official languages of the Court," and which it is possible to consult "within a reasonably short period of time."[183] The accessibility should be assessed in relation to the Court and the other litigant.[184] The fact that a publication is "readily available" does not necessarily render the concerned facts public knowledge, but rather relieves the party from the burden of having to produce it.[185] The facts, however, still need to be proved.[186]

Official state documents, such as national legislation, cyber doctrines, manuals, strategies, directives and rules of engagement, may become relevant in establishing state responsibility for cyber operations.[187] In *Nicaragua*, for instance, the responsibility of the United States for encouraging violations of international humanitarian law was established on the basis of the publication of a manual on psychological operations.[188] According to the Court, "[t]he publication and dissemination of a manual in fact containing the advice quoted above must . . . be regarded as an encouragement, which was likely to be effective, to commit acts

180. ROSENNE, *supra* note 77, at 1246 (footnotes omitted). In the *Bosnian Genocide* Judgment, the Court noted that the parties had produced

> reports, resolutions and findings by various United Nations organs, including the Secretary-General, the General Assembly, the Security Council and its Commission of Experts, and the Commission on Human Rights, the Sub-Commission on the Prevention of Discrimination and Protection of Minorities and the Special Rapporteur on Human Rights in the former Yugoslavia; documents from other inter-governmental organizations such as the Conference for Security and Co-operation in Europe; documents, evidence and decisions from the ICTY; publications from governments; documents from non-governmental organizations; media reports, articles and books.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 211 (Feb. 26); *see also Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 60.

181. Practice Directions of the International Court of Justice, Practice Direction IX bis, paras. (2)(i)–(ii), 2007 Acts & Docs. 163.

182. *Id.*

183. *Id.*

184. *Id.*

185. Rules of Court, art. 56(4), 1978 I.C.J. Acts & Docs. 6. Benzing, *supra* note 56, at 1241.

186. Benzing, *supra* note 56, at 1241.

187. *See* Mark D. Young, *National Cyber Doctrine: The Missing Link in the Application of American Cyber Power*, J. NAT'L SECURITY L. & POL'Y 173, 175–76 (2010) (arguing that a cyber security doctrine can answer questions concerning the roles and responsibilities in cyber operations and events such as cyber attacks).

188. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 113 (June 27).

contrary to general principles of international humanitarian law reflected in treaties."[189] Not all state documents, however, have the same probative value: in *Democratic Republic of the Congo v. Uganda*, the Court dismissed the relevance of certain internal military intelligence documents because they were unsigned, unauthenticated, or lacked explanation of how the information was obtained.[190]

Military cyber documents are frequently classified in whole or in part for national security reasons.[191] According to the doctrine of privilege in domestic legal systems, litigants may refuse to submit certain evidence to a court on confidentiality grounds. No such doctrine exists before the ICJ.[192] One could actually argue that there is an obligation on the litigants to cooperate in good faith with the Court in the proceedings before it, and therefore to produce all requested documents.[193] There is, however, no sanction for failure to do so: Article 49 of the ICJ Statute limits itself to providing that "[t]he Court may, even before the hearing begins, call upon the agents to produce any document or to supply any explanations. *Formal note shall be taken of any refusal*."[194] While the International Criminal Tribunal for the former Yugoslavia (ICTY) has found that "to grant States a blanket right to withhold, for security purposes, documents necessary for trial might jeopardise the very function of the International Tribunal, and 'defeat its essential object and purpose'."[195] The ICJ has been reluctant to draw inferences from the refusal of a party to produce confidential documents.[196] The problem has arisen twice before the Court: in the *Corfu Channel* and in the *Bosnian Genocide* cases. In the former, the ICJ called the United Kingdom, pursuant to Article 49 of the Statute, to produce an admiralty order.[197] The United Kingdom refused to produce the document on grounds of naval secrecy,[198] and witnesses also refused to answer questions in relation to the document.[199] The ICJ decided not to "draw from this refusal to produce the orders any conclusions differing from those to which the actual events gave rise."[200] In the

189. *Id.* para. 256.

190. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 125, 127–28, 133–34, 137 (Dec. 19).

191. *See* Sean Lyngaas, *New Cyber Doctrine Shows More Offense, Transparency*, FCW (Oct. 24, 2014), http://fcw.com/articles/2014/10/24/cyber-offense.aspx (discussing the "past military practice of over-classifying discussions of strategy").

192. One of the problems with applying the doctrine of privilege in inter-state litigation is that international courts are unlikely to be able to verify whether state security interests are genuinely jeopardized by the document disclosure. RIDDELL & PLANT, *supra* note 54, at 208.

193. It has been observed that "when a State becomes a party to the Statute of the ICJ, it necessarily accepts the obligation to produce before the Court all evidence available to it in any case it contests." *Id.* at 49.

194. Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933 (emphasis added).

195. Prosecutor v. Blaškić, Case No. IT-95-14-AR, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, para. 65 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 29, 1997).

196. *E.g.*, Anthony Carty, *The Corfu Channel Case–And the Missing Admiralty Orders,* 3 L. & PRAC. INT'L CTS. & TRIBUNALS 1, 1 (2004) (detailing an instance in which the ICJ did not draw inferences from the failure of the Royal Navy to turn over confidential documents).

197. *Id.*

198. *Id.*

199. Benzing, *supra* note 56, at 1243.

200. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 32 (Apr. 9).

Bosnian Genocide case, even though Bosnia and Herzegovina had called upon the Court to request Serbia and Montenegro to produce certain documents classified as military secrets, the Court decided not to proceed with the request, although it reserved the right subsequently to request the documents *motu proprio*.[201] In its judgment, the ICJ limited itself to noting "the Applicant's suggestion that the Court may be free to draw its own conclusions" from the fact that Serbia and Montenegro had not produced the document voluntarily.[202] However, it does not seem that the Court ultimately drew any inferences from Serbia's non-disclosure of the classified documents.[203] It should be noted that, in both of the above-mentioned cases, alternative evidence was available to the Court.[204] It has been suggested that "it remains a matter of conjecture how the ICJ might respond in cases where a confidential communication is the only possible evidence to determine the veracity of a factual assertion, and no alternative materials are available."[205] A possible solution is that any classified information be produced in closed sittings of the court.[206]

Documents of international organizations may also be presented as evidence.[207] Overall, the Court has given particular credit to U.N. reports, Security Council resolutions, and other official U.N. documents.[208] In *Bosnian Genocide*, the ICJ stated that the probative value of reports from official or independent bodies "depends, among other things, on (1) the source of the item of evidence (for instance, partisan or neutral), (2) the process by which it has been generated (for instance an anonymous press report or the product of a careful court or court-like process), and (3) the quality of the character of the item (such as statements against interest, and agreed or uncontested facts)."[209] Several documents of international organizations address cyber issues.[210] In particular, information security has been on the U.N. agenda since 1998, when the Russian Federation introduced a draft resolution in the First Committee of the U.N. General Assembly.[211] Since then, the General Assembly has adopted a series of annual resolutions on the topic.[212] The resolutions have called for the views of the U.N. Member States on information security and established three Groups of Governmental Experts that have examined threats in cyberspace and discussed "cooperative measures to address them."[213]

201. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 44 (Feb. 26).

202. *Id*. para. 206.

203. RIDDELL & PLANT, *supra* note 53, at 214.

204. *See generally* Carty, *supra* note 196; *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. 43.

205. RIDDELL & PLANT, *supra* note 53, at 217.

206. *Id*. at 218; Benzing, *supra* note 56, at 1243.

207. *See* RIDDELL & PLANT, *supra* note 53, at 85–87.

208. Teitelbaum, *supra* note 65, at 146.

209. *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. para. 227. In the case of the "Fall of Srebrenica" Report of the Secretary-General, the Court concluded that "the care taken in preparing the report, its comprehensive sources and the independence of those responsible for its preparation all lend considerable authority to it." *Id.* para. 229–30.

210. *E.g.*, G.A. Res. 66/24, at 2, U.N. Doc. A/RES/66/24 (Dec 13, 2011) (expressing concern over "international information security").

211. *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. OFFICE FOR DISARMAMENT AFFAIRS, http://www.un.org/disarmament/topics/informationsecurity/ [hereinafter U.N. OFFICE FOR DISARMAMENT AFFAIRS].

212. *Id.*

213. *Id.*

While the first Group, established in 2004, did not produce a substantive report,[214] the second, created in 2009, issued a report in 2010,[215] and the third Group, which met between 2012 and 2013, also adopted a final report containing a set of recommendations.[216] In addition, the views of U.N. Member States on information security are contained in the annual reports of the U.N. Secretary-General on developments in the field of information and telecommunications in the context of international security.[217]

The Court has also relied on fact-finding from commissions and other courts.[218] In *Dem. Rep. Congo v. Uganda*, the Court considered the Report of the Porter Commission, observing that neither party had challenged its credibility.[219] Furthermore, the Court accepted that "evidence [included in the Report] obtained by examination of persons directly involved, and who were subsequently cross-examined by judges skilled in examination and experienced in assessing large amounts of factual information, some of it of a technical nature, merits special attention."[220] For these reasons, facts alleged by the parties that found confirmation in the Report were considered clearly and convincingly proved.[221] There are, however, no examples of reports by judicial commissions in relation to cyber operations.[222] One can at best recall the 2009 Report of the Independent Fact-Finding Mission on the Conflict in Georgia established by the Council of the European Union,[223] which briefly addressed the cyber operations against Georgia.[224] The Report, however, is not of great probative weight, as it did not reach any conclusion on those operations' attribution or legality, simply noting 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."[225] Even if not of

214. U.N. Office for Disarmament Affairs, Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security, http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

215. Grp. of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Sec., Developments in the Field of Information and Telecommunications in the Context of International Security, 65th Sess., U.N. Doc. A/65/201 (July 30, 2010).

216. Grp. of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Sec., Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc A/68/98 (June 24, 2013).

217. *See* U.N. OFFICE FOR DISARMAMENT AFFAIRS, *supra* note 211 (collecting such annual reports).

218. Teitelbaum, *supra* note 65, at 152.

219. *Id.*; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, para. 60 (Dec. 19).

220. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 61.

221. *See* Teitelbaum, *supra* note 65, at 153 ("It appears that when a fact alleged by one of the parties was confirmed by one of the findings of the Porter Commission, the Court accepted the evidence has having met a clear and convincing standard of proof.").

222. *See generally* Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 A.F. L. REV. 121, 121–73 (2009) (providing a holistic review of international cyber operations with no reference to judicial commission reports).

223. INDEP. INT'L FACT-FINDING MISSION ON THE CONFLICT IN GEOR., REPORT 2 (2009), http://rt.com/files/politics/georgia-started-ossetian-war/iiffmcg-volume-ii.pdf.

224. *Id.* at 217–19.

225. *Id.* at 219.

use to establish attribution, however, the Report could be relied on to establish that the cyber operations against Georgia did in fact occur.[226]

Documents produced by NGOs and think tanks may also play an evidentiary role, albeit a limited one. In relation to cyber operations, the CCD COE has prepared reports containing technical and legal discussion of the Estonia, Georgia and Iran cases, as well as of other cyber incidents.[227] Project Grey Goose produced an open source investigation into cyber conflicts, including the 2008 cyber attacks on Georgia.[228] In that case, the Report concluded "with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions."[229] Information security companies like Symantec, McAfee, and Mandiant also regularly compile detailed technical reports on cyber threats and specific incidents.[230] In general, however, reports from NGOs and other non-governmental bodies have been considered by the ICJ as having less probative value than publications of States and international organizations and have been used in a corroborative role only.[231] In *Democratic Republic of the Congo v. Uganda*, for instance, the ICJ considered a report by International Crisis Group not to constitute "reliable evidence."[232] Similarly, in *Oil Platforms* the Court did not find publications such as *Lloyd's Maritime Information Service*, the *General Council of British Shipping* or *Jane's Intelligence Review* to be authoritative public sources, as it had no "indication of what was the original source, or sources, or evidence on which the public sources relied."[233] This "unequal treatment" of documents of international organizations and NGOs has been criticized: "the correct approach is for the Court to apply its general evaluative criteria to documents produced by NGOs just as it does to those generated by UN actors."[234]

As far as press reports and media evidence are concerned, one may recall, in the cyber context, the above-mentioned *New York Times* articles attributing Stuxnet to the United States and Israel.[235] The ICJ, however, has been very reluctant to accept press reports as evidence and has treated them "with great caution."[236] Press reports that rely only on one source, rely on an interested source, or give no account of their

226. *See id.* at 217–19 (detailing the occurrences that point to a clear indication that cyber attacks took place against Georgia).

227. The CCD COE is a think tank based in Tallinn, Estonia that was created after the 2008 DDoS attacks against the Baltic state. *NATO Opens New Centre of Excellence on Cyber Defence*, NATO (May 14, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html. It is not integrated into NATO's structure or funded by it. *Id.* Its reports can be accessed at https://www.ccdcoe.org/publications.html.

228. *See generally* PROJECT GRAY GOOSE, *supra* note 140.

229. *Id.* at 3.

230. *See*, *e.g.*, MANDIANT, APT1, *supra* note 30, at 1–74 (compiling one such report about China's cyber espionage unit).

231. RIDDELL & PLANT, *supra* note 53, at 249.

232. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 129 (Dec. 19).

233. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 60 (Nov. 6).

234. RIDDELL & PLANT, *supra* note 53, at 250.

235. *See supra* text accompanying notes 18–21.

236. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 62 (June 27).

sources have therefore been treated as having no probative value.[237] In the *Bosnian Genocide* case, the Court dismissed an article in *Le Monde*, qualifying it as "only a secondary source."[238] In *Nicaragua*, the Court held that, even when they meet "high standards of objectivity," it would regard the reports in press articles and extracts from books presented by the parties "not as evidence capable of proving facts, but as material which can nevertheless contribute, in some circumstances, to corroborating the existence of a fact, i.e., as illustrative material additional to other sources of evidence."[239] This was dependent on the sources being "wholly consistent and concordant as to the main facts and circumstances of the case."[240] It has been suggested that this expression means that "the press reports in question would have to confirm the facts as alleged by both of the parties, or confirm facts that have not been denied or contested by the parties."[241]

Apart from this, press reports may contribute, together with other sources, to demonstrate public knowledge of facts of which the Court may take judicial notice, thus relieving a party from having to discharge the burden of proof with regard to those facts.[242] The fact that cyber incidents like Stuxnet have received extensive media coverage—and that the *New York Times* article has been followed by many others, including in *The Washington Post*[243]—would not, however, as such increase their probative weight or mean that the covered facts are of public knowledge.[244] As already mentioned, in *Nicaragua* the ICJ noted that "[w]idespread reports of a fact may prove on closer examination to derive from a single source, and such reports, however numerous, will in such case have no greater value as evidence than the original source."[245]

B. Official Statements

Statements made by official authorities outside the context of the judicial proceedings may play an important evidentiary role. In the *Tehran Hostages* case, for instance, the ICJ recalled that it had "a massive body of information from various sources concerning the facts and circumstances of the present case, including numerous official statements of both Iranian and United States authorities."[246]

237. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 68.

238. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 357 (Feb. 26).

239. *Nicar. v. U.S.*, 1986 I.C.J. para. 62.

240. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 68 (citing United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, para. 13 (May 24))

241. Teitelbaum, *supra* note 65, at 140.

242. *Nicar. v. U.S.*, 1986 I.C.J. para. 63.

243. *See* Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html (discussing the similarities between Stuxnet and the sophisticated virus known as "Flame").

244. *See*, *e.g.*, *Nicar. v. U.S.*, 1986 I.C.J. para. 63 (explaining that extensive reports and coverage do not necessarily provide probative evidentiary weight).

245. *Id.*

246. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, para. 13 (May 24).

Statements "emanating from high-ranking official political figures, sometimes indeed of the highest rank, are of particular probative value when they acknowledge facts or conduct unfavourable to the State represented by the person who made them."[247] However, all depends on how those statements were made public: "evidently, [the Court] cannot treat them as having the same value irrespective of whether the text is to be found in an official national or international publication, or in a book or newspaper."[248] In other words, statements that can be directly attributed to a state are of more probative value.

The U.S. Department of Defense's *Assessment of International Legal Issues in Information Operations* confirms that "[s]tate sponsorship might be persuasively established by such factors as . . . public statements by officials."[249] There does not seem to be, however, any official statement by Russian or Chinese authorities directly or even indirectly acknowledging responsibility for the cyber operations against Estonia, Georgia, and the United States; on the contrary, involvement was denied.[250] With regard to Stuxnet, U.S. and Israeli authorities neither admitted nor denied attribution when asked questions about the incident.[251] Whether this allows inferences to be drawn is discussed below.[252]

C. Witness Testimony

Witnesses may be called to provide direct oral evidence by the Court and by the litigants: The latter case is conditioned upon the absence of objections by the other litigant or the recognition by the Court that the evidence is likely to be relevant.[253] The Court may also put questions to the witnesses and experts called by the parties.[254] The ICJ has not made extensive use of oral evidence.[255] In *Corfu Channel*, for instance, naval officers were called to testify by the United Kingdom about the damage suffered by the Royal Navy ships and the nature and origin of the mines.[256] Albania also called witnesses to testify to the absence of mines in the Channel.[257] Nicaragua called five witnesses to testify in the *Nicaragua* case.[258] In the same case,

247. *Nicar. v. U.S.*, 1986 I.C.J. para. 64.

248. *Id.* para. 65.

249. U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 21 (1999), http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [hereinafter ASSESSMENT OF INTERNATIONAL LEGAL ISSUES].

250. *See*, *e.g.*, Klimburg, *supra* note 12, at 41–42 (discussing Russian and Chinese involvement in cyber warfare and plausible deniability of such actions).

251. Richmond, *supra* note 21, at 855; Williams, *supra* note 28.

252. *See infra* Part V (discussing possible inferences).

253. Rules of Court, arts. 62(2), 63, 1978 I.C.J. Acts & Docs. 6. It should be recalled that international courts and tribunals do not normally have the authority or the capability to issue *subpoena* to coercively bring a witness before them. Wolfrum, *supra* note 36, at 560.

254. Rules of Court, art. 65, 1978 I.C.J. Acts & Docs. 6.

255. See the cases in Aguilar Mawdsley, *supra* note 79, at 543.

256. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 7–8, 10 (Apr. 9).

257. *Id.* at 11.

258. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 13 (June 27).

the Court noted that "testimony of matters not within the direct knowledge of the witness, but known to him only from hearsay" is not "of much weight."[259]

It is worth recalling that the Court has also accepted witness evidence given in written form and attached to the written pleadings, but it has treated it "with caution"[260] and has generally considered it of a probative value inferior to that of direct oral witness testimony.[261] Factors to be considered in assessing the probative weight of affidavits include time, purpose and context of production, whether they were made by disinterested witnesses, and whether they attest to the existence of facts or only refer to an opinion with regard to certain events.[262]

D. Enquiry and Experts

According to Article 50 of the ICJ Statute, "[t]he Court may, at any time, entrust any individual, body, bureau, commission, or other organization that it may select, with the task of carrying out an enquiry or giving an expert opinion."[263] Enquiries have never been commissioned by the Court, which has rather relied on fact-finding reports from other sources.[264] Experts may be necessary in cases of a highly technical nature or that involve expertise not possessed by the judges.[265] It is likely, therefore, that the Court will appoint experts in cases involving cyber technologies. The Court, however, would not be bound by their report.

The parties may also call experts.[266] As to the form of their participation in the oral proceedings, in *Pulp Mills* the ICJ reminded the parties that:

> [T]hose persons who provide evidence before the Court based on their scientific or technical knowledge and on their personal experience should testify before the Court as experts, witnesses or in some cases in both capacities, rather than counsel, so that they may be submitted to questioning by the other party as well as by the Court.[267]

In the *Whaling in the Antarctic* case, therefore, the experts called by both Australia and Japan gave evidence as expert witnesses and were cross-examined,[268] and the Court relied heavily on their statements to conclude that the special permits granted

259. *Id*. para. 68.

260. Territorial and Maritime Dispute Between Nicaragua and Honduras in the Caribbean Sea (Nicar. v. Hond.), Judgment, 2007 I.C.J. 659, para. 244 (Oct. 8).

261. *See* RIDDELL & PLANT, *supra* note 53, at 280–81 (noting the Court's "similar view of the inferiority of affidavit evidence relative to direct witness testimony").

262. *Nicar. v. Hond*., 2007 I.C.J. para. 244.

263. Statute of the International Court of Justice art. 50, June 26, 1945, 33 U.N.T.S. 933.

264. Benzing, *supra* note 56, at 1259. For criticism of this practice, see Joyce, *supra* note 68, at 283 (calling for reform of fact-finding processes for the ICJ).

265. In the *Corfu Channel* Case, the Court appointed a Committee of Experts because of the insurmountable differences of opinion between the parties on certain facts. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 9 (Apr. 9).

266. Rules of Court, art. 63, 1978 I.C.J. Acts & Docs. 6.

267. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 167 (Apr. 20).

268. Whaling in the Antarctic (Aust. v. Japan: N.Z. intervening), Judgment, 2014 I.C.J. 148, paras. 20–21 (Mar. 31).

by Japan for the killing, taking, and treatment of whales had not been granted "for purposes of scientific research."[269]

E. Digital Evidence

Digital forensics "deals with identifying, storing, analyzing, and reporting computer finds, in order to present valid digital evidence that can be submitted in civil or criminal proceedings."[270] It includes the seizure, forensic imaging, and analysis of digital media, and the production of a report on the evidence so collected.[271] It seems that most countries "do not make a legal distinction between electronic evidence and physical evidence. While approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence."[272] Of course, not only do data have to be collected, but they also need to be interpreted, and the parties may disagree on their interpretation.

For several reasons, however, digital evidence on its own is unlikely to play a decisive role in establishing state responsibility for cyber operations. First, digital evidence is "volatile, has a short life span, and is frequently located in foreign countries."[273] Second, the collection of digital evidence can be very time consuming and requires the cooperation of the relevant internet service providers, which may be difficult to obtain when the attack originates from other States.[274] Third, although digital evidence may lead to the identification of the computer or computer system from which the cyber operation originates, it does not necessarily identify the individual(s) responsible for the cyber operation (as the computer may have been hijacked, or the IP spoofed).[275] In any case, such digital evidence will say nothing about whether the conduct of those individuals can be attributed to a State under the law of state responsibility.[276]

269. *See id.* para. 227.

270. PRESIDENCY OF THE COUNCIL OF MINISTERS, NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY 42 (2013), *available at* http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

271. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 482 (2012) (describing traceback technology as a way to "identify the source of the attack"); U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, Section 9344 (2011) *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section %20934%20Report_For%20webpage.pdf (discussing ways the U.S. Department of Defense is seeking to improve attribution capabilities through behavior-based algorithms).

272. U.N. OFFICE ON DRUGS AND CRIME, COMPREHENSIVE STUDY ON CYBERCRIME: DRAFT—FEBRUARY 2013, xxiv (2013), *available at* http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf.

273. Fred Schreier, *On Cyberwarfare* 65 (DCAF Horizon 2015, Working Paper No. 7, 2012).

274. *Id.* at 46.

275. *Id.* at 65.

276. *Cf.* TALLINN MANUAL r. 6–7 (noting various ways in which a State might be held responsible for cyber action taken by State and non-state actors).

V. PRESUMPTIONS AND INFERENCES IN THE CYBER CONTEXT

As Judge ad hoc Franck emphasized in *Sovereignty over Pulau Ligitan and Pulau Sipadan*, "[p]resumptions are necessary and well-established aspects both of common and civil law and cannot but be a part of the fabric of public international law."[277] Previously, in his dissenting opinion in *Corfu Channel*, Judge Azevedo had argued that "[i]t would be going too far for an international court to insist on direct and visual evidence and to refuse to admit, after reflection, a reasonable amount of human presumptions with a view to reaching that state of moral, human certainty with which, despite the risk of occasional errors, a court of justice must be content."[278]

Although the difference is often blurred in inter-state litigation, presumptions may be prescribed by law (legal presumptions, or presumptions of law), or be reasoning tools used by the judges (presumptions of fact, or inferences).[279] In other words, "[p]resumptions of law derive their force from *law*, while presumptions of fact derive their force from *logic*."[280] In international law, presumptions of law can derive from treaties, international customs, and general principles of law.[281] According to Judge Owada in his dissenting opinion in the *Whaling in the Antarctic* case, for instance, good faith on the part of a contracting State in performing its obligations under a treaty "has necessarily to be presumed,"[282] although the presumption is subject to rebuttal.[283]

Inferences, or presumptions of fact, are closely linked to circumstantial evidence.[284] In the *Corfu Channel* case, Judge Padawi Pasha defined circumstantial evidence as "facts which, while not supplying immediate proof of the charge, yet make the charge problable [sic] with the assistance of reasoning."[285] Inferences "convincingly" establishing state sponsorship for cyber operations are suggested in the U.S. Department of Defense's *Assessment of International Legal Issues in Information Operations*, including "the state of relationships between the two countries, the prior involvement of the suspect State in computer network attacks,

277. Sovereignty over Pulau Ligitan & Pulau Sipadan (Indon./Malay.), Judgment, 2002 I.C.J. 691, para. 44 (Dec. 17) (dissenting opinion of Judge ad hoc Franck).

278. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 90–91 (Apr. 9) (dissenting opinion of Judge Azevedo).

279. *See* C.F. Amerasinghe, *Presumptions and Inferences in Evidence in International Litigation*, 3 L. & PRAC. INT'L CTS. & TRIBUNALS 395, 395 (2004) (distinguishing irrebuttable presumptions (*juris et de jure*) from rebuttable ones (*juris tantum*) because the former are immune to evidence proving facts that contradict them, while the latter shift the burden of demonstrating the opposite to the other litigant).

280. Thomas M. Franck & Peter Prows, *The Role of Presumptions in International Tribunals*, 4 L. & PRAC. INT'L CTS. & TRIBUNALS 197, 203 (2005) (internal citations omitted).

281. MOJTABA KAZAZI, BURDEN OF PROOF AND RELATED ISSUES: A STUDY ON EVIDENCE BEFORE INTERNATIONAL TRIBUNALS 245 (1996).

282. Whaling in the Antarctic (Austl. v. Japan: N.Z. intervening), Judgment, 2014 I.C.J. 148, para. 21 (Mar. 31) (dissenting opinion of Judge Owada).

283. *Id.* para. 42.

284. RIDDELL & PLANT, *supra* note 53, at 113; *see also* Barcelona Traction, Light and Power Company, Limited. (Belg. v. Spain), 1964 I.C.J. 6, 80 (July 24) (separate opinion of Judge Bustamante) ("[It may] be possible to arrive at a conclusion on the basis merely of inferences or deductions forming part of a logical process . . . .").

285. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 59 (Apr. 9) (dissenting opinion of Judge Pasha).

the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks."[286] In its reply to the U.N. Secretary-General on issues related to information security, the United States also claimed that "the identity and motivation of the perpetrator(s) can only be inferred from the target, effects and other circumstantial evidence surrounding an incident."[287] The commentary to Rule 11 of the *Tallinn Manual* refers to inferences from "the prevailing political environment, whether the . . . operation portends the future use of military force, the identity of the attacker, any record of cyber operations by the attacker, and the nature of the target (such as critical infrastructure)," in order to determine whether a cyber operation qualifies as a use of force under Article 2(4) of the U.N. Charter.[288]

The ICJ, however, "has demonstrated an increasing resistance to the drawing of inferences from secondary evidence."[289] Only inferences to protect state sovereignty are normally drawn by the Court, while others are treated with great caution.[290] The ICJ has drawn inferences in situations such as exclusive control of territory and non-production of documents.[291] As to the first, it has been argued that the State from which the cyber operation originates has presumptive knowledge of such operation. U.S. officials have claimed, for instance, that, with the control that the Iranian government exercises over the internet, it is "hard to imagine" that cyber attacks originating from Iran against U.S. oil, gas, and electricity companies could be conducted without governmental knowledge, even in the absence of direct proof of state involvement.[292] The same considerations may be extended to cyber operations originating from China and other States where access to the Internet is under strict governmental control. The U.S. Department of Defense's *Assessment of International Legal Issues in Information Operations* also claims that "[s]tate sponsorship might be persuasively established by such factors as . . . the location of the offending computer within a state-controlled facility."[293] In literature, Richard Garnett and Paul Clarke have claimed that "in a situation where there have been

286. ASSESSMENT OF INTERNATIONAL LEGAL ISSUES, *supra* note 249, at 21–22. For a critique of the use of the sophistication criterion to establish attribution, see generally Clement Guitton and Elaine Korzak, *The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks*, 158 RUSI J. 62 (2013).

287. *Developments in the Field of Information and Telecommunications*, *supra* note 3, at 16; *see also* DEP'T OF INFO. TECH., GOV'T OF INDIA, DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY 4 (2011) [hereinafter DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY], *available at* http://deity.gov.in/sites/upload_files/ dit/files/ncsp_060411.pdf ("The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Often, the perpetrators of these activities can only be inferred from the target, the effect or other circumstantial evidence.").

288. TALLINN MANUAL r. 11 cmt. 10.

289. Teitelbaum, *supra* note 74, at 157.

290. RIDDELL & PLANT, *supra* note 54, at 413.

291. Waxman has highlighted the need to use "propensity inferences", which are based on the past behavior of a regime and its inclination to undertake certain actions. Waxman, *supra* note 57, at 66. He concludes that "there is no escaping some reliance on propensity inferences because of the limits of forensic evidence." *Id.* at 68. As the author himself points out, however, previous conduct can be misleading when the regime in question bluffs about its capabilities to intimidate or deter, as in the case of Saddam Hussein's Iraq. *Id.*

292. Nicole Perlroth & David E. Sanger, *New Computer Attacks Traced to Iran, Officials Say*, N.Y. TIMES, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=0.

293. ASSESSMENT OF INTERNATIONAL LEGAL ISSUES, *supra* note 249, at 21.

repeated instances of hostile computer activity emanating from a State's territory directed against another State, it seems reasonable to presume that the host State had knowledge of such attacks and so should incur responsibility."[294] At least some cyber attacks against Estonia and Georgia originated from Russian IP addresses, including those of state institutions.[295] The Mandiant Report also traced the cyber intrusions into U.S. computers back to Chinese IP addresses.[296] As has been seen, however, in the *Corfu Channel* case the ICJ held that "it cannot be concluded from the mere fact of the control exercised by a State over its territory . . . that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein . . . ."[297] Only if there are other indications of state involvement may territorial control contribute to establish knowledge.[298] In *Oil Platforms*, the ICJ also refused to accept the US argument that the territorial control exercised by Iran over the area from which the missile against the *Sea Isle City* had been fired was sufficient to demonstrate Iran's responsibility.[299] These conclusions are transposed in the cyber context by Rules 7 and 8 of the *Tallinn Manual*, according to which neither the fact that a cyber operation originates from a State's governmental cyber infrastructure nor that it has been routed through the cyber infrastructure located in a State are sufficient evidence for attributing the operation to those States, although it may be "an indication that the State in question is associated with the operation."[300] The *Tallinn Manual* does not clarify what probative value this "indication" would have.

If control of cyber infrastructure is not on its own sufficient to prove knowledge of the cyber operations originating therefrom, much less direct attribution, it may however have "a bearing upon the methods of proof available to establish the knowledge of that State as to such events."[301] In particular,

> [b]y reason of this exclusive control [within its frontiers], the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a *more liberal recourse to inferences of fact and circumstantial evidence*. This indirect evidence is admitted in all systems of law, and its use is recognized by international decisions.[302]

294. Richard Garnett & Paul Clarke, *Cyberterrorism: A New Challenge for International Law*, *in* ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 465, 479 (Andrea Bianchi ed., 2004).

295. U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 8, at 173; TIKK ET AL., *supra* note 14, at 75.

296. MANDIANT, APT 1, *supra* note 3030, at 4.

297. Corfu Channel (U.K. v. Alb.), Judgment, Merits, 1949 I.C.J. 4, 18 (Apr. 9). *See contra id.* at 44 (separate opinion of Judge Alvarez) ("[E]very State is considered as having known, or as having a *duty* to have known, of prejudicial acts committed in parts of its territory where local authorities are installed . . . .").

298. *See U.K. v. Alb.*, 1949 I.C.J. at 18 ("[T]he fact of this exclusive territorial control exercised by a State within its frontiers has a bearing on the methods of proof available to establish the knowledge of that State as to such events.").

299. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 61 (Nov. 6).

300. TALLINN MANUAL r. 7.

301. *U.K. v. Alb*., 1949 I.C.J. at 18.

302. *Id.* (emphasis added).

According to the Court, then, inferences become particularly valuable, and assume a probative value higher than normal, when a litigant is unable to provide direct proof of facts because the evidence is under the exclusive territorial control of the other litigant.[303] Such indirect evidence "must be regarded as of special weight when it is based on a series of facts linked together and leading logically to a single conclusion."[304] The ICJ, therefore, coupled the exclusive territorial control by Albania with its silence about the mine laying and other circumstantial evidence, and concluded that Albania had knowledge of the mines.[305] Transposed to the cyber context, the presence or origination of the hazard in the cyber infrastructure controlled by a State does not per se demonstrate knowledge by that State, but may contribute to such a finding if it is accompanied by other circumstantial evidence pointing in that direction. In *Corfu Channel*, however, the Court specified that, when proof is based on inferences, these must "leave *no room* for reasonable doubt."[306] In the *Bosnian Genocide* case, the Court confirmed that in demonstrating genocidal intent "for a pattern of conduct to be accepted as evidence of its existence, it would have to be such that it could only point to the existence of such intent."[307] In any case, "no inference can be drawn which is inconsistent with facts incontrovertibly established by the evidence."[308]

Of course, the Court will first have to determine whether the party has "exclusive territorial control"[309] of the cyber infrastructure from which the cyber operations originated (and, therefore, potentially of the evidence of who was responsible for them) before allowing the more liberal recourse to inferences. This may cause particular difficulties in cases of armed conflict: In the *DRC v. Uganda* case, for instance, one of the issues in dispute was whether Uganda had had control over Congolese territory.[310] In the cyber context, determining whether a litigant has "territorial control" of the cyber infrastructure, and whether such control is "exclusive" may be equally difficult to establish and is linked to the ongoing debate on the States' creeping jurisdiction over the Internet and cyberspace in general.[311] In this context, it should be recalled that Rule 1 of the *Tallinn Manual* accepts that "[a] State may exercise control over cyber infrastructure and activities within its sovereign territory."[312]

It should also be noted that the ICJ has not always allowed the "more liberal recourse to inferences of fact and circumstantial evidence" in cases of exclusive

303. *Id.*

304. *Id.* This may, for instance, be the case when a large number of cyber operations originate from the governmental cyber infrastructure of the same country.

305. *Id.* at 22.

306. *U.K. v. Alb.*, 1949 I.C.J. at 18.

307. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 373 (Feb. 26).

308. Temple of Preah Vihear (Cambodia v. Thai.), Judgment, 1962 I.C.J. 39, 109 (June 15) (separate opinion of Sir Spender).

309. *See* Waxman, *supra* note 57, at 72 (discussing situations when shifting the burden of proof may be acceptable under ICJ precedent, such as *Corfu Channel*, in which the party in "exclusive territorial control" inhibits the discovery of evidence).

310. Armed Activities on the Territory of the Congo (Dem Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 167–69.

311. *See* ROSCINI, *supra* note 1, 23–24 (discussing the difficulty in extending "existing rules and principles to . . . cyber operations").

312. TALLINN MANUAL r. 1.

territorial control.[313] In the *Bosnian Genocide* case, Bosnia and Herzegovina argued that, because of Serbia and Montenegro's geographical situation, the standard of proof should be lower, and that the respondent "had a special duty of diligence in preventing genocide and the proof of its lack of diligence can be inferred from fact and circumstantial evidence."[314] The Court rejected this reasoning and established Serbia and Montenegro's responsibility for failure to prevent genocide not on the basis of inferences but on documentary evidence and ICTY testimony.[315]

Does refusal to disclose evidence allow negative inferences? Article 38 of the Rules of Procedure of the Inter-American Commission on Human Rights provides that the facts alleged in the petition "shall be presumed to be true if the State has not provided responsive information during the period set by the Commission under the provisions of Article 37 of these Rules of Procedure, as long as other evidence does not lead to a different conclusion."[316] This is due to the different nature of human rights tribunals, where one of the parties is an individual and the other is a government, while disputes before the ICJ are between sovereign states.[317] According to Article 49 of its Statute, the ICJ may only take "[f]ormal note" of the refusal to disclose evidence: This provision authorizes the Court to draw inferences but does not create a presumption of law.[318] In any case, as has already been seen, in the *Corfu Channel* and the *Bosnian Genocide* cases the Court declined to draw any inferences from refusal to produce evidence, in the former case because there was a series of facts contrary to the inference sought.[319] Of course, if the litigant decides not to produce certain evidence, it will bear the risk that the facts it claims will not be considered sufficiently proved.[320]

VI. INADMISSIBLE EVIDENCE

There are no express rules on the admissibility of evidence in the ICJ Statute. Therefore, "[t]he general practice of the Court has been to admit contested documents and testimony, subject to the reservation that the Court will itself be the judge of the weight to be accorded to it."[321] Evidence may, however, be declared

313. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9).

314. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Fed. Rep. Yugo), Reply of Bosnia and Herzegovina, para. 22 (Apr. 23, 1998).

315. *See* Teitelbaum, *supra* note 74, at 138–39 (analyzing Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 242 (Feb. 26)). For critical comments on the ICJ's reliance on ICTY evidence, see Joyce, *supra* note 68, 298–305.

316. R.P. Inter-Am. Comm'n H.R. art. 38 (2009).

317. *Compare* Jo M. Pasqualucci, *Advisory Practice of the Inter-American Court of Human Rights: Contributing to the Evolution of International Human Rights Law*, 38 STAN. J. INT'L L. 241, 242 (2002) (emphasizing international law rules favorable to the individual in human rights cases), *with* 48 C.J.S. International Law § 61 (describing the differing nature of the ICJ).

318. Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933.

319. *See*, *e.g.*, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 32 (Apr. 9) (explaining the Court's determination that it cannot draw conclusions from the United Kingdom's refusal to produce documents XCU).

320. Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933.

321. Keith Highet, *Evidence, the Court, and the Nicaragua Case*, 81 AM. J. INT'L L. 1, 13 (1987).

inadmissible because it has been produced too late or not in the prescribed form.[322] Another example of inadmissible evidence is provided by the decision of the Permanent Court of International Justice in the *Factory at Chorzów* case, where the ICJ's predecessor held that it "cannot take account of declarations, admissions or proposals which the Parties may have made in the course of direct negotiations [when] . . . the negotiations in question have not . . . led to an agreement between [the parties]."[323] The underlying reason for the inadmissibility of such material is to facilitate the diplomatic settlement of international disputes through negotiations, so that the negotiating parties do not have to fear that what they say in the negotiating context may be used against them in subsequent judicial proceedings.[324]

Is evidence obtained through a violation of international law also inadmissible? Traditional espionage and cyber exploitation, used in support of traceback technical tools, may be a helpful instrument to establish proof of state responsibility for cyber operations.[325] India has noted that "[c]yber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action."[326] It is doubtful whether the above activities constitute internationally wrongful acts, although one commentator has argued, for instance, that cyber espionage may be a violation of the sovereignty of the targeted State whenever it entails an unauthorized intrusion into cyber infrastructure located in another State (be it governmental or

322. Statute of the International Court of Justice art. 52, June 26, 1945, 33 U.N.T.S. 933. Late evidence may be admissible if the other litigant consents to it or if the Court does not reject it. Christian J Tams, *Article 52*, *in* THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY, *supra* note 56, at 1312–16.

323. Factory at Chorzów (Ger. v. Pol.), Claim for Indemnity, 1927 P.C.I.J. (ser. A) No. 9, at 19. The ICJ referred to this limit in Frontier Dispute (Burk. Faso/Mali), Judgment, 1986 I.C.J. 554, para. 147 (Dec. 22); Maritime Delimitation and Territorial Questions between Qatar and Bahrain (Qatar v. Bahr.), Judgment, 1994 I.C.J. 112, para. 40 (July 1).

324. Benzing, *supra* note 56, at 1242.

325. *See* Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229, 234 (2012) ("[I]n addition to technical investigation, intelligence and information analysis is needed in order to profile the authors of the attack . . . ."); U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 8, at 140–41 ("All-source attribution takes into account whatever information is available from efforts at technical attribution, but also uses information from other sources to arrive at a judgment.").

326. *See* DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY, *supra* note 287, at 4.

private).[327] Data monitoring and interceptions may also be a violation of international human rights law.[328]

Assuming, *arguendo*, that espionage and cyber exploitation are, at least in certain instances, internationally wrongful acts, what is the probative value of the evidence so collected? There is no express rule in the Statute of the ICJ providing that evidence obtained through a violation of international law is inadmissible.[329] It is also not a general principle of law, as it seems to be a rule essentially confined to the U.S. criminal system.[330] As Thirlway argues, the rule in domestic legal systems is motivated by the need to protect the defendant against the wider powers of the prosecutor and its possible abuses: In inter-state litigation, there is no criminal trial and no dominant party, as the litigants are States in a position of sovereign equality.[331] In the *Corfu Channel* case, the ICJ did not dismiss evidence illegally obtained by the United Kingdom in Operation Retail; on the contrary, it relied on it in order to determine the place of the accident and the nature of the mines.[332] In fact, Albania never challenged the admissibility of the evidence acquired by the British Navy,[333] and the Court did not address the question.[334] What it found was not that the evidence had been illegally obtained, but that the purpose of gathering evidence did not exclude the illegality of certain conduct.[335] In general,

> the approach of the Court is to discourage self-help in the getting of evidence involving internationally illicit acts, not by seeking to impose

327. *See* Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 129 (2013) ("It could be argued . . . that damage is irrelevant and the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty."); *see also* ASSESSMENT OF INTERNATIONAL LEGAL ISSUES, *supra* note 249, at 19–20 ("An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international community. . . . If an unauthorized computer intrusion can be reliably characterized as intentional and it can be attributed to the agents of another nation, the victim nation will at least have the right to protest, probably with some confidence of obtaining a sympathetic hearing in the world community."); Louise Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, 76 INT'L L. STUD. 163, 172 (2002) (arguing that, when the individual conducts intelligence gathering from outside the adversary's territory through cyber exploitation, "the situation should be no different from someone gathering data from a spy satellite").

328. *See* Jann K. Kleffner & Heather A. Harrison Dinniss, *Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations*, 89 INT'L L. STUD. 512, 512–13 (2013).

329. RIDDELL & PLANT, *supra* note 53, at 158.

330. Hugh Thirlway, *Dilemma or Chimera?—Admissibility of Illegally Obtained Evidence in International Adjudication*, 78 AM. J. INT'L L. 622, 627–28 (1984); Nasim Hasan Shah, *Discovery by Intervention: The Right of a State to Seize Evidence Located Within the Territory of the Respondent State*, 53 AM. J. INT'L L. 595, 607–09 (1959). *Contra* Wolfrum, *supra* note 36, at 563 (stating that evidence obtained in violation of substantive international law could be inadmissible under the ICTY rules).

331. Thirlway, *supra* note 330, at 628–29.

332. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 14–15 (Apr. 9); Shah, *supra* note 330, at 606–07.

333. Thirlway, *supra* note 330, at 632.

334. *Id.*

335. *See U.K. v. Alb.*, 1949 I.C.J. at 34–35 (holding that the United Kingdom's theory of intervention with the purpose of obtaining evidence "might easily lead to perverting the administration of international justice itself.").

> any bar on the employment of evidence so collected, but by making it clear that such illicit activity is not necessary, since secondary evidence will be received and treated as convincing in appropriate circumstances.[336]

In a cyber context, this means that while litigants are not entitled to access direct evidence that is located in another State's computers or networks without authorization to submit it in the proceedings, that evidence's existence allows the court to give more weight to circumstantial evidence.[337]

CONCLUSIONS

The following main conclusions can be drawn from the application to cyber operations of the ICJ's rules and case law on evidence:

-The burden of proof does not shift in the cyber context and continues to rest on the party that alleges a certain fact.

-Whilst it is uncertain that a uniform standard of proof applicable to *all* cases involving international responsibility for cyber operations can be identified, it appears that claims of self-defense against cyber operations, like those against kinetic attacks, must be proved with clear and convincing evidence. On the other hand, fully conclusive evidence is needed to prove that a litigant conducted cyber operations amounting to international crimes, and a slightly less demanding standard seems to apply when what needs to be proved is that the State did not exercise due diligence to stop its cyber infrastructure from being used by others to commit international crimes.

-The Court may take 'formal note' of the refusal of a party to present classified cyber documents, but it has so far refrained from drawing negative inferences from the non-production of documents. In any case, any such negative inferences could not contradict factual conclusions based on consistent evidence produced by the parties.

-The Court gives more probative weight to official documents of States and international organizations such as the United Nations. NGO reports and press articles on cyber incidents are only secondary sources of evidence that may be useful to corroborate other sources or to establish the public knowledge of certain facts, providing they are sufficiently rigorous and only when they are "wholly consistent and concordant as to the main facts and circumstances of the case."[338]

-The drawing of inferences is approached by the ICJ with great caution. When there are objective difficulties for a litigant to discharge the burden of proof because the direct evidence lies within the exclusive territorial control of the other litigant, including its cyber infrastructure, a more liberal recourse to inferences of fact is admissible providing that they leave no room for reasonable doubt.

336. Thirlway, *supra* note 330, at 641. It has been argued, however, that evidence obtained through a *jus cogens* violation—for instance, torture—should be deemed inadmissible. Wolfrum, *supra* note 36, at 563.

337. *U.K. v. Alb.*, 1949 I.C.J. at 18.

338. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 64, para. 13 (May 24).

-Even if a litigant obtains evidence illegally, e.g., through an unauthorized intrusion into the computer systems of another State, the evidence so obtained may be taken into account by the Court, although the purpose of collecting evidence does not exclude the illegality of the conduct.