Between Israel and Iran: Middle-East Attitudes to the Role of International Law in the Cyber-sphere

Tal Mimran*

Abstract :

This Chapter explores the policies outlined by Israel and Iran concerning the application of international law to cyberspace, in a quest to understand if there is some form of a Middle-Eastern approach to the topic. The Chapter demonstrates how Iran and Israel intertwine their security and military interests with their legal perspectives. The Chapter reveals that Israeli policy reflects its self-perception as a technologically advanced State that is part of the dominant camp, composed mostly of Western States. As for Iran, its position is affected from its experience with sanctions, which creates a sense of unfairness, leading Iran to push for promotion of new international law instruments that will regulate this new and constantly developing field, unlike Israel which prefers application of existing international laws to cyberspace.

The Chapter also suggests, more generally, that clearer international law rules could settle questions such as the required standard of proof for attribution, or the procedure through which a State can make a claim of attribution. They could also incentivise States to cooperate in international efforts, encourage them to accept restraint in cross-border cyber operations, and to exercise prudence in their own territory. It can also serve as an important chilling factor. States that have outlined their legal position, such as Israel and Iran, have taken a first step – but this is not enough. As such, declarations by States should be a leverage in this direction rather than a move in a different one.

Keywords: Israel, Iran, Cyberspace, international law, Middle-East.

* Research Director, Federmann Cyber Security Research Center (Hebrew University of Jerusalem); Academic Coordinator, International Law Forum (Hebrew University of Jerusalem); Research Associate, Zefat Academic College. I wish to thank Dr. Asaf Lubin, Maj. Gen. (ret.) Dan Efroni, Lt.-Col. Noam Neuman and Ori Pomson, for his helpful comments.

1. Introduction

The cybersecurity policy of the State of Israel used to focus on building capabilities, and engaging in covert deterrence and retaliation manoeuvres.[1] Recent escalation in cyber risks, exacerbated during the Covid-19 crisis,[2] incentivised Israel to publicly outline its position regarding the application of international law to cyberspace for the first time.[3] The declaration was delivered on 8 December 2020 by the Israel Deputy Attorney General, Roy Schöndorf. It joins other States that recently expressed their legal view on international law in cyberspace.[4] From a regional perspective, Israel follows the lead of the declaration made by the General Staff of the Iranian Armed Forces, on 18 August 2020.[5]

This Chapter will explore the policy outlined by Israel. It will also compare it to that of the Islamic Republic of Iran. Given the mostly hostile relationship between Israel and Iran, it is of interest to compare their legal views and in particular in relation to cyber operations – an area where the two States 'meet' from opposing sides of the screen more often than not. Both declarations dealt with an array of legal questions in cyberspace, but failed to properly address one crucial issue – attribution. This is not surprising, as both States are technologically savvy and well positioned to promote attribution with their own technical and intelligence capabilities. Still, this issue is too central to ignore. Accordingly, I will complement the discussion with international standards and policy considerations in relation to attribution.

---

[1] Deborah Housen-Couriel, *National Cyber Security Organisation: Israel*, NATO Cooperative Cyber Defence Centre of Excellence (2017), <https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf>, visited on 26 January 2022.

[2] François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', 13 *International Conference on Cyber Conflict* 9, 12 (2021).

[3] Roy Schondorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL Talk!* (9 December 2020), <https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/>, visited on 26 January 2022 [hereinafter: Israeli Perspective].

[4] *See, e.g.*: Government Of Australia, Australia's International Cyber Engagement Strategy, Annex A: Supplement To Australia's Position On The Application Of International Law To State Conduct In Cyberspace (2017), <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf>, visited on 26 January 2022 [hereinafter: Israeli Perspective] [hereinafter: Australia's Cyber Strategy].

[5] Declaration by the General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace (July 2020), translated and reproduced in 'Armed Forces Warns of Tough Reaction to Any Cyber Threat – Iran', ALDiplomasy (17 August 2020), available at: <https://www.aldiplomasy.com/en/?p=20901>, visited on 26 January 2022 [hereinafter: Iranian Declaration].

2. The Israeli Declaration

2.1 *Background*

Israel is an advanced cybersecurity actor,[6] demonstrating cyber robustness and resilience.[7] Domestic legislation deals with issues such as licensing;[8] offensive content;[9] and neutrality of the network.[10] Authority on cyber security was initially assigned to two bodies – the National Information Security Authority, and the National Cyber Bureau.[11] After a few years of operation, the authority of both bodies was assigned to the National Cyber Directorate.[12]

Israel used to be politically isolated in the Middle-East, incentivising it to develop military capabilities.[13] Cyber defence and offence capacities have a major part of the Israeli security toolbox, similar to other States.[14] For example, some claim that on 6 September 2007 Israel disabled radar systems in Syria to enable an air strike against a nuclear facility.[15]

Two main military units provide Israel with unique cyber expertise: C4I Corps and Unit 8200. C4I Corps safeguards communication infrastructure and systems against cyber-attacks.[16]

---

[6] Jasper Frei, 'Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations', ETH Zurich (2020), p. 5, <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf>, visited on 26 January 2022.

[7] Housen-Couriel, *supra* note 1. *See also*: Lior Tabansky & Isaac Ben-Israel, *Cyber Security in Israel* (Springer, 2015).

[8] Communications Regulations (Bezeq and Broadcasts) (Proceedings and Conditions for Obtaining a Combined General License) 5770-2010, Wireless Telegraph Ordinance [New Version] 5732-1972.

[9] Communications Law (Bezeq and Broadcasting) 5742-1982, Section 41.

[10] For elaboration, *see*: Office of the Deputy Attorney General (International Law), 'GOI Reply to the Questionnaire by the Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression on: Freedom of Expression in the Telecommunications and Internet Access Sector' (November 2016), <https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/Israel.pdf>, visited on 26 January 2022.

[11] Government Resolution No. 3611 (Advancing National Cyberspace Capabilities, 7 August 2011). For discussion, *see*: Daniel Benoliel, 'Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study', 16 *North Carolina Journal of Law & Technology & Tech.*, p. 435 (2014).

[12] Government Resolution 2444, 15 February 2015, article 3, <https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf>, visited on 26 January 2022. Recently, a new bill seeks to redefine cybersecurity governance in Israel. This is an abbreviated formulation of a previous version that was halted given objections. For discussion, *see*: Deborah Housen-Couriel, Tal Mimran & Yuval Shany, 'Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill', *Lawfare* (7 May 2021), <https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill>, visited on 26 January 2022.

[13] Frei, *supra* note 6, p. 7.

[14] Oona Hathaway et al., 'The Law of Cyber-Attack', *100 Cal. L. Rev.* PP. 817, 830 (2012). *See*, generally: Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (Harper Collins, 2010).

[15] Sharon Weinberger, 'How Israel Spoofed Syria's Air Defense System', *Wired* (10 April 2007), <https://www.wired.com/2007/10/how-israel-spoo/>, visited on 26 January 2022; Kim Zetter, 'Mossad Hacked Syrian Official's Computer Before Bombing Mysterious Facility', *Wired* (11 March 2009), <https://www.wired.com/2009/11/mossad-hack/>, visited on 26 January 2022.

[16] Michael Raska, *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy*, S. Rajaratnam School of International Studies (2016), p. 5, <https://www.michaelraska.de/download/Israel's_Evolving%20Cyber%20Strategy_Raska.pdf>, visited on 26 January 2022.

Unit 8200, in comparison, is responsible for gathering signal intelligence, coding and interception.[17] Unit 8200 was allegedly part of the development and use of Stuxnet, alongside the United States.[18] Stuxnet was a sophisticated malware that infiltrated Iranian nuclear facilities,[19] forced centrifuges to speed up and sent false signals that mislead safety systems.[20] This was the first cyber-attack to damage real-world infrastructure,[21] unlike other incidents like the cyber-attacks in Estonia in 2007.[22] Additional projects are attributed to this unit, such as the Duqo espionage campaign.[23] As will be seen, Israel's capacities guide its legal perspective.

Israel harnesses its capabilities in order to reach out to States and gain international legitimacy.[24] The desire to become more meaningful, particularly regionally, is also evident in the recent normalisation of relations with four Arab States.[25] The situation in Israel is far from being all peaches and cream, of course. Of relevance to this Chapter, in April 2020 Iran targeted Israel's water infrastructure facilities, to which Israel responded with a cyber-operation against Iranian ports.[26] Shortly afterwards, three cyber-attacks hit Israeli companies: Shirbit (an insurance company),[27] Amital Data (an Israeli technology company that provides software solutions

---

[17] Richard Behar, 'Inside Israel's Secret Startup Machine', *Forbes* (11 May 2016), <https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/?sh=4b56996c1a51>, visited on 26 January 2022; Yoav Zitun, A peek inside the IDF 8200's combat intelligence unit, YNET News (10 April 16), <https://www.ynetnews.com/articles/0,7340,L-4862586,00.html>, visited on 26 January 2022.

[18] Sean Cordey, 'The Israeli Unit 8200–An OSINT-based study: Trend Analysis', ETH Zurich (2019), p. 9, <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf>, visited on 26 January 2022.

[19] Delbert Tran, 'The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack', 20 Yale J.L. & Tech., pp. 376, 393 (2018).

[20] Hathaway, *supra* note 14, p. 839. *See also*: David Fidler, 'Was Stuxnet an Act of War? Decoding a Cyberattack', *9 IEEE Sec. & Privacy*, pp. 56, 57 (2011).

[21] Mary Ellen O'Connell, 'Cyber Security without Cyber War', 17(2) *Journal of Conflict & Security Law*, pp. 187, 194 (2012).

[22] Ido Kilovaty, 'Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare', 1(5) *American University National Security Law Brief Volume*, pp. 91, 92 (2014).

[23] Frei, *supra* note 6, p. 7. "Duqu" is a cyber espionage malware, and "Flame" is another information collecting platform, that enables espionage via saving screen shots, browsing through storage devices or switching on the microphone and the camera. For discussion, *see* Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, & Márk Félegyházi, 'The Cousins of Stuxnet: Duqu, Flame, and Gauss', 4(4) *Future Internet*, pp. 971, 980 (2012).

[24] Fabio Cristiano, Israel: 'Cyber Warfare and Security as National Trademarks of International Legitimacy' in *Routledge Companion to Global Cyber-Security Strategy 13* (Scott N. Romaniuk S. & Mary Manjikian eds., 2020).

[25] Sarah Johansson, 'Definitional doom: How Iran and Israel derail legal application in cyberspace', MEI@75 (17 March 2021), <https://www.mei.edu/publications/definitional-doom-how-iran-and-israel-derail-legal-application-cyberspace>, visited on 26 January 2022.

[26] Toi Staff, Israel behind cyberattack that caused 'total disarray' at Iran port – report, Times of Israel (19 May 2020), <https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/>, visited on 26 January 2022.

[27] Israel National Cyber Directorate, Data Breach event at Shirbit (01 December 2020), <https://www.gov.il/en/departments/news/news_shirbit>, visited on 26 January 2022.

in the field of importation and logistics),[28] and Habana Labs (an Artificial Intelligence company, which is owned by Intel).[29] Israeli experts have tied these operations also to Iran.[30] According to the Israeli National Cyber Directorate, 18% of businesses in Israel have experienced a cyber-attack, and in the hi-tech sector as much as one-third of them.[31] As such, these incidents represent the tip of the iceberg of a longstanding campaign carried out against Israeli companies.

2.2 ***Legal Cyberspace Perspective***

Israel's turn to international law derives from a desire to complement its cybersecurity toolbox, and gain legitimacy for its cyber operations. It makes prudent strategic use of this toolbox in accordance with the context within which it operates. This is not the first instance where Israel has had the opportunity to speak out, as it was a member of the fifth United Nations (UN) Group of Government Experts.[32] Its international involvement derives, inter alia, from the desire to establish itself as a leader in the design of international cyber governance.[33] The declaration under discussion is an important step in the pursuit of this strategic goal.

---

[28] Meir Orbach and Golan Hazani, 'Israel's supply chain targeted in massive cyberattack', *CTECH* (13 December 20), <https://www.calcalistech.com/ctech/articles/0,7340,L-3881337,00.html>, visited on 26 January 2022.

[29] Lawrence Abrams, 'Intel's Habana Labs hacked by Pay2Key ransomware, data stolen', *Bleeping Computer* (13 December 2020), <https://www.bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/>, visited on 26 January 2022.

[30] Uri Berkovitz, 'Iranian hackers aim to sow panic in Israel – report', *Globes* (17 Dec, 2020), <https://en.globes.co.il/en/article-iranian-hackers-aim-to-sow-panic-in-israel-report-1001353603>, visited on 26 January 2022.

[31] Huaxia, '18 Pct of Israeli Businesses Suffer Cyberattack: Survey', News (21 July 2021), <http://www.xinhuanet.com/english/2021-07/21/c_1310075937.htm>, visited on 26 January 2022.

[32] The recent round of Groups of Governmental Experts meetings began in 2019. In addition, in 2018 the General Assembly established the Open-ended Working Group, open to all UN members, that operates with a similar mandate to the Groups of Governmental Experts and published its report on March 2021. *See*: General Assembly Res. 73/266 (22 December 2018), <https://undocs.org/en/A/RES/73/266>, visited on 26 January 2022; Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (10 March 2021), <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>, visited on 26 January 2022; Michael Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security* (10 June 2021), <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>, visited on 26 January 2022.

[33] Government Resolution No. 2443 (Advancing National Regulation and Governmental Leadership in Cyber Security, 15 February 2015). Israel is also a signatory to the European Convention on Cybercrime. *See*: Council of Europe, Convention on Cybercrime, Explanatory Report, C.E.T.S. No. 185, P 38 (8 November 2001), <https://rm.coe.int/16800cce5b>, visited on 26 January 2022. For regional instruments, *see*: Arab Convention on Combating Information Technology Offences (adopted 21 December 2010); African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014).

The declaration by Schöndorf was viewed as sophisticated, but cautious.[34] Indeed, Schöndorf suggested that caution must be exercised in determining how international law applies to cyberspace.[35] The Israeli declaration, similar to other declarations made by other States,[36] considers existing laws rather than creation of new norms. This is different from Iran, which supports promotion of an international instrument that will create new and particular law to cyberspace.[37] This difference appears to derive from the self-perception of Israel as among the leading Western States that dominate the discussion on the application of international law in cyberspace, while ignoring its geographical location. Iran, by comparison, was celebrated as the first Middle-Eastern State to present its legal perspective,[38] and the second non-Western one after China.[39] As will be elaborated, while being applauded in this regard Iran suffers from sanctions which affect its legal perspective and sense of fairness on the international plane.

2.3 ***Use of Force in Cyberspace***

The prohibition against the use of force, a *jus cogens* norm, is enshrined in article 2(4) of the UN Charter.[40] Schöndorf clarified that this prohibition is applicable in the cyber domain when hostile cyber operations are expected to cause physical damage, injury or death.[41] An example

---

[34] Michael Schmitt, 'Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law'), *EJIL Talk!* (17 December 2020), <https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/>, visited on 26 January 2022; Johansson, *supra* note 26.

[35] Israeli Perspective, *supra* note 3.

[36] *See, e.g.*,: On the Application of International Law in Cyberspace, Position Paper, The Federal Government of Germany (March 2021), <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>, visited on 26 January 2022 [hereinafter: German Position]; New Zealand, The Application of International Law to State Activity in Cyberspace, (1 December 2020), <https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf>, visited on 26 January 2022 [hereinafter: New Zealand Position].

[37] Islamic Republic of Iran, The Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security Preliminary reflection (April 2020), p. 4, <https://front.un-arm.org/wp-content/uploads/2020/04/iran-preliminary-on-oewg-pre-draft-15-april-2020-1.pdf>, visited on 26 January 2022 ("… OEWG is expected to continue discussions on 'to what extent', and 'how', the existing international law applies and, more importantly, what kind of international binding instrument, including an ICT-specific convention should be developed.") [hereinafter: Iran OWEG Observation].

[38] Johansson, *supra* note 25.

[39] Tian Shaohui, 'International Strategy of Cooperation on Cyberspace', *News* (1 March 2017), <http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm>, visited on 26 January 2022. The regional difference of opinions is evident, for example, in the different understanding the term 'cyber-attack' (in Western eyes) and 'information war' (in the eyes of the Shanghai Cooperation Organization). *See*: Agreement Between the Governments of The Member States of The Shanghai Cooperation Organization on Cooperation in The Field of International Information Security, 61st Plenary Meeting (2 December 2008), Annex I, p. 209, <https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf>, visited on 26 January 2022; US Dep't Of Def., Department of Defense Strategy for Operating in Cyberspace 7 (2011); Hathaway, *supra* note 14, p. 865.

[40] United Nations Charter, 24 October 1945, 1 UNTS XVI; Christine Gray, 'The use of force and the international legal order', in *International Law 617* (Malcolm D. Evans ed., 2010).

[41] Israeli Perspective, *supra* note 3.

would be hacking into the computers of a railroad network and causing a collision between trains. Schöndorf noted that there is room to further examine whether operations not causing physical damage could also amount to use of force, in contrast to States like France and New Zealand which took a stronger stance on the issue.[42]

Schöndorf confirmed Israel's position that States have an inherent right to self-defence against use of force which amounts to an armed attack, against both a State or non-State actor. This is of importance as Israel regularly deploys military force against non-State actors. While this issue is not completely settled in international law,[43] Schmitt noted that this interpretation is reasonable and mirrored by the views of other States.[44]

Three approaches were suggested in order to examine whether a cyber operation is elevated to an illegal use of force: the instrument-based approach, the target-based approach, and the effects-based approach.[45] Out of these three, the most predominant, also opted for by Schöndorf, is the third one.[46] According to the effects-based approach, a use of force must

---

[42] Ministre des Armées, République Française, Droit International Appliqué Aux Opérations Dans Le Cyberespace (2019), p. 7, <https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf>, visited on 26 January 2022 ("En l'absence de dommages physiques, une cyber-opération peut être considérée comme un recours à la force à l'aune de plusieurs critères, notamment les circonstances qui prévalent au moment de l'opération, tels que l'origine de l'opération et la nature de l'instigateur (son caractère militaire ou non), le degré d'intrusion, les effets provoqués ou recherchés par l'opération, ou encore la nature de la cible visée. Ces critères ne sont, bien entendu, pas exhaustifs") [hereinafter: Ministre des Armées] [EN: In the absence of physical damage, a cyber operation can be considered a use of force in the light of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (its military nature or its lack thereof), the degree of intrusion, the effects caused or sought by the operation, or the nature of the intended target. These criteria are, of course, not exhaustive.]; New Zealand Position, *supra* note 36.

[43] *See*: SC Res. 1368 (12 September 2001); SC Res. 1373 (28 September 2001); SC Res. 1530 (11 March 2004); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ 136, ¶139; Christine Gray, *International Law and The Use of Force*, pp. 135–138 (Oxford University Press, 2008).

[44] Schmitt, *supra* note 34. *See*, e.g.: Jeremy Wright, Attorney General, United Kingdom, Cyber and International Law in the 21st Century, Gov.UK (23 May 2018), <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, visited on 26 January 2022 [hereinafter: UK Position].

[45] Hathaway, *supra* note 14, p. 845 (2012); David E. Graham, 'Cyber Threats and the Law of War', *4 J. Nat'l Security L. & Pol'y* 87, 91 (2010).

[46] The instrument-based approach categorizes an act as an armed attack only if it bears characteristics traditionally associated with military force. This was perceived as outmoded. *See*: Duncan B. Hollis, 'Why States Need an International Law for Information Operations', 11 Lewis & Clark L. Rev. 1023, 1041 (2007). The target-based approach classifies a cyber-attack against a critical computer system as an armed attack regardless of physical destruction or casualties. The problem with this approach is that it might increase the risk of a conventional military operation following a cyber-attack, even without physical damage. *See*: Sheng Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defense?', 38 Yale J. Int'l L., PP. 179, 186 (2013).

include significant physical damage.[47] Relevant criteria include the degree of physical destruction; immediacy; invasiveness and measurability of the harm; and State involvement.[48]

States' view on the matter is useful. France considers that a cyber operation without physical effects can be perceived as a use of force.[49] Similarly, the Netherlands accepts that a cyber operation with significant financial or economic harm can qualify as a use of force.[50] In contrast, Australia, Estonia and Finland view cyber operations as a use of force only when they cause injury or death to persons, or damage to or destruction of property.[51] Germany,[52] and New Zealand,[53] also limit their understanding of a use of force to one of kinetic impact. The United States offered examples of cyber-attacks that qualify as a use of force – such as triggering a nuclear plant meltdown, or disabling air traffic control services.[54] Against this backdrop, it seems that Israel presents a reasonable view that joins various Western States.

2.4 Cyberspace and Armed Conflicts

The next issue addressed by Schöndorf, was International Humanitarian Law (*jus in bello*, or "IHL"), which applies to cyber operations during armed conflicts.[55] Under IHL, it is prohibited

---

[47] Marco Roscini, 'Cyber Operations and the Use of Force in International Law', p. 54 (*Oxford Scholarship Online*, 2014).

[48] *See*: Tallinn Manual on The International Law Applicable to Cyber Warfare, p. 46 (Michael N. Schmitt ed., 2013).

[49] Ministre des Armées, *supra* note 42.

[50] Letter from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, app.: International Law in Cyberspace (5 July 2019), <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>, visited on 26 January 2022 [hereinafter: Letter from the Netherlands]. For an example of a costly cyber-attack, *see*: Peter Foster, Bogus' AP tweet about explosion at the White House wipes billions off US markets, the Telegraph (23 April, 2013), <https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html>, visited on 26 January 2022.

[51] Estonia, President of the Republic at the Opening of CyCon 2019, 29 May 2019, < https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Remarks+by+the+President+of+the+Republic+of+Estonia+at+the+Opening+of+CyCon+2019.pdf>, visited on 26 January 2022; [hereinafter: Estonian Perspective]; Australia's Cyber Strategy, *supra* note 4; International Law and Cyberspace - Finland's national positions<https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727>, visited on 26 January 2022 [hereinafter: Finland's Position].

[52] German Position, *supra* note 36. Assessments examine the severity, immediacy, intrusion, and degree of organization of the cyber operation.

[53] New Zealand Position, *supra* note 36.

[54] United States Department of Defense (DoD), *Law of War Manual*, 2015, <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>, visited on 26 January 2022.

[55] For discussion concerning IHL in the cyber-sphere, *see*: Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?', 89 Int'l L. Studies 252 (2013).

to deploy attacks that are directed against civilian targets, based on the principle of distinction,[56] ones that result in excess in harm to civilians and their property, based on the principle of proportionality,[57] and ones which impair infrastructure or indispensable civilian objects.[58]

It is challenging to apply IHL to cyberspace given the integrated nature of dual-use infrastructures.[59] For example, navigation satellite systems serve civilian transportation vehicles and traffic controls, alongside armed forces.[60] Even if an attack was designed to harm a particular system, malware can spread instantly without geographical limitations.[61] Such spill-over effects infringe on IHL principles such as distinction and proportionality. In the Stuxnet incident, for example, the worm spread to computers in India and Russia, causing unplanned damage.[62]

Schöndorf suggested that a cyber operation constitutes an attack under IHL only when it is expected to cause physical damage.[63] In his view, mere loss or impairment of functionality to infrastructure is insufficient. Schmitt suggested that this view is surprising, as it leaves Israel with a narrower leeway of action in the face of cyber-operations against it.[64] In my view, this view derives from two main reasons. First, while critical infrastructures are highly computerised, laying them open to the risk of cyber-attacks,[65] an operation against them requires advanced expertise.[66] Second, the Stuxnet incident, in which Israel was allegedly involved, led precisely to impairment of functionality of infrastructure.[67] As such, it is preferable for Israel to treat malware like Stuxnet as falling outside the ambit of IHL.

---

[56] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, Arts. 48 & 54 [hereinafter: Protocol I]; Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law*, rules 7 & 54 (2006).

[57] Protocol I, *supra* note 56, Art. 51; Gabriella Blum & Philip Heymann, 'Law and Policy of Targeted Killing', 1 Harv. Nat'l Sec. J. 145 (2010).

[58] Protocol I, *supra* note 56, Arts. 48 & 54.

[59] Hathaway, *supra* note 14, p. 852 (2012). *See also*: Michael N. Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations', 101 *International Review of The Red Cross*, p. 333 (2019).

[60] Laurent Gisel, Tilman Rodenhäuser & Knut Dörmann, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts', 102 *International Review of the Red Cross*, pp. 287, 320 (2020).

[61] Examples include, amongst others, the CrashOverride, WannaCry and NotPetya incidents. For discussion, *see* Laurent Gisel and Lukasz Olejnik, 'The Potential Human Cost of Cyber Operations: Starting the Conversation', *Humanitarian Law and Policy Blog*, 14 November 2018, <https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/>, visited on 26 January 2022.

[62] O'Connell, *supra* note 21.

[63] Israeli Perspective, *supra* note 3.

[64] Schmitt, *supra* note 34.

[65] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', 17(2) *Journal of Conflict & Security Law*, pp. 229, 231 (2012).

[66] Kenneth Geers, 'The Cyber Threat to National Critical Infrastructures: Beyond Theory', 18 *Information Security Journal: A Global Perspective*, pp. 1, 2 (2009).

[67] O'Connell, *supra* note 21, p. 194.

Schöndorf recognised that, even if a hostile cyber operation does not constitute an attack, other safeguards nevertheless apply.[68] Another question addressed is whether data can be considered as an object and possess a military or civilian nature.[69] The position of Israel in this regard is that only tangible things can constitute objects,[70] similar to the view presented in the Tallinn Manual[71] but in contrast to States such as France, which accepts that civilian data constitutes a protected object.[72] Iran chose not to deal with IHL in its current declaration, as it has traditionally demonstrated resistance to the application of IHL to cyberspace.[73]

2.5 ***Sovereignty and The Rule of Non-intervention***

Schöndorf distinguishes between a general concept of sovereignty that connotes independence and the legal rule of territorial sovereignty.[74] The declaration relates to the debate surrounding the question whether sovereignty is a principle or a primary rule of international law,[75] while not taking an unequivocal stance.[76] This is since Schöndorf clarified that it is unclear if transit through networks located in other States amounts to violations of their sovereignty.[77]

In a natural development, the declaration moved to consider non-intervention, a customary rule that is anchored in Article 2(7) of the UN Charter.[78] Intervention entails coercive interference by a State in the internal affairs of other States.[79] For an intervention to be illegal, two elements are required: 1) Intervention with matters which a State is free to decide on its

---

[68] For discussion, *see*: Tal Mimran and Yuval Shany, 'Israel, Cyberattacks and International Law', *Lawfare* (30 December 2020), < https://www.lawfareblog.com/israel-cyberattacks-and-international-law>, visited on 26 January 2022.

[69] For illustrative discussion, *see*: Ori Pomson, 'Objects'? The Legal Status of Computer Data under International Humanitarian Law' (1 March 2021), <https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3795479>, visited on 26 January 2022.

[70] Israeli Perspective, *supra* note 3.

[71] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, p. 373 (Michael N. Schmitt ed., Washington DC, 2017) [hereinafter Tallinn Manual 2.0]. *See also*: Michael N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision', *48 Isr. L. R.* pp. 81, 93 (2015).

[72] Ministre des Armées, *supra* note 42, p. 16 ("la France considère que des données civiles de contenu peuvent être considérées comme des biens protégés" [France considers that civil content data can be considered as protected property]).

[73] Iran OWEG Observation, *supra* note 37, p. 2 ("applying international humanitarian law, which is exclusively for armed conflicts, in the ICT environment… needs to be avoided").

[74] Israeli Perspective, *supra* note 3.

[75] Schmitt, *supra* note 34.

[76] Currently, only the United Kingdom asserts that sovereignty is merely a principle and not a primary rule of international law. *See*: UK Position, *supra* note 44.

[77] Israeli Perspective, *supra* note 3.

[78] United Nations Charter, 24 October 1945, 1 UNTS XVI, Art. 2, ¶7; Michael N. Schmitt & Andru E. Wall, 'The International Law of Unconventional Statecraft', 5 *Harv. Nat'l Sec. J.* 349–376, pp. 349, 355 (2014).

[79] Philip Kunig, *Intervention, Prohibition of, in The Max Planck Encyclopedia of Public International Law* 1, ¶4, <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?prd=EPIL>, visited on 26 January 2022.

own;[80] 2) Intervention which involves coercion.[81] Cyber operations can often meet the first condition,[82] but rarely the second one.[83] Schöndorf explained that a high threshold limits the rule mostly to military interventions. In his view, however, the rule can apply to a cyber operation that interferes with another State's ability to hold an election.[84]

Indeed, cyber capabilities allow for new ways of non-physical intervention, in order to manipulate elections or change public opinion.[85] Some States, such as Germany, assert that hostile cyber operations targeting foreign elections might constitute an illegal intervention.[86] This is not a theoretical issue, as was evident during the 2016 and 2020 elections in the United States,[87] or ahead of the 2010 elections in Burma.[88] Israel adds its part to the discussion by accepting the possibility that cyber operations can amount to illegal intervention.

2.6 Due Diligence, Attribution and Countermeasures

A more controversial part of the Israeli position is the one regarding the principle of due diligence (DD). Schöndorf asserted that this principle is not a binding rule in the cyber context.[89] In his opinion, prudence must guide interpretation of rules from a different context – environmental law in the case of DD.[90] This presentation of DD is, in my view, too narrow.

---

[80] Military and Paramilitary Activities in and against Nicaragua (*Nicar.* v. *USA*), Merits, 1986 ICJ Rep 14 (27 June), p. ¶205.
[81] Other terms parallel to coercive are forcible or dictatorial. *See*: Oppenheim's International Law, p. 43 (Robert Jennings & Arthur Watts (eds.), 9th ed. 1992).
[82] Thibault Moulin, 'Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward', 25 *J. Conflict & Security L.*, pp. 423, 430 (2020).
[83] Rebecca Crootof, International Cybertorts: 'Expanding State Accountability in Cyberspace', 103 *Cornell L. Rev.*, pp. 565, 623 (2018).
[84] Israeli Perspective, *supra* note 3.
[85] For discussion, *see*: Terry Gill, 'Non-Intervention in the Cyber Context', in *Peacetime Regime for State Activities in Cyberspace*, p. 234 (Katharina Ziolkowski, ed.) (CCDOE, Tallinn 2013). For discussion on cyber and espionage, *see*: Russell Buchan, *Cyber Espionage and International Law* (Bloomsbury Publishing 2018).
[86] German Position, *supra* note 36.
[87] Press Release, Dep't of Homeland Sec., Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (7 October 2016), <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>, visited on 26 January 2022; Statement by NCSC Director William Evanina: Election Threat Update for the American Public, News Release No. 29-20, Office of the Director of National Intelligence (7 August 2020), <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>, visited on 26 January 2022 ("We assess that Iran seeks to undermine U.S. democratic institutions, President Trump, and to divide the country in advance of the 2020 elections.").
[88] Burma Hit by Massive Net Attack Ahead of Election, BBC NEWS (4 November 2010), <http://www.bbc.co.uk/news/technology-11693214>, visited on 26 January 2022.
[89] Mimran & Shany, *supra* note 68.
[90] Israeli Perspective, *supra* note 3.

DD requires a State to take possible measures to safeguard against misusing its territory to commit violations of international law.[91] Its application is wide, and its status is longstanding.[92] A failure to meet the principle might give rise to a violation of international law.[93] This rule has been recognised as applicable in cyberspace by Brazil,[94] Finland[95] and France.[96] DD was also recognised in the past by Iran as applicable to cyberspace,[97] though it did not do so in the declaration under discussion. The Tallinn Manual suggests that States should use feasible measures to halt hostile cyber operations from their territory which are directed against another State.[98] Israel's rejection of this rule is, hence, somewhat disappointing.

Finally, Schöndorf referred briefly to two related legal issues – countermeasures, and attribution. Countermeasures are an important self-help tool in a decentralised international legal system.[99] Schöndorf noted that there is no absolute duty under international law to notify in advance of taking countermeasures in cyberspace, since doing so might render them obsolete.[100] This view is in line with the one presented by several States, such as the Netherlands,[101] and New Zealand.[102] Lawful countermeasures are acts whose wrongfulness is precluded if they respond to a prior unlawful act, and if they meet requirements such as notification and proportionality.[103] Article 52(2) of the International Law Commission Articles on State Responsibility for Internationally Wrongful Acts ("ARSIWA") substantiates the assertion by Schöndorf, as it allows for urgent countermeasures where prior notice is not required.[104]

---

[91] Corfu Channel (*U.K.* v. *Alb.*), Judgment, 1949 ICJ Rep. 4, 18, 22 (9 April).
[92] For early discussion of this principle, *see* The Alabama Claims of the United States of America against Great Britain (*US* v. *UK*), 29 R.I.A.A. 125, 131 (1871). For a more recent application of the principle, *see*: Hum. Rts. Comm., General Comment No. 31, U.N. Doc. CCPR/C/21/Rev.1/Add.13, ¶ 8 (26 May 2004).
[93] Tsagourias, *supra* note 65, p. 242.
[94] Schmitt, *supra* note 34.
[95] Finland's Position, *supra* note 51.
[96] Ministre des Armées, *supra* note 42, p. 6 ("Conformément à l'obligation de diligence requise13, elle veille à ce que son territoire ne soit pas utilisé pour commettre des faits internationalement illicites à l'aide des TIC." [EN: In accordance with the obligation of due diligence 13, it will ensure that its territory is not used to commit internationally wrongful acts using ICTs]).
[97] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (10 March 2021), <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>, visited on 26 January 2022.
[98] Tallinn Manual 2.0, *supra* note 71, Rules 6 & 7.
[99] Andreas Paulus, 'Whether Universal Values can Prevail over Bilateralism and Reciprocity', in *Realizing Utopia: The Future of International Law*, p. 90 Antonio Cassese (ed.), (Oxford Scholarship Online, 2012).
[100] Israeli Perspective, *supra* note 3.
[101] Letter from the Netherlands, *supra* note 50.
[102] New Zealand Position, *supra* note 36.
[103] Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83 (12 December 2001), Art. 22; Gabčíkovo-Nagymaros-Project (Hung./Slovk.), 1997 ICJ 7, ¶83 (dissenting opinion of Judge Vereshchetin).
[104] G.A. Res. 56/83, Responsibility of States for internationally wrongful acts (28 January, 2002).

Regarding attribution, Schöndorf asserted that attribution remains a mostly technical matter that should not be overregulated, and that the choice of disclosing information supporting attribution claims remains at the exclusive discretion of the State.[105] Indeed, States were traditionally cautious in disclosing evidence in the context of cyber-attacks, even when denouncing and attributing it.[106] This reluctance derives from political and operational considerations, e.g. to safeguard espionage activities.[107] Also, powerful and tech-savvy States, such as Israel and Iran, are well positioned to promote attribution, with their own capabilities.[108] Another reason is the lack of an international attribution mechanism.[109] Recently, though, the tide is turning, as some States that fell victim to cyber-attacks were willing to attribute them.[110] This trend coincides with growing threats during the Covid-19 crisis against the health-care sector,[111] international organisations,[112] and research institutions in search of a vaccine.[113] While the proposition by Schöndorf that States are not obligated to disclose information is an accepted one,[114] the suggestion that attribution should not be over-regulated is problematic. Given that, I will dedicate some discussion in the final section to attribution.

---

[105] Israeli Perspective, *supra* note 3.
[106] Tran, *supra* note 19, p. 382.
[107] Yaël Ronen, 'Some Evidentiary Dimensions of Attributing Unlawful Cyber Operations to States', Hebrew University of Jerusalem Legal Research Paper 20-11, 28 (2020), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3579029>, visited on 26 January 2022.
[108] For discussion, *see*: Michael N. Schmitt, 'Grey Zones in the International Law of Cyberspace', 42 *Yale Journal of International Law Online* 1 (2017).
[109] Yuval Shany & Michael N. Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations', 96 Int'l L. Stud. pp. 196, 199 (2020).
[110] Mimran & Shany, *supra* note 68.
[111] Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?', Just Security, 27 March 2020, <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/>, visited on 26 January 2022; Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector, May 2020 (Oxford Statement), <https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea#/>, visited on 26 January 2022; The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, August 2020, <https://elac.web.ox.ac.uk/article/the-second-oxford-statement#/>, visited on 26 January 2022.
[112] World Health Organization, *WHO reports fivefold increase in cyber attacks*, (23 April 2020), <https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance>, visited on 26 January 2022.
[113] Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan B. Hollis, Harold Hongju Koh, James C. O'Brien & Tsvetelina van Benthem, The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, Just Security (11 August 2020), <https://www.justsecurity.org/71952/the-second-oxford-statement-on-international-law-protections-of-the-healthcare-sector-during-covid-19-safeguarding-vaccine-research/>, visited on 26 January 2022.
[114] Shany & Schmitt, *supra* note 109, p. 214; Brian J. Egan, 'International Law and Stability in Cyberspace', 35 *Berkeley Journal of International Law* pp. 169, 177 (2017); Tallinn Manual 2.0, *supra* note 71, p. 83.

In sum, Israeli policy reflects its self-perception as part of the dominating camp in the discussion on applicability of international law in cyberspace. Its legal views generally coincide with views adopted by Western States, with some unique characteristics. Schmitt concluded that the positions presented by Israel are sophisticated and surgical,[115] while Johansson termed it a reserved stance that demonstrated strategic commitment to its security interests.[116] For me, it is an important step forward that pushes further the inter-State dialogue on the application of international law to cyberspace.

3. The Iranian Perspective

3.1 *Background*

Iran is tech-savvy, with a well-organised cyber governance structure and significant cyber capabilities.[117] But still, it was also the target of cyber operations, most notably Stuxnet.[118] Recently, it faced cyber-attacks in response to the downing of a United States drone.[119] The declaration elaborates on three issues – sovereignty, intervention, and the use of force. Iran chose not to deal with attribution in this text. In the past, before the UN Open-ended Working Group, Iran opined that it is premature to deal with attribution in cyberspace.[120]

At the outset, Iran clarifies that it reserves the right to react against threats by any State, group, or any other entity supported, controlled or directed by any State.[121] This is a State-centric view that conditions the response on attribution to a State.[122] It is a different view than the one suggested by Schöndorf, notably in relation to the use of force against non-State actors.

---

[115] Schmitt, *supra* note 34.
[116] Johansson, *supra* note 26.
[117] Michael N. Schmitt, Noteworthy Releases of International Cyber Law Positions - Part II: Iran, Articles of War (27 Aug 2020), <https://lieber.westpoint.edu/iran-international-cyber-law-positions/>, visited on 26 January 2022 [hereinafter: Schmitt on Iran].
[118] For discussion, see: Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown, 2015).
[119] Andrew Hanna, 'The Invisible U.S.-Iran Cyber War', United States Institute of Peace (25 October 2019), <https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war>, visited on 26 January 2022; Idrees Ali & Phil Stewart, Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack, Reuters (16 October 2019), <https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK>, visited on 26 January 2022.
[120] Open-ended Working Group, Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security, 11 March 2020, p. 4, <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf>, visited on 26 January 2022 ("it is premature to discuss the specific secondary rules, including attribution, of the ICT environment…").
[121] Iranian Declaration, *supra* note 5.
[122] For discussion on the classic State-centred legal order, *see*: Yaël Ronen, **'**Entities that Can Be States but do not Claim to Be', in *Statehood and Self-Determination: Reconciling Tradition and Modernity in International Law*, p. 23, Duncan French (ed.), (Cambridge University Press, 2013).

Israel's view is consistent with its need to justify deployment of military force against non-State actors, a view that is shared with other States.[123] Iran, in contrast, does not face similar threats and is actually supporting non-State actors against other States – including Israel.[124]

In theoretical terms, Israel and Iran are interpreting the law in a way that will fit their interests. This is a demonstration of the strength of the realist theory that seeks to describe compliance with international law.[125] In this regard both States can be described as being as like-minded as they can be.[126] This is not a good sign, though, as stability is fragile when States pursue their own interests instead of opting for a comprehensive framework.[127]

The declaration begins with an accepted position, namely that cyberspace should be universally accessible,[128] and adds that States have a common but different responsibility.[129] Dividing responsibilities based on 'width of shoulders' is common in environmental law[130] and relating to DD.[131] Iran has also maintained this position in the past,[132] as it perceives the international plane as inequitable, perhaps given its subjection to sanctions.[133] It previously went as far as referring to the current situation as "information colonialism", and it also warned against the risk of the "monopolisation of the internet".[134]

---

[123] Schmitt, *supra* note 34.

[124] *See*, e.g.: Keith A. Petty, 'Veiled Impunity: Iran's Use of Non-State Armed Groups', *36 Denver Journal of International Law and Policy*, p. 191 (2008); Matthew Lewitt, The Origins of Hezbollah, The Atlantic (23 October 2013), <http://www.theatlantic.com/international/archive/2013/10/the-origins-of-hezbollah/280809/>, visited on 26 January 2022.

[125] For discussion, see: Moshe Hirsch, 'Compliance with International Norms in the Age of Globalization: Two Theoretical Perspectives', in *The Impact of International Law on International Cooperation: Theoretical Perspectives*, p. 166, Eyal Benvenisti & Moshe Hirsch (eds.), (Cambridge University Press, 2004).

[126] Others believe that compliance is best gained through coercive measures. *See*: Andrew T. Guzman, 'A Compliance-Based Theory of International Law', *90 Cal. L. Rev. 1823* (2002). For a critical view, *see*: Oona A. Hathaway, 'Do Treaties Make A Difference?', *111 Yale L.J. 1365* (2002).

[127] Dan Efrony, 'The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence', Just Security (16 July 2021), <https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/>, visited on 26 January 2022. This concern is especially pertinent in an area as dominated by political and military conflicts as the Middle East.

[128] Schmitt on Iran, *supra* note 117.

[129] Iranian Declaration, *supra* note 5.

[130] *See*: Daria Shapovalova, 'In Defence of the Principle of Common but Differentiated Responsibilities and Respective Capabilities' (2021), in *Debating Climate Law*, p.63 Benoit Mayer and Alexander Zahar (eds.), (Cambridge University Press 2021).

[131] Nicholas Tsagourias, 'Self-Defence against Non-state Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule', *29 Leiden J. Int'l L.*, pp. 801, 817 (2016).

[132] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (10 March 2021), <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>, visited on 26 January 2022.

[133] For discussion, *see*: Tom Ruys, Sanctions, 'Retorsions and Countermeasures: Concepts and International Legal Framework', in *Research Handbook on UN Sanctions and International Law 19* Larissa van den Herik (ed.), (Elgar online, 2017), <https://ssrn.com/abstract=2760853>, visited on 26 January 2022.

[134] *See* the comments by Iran to the zero draft report of the open-ended working group on developments in the field of information and telecommunications in the context of international security, <https://front.un-arm.org/wp-

3.2 Sovereignty

Unlike the Israeli declaration, the Iranian one clarifies that the sovereignty of States extends to cyberspace,[135] adopting the common view reflected by the recent report by the UN Groups of Governmental Experts.[136] Specifically – Iran views the following situations as infringements of sovereignty: 1) cyber-force with tangible or non-tangible implications; 2) intrusion in State cyber structures; 3) limiting measures, including sanctions.[137]

Iran aligns itself with the view that sovereignty is a rule of international law rather than an abstract principle.[138] The first two examples represent the majority view on the international plane.[139] As for the third example, it was probably raised since Iran is subject to limiting measures in light of its pursuit of nuclear technology[140] – sanctions that restrict its arms trading, freeze assets, and limit management of natural resources.[141] The Iranian assertion is misleading, though, since sanctions are considered as retorsion rather than an infringement of international law.[142]

3.3 Non-intervention

The next issue addressed is non-intervention. Iran stressed that every State "enjoys the inherent right to the full development of information system and mass media and their employment, without intervention, to advance their own political, social, economic, and cultural interests and aspirations".[143] The declaration provides the following examples of violations of the rule: 1) cyber manipulation of elections; 2) cyber activities paralysing websites to provoke internal

---

content/uploads/2021/02/I.R.Iran-Zero-Draft-final.pdf>, visited on 26 January 2022. For discussion on the influence of events on the international plane that are perceived by Iran as hostile – such as the United States Diplomatic and Consular Staff case, controversies over the Iranian islands in the Persian Gulf and Iran's nuclear program – *see* Pouria Askary and Sina Etezazian, 'Critical Pedagogy Symposium: Critical Pedagogical Approaches towards International Law Teaching in Iran–From Classroom to Virtual Space', *Opinio Juris* (1 September 2020), <http://opiniojuris.org/2020/09/01/critical-pedagogy-symposium-critical-pedagogical-approaches-towards-international-law-teaching-in-iran-from-classroom-to-virtual-space/>, visited on 26 January 2022. As discussed by Askary and Etezazian, these events affected the way international law is thought of in Iran (*e.g.* emphasis on Iranian and third world approaches in international law.

[135] Iranian Declaration, *supra* note 5.

[136] Przemysław Roguski, 'Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace', Just Security (3 September 2020), <https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/>, visited on 26 January 2022.

[137] Iranian Declaration, *supra* note 5.

[138] Przemysław, *supra* note 136.

[139] Schmitt on Iran, *supra* note 117.

[140] N. Jansen Calamita, 'Sanctions, Countermeasures, and the Iranian Nuclear Issue', *42 VAND. J. TRANSNAT'L L.* pp. 1393, 1397 (2009).

[141] For discussion, *see*: Peter Seeberg, The EU and the International Sanctions Against Iran: European and Iranian Foreign and Security Policy Interests, and a Changing Middle East, *2 Palgrave Communications* p. 1 (2016), <https://ssrn.com/abstract=2877735>, visited on 26 January 2022.

[142] Tallinn Manual 2.0, *supra* note 71, p. 324.

[143] Iranian Declaration, *supra* note 5.

tensions; 3) armed intervention via cyber tools; 4) interference in the political, social, or economic order of other States. Iran sets a low threshold for application of the rule, for instance relating to the fourth example, while echoing the consensual position that armed intervention would constitute a breach.[144] Israel's declaration, by contrast, sets a high legal threshold that perhaps seeks to limit condemnation of actions that it might undertake.[145]

Relating to cyber manipulation of elections, Iran conforms with Israel as well as other States such as Australia.[146] Iran does take a step further in arguing that prohibited intervention includes influence operations aimed at affecting voter behaviour.[147] This is going beyond the common understanding of the rule of non-intervention,[148] in a world in which digital platforms allow and are used for global influencing.[149] Indeed, only a few weeks after the release of its statement – Iran itself interfered, under its own standards, in the 2020 United States elections.[150]

3.4 The Prohibition Against the Use of Force

Iran maintains that cyber operations resulting in material damage, or that will logically lead to it, constitute a prohibited use of force.[151] This is a widely accepted position adopted by States such as France and the United Kingdom, as well as the Tallinn Manual.[152] As for cyber operations that are neither destructive nor injurious, Iran adopts a restrictive position that might derive from the concern that a low threshold cyber operation would open the door to a military response.[153] In its declaration, Iran places emphasis on critical infrastructure,[154] in line with the growing importance of technologies in State infrastructures.[155] Both Israel and Iran seem to agree that under existing law a use of force must involve actual or expected physical damage, injury or death.[156] As such, both set a high threshold for what constitutes a use of force.

---

[144] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV) (24 October 1970).
[145] Johansson, *supra* note 25.
[146] Australia's Cyber Strategy, *supra* note 4.
[147] Przemysław, *supra* note 136.
[148] Schmitt on Iran, *supra* note 117.
[149] *See*: W. Lance Bennett & Steven Livingston (eds.), 'A Brief History of the Disinformation Age: Information Wars and the decline of Institutional Authority', in *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States* (Cambridge University Press, 2020) p. 3.
[150] Johansson, *supra* note 25.
[151] Iranian Declaration, *supra* note 5.
[152] Przemysław, *supra* note 136; Tallinn Manual 2.0, *supra* note 71, p. 83.
[153] Schmitt on Iran, *supra* note 117.
[154] Iranian Declaration, *supra* note 5.
[155] Tsagourias, *supra* note 65, p. 231; Geers, *supra* note 66, p. 2.
[156] Przemysław, *supra* note 136.

A low threshold for considering what amounts to use of force provides States with greater discretion in responding to malicious activity.[157] The concern with lowering the bar, though, is that of military escalation.[158] States such as the Netherlands,[159] and Finland,[160] refrained from conditioning that a cyber operation must include physical damage for it to amount to a use of force. Yet, for Iran and Israel, physical damage is a necessary requirement.

3.5 ***Intermediary conclusion***

In sum, Iran and Israel intertwine their security and military interests with their legal perspectives. Israel attempts to adapt its view to other Western States, with small differences (such as its view concerning DD), while Iran cannot afford to move away from its more immediate interests as it sees itself limited by sanctions and political pressure (most notably relating to its nuclear programme). Iran's experience with political pressure creates a sense of unfairness, leading it to push for promotion of new international law instruments that will regulate cyberspace and make sure that this field will be more equitable. This is in contrast to Israel, which prefers the application of existing international laws to cyberspace, as it sees itself as better situated in the international arena, though it certainly suffers from its share of political problems.

Iran presents a State-centric position, in comparison to Israel, which asserts rights against non-State actors. Another difference is that Iran recognises the applicability of sovereignty to cyberspace, out of its desire to respond to cyber-attacks whether their implications are tangible or not, while Israel presents a more suspicious view in this regard (which suffers from lack of clarity). An additional difference can be seen in Iran's low threshold for non-intervention, seeking discretion in *responding* to cyber threats, contrary to the high standard suggested by Israel, aiming for leeway of *action*. One issue which both States agree upon is the required high threshold for an armed attack to occur – allowing leeway of action when promoting hostile cyber operations, while minimising escalation to a full-fledged military conflict. Their view also coincides, to a certain extent, relating to cyber manipulation of elections.

One issue that both Israel and Iran have chosen not to properly address is attribution – a key issue in cyberspace. This indicates, broadly speaking, the need to promote an interna-

---

[157] Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense', *38 Stanford J. Int'l L.*, pp. 207, 228 (2002).
[158] Christine Gray, 'The Limits of Force', 376 Recueil des Cours, pp. 93, 109 (2016).
[159] Letter from the Netherlands, *supra* note 50.
[160] Finland's Position, *supra* note 51.

tional legal framework that can offer more consensus, rather than the current fragmented situation in which every State pulls in the direction of its own interests. This will not be easy, of course, politically or practically, but it is of great importance. Clear international law rules for cyberspace could settle open questions, provide accepted procedures – for example for raising a claim of attribution – and incentivise cooperation, restraint and prudence. Given that, before concluding I shall make some general points on the issue of attribution.

4. Attribution, and a look ahead

Establishing the identity of the attacker is crucial to craft a response, and it also has significance in terms of legal responsibility for the attack.[161] Some advances have been made, such as tools that trace technological footprints.[162] Yet, attributing malicious acts to a specific agent is far from being an easy task.

The rules of State responsibility were codified into ARSIWA.[163] In cyberspace, state responsibility usually can arise when illegal acts or omissions are performed by an organ of the State, persons entrusted with governmental authority, or if the State instructed, directed or controlled a non-state entity.[164] States are also responsible for acts that they acknowledged and adopted as their own.[165] While there is a legal framework to work with, there are some noteworthy challenges when dealing with cyberspace.

Some problems derive from the structural design of the Internet.[166] Attackers can delay actions and perform them through intermediary systems in other jurisdictions.[167] They are able to harness proxy servers, via techniques such as 'spoofing' or 'stepping stones', leaving behind little evidence.[168] For example, the attacks in Estonia involved nearly 100,000 hijacked computers from almost 180 States.[169] The gap between cyber forensics and kinetic forensics might

---

[161] Broadly speaking, fact-finding contributes to the rule of law in the international plane. See: Dan Saxon, 'Purpose and Legitimacy in International Fact-Finding Bodies', in *Quality Control in Fact-Finding*, pp. 211, 219 Morten Bergsmo (ed.), (Torkel Opsahl, 2013). For discussion on international rule of law, more generally, *see*: Jan Klabbers, Anne Peters & Geir Ulfstein, *The Constitutionalization of International Law* (*EJIL: Talk!* 2009).
[162] Thomas Rid & Ben Buchanan, 'Attributing Cyber Attacks', *38 J. Strategic Stud.* pp. 4, 15 (2014). *See also*: François Delerue, Cyber Operations and International Law 55 (Cambridge University Press 2020).
[163] G.A. Res. 56/83, Responsibility of States for internationally wrongful acts (28 January 2002).
[164] *Ibid*, Arts. 4, 5 & 8.
[165] *Ibid*, Art. 11. *See also*: United States Diplomatic and Consular Staff in Tehran (*United States of America* v. *Iran*), Judgment, 1980 ICJ Rep. 3 (24 May).
[166] Tran, *supra* note 19, p. 387.
[167] David Wheeler et al., 'Techniques for Cyber Attack Attribution', *Institute for Defense Analyses 53* (October 2003), <https://apps.dtic.mil/sti/pdfs/ADA468859.pdf>, visited on 26 January 2022.
[168] Tran, *supra* note 19, p. 387; *Georg Kerschischnig - Cyberthreats and International Law*, (The Hague: Eleven International Publishing, 2012) p. 7; Jack Goldsmith, 'What Is the Government's Strategy for the Cyber-Exploitation Threat?', Lawfare Blog (10 August 2011), <https://www.lawfareblog.com/what-governments-strategy-cyber-exploitation-threat>, visited on 26 January 2022.
[169] Tsagourias, *supra* note 65, p. 233.

decrease over time, but there is still much work ahead.[170] The difficulty in obtaining evidence, sometimes from areas under the control of other States,[171] is also pertinent.[172]

At times, the context of the attack might indicate the perpetrator. Illustrations include the Stuxnet malware, in the midst of a United States and Israel-led campaign dealing a blow to the Iranian nuclear plan,[173] and the cyber-attack on Sony Pictures, against the backdrop of the theatrical release of 'The Interview', a comedy which ridiculed Kim Jong Un.[174] In order to evaluate whether claims of attribution can hold water, there is a need to look into international standards of gathering evidence and standards of proof. While some States (such as Israel) assert that there is no duty to disclose evidence when making a claim for attribution,[175] it is crucial to substantiate a legal assertion through evidence while meeting the relevant international standards of proof. It is an open question, though, whether there is such a standard when it comes to cyber-attacks.

International dispute resolution mechanisms are lenient in terms of admitting evidence, especially when there is a need to collect evidence from the jurisdiction of other States.[176] International law jurisprudence is reflected by the absence of explicit articulations of the standard of proof and the type of evidence that is required in judicial proceedings.[177] As for the burden of proof, this falls on the party that presents its submissions.[178]

It is hard to capture the multifarious standards of proof set by the International Court of Justice: ranging from 'too improbable' in the *Corfu Channel* Case[179] to 'consistent with the probabilities' in the *Nicaragua* case,[180] from proof 'to the Court's satisfaction' in the *Armed Activities* case[181] to 'sufficient certainty' in the *Oil Platform* case,[182] and from 'evidence that is

---

[170] William C Banks, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution', *113 AJIL Unbound*, pp.191, 192 (2019).
[171] *See*, in the context of the use of military force: *Nicaragua* case, *supra* note 80, p. ¶57.
[172] For discussion, *see*: Marco Roscini, 'Digital Evidence as a Means of Proof before the International Court of Justice', *21 Journal of Conflict and Security Law*, p. 541 (2016).
[173] Tran, *supra* note 19, p. 394. *See also*; O'Connell, *supra* note 21, p. 188.
[174] Andrea Peterson, The Sony Pictures Hack, Explained, Wash. Post (18 December 2014), <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>, visited on 26 January 2022.
[175] Shany & Schmitt, *supra* note 109, p. 214. *See also*: Tallinn Manual 2.0, *supra* note 71, p. 83.
[176] *Corfu Channel* case, *supra* note 91, p. 18.
[177] Ronen, *supra* note 107, p. 2. *See also*: Eritrea-Ethiopia Claims Commission, Partial Award: Prisoners of War - Eritrea's Claim 17 (2003) XXVI RIAA 23 para. 44 ("44. Also reflecting common international practice, the Rules do not articulate the quantum or degree of proof that a party must present to meet this burden of proof").
[178] Pulp Mills on the River Uruguay (*Argentina* v. *Uruguay*), Judgment, [2010] ICJ Rep 14, ¶162.
[179] *Corfu Channel* case, *supra* note 91, p. 14.
[180] *Nicaragua* case, *supra* note 80, p. ¶158.
[181] Case concerning Armed Activities on the Territory of the Congo (*Democratic Republic of the Congo* v. *Uganda*), Judgment, ICJ [2005] Reports 2005, ¶62.
[182] Oil Platforms (*Iran* v. *USA*), 2003 ICJ 161 (Separate Opinion of Judge Kooijmans), ¶63. Similar terms were used in the *Corfu Channel* case: 'a degree of certainty'; 'decisive legal proof'; 'firm conclusion' and 'conclusive' evidence. *See: Corfu Channel* case, *supra* note 91, pp. 9, 16 & 17.

fully conclusive' in the *Bosnia Genocide* case[183] to 'beyond any reasonable doubt' in the *South West Africa* case.[184] Ronen noted that most common among these are 'beyond reasonable doubt', 'clear and convincing' evidence and 'preponderance of evidence'.[185] One general understanding can be extracted – that a claim of exceptional gravity against a State needs to be proved by fully conclusive evidence.[186] Similarly, the Tallinn 2.0 Manual suggested that the standard of proof be linked to the severity of the breach.[187]

As for scholarly views, Schmitt supports the need for clear and compelling evidence.[188] Kilovati and Tsagourias, in comparison, suggest that States are required to provide reasonably compelling evidence.[189] Others suggested lowering the standard of proof when dealing with cyber operations, given evidential difficulties.[190] Antonopoulos, for example, proposes a presumption of responsibility for States to debunk in cases where a cyber operation can be traced to their territory.[191] Margulies suggests that when a State funds or has another connection with a non-State entity that was engaged in a cyber-attack, it will be up to that State to demonstrate it does not bear responsibility.[192] These suggestions are of interest, but any evaluation of them must consider that the risk of lowering the standard lies in the possibility of escalation based on misattribution.[193]

Looking forward, it is important to recognise an international standard of proof in cyberspace. Such a standard, which should be accompanied by a procedure to meet it, will incentivise States to cooperate in attribution efforts. Reliance on international law might encourage States to accept restraint in cross-border cyber operations and to exercise more control over non-State actors. It might also serve as a chilling factor.[194] States such as Israel and Iran have

---

[183] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosn. & Herz.* v. *Serb. & Montenegro*), 2007 ICJ Rep. 43 (26 February), ¶209.
[184] South West Africa (*Ethiopia* v. *South Africa*; *Liberia* v. *South Africa*), ICJ Reports 1962, 465, 473 Joint Dissenting Opinion of Judges Spender and Fitzmaurice. *See also*: *Oil Platforms* case, *supra* note 183, p. ¶56. Similar terms were also used, like 'no reasonable doubt'. *See:* Case concerning the Aerial Incident of July 27, 1955 (*Israel* v. *Bulgaria*), ICJ Reports 1959, Joint Dissenting Opinion of Judges Lauterpacht, Wellington Koo and Spender, 162.
[185] Ronen, *supra* note 107, p. 13.
[186] Separate Opinion of Judge Higgins in Case Concerning Oil Platforms (*Islamic Republic of Iran* v. *USA*) (Merits) [2003] ICJ Rep 161, ¶33.
[187] Tallinn Manual 2.0, *supra* note 71, pp. 81–82.
[188] Michael N. Schmitt, 'Cyber Operations and the Jus ad Bellum Revisited', 56 *Vill. L. Rev.* pp.569, 595 (2011).
[189] Kilovaty, *supra* note 22, p. 118 (2014); Tsagourias, *supra* note 65, p. 235.
[190] Ronen, *supra* note 107, p. 20.
[191] Constantine Antonopoulos, 'State Responsibility in Cyberspace', in Nicholas Tsagourias and Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace*, p. 55 (Edward Elgar, 2015).
[192] Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility', 14 Melbourne J. Intl L., pp. 496, 506 (2013).
[193] Lorraine Finlay and Christine Payne, 'The Attribution Problem and Cyber Armed Attacks', *113 American Journal of International Law*, pp. 202, 204 (2019).
[194] Shany & Schmitt, *supra* note 109, pp. 220–221.

taken the first step – in releasing legal opinions, and participating in the initiatives of international organisations. However, lack of a comprehensive legal framework endangers peace and stability. The cyber-attacks against Yahoo[195] and Sony[196] indicate that this effort should not stop with States, as this is an opportunity to involve non-State actors which might help in dealing with future threats.[197] This will not be an easy task given the need to bridge between leading political and technical powers.[198] But still, given its importance, this endeavour should not be discarded.

5. Conclusion

Israeli policy reflects its self-perception as a technologically advanced State that is part of the dominant camp, and generally coincides with many of the views adopted by Western states in that camp, apart from some unique characteristics. As for Iran, its State-centric position is affected both by its advanced technological abilities, and from its experience with sanctions. This experience creates a sense of unfairness, leading Iran to push for promotion of new international law instruments that will regulate this new and constantly developing field, in contrast to Israel, which prefers application of existing international laws to cyberspace.

Given its experience with non-State actors, Israel emphasises the right of self-defence against them, while adopting the mainstream interpretation of the definition of illegal use of force. Similarly, Israel defines an attack under IHL as one which causes significant physical damage. The intention behind both assertions is to allow Israel more flexibility while conducting cyber operations of a military nature, both during armed conflicts and in peacetime. Israel maintains some ambiguity regarding sovereignty, and particularly the legal responsibility of a third party when information transits through that third party's territory. Moreover, it asserts that the principle of DD does not constitute a binding rule in the cyber context – a questionable contention. Regarding attribution, Israel does not support its overregulation. Israel's position on countermeasures is reasonable, and conforms with the existing state of international law.

Some differences emerge from the comparison between the two States. In contrast to Israel, Iran unreservedly recognises the applicability of sovereignty to cyberspace, out of its

---

[195] Mike Levine & Emily Shapiro, How Russian Agents Allegedly Directed Massive Yahoo Cyberattack, ABC News (15 March 2017), <https://abcnews.go.com/US/russian-agents-facing-charges-yahoo-hacking-attacks/story?id=46142396>, visited on 26 January 2022.
[196] Peter Elkind, Inside the Hack of the Century: Part III, Fortune (27 June 2015), <https://fortune.com/long-form/sony-hack-part-two/>, visited on 26 January 2022.
[197] O'Connell, *supra* note 21, p. 208.
[198] Matthew C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', *36 Yale J. Int'l L.*, pp. 421, 425 (2011).

desire to broaden the spectrum of response to cyber-attacks, even without tangible implications. This interest is also evident in Iran's low threshold for non-intervention, contrary to the high standard suggested by Israel, seeking wider leeway of response. Some convergence of views between Israel and Iran exists in their requirement of a high threshold for an armed attack to occur, and relating to cyber manipulation of elections. This analysis of the Israeli and Iranian positions highlights the strengths and weaknesses of the current state of affairs, but at the same time illustrates that States are using declarations such as those under discussion to promote their own strategic interests, which in turn derives from their unique experience and values.

One issue that was neglected by both States is attribution – one of the most pressing challenges in cyberspace. Failure to properly deal with this central issue exemplifies the need to promote an international legal framework that can facilitate more consensus, rather than the current fragmented situation in which every State tries to pull in the direction of its own interests. Clear international law rules could settle questions such as the required standard of proof for attribution, or the procedure through which a State can make a claim of attribution, and will incentivise States to cooperate in international efforts, encourage them to accept restraint in cross-border cyber operations, and to exercise prudence in their own territory. Such rules can also serve as an important chilling factor. States that have submitted their declaration, like Israel and Iran, have taken a first step – but this is not enough. The goal of reaching a comprehensive legal framework cannot be neglected, and declarations by States should operate as leverage in this direction rather than a move to a different one.