EXPOSÉ

Vorläufiger Arbeitstitel:

HUMAN RIGHTS IMPLICATIONS OF CYBER OPERATIONS

Mag.iur. Markus Stemeseder

Angestrebter akademischer Grad:

Doktor der Rechtswissenschaften (Dr.iur.)

Dissertationsfach: Völkerrecht
Studienrichtung laut Studienblatt: Doktoratsstudium Rechtswissenschaften UG 2002
Studienkennzahl: A 783-101
Betreuer:innen: Prof. Ursula Kriebaum und Prof. Stephan Wittich

Table of Contents

1. Introduction

Few technologies have changed the world as profoundly as the internet. However, while it has endowed individuals with an unprecedented level of freedom to receive and impart information, it also entails an increased potential of human rights violations.[1] After all, individuals and states are becoming ever more dependent on cyberinfrastructure,[2] which is exploited by states, terrorists, and criminals alike to sabotage other states, ruin businesses and harm individuals. Analyzing the human rights obligations of states in the context of cyber operations is the subject of this research proposal.

2. Background

Cyber operations, that is to say, 'operations that employ capabilities aimed at achieving objectives in or through cyberspace'[3] may occur in various forms. By utilizing an ever more diversified arsenal of weaponized code, they may e.g. manipulate frequency converter drives to bring centrifuges used for uranium enrichment to break,[4] cripple a state's power grid by incapacitating energy distribution companies[5] or cause damage to industrial plants by manipulating blast furnace control.[6] They may disrupt vaccine research facilities,[7] meddle in elections by influencing media, voting infrastructure or discrediting candidates,[8] take down websites of banks, newspapers, broadcasters and state agencies,[9] or may even cause the loss of life.[10]

---

[1] David P Fidler, 'Cyberspace and Human Rights' in Nicholas Tsagourias and Russel Buchan (eds), *Elgar Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 137.

[2] Helen McDermott, 'Application of the International Human Rights Law Framework in Cyber Space' in Dapo Akande and others (eds), *Human Rights and 21st Century Challenges* (OUP 2020) 190.

[3] Yoram Dinstein and Arne Willy Dahl (eds), *Oslo Manual on Select Topics of the Law of Armed Conflict* (Springer 2020) Rule 20.

[4] E.g. the Stuxnet worm, see Josh Halliday, 'Stuxnet Worm is Aimed to Sabotage Iran's Nuclear Ambition, New Research Shows' (*The Guardian*, 16 November 2016) <www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear> accessed 16 May 2022.

[5] As it happened in Ukraine in 2015 and during the Russian invasion in February 2022, see François Delerue, *Cyber Operations and International Law* (CUP 2020) 76-77; Patrick Howell O'Neal, 'Russian Hackers Tried to Bring Down Ukraine's Power Grid to Help the Invasion' (*MIT Technology Review*, 12 April 2022) <www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/> accessed 16 May 2022.

[6] Which occurred in Germany in 2015 by manipulating the plant's control system, see BBC, 'Hack Attack Causes "Massive Damage" at Steel Works' (*BBC*, 22 December 2014) <www.bbc.com/news/technology-30575104> accessed 16 May 2022.

[7] Akande and others, 'Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector' (*EJIL:Talk!*, 21 May 2020) <www.ejiltalk.org/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/> accessed 18 May 2022.

[8] Michael Schmitt, 'Foreign Cyber Interference in Elections' (2021) 97 United States Naval War College International Law Studies 739.

[9] By so-called DDoS (Directed Denial of Service) Attacks, which flood the bandwidth of the target system with numerous visits, as happened in Estonia in 2007, see Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia' (*The Guardian*, 17 May 2007) <www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 16 May 2022.

[10] On so-called ransomware attacks, which encrypt hard drive files and demand payment for allowing affected persons to regain access, targeted a hospitals, which was impeded to perform critical surgery, see Joseph Marks, 'Ransomware Attack Might have Caused Another Death' (*The Washington Post*, 11 October 2021) <www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/> accessed 17 May 2022.

Finally, the ongoing Russian aggression against Ukraine shows the danger emanating from cyber operations and their potential to infringe human rights,[11] regardless of whether state or non-state actors are their authors. For instance, to facilitate the Russian invasion, a cyberattack targeted a satellite communication provider, causing outages in communications to Ukrainian state agencies, businesses, and individuals.[12] At the same time, several wiper malware attacks erased hard drives of Ukrainian ministries and individuals, leading to a substantial loss of data.[13] Both had spillover effects across entire Europe.[14]

At the same time, cyber operations are becoming indispensable for states to counter malicious activities in cyberspace, which may originate both from within their own territory or abroad. Meanwhile, police units patrol dark web marketplaces to arrest vendors of drugs and firearms,[15] take down botnets[16] that use remotely controlled computers of individuals for cybercrime purposes[17] or erase malware used for crypto-jacking campaigns.[18]

Considering this multitude of cyber operations that may be effectuated by state and non-state actors alike, the scrutiny of states' human rights obligations appears integral for the future of human rights protection in cyberspace. However, despite the apparent potential of cyber operations to violate individuals' rights and freedoms, a comprehensive analysis of their place within the human rights law framework is yet missing. This thesis aims to explore the human

---

[11] UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; OSCE Representative on Freedom of the Media; Inter-American Commission on Human Rights Special Rapporteur for Freedom of Expression; African Commission Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information' (4 May 2022) <www.ohchr.org/en/statements-and-speeches/2022/05/ukraine-joint-statement-russias-invasion-and-importance-freedom> accessed 2 June 2022; Gordon Corera, 'Ukraine War: Don't Underestimate Russia Cyber-Threat, Warns US' (*BBC*, 12 May 2022) <www.bbc.com/news/technology-61416320> accessed 16 May 2022.

[12] European Council and Council of the European Union, 'Russian Cyber Operations against Ukraine: Declaration by the High Representative on behalf of the European Union' (*EU*, 10 May 2022) <www.consilium.europa.eu/de/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/> accessed 18 May 2022.

[13] Kyle Fendorf and Jessie Miller, 'Tracking Cyber Operations and Actors in the Russia-Ukraine War' (*Council on Foreign Relations*, 24 March 2022) <www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war> accessed 18 May 2021.

[14] *Ibid*.; European Council and Council of the European Union (2022); Chris Vallance, 'UK Blames Russia for Satellite Internet Hack at Start of War' (*BBC*, 11 May 2022) <www.bbc.com/news/technology-61396331> accessed 17 May 2022.

[15] EUROPOL, 'Global Law Enforcement Action against Vendors and Buyers on the Dark Web' (*EUROPOL*, 26 March 2019) <www.europol.europa.eu/media-press/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web> accessed 18 May 2022.

[16] EUROPOL, 'World's Most Dangerous Malware EMOTET Disrupted through Global Action' (*EUROPOL)* <www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action> accessed 17 May 2022.

[17] 'Botnets' are networks of remotely controlled private computers that are infected with malware without the owners' knowledge and used to carry out orders of the person in control of the botnet. Botnets are usually used for financial gain, including data mining or the theft of social security or credit card data as well as spreading viruses or launching DDoS attacks. See National Cybersecurity Alliance, 'Identity Theft, Fraud and Cybercrime: Malware, Botnets and Ransomware' (*National Cybersecurity Alliance*) <https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/malware-and-botnets/> accessed 24 May 2022.

[18] 'Cryptojacking is the unauthorized use of victims' computing power to mine cryptocurrency for the cybercriminals. In cryptojacking, the victims unwittingly install a programme with malicious scripts that allow the cybercriminals to access their computer or other Internet-connected devices', INTERPOL, 'INTERPOL-Led Action Takes Aim at Cryptojacking in Southeast Asia' (*INTERPOL*, 8 January 2020) <www.interpol.int/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia> accessed 18 May 2022.

rights obligations of states, both when conducting cyber operations – for benevolent or malicious purposes alike – and when they or their residents become their target. This requires analysis of the applicability of human rights law in the context of cyber operations, the potential interference of cyber operations with human rights, whether such interferences may be justified within the framework of human rights law, and to what extent states are under a due diligence obligation to prevent human rights violations by non-state actors or other states.

3. State of Current Research

While the body of literature on cyber operations in the context of general international law,[19] state responsibility,[20] and international humanitarian law[21] has grown significantly, academia has paid little attention to their human rights implications.[22] The human rights community was rather concerned with advocating the application of human rights in cyberspace,[23] focusing particularly on everyday situations, such as communication on social media networks and content moderation[24] and the relationship between hate speech and the freedom of expression.[25] Also the question whether internet access is a human right[26] and whether surveillance and data

[19] E.g. Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017); Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (2019) Chatham House Research Paper 18 <www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf> accessed 15 May 2021.

[20] E.g. Delerue (2020); Constantine Antonopoulos, 'State Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015); Nicholas Tsagourias and Russel Buchan (eds), *Elgar Research Handbook on International Law and Cyberspace* (Edward Elgar 2021); Yoram Dinstein, 'Computer Network Attacks and Self-Defence' in Michael Schmitt and others (eds), *Computer Network Attack and International Law* (Naval War College 1999); Berenice Boutin, 'Shared Responsibility for Cyber Operations' (2019) 113 AJIL Unbound 197.

[21] Heather H Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012); International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper, November 2019' (2020) 102 International Review of the Red Cross 481; Christopher Whyte and Brian Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy* (Routledge 2018); Jonathan Horowitz, 'Cyber Operations under International Humanitarian Law: Perspectives from the ICRC' (2020) 24(11) ASIL insights <www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc> accessed 15 Mai 2021.

[22] David P Fidler, 'Cyberattacks and International Human Rights Law' in Stuart Casey-Maslen (ed), *Weapons under International Human Rights Law* (CUP 2014) [online] ('For the most part, the human rights community has not joined in the hype surrounding perceived threats to national and global cybersecurity, except to remain vigilant that increased cybersecurity should not infringe on the enjoyment of human rights in virtual and non-virtual spaces'); François Delerue, *Cyber Operations and International Law* (CUP 2020) 260 ('Given its significance, this question deserves further and extensive attention […]').

[23] David P Fidler, 'Cyberspace and Human Rights' in Nicholas Tsagourias and Russel Buchan (eds), *Elgar Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 137; McDermott (2020).

[24] Barrie Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation' (2020) 43 Fordham International Law Journal 939; Thiago Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' [2020] Human Rights Law Review 607.

[25] Viera Pejchal, *Hate Speech and Human Rights in Eastern Europe: Legislating for Divergent Values* (Routledge 2020); Wolfgang Benedek and Matthias C Kettemann, *Freedom of Expression and the Internet* (2nd rev edn, CoE 2020).

[26] Ryan Shandler and Daphna Canetti, 'A Reality of Vulnerability and Dependence: Internet Access as a Human Right' (2019) 52 Israel Law Review 77.

gathering aimed to counter cybercrime and terrorism may be lawful in light of the right to privacy was to a large extent thoroughly analyzed.[27] A more limited amount of literature exists on cyber interference in elections and their potential effect on the right to self-determination.[28]

However, particularly if cyber operations seek to detrimentally affect cyberinfrastructure to produce physical harm, they may breach several other human rights, reaching from the right to property to the right to life. For instance, in 2021, the US-based Colonial Pipeline Company fell victim to a data theft operation and a ransomware attack, resulting in its temporary shutdown. This entailed gas shortages in the South and East Coasts and the unavailability of gas and jet fuel at gas stations and airports, while panic buying led to price spikes and four US federal states declared a state of emergency.[29] In recent years, such ransomware attacks have increased dramatically[30] and even targeted hospitals to encrypt computers[31] and steal patients' protected health data.[32] The inaccessibility of patients' health information causes delays in treatment and ultimately can lead to the death of patients.[33] Thus, not only the states that effectuate such cyber operations may breach the rights to life, health, privacy, and property, but also those states in whose territory the affected companies or hospitals are located may be responsible for failing to protect these rights by taking all reasonable measures to prevent cyber incidents from happening.[34] Finally, also state action aimed to curb cybercrime may violate human

---

[27] See e.g. Laura K Donohue, 'Privacy and Surveillance' *The Cost of Counterterrorism: Power, Politics, and Liberty* (CUP 2008); Katherine J Strandburg, 'Surveillance of Emergent Associations: Freedom of Association in a Network Society' in Alessandro Acquisti and others (eds), *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications 2007); Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27; Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2013) 82 Fordham Law Review 2137; Anne Peters, 'Surveillance without Borders? The Unlawfulness of the NSA-Panopticon (*EJIL:Talk!*, 1 November 2013) <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/> accessed 16 May 2022.

[28] Michael Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 Chicago Journal of International Law 30; Schmitt (2021) 739; Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Rowman & Littlefield 2019); Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (CUP 2020); Jens David Ohlin and Duncan B Hollis (eds), *Defending Democracies, Combatting Foreign Election Interference in the Digital Age* (OUP 2021).

[29] Cyber Law Toolkit, 'Colonial Pipeline Ransomware Attack (2021)' (*Cyber Law Toolkit*) <https://cyberlaw.ccdcoe.org/wiki/Colonial_Pipeline_ransomware_attack_(2021)> accessed 25 May 2022. Some suspect a hacker gang that operated from Russian territory 'with tacit approval' of the Kremlin, see Emily Harding, 'Holding Moscow Accountable for Its Criminal Networks' (*Center for Strategic and International Studies*, 1 June 2021) <www.csis.org/analysis/holding-moscow-accountable-its-criminal-networks> accessed 24 May 2022.

[30] Amounting to 304 million attacks in 2020, constituting a 62% increase from the previous year, see Statista, 'Annual Number of Ransoware Attacks Worldwide from 2016 to 2020' (*statista*, 22 July 2021) <www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/#:~:text=According%20to%20an%20annual%20report%20on%20global%20cyber,attacks%20worldwide%20from%202016%20to%202020%20%28in%20millions%29> accessed 3 June 2022.

[31] As happened in Alabama and Germany, see Marks (2021).

[32] Heather Landi, 'Healthcare Data Breaches Hit All-Time High in 2021, Impacting 45M People' (*Fierce Healthcare*, 1 February 2022) <www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people> accessed 25 May 2022.

[33] See Marks (2021); Nicole Wetsman, 'Hospitals Say Cyberattacks Increase Death Rates and Delay Patient Care' (*The Verge*, 27 September 2021) <www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients> accessed 3 June 2022.

[34] Cyber Law Toolkit, 'Scenario 20: Cyber Operations against Medical Facilities' (*Cyber Law Toolkit*) <https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities#International_human_rights_law> accessed 25 May 2022.

rights. For example, the growing practice of 'covert policing' in the dark web, which involves police officers who pretend to be administrators of illegal marketplaces to identify criminals[35] raises questions on the admissibility of evidence, the right to due process, and the right to privacy. Scenarios of this kind have not yet received awareness from the academic community. Rather, scholars have only drawn attention to a variety of human rights cyber operations could interfere with, but without examining their scope of protection, whether states' actions would constitute an interference with the identified human rights or whether potential violations could be justified.[36]

In his brief overview of 'Cyber Operations and Human Rights',[37] Delerue intentionally 'only skims the surface'[38] by enumerating a variety of potentially affected human rights.[39] Equally listing several rights,[40] the experts of the Tallinn Manual confine their analysis to general remarks, e.g. that the enjoyment of economic, social and cultural rights 'is increasingly dependent on cyber activities',[41] that human rights law[42] and its limitations[43] apply in cyberspace, or that states are under the same obligations online as they are offline.[44] Milanovic points at a diverse array of scenarios in which human rights could be violated,[45] but focusses on their extraterritorial application. Fidler explains the lack of interest in the subject of cyber operations and human rights with the lack of perceived threats posed to cybersecurity, and hence the lack of forced policy change that would spark interest in this field.[46] He equally lists a variety of potentially affected human rights[47] and points to states' due diligence obligations with regard to countering cybercrime by non-state actors, which he, however, dismisses due to the difficulties arising from extraterritorial enforcement.

---

[35] Gemma Davies, 'Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers' (2020) 84 Journal of Criminal Law 407, 411.
[36] Delerue (2020) 261.
[37] *Ibid*., 260-271.
[38] *Ibid*., 260.
[39] *Ibid*., 268-269, 270, listing *inter alia* the right to property, the right to life, the right to privacy, the right to security of the person, the right to social security, the freedom of expression as well as the right to due process and the presumption of innocence.
[40] Michael Schmitt, 'International Human Rights Law' in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 194. On civil and political rights, the freedom of expression, the freedom of peaceful assembly, the freedom of opinion, the right to privacy, the right to due process. On economic, social and cultural rights, they enumerate 'the right to an adequate standard of living, including adequate food, the right to the enjoyment of the highest attainable standard of physical and mental health, the right to work, the right to education, and the right to take part in cultural life'.
[41] *Ibid*.
[42] *Ibid*., Rule 34.
[43] *Ibid*., Rule 37.
[44] *Ibid*., Rule 36.
[45] '[F]rom the rights to privacy and the freedom of expression, to the right to life and the right to health, of persons located outside their territories', see Marko Milanovic 'Surveillance and Cyber Operations' in Mark Gibney and others (eds), *The Routledge Handbook on Extraterritorial Human Rights Obligations* (Routledge 2021) 367.
[46] Fidler (2014) [online] ('None of these cybersecurity contexts revealed new or worsened human rights problems caused by the actual or potential use of cyberweapons by criminals, terrorists, spies, belligerents, or governments. In this light, the lack of human rights interest in cyberweapons as features of the cybersecurity crisis that has emerged since 2000 makes sense.')
[47] *Ibid.*, listing the right to property, the right to life, the right to health, the freedom of expression and the freedom of association.

Due to the lack of physical borders in cyberspace, questions of jurisdiction are undoubtedly among the most crucial issues raised by cyber operations and human rights.[48] Some have already addressed this question, offering solutions that vary in depth and detail. Explaining that cyber technology necessarily lets the traditional notion of 'effective control' within the spatial and personal model collapse, many endorse either the functional model of jurisdiction or the framework proposed by Milanovic.[49] In essence, Milanovic argues that whenever there is effective control over areas or persons, states are under the (positive) obligation to protect human rights, whereas the (negative) obligation to respect human rights applies without territorial restrictions.[50] Based on this concept, he argues that if states exercise jurisdiction through surveillance activities, they *a fortiori* do so when conducting other, more invasive cyber operations. Thus, states inevitably exercise extraterritorial jurisdiction when conducting cyber operations, be it by destroying data, disrupting critical infrastructure or by conducting misinformation campaigns.[51] Marguiles agrees with the unrestricted state obligation to respect human rights extraterritorially and, additionally, proposes the notion of 'virtual control', engaging states' obligations to protect whenever they are in a position to screen or control individual's communications, e.g. in cases of surveillance abroad.[52] Although these concepts provide desirable outcomes to avoid gaps in legal protection, they mainly focus on surveillance and are not yet accepted by courts or supported by state practice. Rather, (quasi) judicial bodies have recently shown to favor the functional model of jurisdiction when deciding borderline cases.[53] The functional model, which was primarily developed by scholars, is based on the premise that 'control' needs to be understood as states' capacity to affect individuals' enjoyment of human rights,[54] e.g. when a state could regulate extraterritorial activities of enterprises incorporated within its jurisdiction.[55] While both approaches are promising, they leave room for additional scrutiny. Since it is meanwhile accepted that the extraterritorial application of human rights treaties may pertain only to a specific right or element of the concomitant obligation,[56] the analysis of extraterritorial obligations requires an examination that goes beyond an *a fortiori* argument. Considering the myriad ways in which states may act extraterritorially through cyber operations, the concrete means of how cyber operations are effectuated and how the notions of 'jurisdiction'

[48] McDermott (2020) 199.
[49] *Ibid.,* 200ff; Delerue (2020) 263f.
[50] Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP 2011) 263; see also Elif Askin, 'Economic and Social Rights, Extraterritorial Application' *Max Planck Encyclopedia of Public International Law* (January 2019) <https://opil.ouplaw.com> accessed 19 May 2022.
[51] Milanovic (2021); Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81.
[52] Margulies (2013) 2150-2152.
[53] *The Environment and Human Rights*, Advisory Opinion OC-23/17, Inter-American Court of Human Rights Series A No 23 (15 November 2017) paras 101-102; *Yassin and Others v Canada*, Human Rights Committee (7 December 2017) UN Doc CCPR/C/120/D/2285/2013; *A.S. and Others v Malta*, Human Rights Committee (27 January 2021) UN Doc CCPR/C/128/D/3043/2017; *A.S. and Others v Italy*, Human Rights Committee (27 January 2017) UN Doc CCPR/C/130/D/3042/2017; see also Human Rights Committee, 'General Comment No 36: The Right to Life' (30 October 2018) UN Doc CCPR/C/GC/36, para 10.
[54] Philipp Janig, 'Extraterritorial Application of Human Rights', *Elgar Human Rights Encyclopedia* (2022) para 34; Milanovic (2021) 372.
[55] *Yassin and Others v Canada*, Human Rights Committee (2017) para 6.5.
[56] *Al-Skeini and Others v the United Kingdom* (GC) App no 55721/07 (ECtHR, 7 July 2011) para 137; Janig (2022) para 13.

and 'control' could be construed in accordance with the functional model of jurisdiction in cyberspace, thus, deserves further scrutiny.

Since cyber operations that result in physical harm may have far-reaching consequences, the causal link between states' actions or omissions and the human rights violations caused by cyber operations appears to be equally crucial. However, the issue of causation in international human rights law has not yet seen sufficient examination,[57] let alone in the realm of cyberspace. Also in this respect, there is room for additional research.

With regard to due diligence obligations of states in cyberspace, 'substantial approaches to concretize the cyber obligations of states are still missing'.[58] Monnheimer provides an elaborate theoretical outline, which is so far the most comprehensive analysis within the scarce literature on due diligence obligations in this context.[59]

Apart from these (partly) short outlines of potential human rights implications of cyber operations, a comprehensive analysis of state obligations in the course of such operations does not yet exist. Several issues remain unaddressed, which *inter alia* pertain to

- the scope of protection and potential interferences with specific human rights via cyber means (e.g. Could accessing individuals' mobile devices to delete malware interfere with their right to privacy? Does data destruction or encryption affect the right to property? How should police patrolling in the dark web be assessed in light of due process guarantees?),
- the link of causation between cyber operations and their potentially far-reaching effects on human rights,
- whether cyber operations may constitute a lawful limitation of human rights in light of the conditions of legality, legitimacy and proportionality[60] and
- whether this assessment differs when considering cyber activities that are conducted within a state's territory and abroad.[61]

The planned thesis attempts to fill this research gap. It aims to explore the individual's standards of protection against states' acts in cyberspace, a field whose significance will continue to grow due to relentless technological progress. Finally, it attempts to draw the attention of the academic and human rights community to cyber activities and cybersecurity, which appear to be ever more pressing human rights issues.[62]

---

[57] Vladislava Stoyanova, 'Causation between State Omission and Harm within the Framework of Positive Obligations under the European Convention on Human Rights' (2018) 18 Human Rights Law Review 309.
[58] Maria Monnheimer, 'Lessons to Be Learned from the Application of Due Diligence Obligations in Other Fields of International Law' *Due Diligence Obligations in International Human Rights Law* (CUP 2021) 188.
[59] Christian Walter, 'Obligations of States Before, During, and After a Cyber Security Incident' (2015) 58 German Yearbook of International Law 67; Antonopoulos in Tsagourias and Buchan (2021); Oliver Dörr, 'Obligations of the State of Origin of a Cyber Security Incident' (2015) 58 German Year Book of International Law 87; Karine Bannelier Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' (2014) 14 Baltic Yearbook of International Law 23; Michael Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 Yale Law Journal Forum 68.
[60] Delerue (2020) 261.
[61] Milanovic (2015) 138-139 and (2021) 374.
[62] Deborah Brown, 'It's Time to Treat Cybersecurity as a Human Rights Issue' (*Human Rights Watch*, 26 May 2020) <www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue> accessed 27 May 2022.

4. Proposed Research Questions

I. Which types of cyber operations [a.-d.] may become relevant for human rights and what is their technical functioning?

II. How may those cyber operations identified in RQ I [a.-d.] affect human rights?
   1. When do states exercise jurisdiction and thereby engage their extraterritorial human rights obligations in the course of these cyber operations?
   2. Are there legal differences regarding the human rights implications of cyber operations carried out in the context of armed conflict and in times of peace?
   3. In which way may the identified cyber operations interfere with which human rights?

III. To what extent are the cyber operations identified in RQ I [a.-d.] in conformity with human rights law?
   1. What is the scope of states' human rights obligations when conducting such cyber operations and to what extent can these constitute legitimate restrictions of human rights?
   2. What is the extent of the due diligence obligations of states targeted by cyber operations to prevent such by foreign states and non-state actors?

5. Methods for Answering the Research Questions

These research questions are both descriptive and partly normative. Since the problem of attribution of cyber operations would be beyond the scope of this thesis, attribution to a state will be presumed to exist wherever necessary.

I. Which types of cyber operations [a.-d.] may become relevant for human rights and what is their technical functioning?

The first research question aims to establish the technological basis by analyzing the technical underpinnings and functioning of cyber operations. This research question will be addressed by comparing existing legal and technical literature[63] to develop a comprehensible illustration and categorization of cyber operations that may affect human rights in the most probable scenarios. The analysis involves particularly the means of how systems are infected with malware (e.g. through phishing) and the released 'payload' (e.g. viruses, worms, etc.). The

[63] Particularly the wonderfully accessible book by Delerue, *Cyber Operations and International Law* (CUP 2020) and the ICRC and NATO Cooperative Cyber Defence Centre of Excellence sponsored 'Cyber Law Toolkit' <https://cyberlaw.ccdcoe.org/wiki/Main_Page> accessed 19 May 2022.

preliminary list of cyber operations to be analyzed includes: a. DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks; b. unauthorized access for c. malware implementation and data manipulation as well as d. law enforcement operations to counter cybercrime and cyberattacks. The scenarios in which these operations may be employed will be drawn partly from the 'Cyber Law Toolkit' database on cyber operations and international law.[64] It provides over 50 briefly described real-world examples of cyber operations, which include explanations on *inter alia* the suspected actor, target system, method of the operation, its results and consequences. Moreover, it provides 25 scenarios of cyber operations and incidents, which are analyzed (and peer-reviewed) in light of public international law.[65] Based on these materials and scenarios (such as cyber operations against medical facilities, vaccine research, power grids, as well as ransomware attacks and the consequences of misattribution) this section will develop an identification of determinants, such as the effect on legally protected interests, which will be used for answering the second research question.

II. How may those cyber operations identified in RQ I [a.-d.] affect human rights?
   1. When do states exercise jurisdiction and thereby engage their extraterritorial human rights obligations in the course of these cyber operations?
   2. Are there legal differences regarding the human rights implications of cyber operations carried out in the context of armed conflict and in times of peace?
   3. In which way may the identified cyber operations interfere with which human rights?

The second research question puts cyber operations into the context of human rights standards enshrined in international and regional human rights conventions and customary international law. Since no analysis on how cyber operations affect human rights exists, this is probably the most comprehensive research question. It involves the doctrinal analysis of human rights standards enshrined in treaties, respective case law, general comments of human rights treaty bodies and literature. Answering it requires addressing two preliminary questions, which both concern the scope of application of human rights law in situations of cyber operations.

First, since cyber operations increasingly occur in hybrid conflicts, it requires analysis of which norms of international humanitarian law derogate as *lex specialis* human rights norms or whether these are applicable in parallel.[66] Second, the virtual nature of cyber operations and

[64] International Cyber Law: Interactive Toolkit Contributors, 'Cyber Law Toolkit' (*Cyber Law Toolkit*) <https://cyberlaw.ccdcoe.org/wiki/Main_Page > accessed 3 June 2022.
[65] Cyber Law Toolkit, 'List of Real World Examples' <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Real-world_examples> accessed 19 May 2022.
[66] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 25; *Legal Consequences of the Construction of a Wall in the Occupied Territory* (Advisory Opinion) [2004] ICJ Rep 136, para 106; *Armed Activities on the Territory of the Congo (DRC v Uganda)* [2005] ICJ Rep 116, para 216; René Provost, *International Human Rights and Humanitarian Law* (CUP 2002); Andrew Clapham, 'The Complex Relationship Between the Geneva Conventions and International Human Rights Law' in Andrew Clapham, Paola

their (partly) extraterritorial dimension require the analysis of the notion 'jurisdiction' and how it can be understood in cyberspace. Since no human rights body has yet ruled on this particular subject, it will be necessary to review the jurisdictional clauses of human rights treaties, respective state practice and case law of international[67] and regional[68] (quasi) judicial human rights bodies, general comments[69] as well as literature[70] on extraterritoriality to conceptualize the notion 'authority and control' in cyberspace. In this regard, the analysis will rely both on the concept developed particularly by Milanovic[71] and the functional model to examine where these approaches intersect and to refine the extraterritorial scope of application of human rights in the context of cyber operations. Thus, this research question inevitably entails a normative approach – how jurisdiction should be framed when it comes to cyber operations.

The third sub-question puts the preceding analysis into the context of cyber operations and examines how these may interfere with certain human rights. Due to the (perhaps unavoidable) lack of a conclusive list of human rights that may be violated by cyber operations, this section will rely on the categorization and scenarios established under the first research question, taking into account how the respective human rights violation was caused and whether the requirement of a causal link is fulfilled. The rights thus identified will be compared with those human rights that were deemed to be the most susceptible to interference by cyber operations as argued in literature[72] and state practice.[73] The latter can be found especially in the documents

---

Gaeta and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015); Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar 2019).

[67] *Inter alia A.S. and Others v Malta*, Human Rights Committee (27 January 2021) UN Doc CCPR/C/128/D/3043/2017; *A.S. and Others v Italy,* Human Rights Committee (27 January 2017) UN Doc CCPR/C/130/D/3042/2017; *Yassin and Others v Canada*, Human Rights Committee (7 December 2017) UN Doc CCPR/C/120/D/2285/2013.

[68] *Inter alia Al-Skeini and Others v the United Kingdom* (GC) App no 55721/07 (ECtHR, 7 July 2011); *Banković and Others v Belgium and Others* (GC) App no 52207/99 (ECtHR, 12 December 2001); *M.N. and Others v Belgium* (GC) App no 3599/18 (ECtHR, 5 March 2020); *The Environment and Human Rights*, Advisory Opinion OC-23/17, Inter-American Court of Human Rights Series A No 23 (15 November 2017); *Association pour la sauvegarde de la paix au Burundi v Kenya, Uganda, Rwanda, Tanzania, Zaire (DRC), Zambia* Communication no 157/96 (ACHPR, 15-29 May 2003); *Georgia v Russia (II)* (GC) App no 38263/08 (ECtHR, 21 January 2021); *Al-Skeini and Others v the United Kingdom* (GC) App no 55721/07 (ECtHR, 7 July 2011); *Banković and Others v Belgium and Others* (GC) App no 52207/99 (ECtHR, 12 December 2001); *M.N. and Others v Belgium* (GC) App no 3599/18 (ECtHR, 5 March 2020).

[69] Human Rights Committee, 'General Comment No 36: The Right to Life' (3 September 2019) UN Doc CCPR/C/GC/36; CESCR 'General Comment No 24: State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities' (10 August 2017) UN Doc E/C.12/GC/24 para 27; CESCR 'General Comment No 8: The Relationship between Economic Sanctions and Respect for Economic, Social and Cultural Rights' (12 December 1997) UN Doc E/C.12/1997/8 paras 3-16; CESCR 'General Comment No 12: The Right to Adequate Food' (12 May 1999) UN Doc E/C.12/1999/5 para 36; CESCR 'General Comment No 15: The Right to Water' (20 January 2003) UN Doc E/C.12/2002/11 para 29; CESCR 'General Comment No 18: The Right to Work' (6 February 2006) UN Doc E/C.12/GC/18 para 29; CESCR 'General Comment No 19: The Right to Social Security' (4 February 2008) UN Doc E/C.12/GC/19 para 54.

[70] ETO Consortium, 'Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights' (ETO 2013); Milanovic (2011); Mark Gibney and others (eds), *The Routledge Handbook on Extraterritorial Human Rights Obligations* (Routledge 2021); Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2013) 82 Fordham Law Review 2137, 2150-2152.

[71] Milanovic (2015) 81; Milanovic (2021).

[72] *Cf.* Fidler (2014); Schmitt (2017); Milanovic (2021).

[73] Cyber Law Toolkit, 'International Human Rights Law' (*Cyber Law Toolkit*) <https://cyberlaw.ccdcoe.org/wiki/International_human_rights_law> accessed 3 June 2022.

originating from the current negotiations of the 'Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' under the auspices of the UNODC.[74] The rights to be analyzed are:

- the right to life,
- the right to privacy,
- the right to security of the person,
- the freedom of expression,
- the freedom of opinion,
- the freedom of peaceful assembly,
- the right to property,
- the right to take part in public affairs,
- the right to social security,
- the right to an adequate standard of living, including adequate food,
- the right to the enjoyment of the highest attainable standard of physical and mental health,
- the right to work,
- the right to education,
- the right to take part in cultural life,
- the right to due process and the presumption of innocence
- the right to self-determination.

In this regard, this doctrinal analysis focusses on their scope of protection, which involves examining and comparing human rights standards in treaties,[75] case law and general comments

[74] UNODC, 'First Session of the Ad Hoc Committee: Submissions from Member States Related to the First Session of the Ad Hoc Committee' (*UNODC*) <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html> accessed 18 May 2022.

[75] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR); International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR); African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) (Banjul Charter); American Convention on Human Rights "Pact of San José, Costa Rica" (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 (ACHR); Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS No. 005 (ECHR); Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 20 March 1952, entered into force 18 May 1954) ETS No 009.

of treaty bodies,[76] literature on international[77] and regional human rights treaties[78] as well as other literature that deals with the requirement of causation.[79]

III. To what extent are the cyber operations identified in RQ I [a.-d.] in conformity with human rights law?
   1. What is the scope of states' human rights obligations when conducting such cyber operations and to what extent can these constitute legitimate restrictions of human rights?
   2. What is the extent of the due diligence obligations of states targeted by cyber operations to prevent such by foreign states and non-state actors?

The third research question examines whether and how cyber operations can be in conformity with the identified human rights by drawing from similar sources as the second research question.[80] This entails two descriptive doctrinal sub-questions. The first regards the obligations of the state conducting a cyber-operation and whether such an operation can fulfil the conditions of legality, legitimacy and proportionality. Answering this sub-question requires the doctrinal analysis of the system of restriction of those human rights that were found to be affected by cyber operations under the preceding research question. Moreover, it entails a descriptive doctrinal and normative analysis on whether this assessment differs – or should differ – when states conduct cyber operations within their own territory and such that are effectuated abroad, taking into account the different means states have at their disposal to achieve their goals. The second

[76] On the scope of protection, e.g. Human Rights Committee 'General Comment No 31: The Nature of General Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add13; 'General Comment No 33: The Obligations of States Parties under the Optional Protocol to the International Covenant on Civil and Political Rights' (25 June 2009) UN Doc CCPR/C/GC/33; 'General Comment No 34: Freedom of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34; 'General Comment No 35: Liberty and Security of Person' (16 December 2014) UN Doc CCPR/C/GC/35; 'General Comment No 36: The Right to Life' (3 September 2019) UN Doc CCPR/C/GC/36; General Comment No 37: The Right to Peaceful Assembly' (17 September 2020) UN Doc CCPR/C/GC/37; 'General Comment No 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service' (27 August 1996) UN Doc CCPR/C/21/Rev.1/Add.7; 'General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev.1 at 21.

[77] Eg. Wiliam A Schabas, *Nowak's CCPR Commentary* (3rd rev edn, N.P. Engel 2019); Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2nd edn, N.P. Engel 2005); Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (3rd edn, OUP 2013); Paul M Taylor, *A Commentary on the International Covenant on Civil and Political Rights* (CUP 2020); Olivier de Schutter, *International Human Rights Law: Cases, Materials, Commentary* (3rd edn, CUP 2019); Ilias Bantekas and Lutz Oette, *International Human Rights Law and Practice* (3rd edn, CUP 2020); Dinah Shelton, *The Oxford Handbook of International Human Rights Law* (OUP 2015); Rhona KM Smith, *Texts and Materials on International Human Rights* (3rd edn, Taylor & Francis Ltd 2013); Rhona KM Smith, *International Human Rights Law* (9th edn, OUP 2020); Henry J Steiner, Philip Alston and Ryan Goodman, *International Human Rights in Context: Law, Politics, Morals* (3rd edn, OUP 2008).

[78] William A Schabas, *The European Convention on Human Rights: A Commentary* (OUP 2015); Rachel Murray, *The African Charter on Human and Peoples' Rights* (OUP 2019); Thomas M Antkowiak and Alejandra Gonza, *The American Convention on Human Rights: Essential Rights* (OUP 2017).

[79] Alexdander Orakhelashvili, *Causation in International Law* (Edward Elgar 2022); Vladislava Stoyanova, 'Causation between State Omission and Harm within the Framework of Positive Obligations under the European Convention on Human Rights' (2018) 18 Human Rights Law Review 309; Ilias Plakokefalos, 'Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity' (2015) 26 EJIL 471.

[80] See fn 76-79.

sub-question focusses on the human rights obligations of states that (or whose residents) have fallen victim to cyber operations launched by non-state actors or by another state. The doctrinal analysis will elucidate the due diligence obligations of states to prevent harm caused through cyber operations, drawing from existing literature on due diligence obligations in human rights law and cyber incidents, and refined with regard to the scenarios established in the first research question.

6. Sources

Primary sources are on the international level the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights; on the regional level, the African Convention on Human and Peoples' Rights, the American Convention on Human Rights and the European Convention on Human Rights.

Regarding secondary sources, this work will rely on international and regional case law of (quasi) judicial human rights bodies, general comments of the Human Rights Committee and the Committee on Economic, Social and Cultural Rights, as well as their views on individual communications. In terms of literature, it will rely on commentaries on international and regional human rights treaties, technical guides and other literature.

7. Proposed Outline

Part I. The Technological and Human Rights Aspects of Cyber Operations

This first part introduces the terminology used in the study and explains the technological aspects of the most prevalent cyber operations that may affect human rights. Moreover, it categorizes the different kinds of cyber operations in light of their effect on the enjoyment of rights.

Chapter 1. Methods of Cyber Operations

This chapter identifies and analyses cyber operations from a technical and legal perspective, focusing on law enforcement operations by police units to counter cybercrime as well as disruptive cyber activities to restrict online content, manipulate control systems of a variety of institutions to cause harm, steal and release confidential data as well as ransomware and wiper malware attacks.

Chapter 2. Categorizing Cyber Operations in the Context of Human Rights Law

This chapter elaborates determinants that help assessing how cyber operations may constitute an interference with human rights, focusing on their varying effects on individuals' rights and freedoms.

Part II. Cyber Operations' Interference with Human Rights

The second part connects the technological aspects of cyber operations with the applicability of human rights law to cyber activities.

Chapter 2. Human Rights and Cyber Operations in Times of Peace and War

This chapter analyses the situations in which cyber operations occur as well as the interplay between human rights obligations and international humanitarian law.

Chapter 3. The Notion 'Jurisdiction' and Cyber Operations

This chapter looks at the jurisdictional clauses of international and regional human rights instruments and assesses under which conditions they may apply to cyber operations.

Chapter 4. Affected Human Rights

This chapter maps those human rights that may be affected by cyber operations in analyzing their scope of protection and how cyber operations interfere with these rights.

Part III. Cyber Operations and their Conformity with Human Rights

The third part assesses the legality of cyber operations that cause an interference with the previously determined rights.

Chapter 5. Obligations of States in Conducting Cyber Operations

This chapter looks at the limitation clauses of relevant human rights and whether and to what extent cyber operations may constitute a lawful restriction.

Chapter 6. Obligations of States in Preventing Cyber Operations

This chapter analyses the human rights due diligence obligations of states to prevent cyber operations conducted by state and non-state actors from occurring.

Part IV. Conclusion

Preliminary Bibliography

Treaties

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR)

African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) (Banjul Charter)

American Convention on Human Rights "Pact of San José, Costa Rica" (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 (ACHR)

Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS No. 005 (ECHR)

Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 20 March 1952, entered into force 18 May 1954) ETS No 009

Literature

Antkowiak TM and Gonza A, *The American Convention on Human Rights: Essential Rights* (OUP 2017)

Antonopoulos C, 'State Responsibility in Cyberspace' in Tsagourias N and Buchan R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

Bannelier Christakis K, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' (2014) 14 Baltic Yearbook of International Law 23

Bantekas I and Oette L, *International Human Rights Law and Practice* (3rd edn, CUP 2020)

Boutin B, 'Shared Responsibility for Cyber Operations' (2019) 113 AJIL Unbound 197

Clapham A, 'The Complex Relationship Between the Geneva Conventions and International Human Rights Law' in Clapham A, Gaeta P and Sassòli M (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015)

Coomans F and Kamminga MT (eds), *Extraterritorial Application of Human Rights Treaties* (Intersentia 2004)

Davies G, 'Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers' (2020) 84 Journal of Criminal Law 407

de Schutter O, *International Human Rights Law: Cases, Materials, Commentary* (3rd edn, CUP 2019)

Delerue F, *Cyber Operations and International Law* (CUP 2020)

Demaria T, *Le lien de causalité et la réparation des dommages en droit international public* (Pedone 2021)

Dinniss HH, *Cyber Warfare and the Laws of War* (CUP 2012)

Dinstein Y, and Dahl AW, *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary* (Springer 2020)

id., 'Computer Network Attacks and Self-Defence' in Schmitt M and others (eds), *Computer Network Attack and International Law* (Naval War College 1999)

Dörr O, 'Obligations of the State of Origin of a Cyber Security Incident' (2015) 58 German Yearbook of International Law 87

ETO Consortium, 'Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights' (ETO 2013)

Fidler DP, 'Cyberspace and Human Rights' in Tsagourias N and Buchan R (eds), *Elgar Research Handbook on International Law and Cyberspace* (Edward Elgar 2021)

id., 'Cyberattacks and International Human Rights Law' in Stuart Casey-Maslen (ed), *Weapons under International Human Rights Law* (CUP 2014) [online]

Hathaway OA and others, 'The Law of Cyber Attack' (2012) 200 California Law Review 817

International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019' (2020) 102 International Review of the Red Cross 481

Joseph S and Castan M, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (3rd edn, OUP 2013)

Kilovaty I, 'Cybersecurity abroad, Election Interference and the Extraterritoriality of Human Rights Treaty Obligations' in Hollis DB and Ohlin JD (eds), *Defending Democracies, Combatting Foreign Election Interference in the Digital Age* (OUP 2021)

id., 'An Extraterritorial Human Right to Cybersecurity' (2020) 10 Notre Dame Journal of International and Comparative Law 35

Margulies P, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2013) 82 Fordham Law Review 2137

McDermott H, 'Application of the International Human Rights Law Framework in Cyber Space' in Akande D and others (eds), *Human Rights and 21st Century Challenges* (OUP 2020)

Milanovic M, 'Surveillance and Cyber Operations' in Gibney and others (eds), *The Routledge Handbook on Extraterritorial Human Rights Obligations* (Routledge 2021)

id., 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81

id., *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP 2011)

Monnheimer M, ‘Lessons to Be Learned from the Application of Due Diligence Obligations in Other Fields of International Law’ *Due Diligence Obligations in International Human Rights Law* (CUP 2021)

Murray R, *The African Charter on Human and Peoples’ Rights* (OUP 2019)

Nowak M, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2nd edn, N.P. Engel 2005)

Ohlin JD, *Election Interference: International Law and the Future of Democracy* (CUP 2020)

Orakhelashvili A, *Causation in International Law* (Edward Elgar 2022)

Plakokefalos I, ‘Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity’ (2015) 26 EJIL 471

Provost R, *International Human Rights and Humanitarian Law* (CUP 2002)

Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP 2014)

Sassòli M, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar 2019)

Schabas WA, *Nowak's CCPR Commentary* (3rd rev edn, N.P. Engel 2019)

id., *The European Convention on Human Rights: A Commentary* (OUP 2015)

Schmitt M, ‘Foreign Cyber Interference in Elections’ (2021) 97 United States Naval War College International Law Studies 739

id., ‘“Virtual” Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law’ (2018) 19 Chicago Journal of International Law 30

id. (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)

id., ‘In Defense of Due Diligence in Cyberspace’ (2015) 125 Yale Law Journal Forum 68

Shany Y, ‘Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law’ (2013) 7 The Law and Ethics of Human Rights 47

Shelton D, *The Oxford Handbook of International Human Rights Law* (OUP 2015)

Smith RKM, *International Human Rights Law* (9th edn, OUP 2020)

id., *Texts and Materials on International Human Rights* (3rd edn, Taylor & Francis 2013)

Steiner HJ, Alston P and Goodman R, *International Human Rights in Context: Law, Politics, Morals* (3rd edn, OUP 2008)

Stoyanova V, ‘Causation between State Omission and Harm within the Framework of Positive Obligations under the European Convention on Human Rights’ (2018) 18 Human Rights Law Review 309

Taylor PM, *A Commentary on the International Covenant on Civil and Political Rights* (CUP 2020)

Tsagourias N, ‘Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace’ in Broeders D and van den Berg B (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Rowman & Littlefield 2019)

id. and Buchan R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

id. and Buchan R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021)

van der Sloot B, ‘The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases’ 11 (2020) JIPITEC 160

Walter C, ‘Obligations of States Before, During, and After a Cyber Security Incident’ (2015) 58 German Yearbook of International Law 67

Whyte C and Mazanec B, *Understanding Cyber Warfare: Politics, Policy and Strategy* (Routledge 2018)

Case law

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226

Legal Consequences of the Construction of a Wall in the Occupied Territory (Advisory Opinion) [2004] ICJ Rep 136

Armed Activities on the Territory of the Congo (DRC v Uganda) [2005] ICJ Rep 116, para 216

A.S. and Others v Malta, Human Rights Committee (27 January 2021) UN Doc CCPR/C/128/D/3043/2017

A.S. and Others v Italy, Human Rights Committee (27 January 2017) UN Doc CCPR/C/130/D/3042/2017

Yassin and Others v Canada, Human Rights Committee (7 December 2017) UN Doc CCPR/C/120/D/2285/2013

Al-Skeini and Others v the United Kingdom (GC) App no 55721/07 (ECtHR, 7 July 2011)

Banković and Others v Belgium and Others (GC) App no 52207/99 (ECtHR, 12 December 2001)

Georgia v Russia (II) (GC) App no 38263/08 (ECtHR, 21 January 2021)

M.N. and Others v Belgium (GC) App no 3599/18 (ECtHR, 5 March 2020)

The Environment and Human Rights, Advisory Opinion OC-23/17, Inter-American Court of Human Rights Series A No 23 (15 November 2017)

Association pour la sauvegarde de la paix au Burundi v Kenya, Uganda, Rwanda, Tanzania, Zaire (DRC), Zambia Communication no 157/96 (ACHPR, 15-29 May 2003)

UN Documents

CESCR 'General Comment No 8: The Relationship between Economic Sanctions and Respect for Economic, Social and Cultural Rights' (12 December 1997) UN Doc E/C.12/1997/8

id., 'General Comment No 12: The Right to Adequate Food' (12 May 1999) UN Doc E/C.12/1999/5

id., 'General Comment No 15: The Right to Water' (20 January 2003) UN Doc E/C.12/2002/11

id., 'General Comment No 18: The Right to Work' (6 February 2006) UN Doc E/C.12/GC/18

id., 'General Comment No 19: The Right to Social Security' (4 February 2008) UN Doc E/C.12/GC/19

id., 'General Comment No 24: State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities' (10 August 2017) UN Doc E/C.12/GC/24

Human Rights Committee 'General Comment No 31: The Nature of General Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add13

id., 'General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev.1 at 21.

id., 'General Comment No 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service' (27 August 1996) UN Doc CCPR/C/21/Rev.1/Add.7

id., 'General Comment No 33: The Obligations of States Parties under the Optional Protocol to the International Covenant on Civil and Political Rights' (25 June 2009) UN Doc CCPR/C/GC/33

id., 'General Comment No 34: Freedom of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34

id., 'General Comment No 35: Liberty and Security of Person' (16 December 2014) UN Doc CCPR/C/GC/35

id., 'General Comment No 36: The Right to Life' (3 September 2019) UN Doc CCPR/C/GC/36

id., General Comment No 37: The Right to Peaceful Assembly' (17 September 2020) UN Doc CCPR/C/GC/37

Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) UN Doc A/HRC/17/27

Websites and Online Sources

Access Now, 'Updates: Digital Rights in the Russia-Ukraine Conflict' (1 June 2022) <www.accessnow.org/digital-rights-ukraine-russia-conflict/> accessed 2 June 2022.

Bitdefender, 'Mid-Year Threat Landscape Report 2020' [online] <www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf> accessed 25 May 2022

ECtHR (Research Division), 'Internet: case-law of the European Court of Human Rights' (June 2015) <www.echr.coe.int/documents/research_report_internet_eng.pdf> accessed 23 May 2022

Fendorf K and Miller J, 'Tracking Cyber Operations and Actors in the Russia-Ukraine War' (*Council on Foreign Relations*, 24 March 2022) <www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war> accessed 18 May 2021

Horowitz J, 'Cyber Operations under International Humanitarian Law: Perspectives from the ICRC' (2020) 24(11) ASIL insights <www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc> accessed 15 Mai 2021

International Cyber Law: Interactive Toolkit Contributors, 'Cyber Law Toolkit' <https://cyberlaw.ccdcoe.org/wiki/Main_Page> accessed 19 May 2022

Moynihan H, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (2019) Chatham House Research Paper 18 <www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf> accessed 15 May 2022

NATO, 'NATO Term: The Official NATO Terminology Database' *(NATO)* <https://nso.nato.int/natoterm/Web.mvc> accessed 15 May 2022

UNODC, 'Database of Legislation' (*Sherloc*) <https://sherloc.unodc.org/cld/v3/sherloc/legdb/> accessed 17 May 2022

UNODC, 'First Session of the Ad Hoc Committee: Submissions from Member States Related to the First Session of the Ad Hoc Committee' (*UNODC*) <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html> accessed 18 May 2022