CYBERTERRORISM WITHIN THE BROADER INTERNATIONAL COUNTER-TERRORISM FRAMEWORK

Kalle Tuominen

Master's thesis

Advanced International Law and Technology

University of Turku

Faculty of Law

April 2021

UNIVERSITY OF TURKU
Faculty of Law

TUOMINEN, KALLE: Cyberterrorism within the Broader International Counter-Terrorism Framework
Master's thesis, XIII + 58 pp.
International law
April 2021
The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

Terrorism has caused a tremendous amount of direct and indirect human suffering on a global scale in the 20th and 21st centuries. As a response, a vast collection of international and domestic regulation to combat this fundamental threat has emerged during the last few decades. However, the advent of the internet and the rapid wave of technological advancement that has resulted from it have created a new type of terrorist threat, that of cyberterrorism.

The central aim of this thesis is to compare the global counter-terrorism framework applicable to conventional terrorism with that applied specifically to cyberterrorism and to analyze their potential similarities and discrepancies in a larger context. This comparison is performed through an analysis of the central sources of international counter-terrorism regulation such as the U.N. "sectoral treaties" on terrorism, the (negotiated) U.N. Draft Comprehensive Convention on Terrorism and customary international law. This thesis seeks to also highlight some of the inherent biases of international law and how they are reflected in the global counter-terrorism framework.

This thesis presents a generally critical view of the prevailing counter-terrorism framework based on a combination of constructivist and hermeneutic ideas, including deconstruction, post-structuralism and social constructionism. In addition to legal dogmatism, the methods of phenomenography and phenomenology are also used in the thesis' analysis of the subjects, norms and legislative theories of counter-terrorism and cyberterrorism regulation.

Based on the analysis of this thesis, the main weaknesses of the current international framework are the lack of a general definition of terrorism in both treaty and customary law and the politically sensitive issue of whether to include in the normative instruments the exceptions for state terrorism and for the right of freedom movements to resist foreign occupation under their right of self-determination. These issues, in addition to the specific problem regarding attribution in cyberspace, are also the central weak points of cyberterrorism regulation. Several elements of the current response to terrorism are also guided by domestic and global politics, islamophobia and neo-colonialism.

This thesis concludes that, despite its flaws, the most effective and justified solution to the aforementioned issues would be to either finally conclude the U.N. Draft Comprehensive Convention on Terrorism or to draft new "sectoral" international treaties that are specifically targeted at cyberterrorist threats.

Keywords: international law, terrorism, Cybersecurity

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

TUOMINEN, KALLE: Cyberterrorism within the Broader International Counter-Terrorism Framework
OTM-tutkielma, XIII + 58 s.
Kansainvälinen oikeus
Huhtikuu 2021
Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -järjestelmällä.

Terrorismi on aiheuttanut suunnattoman määrän suoraa ja epäsuoraa kärsimystä maailmanlaajuisesti 1900- ja 2000-luvuilla. Tämän seurauksena viime vuosikymmeninä on säädetty laaja kokoelma kansallisia ja kansainvälisiä säädöksiä terrorismin uhan torjumiseksi. Internetin yleistyminen ja sitä seurannut räjähdysmäinen teknologinen kehitys on kuitenkin luonut uudentyyppisen terrorismiuhan, kyberterrorismin.

Tämän tutkielman tavoitteena on verrata tavanomaiseen terrorismiin ja kyberterrorismiin sovellettavia kansainvälisiä säädöskehikkoja keskenään ja analysoida niiden potentiaalisia yhtäläisyyksiä ja eroja laajemmassa kontekstissa. Tämä vertailu toteutetaan analysoimalla keskeistä kansainvälistä terrorismilainsäädäntöä kuten Y.K.:n ”sektoraalisia” terrorismisopimuksia, luonnosta Y.K.:n kokonaisvaltaiseksi terrorismisopimukseksi sekä kansainvälistä tapaoikeutta. Tutkielma pyrkii myös korostamaan eräitä kansainvälisen oikeuden rakenteellisia, haitallisia ennakkoasenteita ja sitä miten ne heijastuvat kansainväliseen terrorisminvastaiseen sääntelyyn.

Tutkielma esittää yleisesti kriittisen näkemyksen voimassaolevasta kansainvälisestä terrorismisääntelykehikosta pohjautuen konstruktivistisiin ja hermeneuttisiin ideoihin kuten dekonstruktioon, post-strukturalismiin ja sosiaalisen konstruktionismiin. Lainopin lisäksi tutkielmassa hyödynnetään fenomenografiaa ja fenomenologiaa analysoitaessa terrorismin- ja kyberterrorisminvastaisen sääntelyn subjekteja, säännöksiä ja oikeudellisia teorioita.

Tutkielman analyysiin perustuen, nykyisen kansainvälisen sääntelykehikon keskeisimmät heikkoudet ovat terrorismin yleisen määritelmän puuttuminen sekä kansainvälisissä sopimuksissa että tapaoikeudessa ja poliittinen ongelma siitä, pitäisikö oikeudellisiin instrumentteihin sisällyttää poikkeukset valtionterrorismille sekä vapautusliikkeiden oikeudelle vastustaa vieraan vallan miehitystä itsemääräämisoikeutensa perusteella. Nämä ongelmat, yhdessä kyberavaruuden aiheuttaman erillisen syyksilukemisen problematiikan, kanssa ovat myös kyberterrorismisääntelyn heikoimmat kohdat. Useat elementit nykyisestä terrorisminvastaisesta sääntelystä ovat myös kansallisen ja kansainvälisen politiikan, islamofobian sekä uuskolonialismin ohjaamia.

Tämä tutkielma päätyy siihen johtopäätökseen, että, siihen liittyvistä puutteista huolimatta, tehokkain ja oikeudenmukaisin keino edellä kuvattujen ongelmien ratkaisemiseen olisi joko lopulta hyväksyä Y.K.:n kansainvälinen kokonaisvaltainen terrorismisopimus tai säätää uusia, erityisesti kyberterrorismiuhkien torjuntaan kohdistettavia ”sektoraalisia” sopimuksia.

Avainsanat: kansainvälinen oikeus, terrorismi, kyberturvallisuus

CONTENTS

SOURCES

Bibliography

Ambos, K, “Judicial creativity at the Special Tribunal for Lebanon: Is there a crime of terrorism under international law” (2015) 24(3) Leiden Journal of International Law 655

Arquilla, J and Ronfeldt, D (eds), *Networks and Netwars: The Future of Terror, Crime and Militancy* (RAND 2001)

Awan, I, “Cyber-Extremism: Isis and the Power of Social Media” (2017) 54 Society 138

Bassiouni, C, "A Functional Approach to 'General Principles of International Law'" (1990) 11(3) Michigan Journal of International Law 768

Bassiouni, C, *International Terrorism: Multilateral Convention* (Transnational Publishers 2001)

Bassiouni, C, *Introduction to International Criminal Law* (2nd edn, Martinus Nijhoff Publishers 2013)

Bianchi, A (ed), *Enforcing International Law Norms Against Terrorism* (Hart Publishing 2004)

Cassese, A (ed), *The Oxford Companion to International Criminal Justice* (OUP 2009)

Chomsky, N, *Culture of Terrorism* (2nd edn, Pluto Press 2015)

Clapham, A and Gaeta, P (eds), *The Oxford Handbook of International Law in Armed Conflict* (2014 OUP)

Crawford, J, *Brownlie’s Principles of Public International Law* (9th edn, OUP 2019)

Cryer, R et al. (eds), *An Introduction to International Criminal Law and Procedure* (2nd edn, CUP, 2010)

Cryer, R et al. (eds), *An Introduction to International Criminal Law and Procedure* (4th edn, CUP 2019)

Derrida, J, *Deconstruction in a Nutshell: A Conversation with Jacques Derrida, With a New Introduction*, (John D. Caputo ed, Fordham University Press 2021)

Dinstein, Y, “Terrorism as an international crime” (1989) 19 Israel Yearbook on Human Rights 55

Duvic-Paoli, L, *The Prevention Principle in International Environmental Law* (CUP 2018)

Fidler, D P, “Cyberspace, Terrorism and International Law” (2016) 21(3) Journal of Conflict and Security Law 475

Fletcher, G, “Responding to terrorism: The quest for a legal definition. The indefinable concept of terrorism’ (2006) 4 Journal of International Criminal Law 894

Friedmann, W, *The Changing Structure of International Law* (Stevens & Sons 1964)

Gaeta, P (ed), *The UN Genocide Convention: A Commentary* (OUP 2009)

Gillett, M and Schuster, M, “Fast-track justice: The Special Tribunal for Lebanon Defines Terrorism” (2011) 9(5) Journal of International Criminal Justice 989

Gray, C, *International Law and the Use of Force* (OUP 2000)

Halpin, E et al. (eds), *Cyberwar, Netwar and the Revolution in Military Affairs* (Palgrave Macmillan UK 2016)

Hmoud, M, "Negotiating the Draft Comprehensive Convention on International Terrorism" (2006) 4 Journal of International Criminal Justice 1031

Jacobson, M, "Terrorist Financing and the Internet" (2010) 33(4) Studies in Conflict and Terrorism 353

Jarvis, L, Macdonald, S and Nouri, L, "The Cyberterrorism Threat: Findings from a Survey of Researchers" (2014) 37(1) Studies in Conflict & Terrorism 68

Jessup, P, *A Modern Law of Nations* (The Macmillan Company 1948)

Kearns, E, Betus, A and Lemieux, A, "Why Do Some Terrorist Attacks Receive More Media Attention Than Others?" (2019) 36(6) Justice Quarterly 985

Khawaja, A S and Khan, A H, "Media Strategy of ISIS: An Analysis" (2016) 36(2) Strategic Studies 104, available at <www.jstor.org/stable/48535950> accessed 10 December 2020

King, G, Schneer, B and White, A, "How the news media activate public expression and influence national agendas" (2017) 358 Science 776

Kwarteng, A H and Botchway, T P, "The North and South Divide in the Practice and Application of International Law: A Humanitarian and Human Right Law Perspective" (2018) 11(1) Journal of Politics and Law 79

Lock, A and Strong, T, *Social Constructionism: Sources and Stirrings in Theory and Practice* (CUP 2010)

Milanovic, M "An odd couple – Domestic crimes and international responsibility in the Special Tribunal for Lebanon" (2007) 5 Journal of International Criminal Law 1139

Olásolo, H, "A Note on the Evolution of the Principle of Legality in International Criminal Law" (2007) 18(3–4) Criminal Law Forum 301

Sassòli, M, "Terrorism and war" (2006) 4 Journal of International Criminal Law 960

Saul, B, *Defining Terrorism in International Law* (OUP 2006)

Saul, B, "Legislating from a radical Hague: The United Nations Special Tribunal for Lebanon invents an international crime of transnational terrorism" (2015) 24(3) Leiden Journal of International Law 677

Saul, B (ed), *Research Handbook on International Law and Terrorism* (2nd edn, Edward Elgar Publishing 2020)

Schabas, W, "The Special Tribunal for Lebanon: Is a Tribunal of an international character equivalent to an international criminal court?" (2008) 21 Leiden Journal of International Law 513

Schmid, A, "Terrorism: The definitional problem" (2004) 36 Case Western Reserve Journal of International Law 375

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

Schuerch, R, *The International Criminal Court at the Mercy of Powerful States* (T.M.C. Asser Press 2017)

Shiryaev, Y, "Cyberterrorism in the Context of Contemporary International Law" (2012) 14 San Diego International Law Journal 139

Steyn, J, "Guantanamo Bay: The Legal Black Hole" (2004) 53(1) The International and Comparative Law Quarterly 1

Talihärm, A, "Cyber Terrorism; in Theory or in Practice?" (2010) 3(2) Defence Against Terrorism Review 59

Tierney, J, "Terror at Home: The American Revolution and Irregular Warfare" (1977) 12 Stanford Journal of International Studies 1

Tomuschat, C and Thouvenin, J (eds), *The Fundamental Rules of the International Legal Order: Jus Cogens and Obligations Erga Omnes* (Martinus Nijhoff Publishers 2005)

Tsagourias, N, "Cyber Attacks, Self-Defence and the Problem of Attribution" (2012) 17(2) Journal of Conflict and Security Law 229

Tsagourias, N and Buchanan, R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015)

Van den Herik, L and Schrijver, N, *Counter-Terrorism Strategies in a Fragmented International Legal Order: Meeting the Challenges* (CUP 2013)

Van Schaak, B, "Crimen sine lege: judicial law-making at the intersection of law and morals" (2008) 97 Georgetown Law Journal 119

Ventura, M, "Terrorism according to the STL's Interlocutory Decision on the applicable law: A defining moment or a moment of defining?" (2011) 9 Journal of International Criminal Justice 1021

Weigend, T, "The universal terrorist: The international community grappling with a definition" (2006) 4 Journal of International Criminal Law 912

Williams, J, *Understanding Poststructuralism* (Routledge 2015)

Internet sources

"A Decade of Deception and Defiance" (12 September 2002), White House Background Paper on Iraq <https://2001-2009.state.gov/p/nea/rls/13456.htm> accessed 11 March 2021.

Amnesty International, "Guantánamo: A Decade of Damage to Human Rights" (December 2011) https://www.amnestyusa.org/reports/guantanamo-a-decade-of-damage-to-human-rights/ accessed 26 February 2021

Beaumont, P, "Iran nuclear experts race to stop spread of Stuxnet computer worm", The Guardian (26 September 2010) <https://www.theguardian.com/world/2010/sep/26/iran-stuxnet-worm-nuclear> accessed 21 March 2021.

Bossmann, J, "Top 9 ethical issues in artificial intelligence", World Economic Forum (21 October 2016) <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/> accessed 10 December 2020

Bright, M, Vulliamy, E and Beaumont, P, "Revealed: US dirty tricks to win vote on Iraq war" The Guardian (2 March 2003) <https://www.theguardian.com/world/2003/mar/02/usa.iraq> accessed 24 March 2021

Brown, S, "MIT Sloan research about social media, misinformation, and elections", MIT Sloan School of Management (5 October 2020), <https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections> accessed 6 December 2020

"Centcom Acknowledges Social Media Sites 'Compromised'", U.S. Central Command News Release (12 January 2015) <https://www.defense.gov/Explore/News/Article/Article/603906/> accessed 29 April 2021

Cooper, H, "ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts", The New York Times (12 January 2015) <https://www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html> accessed 29 April 2021

Council of the European Union, "EU's response to the terrorist threat" (2020), <https://www.consilium.europa.eu/en/policies/fight-against-terrorism/#> accessed 4 December 2020

Crocker, A and Cohn, C, "Don't Worry, the Government Still Has Plenty of Surveillance Power If Section 215 Sunsets", Electronic Frontier Foundation (31 May 2015) https://www.eff.org/deeplinks/2015/05/dont-worry-government-still-has-plenty-surveillance-power-if-section-215-sunsets accessed 28 February 2021

European Commission, "EU Emissions Trading System (EU ETS)" <https://ec.europa.eu/clima/policies/ets_en#tab-0-0> accessed 28 April 2021

European Commission, "The Court annuls, for the third time, a Council decision freezing the funds of the People's Mojahedin Organization of Iran", press release (4 December 2008) <https://ec.europa.eu/commission/presscorner/detail/en/CJE_08_84> accessed 29 April 2021

Faiola, A and Kirchner, S, "Islam is Europe's 'new fascism', and other things European politicians say about Muslims", The Washington Post (7 June 2016), <https://www.washingtonpost.com/news/worldviews/wp/2016/06/07/ten-things-outspoken-european-politicians-are-saying-about-islam/> accessed 4 December 2020

"French police operations underway after beheading of teacher", The Associated Press (2 November 2020), <https://apnews.com/article/paris-nice-europe-france-bcba9ca5f91cb43faffe4d4d5febc2e8> accessed 4 December 2020

Gardner, F, "Will the 'War on Terror' Ever End?", BBC (24 June 2020), <https://www.bbc.com/news/world-53156096> accessed 3 December 2020

Global Policy Forum, "Comparison of the World's 25 Largest Corporations with the GDP of Selected Countries" (2010), <https://www.globalpolicy.org/images/pdfs/Comparison_of_Corporations_with_GDP_of_Countries_table.pdf> accessed 8 December 2020

Global Terrorism Database <https://www.start.umd.edu/gtd/> accessed 3 December 2020

Heller, K, "NBC: Israel and MEK Responsible for Murdering Iranian Scientists", Opinio Juris (11 February 2012) <http://opiniojuris.org/2012/02/11/nbc-israel-and-mek-responsible-for-murdering-iranian-scientists/> accessed 11 March 2021

"Information Revolution Vs. Industrial Revolution", Encyclopedia.com (2020), <https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/information-revolution-vs-industrial-revolution> accessed 6 December 2020

Jenkins, J, "Oklahoma City bombing", Encyclopædia Britannica (most recently revised 6 August 2020), <https://www.britannica.com/event/Oklahoma-City-bombing> accessed 3 December 2020

Keller, M H and Dance, G J X, "Child Abusers Run Rampant as Tech Companies Look the Other Way", The New York Times (9 November 2019), <https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html> accessed 6 December 2020

Keller, M H and Dance, G J X, "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?", The New York Times (28 September 2019),

<https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html> accessed 6 December 2020

McGreal, C, "MEK decision: multimillion-dollar campaign led to removal from terror list", The Guardian (21 September 2012) <https://www.theguardian.com/world/2012/sep/21/iran-mek-group-removed-us-terrorism-list> accessed 11 March 2021

McKinney, I, "Reform or Expire", Electronic Frontier Foundation (26 February 2020) https://www.eff.org/deeplinks/2020/02/reform-or-expire accessed 28 February 2021

Merat, A, "Terrorists, cultists – or champions of Iranian democracy? The wild story of the MEK", The Guardian (9 November 2018), <https://www.theguardian.com/news/2018/nov/09/mek-iran-revolution-regime-trump-rajavi> accessed 12 March 2021

Nakashima, E and Warrick, J, "Stuxnet was work of U.S. and Israeli experts, officials say", The Washington Post (2 June 2012) <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html> accessed 21 March 2021.

NATO, Countering Terrorism (2019), <https://www.nato.int/cps/en/natohq/topics_77646.htm> accessed 15 February 2021

Nowrasteh, A, "More Americans Die in Animal Attacks than in Terrorist Attacks" (8 March 2018) the Cato Institute <https://www.cato.org/blog/more-americans-die-animal-attacks-terrorist-attacks> accessed 28 April 2021

Parlapiano, A and Lee, J C, "The Propaganda Tools Used by Russians to Influence the 2016 Election", The New York Times (16 February 2018), <https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html> accessed 6 December 2020

Ray, M, "Paris attacks of 2015", Encyclopædia Britannica (most recently revised 6 November 2020), <https://www.britannica.com/event/Paris-attacks-of-2015> accessed 4 December 2020

Ritchie, H, Hasell, J, Appel, C and Roser, M, "Terrorism", Our World in Data (2013, last updated in 2019), <https://ourworldindata.org/terrorism#global-distribution-of-terrorism> accessed 10 December 2020

Roose, K, "What Is QAnon, the Viral Pro-Trump Conspiracy Theory" The New York Times (4 March 2021) <https://www.nytimes.com/article/what-is-qanon.html> accessed 27 April 2021

Rubin, E, "An Iranian Cult and Its American Friends, The New York Times (13 August 2011) <https://www.nytimes.com/2011/08/14/opinion/sunday/an-iranian-cult-and-its-american-friends.html?pagewanted=all> accessed 11 March 2021

Sanger, D, "Obama Order Sped Up Wave of Cyberattacks Against Iran", The New York Times (1 June 2012) <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> accessed 21 March 2021

Savage, C, "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads", The New York Times (25 February 2020) https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html accessed 28 February 2021

The Editors of Encyclopaedia Britannica, "Industrial Revolution", Encyclopædia Britannica (revised 21 February 2021), <https://www.britannica.com/event/Industrial-Revolution> accessed 6 December 2020

The Permanent Mission of Italy to the U.N., "Antonio Cassese appointed as President of Special Tribunal for Lebanon" (24 March 2009) <https://italyun.esteri.it/rappresentanza_onu/en/comunicazione/archivio-news/2009-03-24-cassese.html> accessed 28 April 2021

Townsend, M, Harris, P, Duval Smith, A, Sabbagh, D and Halliday, J, "Wikileaks backlash: The first global cyber war has begun, claim hackers", The Guardian (11 December 2010) <https://www.theguardian.com/media/2010/dec/11/wikileaks-backlash-cyber-war> accessed 23 March 2021

U.S. Department of State, "Delisting of the Mujahedin-e Khalq", press release (28 September 2012) <https://2009-2017.state.gov/r/pa/prs/ps/2012/09/198443.htm> accessed 11 March 2021

United Nations, Office of Counter-Terrorism, "International Legal Instruments", <https://www.un.org/counterterrorism/international-legal-instruments> accessed 3 December 2020

Wallenfeldt, J, "The Troubles", Encyclopædia Britannica (14 May 2019), <https://www.britannica.com/event/The-Troubles-Northern-Ireland-history> accessed 3 December 2020

Official sources

Charter of the United Nations of 26 June 1945

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 23 September 1971

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation of 10 March 1988

Convention for the Suppression of Unlawful Seizure of Aircraft of 16 December 1970

Council Decision (2009/62/EC) of 26 January 2009 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing Decision 2008/583/EC

Council Framework Decision of 13 June 2002 on combating terrorism, 2002 O.J. (L 164)

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, 2002 O.J. (L 190)

Declaration on Measures to Eliminate International Terrorism, Annex to UN General Assembly Res 49/60 (9 December 1994)

Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, Annex to UN General Assembly resolution 2625 (XXV) (24 October 1970)

Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, Annex to UN General Assembly Res 51/210 (17 December 1996)

H.R. 3162 – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

International Convention against the Taking of Hostages of 17 December 1979

International Convention for the Suppression of Acts of Nuclear Terrorism of 13 April 2005

International Convention for the Suppression of Terrorist Bombings of 15 December 1997

International Convention for the Suppression of the Financing of Terrorism of 9 December 1999

Org. of African Unity, *Algiers Plan of Action on the Prevention and Combating of Terrorism in Africa* (September 11–14, 2002)

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

Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft of 10 September 2010

Report of the Ad Hoc Committee, 6th Session (28 January–16 October, 2002) U.N. Doc A/57/37, Annex IV

Report of the Ad Hoc Committee, 14th Session (12–16 April, 2010) U.N. Doc A/65/37

Report of the Committee against Torture, U.N. Doc. A/59/44 (2004)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, E/CN.4/2006/98 (28 December 2005)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/34/61 (21 February 2017)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/37/52 (27 February 2018)

Report of the Working Group, "Measures to Eliminate International Terrorism", (3 November 2010) U.N. Doc A/C.6/65/L.10, Annex I, 16

Rome Statute of the International Criminal Court of 17 July 1998

Treaty on the European Union, O.J. (C 191, 29 July 1992)

United Nations General Assembly Res. 54/110 of 9 December 1999

UN Security Council Resolution 1757 (30 May 2007)

UN Treaty Series Vol. 1704 (China)

UN Treaty Series Vol. 1821 (India)

Vienna Convention on the Law of Treaties of 23 May 1969

Case law

Appeals Chamber of the Special Tribunal for Lebanon, *Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging*, STL-11-01/I/AC/R176bis, 16 February 2011

Defence Office's Submissions Pursuant to Rule 176 bis (B), 31 January 2011 (STL-11–01/I)

Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, STL-11-01/I/AC/R176bis, 16 February 2011

International Criminal Tribunal for the former Yugoslavia, *Prosecutor v Tadić* (*Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*), IT-94–1 (2 October 1995)

Judgment of 27 June 1986 of the International Court of Justice in the case of Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)

North Sea Continental Shelf (Federal Republic of Germany v Denmark) (Merits) [1969] ICJ Rep 3

Order on Preliminary Questions Addressed to the Judges of the Appeals Chamber Pursuant to Rule 68, Paragraph (G) of the Rules of Procedure and Evidence, 21 January 2011 (STL-11-01-/I/AC/R176bis)

Prosecutor v Stanislav Galić (Trial Judgment), International Criminal Tribunal for the Former Yugoslavia (ICTY, Case no. IT-98-29-T, 5 December 2003)

Prosecutor's Brief Filed Pursuant to the President's Order of 21 January 2011 Responding to the Questions Submitted by the Pre-Trial Judge (Rule 176 bis), 31 January 2011 (STL-11–01/I)

Rule 68(G) of the Tribunal's *Rules of Procedure and Evidence* (STL/BD/2009/01/Rev. 6)

Sabra Motion for Reconsideration of Rule 176bis Decision – 'International Terrorism', 13 June 2012 (STL-11–01/PT/AC)

Special Tribunal for Lebanon, *Ayyash et al. Case* (STL-11-01)

Trail Smelter Case (United States, Canada) (16 April 1938 and 11 March 1941) 3 U.N. Rep. International Arbitration Awards 1905

Other sources

Jahangiri, A, "Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion", Worldwide Security Conference 6: Background Materials and Selected Speakers Notes 29 (2009)

ABBREVIATIONS

EU	European Union
ICC	International Criminal Court
ICJ	International Court of Justice
OIC	Organization of Islamic Cooperation
UNGA or General Assembly	General Assembly of the United Nations
UN	United Nations

1 INTRODUCTION

1.1 BACKGROUND AND RESEARCH THEMES

It is quite rare for a single event to bring a topic into the forefront of global politics and public discussion, but that is exactly what happened as a result of the terrorist attacks on September 11th, 2001. Terrorism was by no means a new or unknown phenomenon even at the time of the 9/11 attacks – the conflict in Northern Ireland commonly known as the Troubles had led to over 3,600 deaths in the period between 1968 and 1998[1], while the Oklahoma City bombing of 1995 alone had claimed 168 lives in the United States.[2] However, the scale, organized nature and sheer shock value of the 9/11 attacks kickstarted the United States' seemingly never-ending War on Terror[3] and put pressure on the international community to build stronger international counter-terrorism regulations (namely the 2005 Convention for the Suppression of Acts of Nuclear Terrorism and the 2006 UN Global Counter-Terrorism Strategy) upon the already existing framework of UN conventions adopted by 2001.[4] As a result, various other organizations such as the European Union[5] (EU), the North Atlantic Treaty Organization[6] (NATO) and the African Union[7] (AU) strengthened their own counter-terrorism responses in the years following the attacks.

---

[1] See, e.g., Jeff Wallenfeldt, 'The Troubles', Encyclopædia Britannica (14 May 2019) <https://www.britannica.com/event/The-Troubles-Northern-Ireland-history> accessed 3 December 2020. While the acts committed during the Troubles are not universally recognized as terrorist acts, they are classified as such by one of the most comprehensive publicly available databases, the Global Terrorism Database <https://www.start.umd.edu/gtd/> accessed 3 December 2020.

[2] See, e.g., John Philip Jenkins, 'Oklahoma City bombing', Encyclopædia Britannica (most recently revised 6 August 2020), <https://www.britannica.com/event/Oklahoma-City-bombing> accessed 3 December 2020.

[3] Frank Gardner, 'Will the "War on Terror" Ever End?', BBC (24 June 2020) <https://www.bbc.com/news/world-53156096> accessed 3 December 2020. Although the Obama administration tried to change the rhetoric on the issue by officially refraining from the use of the term "War on Terror", its counter-terrorism actions were very much in line with those of the Bush administration.

[4] International Legal Instruments, United Nations, Office of Counter-Terrorism, <https://www.un.org/counterterrorism/international-legal-instruments> accessed 3 December 2020. 12 of the 19 legal instruments adopted since 1963 related to the prevention of terrorist acts were already in place at the time of the September 11 attacks.

[5] E.g., Council Framework Decision of 13 June 2002 on combating terrorism, 2002 OJ (L 164), 3–7 and Council Framework decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, 2002 OJ (L 190), 1–20.

[6] On 4 October 2001 NATO agreed on eight specific measures to support the United States terrorism, after which the organization launched its first-ever counter terrorism operations, Operation Eagle Assist and Operation Active Endeavour. For a general timeline and additional information see, e.g., NATO, Countering Terrorism (2019) <https://www.nato.int/cps/en/natohq/topics_77646.htm> accessed 15 February 2021.

[7] E.g., Organization of African Unity [OAU], 'Algiers Plan of Action on the Prevention and Combating of Terrorism in Africa' (September 11–14, 2002), <https://www.peaceau.org/uploads/au-anti-terrorism-plan-of-action.pdf> accessed 6 April 2021.

Terrorism as a broad concept has been a topic of debate on the international political arena for decades, albeit its influence on both the domestic and international politics and policies of the U.S. and of many European states reached a new level – in no small part due to the media – after the WTC attacks. This heightened role in the public consciousness was amplified further by the terrorist attacks in Paris in 2015.[8] In recent years, the conversation in Europe regarding terrorism has turned into a confusing web of competing points ranging from joint attempts to tackle the issue through domestic and EU legislation[9] to sweeping rejections and generalizations of the religion of Islam itself by several right-wing politicians.[10]

The most recent round of debate about additional measures to combat and prevent terrorism – Islamic extremism in particular – was spurred by the beheading of a teacher in France by an 18-year-old Chechen refugee after the teacher had opened a debate on free speech in his classroom by showing his students caricatures of the prophet of Islam, which were originally published by the satirical newspaper Charlie Hebdo.[11] These and multiple other highly publicized acts of terror demonstrate that the threat of terrorism and attempts to combat it have remained front and center of both politics and public debate, although it seems that the majority of the proposed responses have been driven by emotion and populism instead of proportionality and reasonableness.

When taking into account the persistence of terrorism as a nearly-constant talking point during the 21st century on both national and international avenues as well as in the news, relatively little concrete progress has been made on the international level. The problematic nature of the issue is perhaps best reflected in the over 20-year-long negotiations over a Draft Comprehensive Convention on International Terrorism. The Draft Convention, first introduced by the General Assembly of the UN in 1999[12], aimed to develop an "umbrella" or "supplementary" legal framework since it was seen that the "sectoral" instruments already adopted or in development

[8] See, for example, Michael Ray, 'Paris attacks of 2015', Encyclopædia Britannica (most recently revised 6 November 2020) <https://www.britannica.com/event/Paris-attacks-of-2015> accessed 4 December 2020.
[9] Council of the European Union, 'EU's response to the terrorist threat' (revised 18 March 2021) <https://www.consilium.europa.eu/en/policies/fight-against-terrorism/#> accessed 6 April 2021.
[10] Anthony Faiola and Stephanie Kirchner, 'Islam is Europe's "new fascism", and other things European politicians say about Muslims', The Washington Post (7 June 2016) <https://www.washingtonpost.com/news/worldviews/wp/2016/06/07/ten-things-outspoken-european-politicians-are-saying-about-islam/> accessed 4 December 2020.
[11] 'French police operations underway after beheading of teacher', The Associated Press (2 November 2020) <https://apnews.com/article/paris-nice-europe-france-bcba9ca5f91cb43faffe4d4d5febc2e8> accessed 4 December 2020. Additionally, the killing and the response to it by President Emmanuel Macron of France caused a larger debate about the possible limits of free speech and its relation to the freedom of religion.
[12] UNGA Res. 54/110 of 9 December 1999.

at the time were not sufficient in their scope and that the more general international legal framework only targeted certain methods or aspects of terrorism.[13]

Originally, the most contentious points of the Draft Convention were the exact definition of terrorism, the scope of the treaty and the relationship between the draft treaty and the sectoral treaties dealing with specific crimes of terrorism. Even though it appears that the most recent arguments put forward in the negotiations have focused mainly on the scope of the treaty and on the right to self-determination, the states' all-or-nothing approach to adopting the treaty means that even the most universally accepted definition of terrorism is still based on a gridlocked draft convention.[14] Since international cyberterrorism legislation is effectively based on or at least greatly influenced by the existing "general" terrorism regulations, the lack of an unambiguous legal definition of terrorism further complicates the already difficult task of applying the existing counter-terrorism framework to acts committed in an arena as complex as that of cyberspace.

While my thesis focuses mainly on cyberterrorism and its unique issues in the international law context, the larger debates and the international legislative framework surrounding the general crime of terrorism are crucial in understanding how, and to what degree, the current legal instruments can – or cannot – be applied to acts of terrorism in cyberspace. One of the main goals of my thesis is to compare the global counter-terrorism framework applicable to conventional terrorism with that applied specifically to cyberterrorism and to analyze their potential similarities and discrepancies in a larger context. It should be noted, however, that due to the lack of comprehensive international cyberterrorism regulation, terrorist acts in cyberspace must be primarily interpreted through the general counter-terrorism framework and only alternatively under specific cyberterrorism norms such as those defining distinct acts in cyberspace. While this does certainly reflect the broader, fundamental difficulties related to the drafting of international legislation, I believe it to also be a representation of the gradual and often ambiguous process in recent decades under which traditional terrorism has transformed into a vast net of terrorist acts that includes traditional attacks, pure cyber-based acts and various types of hybrid offences combining elements of conventional and cyber acts.[15] Through my analysis of the current framework, I aim to recognize the main strengths and weaknesses of the current approach and to suggest viable alternative solutions and/or modifications to it.

[13] Mahmoud Hmoud, 'Negotiating the Draft Comprehensive Convention on International Terrorism' (2006) 4 Journal of International Criminal Justice 1031, 1031–1032.
[14] Supra Hmoud (2006).
[15] I will elaborate on the definitional issues caused by these hybrid acts in Chapter 1.2.

1.2 RESEARCH QUESTIONS

All analysis of a legislative framework must start with identifying its most influential sources, assessing both their theoretical and practical effects on the issue and forming a picture of the current framework that includes its most central goals, influences and biases. Only after this process can one begin to understand the fundamental principles – in their broadest sense – that have led to the adoption of the current approach and, consequently, to the rejection of others. Once we have reached a deep understanding of these underlying legislative, political and sociological principles, can we start to adapt and apply them through legislative and other measures to new, emerging sectors such as that of cyberspace.

With a subject of international law as broad as terrorism, of which cyberterrorism is only a part, the task of identifying and summarizing the "larger story" of international counter-terrorism regulation and subsequently applying its most successful principles to the area of cyberspace may ultimately prove to be too great a task to accomplish in a single thesis paper. Nevertheless, my hope is that I can at least provide a starting point for this timely discussion by presenting the current international counter-terrorism framework in a broader context that recognizes both its inherent biases and flaws as well as its triumphs and by demonstrating how these solutions have – or have not been – replicated in the global response to cyberterrorism. After all, justifiable or reasonable criticism is the root of all legislative, political and societal progress at least on issues where evidence-based research can only provide inconclusive results or supplemental guidance in determining the most "just"[16] course of action. The first step in solving a problem is recognizing its existence, no matter how complex or structural it may appear.

The last few decades have brought with them an extraordinarily rapid wave of technological advancement the impact of which could even be compared to that of the First Industrial Revolution of the late 18th and early 19th centuries.[17] This development has had a significant influence on practically every aspect of modern society ranging from new telecommunications

[16] While the term "just" is highly subjective and ambiguous in itself, in this paper it refers to a general situation wherein a significant majority agrees on the "justifiableness" of the solution and in which the solution can also be directly or indirectly derived from a formerly agreed upon authority such as that of fundamental human rights (e.g. the UN Charter).

[17] 'Information Revolution Vs. Industrial Revolution', Encyclopedia.com (2020) <https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/information-revolution-vs-industrial-revolution> accessed 6 December 2020. More generally on the Industrial Revolution see, e.g., The Editors of Encyclopaedia Britannica, 'Industrial Revolution', Encyclopædia Britannica (revised 21 February 2021) <https://www.britannica.com/event/Industrial-Revolution> accessed 6 April 2021.

opportunities to its various business applications, but it has also forced us to consider our approach to cyberspace and its various and ever-evolving uses from a legislative standpoint. By no means are these legislative considerations limited to cyberterrorism or even to cybercrimes in general, one example of which is the amount of public criticism that several big technology companies such as Facebook and Twitter have found themselves under in recent years as they have been accused of, among other things, indirectly aiding the spread of misinformation[18] and of child pornography[19] on their platforms through half-measures or inaction.[20]

Since traditional terrorist acts and the methods used to commit them can vary quite significantly from those seen and used in the cyberspace, these differences must be taken into account when analyzing the current and potential responses – in a broad sense – to cyberterrorism. Classifying and characterizing modern terrorist acts is further complicated by activities that seem to fall in between the physical and cyber territories. Is detonating a small explosive in an empty server room with the specific intent of causing chaos by hampering the city's vast power network considered terrorism, cyberterrorism, cybercrime or something else entirely? Would the act's legal classification change if the explosive in the server room was detonated remotely, for example, through a smartphone application? Although the current framework might already provide an answer to the specific questions posed above, these hypotheticals act as mere examples of the types of definition-related issues that international lawyers, politicians and the international community as a whole must eventually solve whether in applying the conventional terrorism regulations to these sophisticated hybrid threats or in adopting additional legislation targeted specifically at various criminal acts in cyberspace.

Difficulties in describing these hybrid acts in normative terms are clearly integrated into the debates about the definition of cyberterrorism itself at a time when even these definitions seem

[18] Alicia Parlapiano and Jasmine C. Lee, "The Propaganda Tools Used by Russians to Influence the 2016 Election", The New York Times (16 February 2018) <https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html> accessed 6 December 2020 and Sara Brown, "MIT Sloan research about social media, misinformation, and elections", MIT Sloan School of Management (5 October 2020) <https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections> accessed 6 December 2020.

[19] Michael H. Keller and Gabriel J.X. Dance, "Child Abusers Run Rampant as Tech Companies Look the Other Way", The New York Times (9 November 2019) <https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html> accessed 6 December 2020 and Michael H. Keller and Gabriel J.X. Dance" 'The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?", The New York Times (29 September 2019), <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html> accessed 6 December 2020.

[20] *Ibid*.

to be as varied as the international lawyers advocating for them.[21] As already mentioned above, the failure of international lawyers and legislators to agree on clear and comprehensive terms for terrorist acts has created an unfortunate vacuum in international counter-terrorism legislation wherein domestic or international political agendas could potentially be utilized to label myriad types of activities as acts of terrorism. While this ongoing confusion about the definitions of both kinetic and cyber-based terrorist attacks is problematic, the states could ultimately decide to agree to apply their corresponding domestic laws' definitions and focus on solving other aspects of terrorism such as scope and jurisdiction issues on an international level through treaties or soft law instruments.

Finally, the ongoing debates about the definition of terrorism also provide a starting point for my critical analysis of the various biases of international law and politics. My thesis will take a generally critical approach to contemporary international terrorism legislation and to the influences of contemporary international law more broadly. Since whole sub-sections of international law have been created on the basis of various kinds of critical approaches to global legislation and politics, any attempt at comprehensively describing and proving these biases in a single thesis would not do justice to the complexity of neither those critiques nor of international law as an ever-evolving legislative regime.

Therefore, I aim to bring up these various biases and structural influences on issues where they seem to be guiding the conversation in one way or another in order to demonstrate the potentially harmful stereotypes and systems acting in the background of international counter-terrorism legislation. My ultimate hope is that by defining and recognizing these biases we can develop a more inclusive, more effective and truly global approach to counter-terrorism.

By building on the elements presented in this chapter, the primary research question of my thesis is "To what extent can – and should – the current international counter-terrorism framework be applied to cyberterrorism?". The secondary research question of "How are the various biases of international law reflected in the broader counter-terrorism responses and how should they be taken into account in future regulation?" will deepen my analysis of the issue by providing a more comprehensive view of the guiding principles and ultimate goals of global counter-terrorism regulation.

[21] Ali Jahangiri, "Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion" Worldwide Security Conference 6: Background Materials and Selected Speakers Notes 29 (2009) as cited in Yaroslav Shiryaev, "Cyberterrorism in the Context of Contemporary International Law" (2012) 14 San Diego International Law Journal 139, 147.

1.3 METHODOLOGY

Legal scholars are often quite reluctant to explore the various complex traditions of scientific thought (i.e. the philosophy of science) in their research in favor of the seemingly unproblematic traditions of scientific realism connected with an unnuanced view of empiricism. Although this general rejection of the philosophy of science seems to be an especially broad among the mainly domestic legal experts, I believe that it has also contributed at least partly to the rigid and often homogenous structures and ideas of international law and global politics.

The aforementioned phenomenon could be explained in large part by the very nature of legal studies, at least on the Bachelor's and Master's degree levels. Law school students are generally taught to recognize and internalize various overlapping legal instruments and their fundamental principles and to apply them to the numerous types of legal elements of our society. From the time they open their first textbooks at the start of the first semester, law students are conditioned to see and interpret the world in terms of a relatively static collection of rules, recommendations and regulations, which have seemingly been created by a large majority of the members of a perfectly democratic government with the singular goal of promoting and enforcing the ideal values of a well-functioning society. Only rarely are law students tasked with trying to understand and explain the complex mechanisms, biases or other sociological and political influences that have led to the promulgation of a particular law or to the prevalence of a general principle of law.

Of course, this approach is entirely understandable when viewed in the particular context of the legal profession. Especially in civil law countries, a judge is not particularly interested in "why" a particular law is written in the way it is, since his/her job is to "accept" the text of the law as a given and apply it to the best of his/her abilities to the case at hand.[22] Additionally, lawyers would achieve very little in their day-to-day activities, if they spent a significant amount of time questioning the very premises of the laws that they are meant to follow and work with. In my experience, the majority of lawyers would agree with this view of the legal field, while the people that work in legal academia as professors, researchers and other scholars would quite possibly challenge this view by pointing to various works of legal research that include a fair amount of *de lege ferenda* analysis.

[22] I recognize that this is a reductive view of the issue, since judges – appellate court judges in particular – have to interpret and analyze the original intentions of the legislator through various methods of textual analysis. However, as a general rule, judges prefer to see themselves as objective and independent enforcers of the law instead of inherently political actors creating or developing legislation.

One of the main goals of my thesis is to broaden this traditional approach that continues to dominate the field of legal research. I aim to take a generally critical view of the current counter-terrorism sector and of the structures and biases that have influenced it through a combination of constructivist and hermeneutic ideas, including deconstruction[23], post-structuralism[24] and social constructionism[25].

I recognize, however, that the space constraints of a thesis paper and the necessary description and pragmatic legal analysis of the broad legislative framework of counter-terrorism might lead to a certain kind of shallowness in my criticisms, which might – quite paradoxically – invite criticisms towards my approach from both the legal and social science fields. Therefore, I do not intend to provide a comprehensive, all-encompassing criticism of international law or even of international cyberterrorism legislation but instead start a conversation about the explicit and implicit biases and structures of counter-terrorism as a first step towards addressing the problems that they create and reinforce.

The main focus of my research will be performed through qualitative research methods. In addition to legal dogmatism, I will also apply the multi-faceted methods of phenomenography and phenomenology in my analysis of the subjects, norms and legislative theories of counter-terrorism and cyberterrorism regulation. These elements also form the fundamental data points of my analysis. Through these methods, I will analyze, for example, the relevant texts of a piece of legislation through the lens of constructivism and hermeneutics by attempting to deconstruct and recognize the "larger story" behind cyberterrorism legislation and international law as a whole. This method of research requires me to analyze the terrorism framework at its smallest level – the significance and influences behind the sentences and words of the legal texts – while simultaneously recognizing the roles that the text have in the broader context of a global counter-terrorism strategy.

I also aim to address the practical threat of an imminent act of cyberterrorism by contextualizing the story of international counter-terrorism efforts and estimating whether the current concerns about imminent terrorist attacks are overblown, potentially as a result of the massive amount of

[23] For example, Jacques Derrida, *Deconstruction in a Nutshell: A Conversation with Jacques Derrida, With a New Introduction* (John D. Caputo ed, Fordham University Press 2021).
[24] For example, James Williams, *Understanding Poststructuralism* (Routledge 2015).
[25] For example, Andrew Lock and Thomas Strong, *Social Constructionism: Sources and Stirrings in Theory and Practice* (CUP 2010).

media coverage granted to the issue. In addition, I will apply the results of this analysis to the specific problem of cyberterrorism by comparing both the attention given to each issue and the prevalence and actual threats posed by them to national and international peace and social justice.

As is the case with almost any issue of international law, cyberterrorism and the field of international terrorism regulation is influenced by several, often overlapping doctrines, subjects and sources of international law. Some of these doctrines, such as that of the sources of international law, are universally applied, overarching constructions that guide all sectors of international legislation, whereas some are more closely linked to the specific issues of conventional terrorism or cyberterrorism. While the issues around cyberterrorism and conventional counter-terrorism legislation touch upon numerous additional fields of international law not comprehensively analyzed in this thesis such as the issues of jurisdiction, the conflict of laws between domestic and international terrorism legislation, the many immunities of state officials and the nationality of the perpetrators, I have limited my analysis to the sources, subjects and doctrines that I view as the most central elements driving the global response to conventional terrorism and cyberterrorism.

1.4 STRUCTURE

The first chapter briefly introduces the subjects of international law most relevant in the global counter-terrorism field. The second chapter focuses on the pieces of international legislation currently at the heart of the counter-terrorism response, mainly the sectoral UN treaties and the Draft Comprehensive Convention on Terrorism. The third chapter analyzes the potential emergence of a crime of terrorism under customary international law. The fifth chapter explores the specific question of statehood in the counter-terrorism field as well as some of the most overtly political aspects of responding to terrorist threats. The sixth chapter compares the perceived and actual threat posed by conventional terrorism with that of cyberterrorist acts.

2 THE MAIN ISSUES OF INTERNATIONAL COUNTER-TERRORISM REGULATION

2.1 THE FUNDAMENTAL ROLE OF STATES

One of the most central doctrines of international law is that focused on identifying and classifying the various subjects or actors taking part in the arena of international law. According to the – admittedly broad – traditional definition "a subject of international law is an entity possessing international rights and obligations and having the capacity (1) to maintain its rights by bringing international claims and (2) to be responsible for its breaches of obligation by being subjected to such claims".[26] Due to the vague nature of the definition, the actual characterization of a potential subject of international law must generally be made on a case-by-case basis, although it is important to note that states have generally been seen as the primary actors of international law[27] and most of the issues of international law are still mainly interpreted and analyzed through the relations and actions between independent states.[28] The traditional approach is also visible in the field of counter-terrorism where the most comprehensive legislative instruments have been negotiated and adopted between states either through the various multilateral "sectoral" treaties or the (albeit deadlocked) negotiations over the abovementioned Draft Comprehensive Convention on International Terrorism.

In addition to the various multilateral treaties, states have also played a significant role in developing the field of counter-terrorism legislation through their domestic laws, in certain cases even going further than international legislation, which has in turn raised some concerns among legal scholars and several interest groups and organizations about the possible overreaches and human rights violations that could potentially be justified by political leaders under these new domestic laws.[29] It remains to be seen whether the states negotiating international counter-terrorism legislation will eventually utilize the various national laws in

[26] James Crawford, *Brownlie's Principles of Public International Law* (9th edn, OUP 2019) 105. See the specific page for a more comprehensive list of sources.
[27] *Ibid* 106 and Wolfgang Friedmann, *The Changing Structure of International Law* (Stevens & Sons 1964) 67, quoting Philip Jessup, *A Modern Law of Nations* (The Macmillan Company 1948) 17.
[28] The prevailing primary role of states as subjects of international law is additionally reflected in the fact that states, along with e.g. international organizations, are still classified in international legal literature as "established legal persons" while corporations are viewed as entities possessing a "special type of legal personality", although the revenues of several multinational companies are already significantly higher than the GDP of small or medium-sized states. See for example Global Policy Forum, "Comparison of the World's 25 Largest Corporations with the GDP of Selected Countries" (2010), <https://www.globalpolicy.org/images/pdfs/Comparison_of_Corporations_with_GDP_of_Countries_table.pdf> accessed 8 December 2020. See more generally, for example, *supra*, Crawford 2019, 106–116.
[29] Larissa Van den Herik and Niko Schrijver, *Counter-Terrorism Strategies in a Fragmented International Legal Order: Meeting the Challenges* (CUP 2013) 652–665.

reaching an agreement on the definition of terrorism or do they reject even these solutions in fear of the potentially harmful human rights developments caused by overly broad definitions.

In my opinion, mainly regulating (cyber)terrorism on a national level through domestic legislation may ultimately prove to be an ineffective solution due to the inherently global nature of terrorism. Coordination between states will become even more essential in the future as acts of cyberterrorism will most likely blur the line between domestic and international terrorism even further through the use of advanced technologies in cyberspace by numerous direct and indirect actors from several states. As a result, the many flaws and inefficiencies of a domestic-centered terrorism approach are exacerbated when these national frameworks are applied to terrorist acts committed in cyberspace.

2.2 THE INFLUENCE OF MULTINATIONAL BODIES AND CORPORATIONS

Other important actors in this debate such as NATO and the EU should not be overlooked, as they could potentially provide some guidance to other states and organizations by formulating and agreeing on their own definition of terrorism. However, due to the complex internal politics and power dynamics of these organizations, any final definition that they agree upon should be analyzed carefully and critically in light of the specific voting procedures, power imbalances and political calculations that might have affected the final wording of the definition. If these various factors are not sufficiently taken into account, other bodies – such as the UN General Assembly – that base their definition on one accepted by, for example, NATO, might effectively agree on a broader – or narrower – definition than they originally intended purely due to the inherent structures that guided the passing of the "model" definition.

Due to its size, influence and considerable independent powers in international affairs, it is sometimes easy to forget that the UN, as an international organization, has only acquired its legal personality through the powers delegated to it by the states. UN's significant role as the main coordinator and consensus-builder in terrorism legislation was strengthened by UN General Assembly Resolution 71/291, which established the UN Office of Counter-Terrorism (UNOCT) whose mandate is derived from the biannually reviewed UN Global Counter-Terrorism Strategy. The UNOCT "works in close collaboration" with the subsidiary bodies of the Security Council to improve the Member States' capacity to "prevent and respond to terrorist acts". These Security Council bodies include the Counter-Terrorism Committee, the ISIL (Da'esh) and Al-Qaida Sanctions Committee and the 1540 Committee on the non-

proliferation of nuclear, chemical and biological weapons, which are significant cooperation bodies in themselves.[30] Through the actions of the UNOCT and of the various subsidiary bodies of the Security Council, the UN – in addition to already acting as one of the most significant forums of debate regarding the global counter-terrorism response – has gained the powerful ability to guide current and future counter-terrorism discussions.

Regardless of the states' understandably strong influence in international affairs and international law, certain relatively recent developments and new legal constructs such as the "ever closer union"[31] approach of the EU and the extraordinary influence of large technology companies have made international lawyers question whether some of the biggest companies or other actors have effectively replaced states as the most influential subjects of international law, or if they at the very least stand on equal ground with the states as international actors in the legal arena. This debate does have some relevance in the cyberterrorism field due to the significant role of Facebook, Twitter and other big technology companies as potential platforms for radicalization, terrorism recruiting and the spread of misinformation.[32]

The internet in general has played a significant role in facilitating the financing of terrorism through means such as e-commerce, the exploitation of online payment facilities and even the use of charitable organizations, in addition to direct solicitation.[33] An equally concerning development relates, quite paradoxically, to one of the internet's greatest accomplishments, its ability to connect people. By making it quite effortless for "like-minded" individuals to find each other through various types of discussion forums and social media platforms, the internet has allowed the followers of some of the most harmful and dangerous ideologies to reach a certain sense of inclusion, at least within their online communities, whereas until relatively

[30] UN Office of Counter-Terrorism, *About us*, <https://www.un.org/counterterrorism/about> accessed 8 December 2020.
[31] Preamble of the Treaty on European Union.
[32] Max Fisher and Amanda Taub , "How Everyday Social Media Users Become Real-World Extremists", The New York Times (25 April 2018) <https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html?action=click&module=RelatedLinks&pgtype=Article> accessed 8 December 2020, J.M. Berger, "How ISIS Games Twitter" The Atlantic (16 June 2014) <https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/> accessed 8 December 2020, Emerson T. Brooking and P. W. Singer, "War Goes Viral", The Atlantic (November 2016) <https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/> accessed 8 December 2020, The Editorial Board, "The New Radicalization of the Internet", The New York Times (25 April 2018) <https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html?action=click&module=RelatedLinks&pgtype=Article> accessed 8 December 2020.
[33] UN Office on Drugs and Crime, "The Use of the Internet for Terrorist Purposes", (2012), available at <https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html> accessed February 20th 2021. See also, for example, Michael Jacobson, "Terrorist Financing and the Internet", 33 (4) Studies in Conflict and Terrorism (2010) 353.

recently those same individuals would have mostly likely remained as rejected outcasts within their analogue communities.[34] It is also important to keep in mind that while terrorism recruiting, radicalization efforts and the sharing of misinformation must – at least to a certain degree – be done in public platforms in order to be effective, the financing of terrorism has become significantly easier to hide through recent technological advancements such as the rise of cryptocurrencies.

While preventing these unfortunate developments in the social media sphere from causing, aiding or perpetuating the prevalence and impact of extremist ideologies and terror attacks is clearly an essential part of the broader counter-terrorism strategy, it is an extremely difficult and complex field to regulate from a legislative standpoint due to its constantly evolving nature and the ability of terrorists to transfer their activities to another platform if one platform adopts new, stronger regulations regarding hate speech and misinformation. Furthermore, I believe that it is extremely unlikely that private actors, even those as influential and powerful as Facebook or Google, could resolve the most fundamental issues of the current counter-terrorism framework that are the central focus of this thesis such as the definition of terrorism or the underlying biases of current regulation. Truthfully, I would find it quite unnerving from both an ethical and an international law standpoint if these multinational corporations had the legislative or practical power to dictate the global response to one of the most heinous crimes known to humankind. This does not mean that there are no benefits to coordination and collaboration between private and public sector actors. In many instances, market-based solutions and economic models are able to provide useful and innovative solutions to emerging issues.[35] However, in regulating crimes with an international reach such as that of terrorism, the main focus should remain on the public sector due to the criminal law aspects of these crimes, whereas coordination efforts could help prevent some of the various indirect forms and elements of modern terrorism described above.

Therefore, the main focus of this thesis as regards the subjects of international law most relevant to kinetic counter-terrorism and cyberterrorism regulation is on the states negotiating

[34] Some of these ideologies, such as neo-Nazism and more broadly neo-fascism, are revived versions of past ideologies, whilst some, such as the set of conspiracy theories known as QAnon, have emerged within certain online communities. Generally on QAnon, see, for example, Kevin Roose, "What Is QAnon, the Viral Pro-Trump Conspiracy Theory" The New York Times (4 March 2021) <https://www.nytimes.com/article/what-is-qanon.html> accessed 27 April 2021.

[35] Regardless of its issues, the emissions trading system is a useful recent example of a market-based solution to the global issue of climate change. See, for example, European Commission, "EU Emissions Trading System (EU ETS)" <https://ec.europa.eu/clima/policies/ets_en#tab-0-0> accessed 28 April 2021.

multilateral treaties as well as on the UN, which has also made significant contributions to the fight against terrorism through various measures such as Security Council and General Assembly resolutions, global cooperation and proposals for counter-terrorism policies,[36] while simultaneously recognizing the potentially significant role of the private sector in solving some of the supplementary issues connected to international terrorism and cyberterrorism in the near future.

[36] See, for example, UN Global Counter-Terrorism Strategy, <https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy> accessed 8 December 2020.

3 THE CENTRAL WRITTEN SOURCES OF INTERNATIONAL COUNTER-TERRORISM LAW

3.1 THE "SECTORAL" TREATIES

In the case of many other emerging technologies, such as cryptocurrencies and artificial intelligence, the states' influence as legislative pioneers has practically evaporated as the sheer speed of technological development has effectively left them at the mercy of private law fields such as contract law and global commercial law in general. In the area of cyberterrorism, however, the focus has largely remained on states even though cyberterrorism possesses certain elements that touch upon complex technological fields such as essential telecommunications infrastructures, "cloud" databases and the control of nuclear weapons and other highly volatile materials through – for example – a nuclear base's technological control network. This is mainly due to the fact that no comprehensive cyberterrorism regulation has been adopted at the international level and thus terrorist acts in cyberspace are still mainly regulated under the general counter-terrorism framework or, for example, through relevant parts of international humanitarian law and general – domestic and/or regional – cybercrime laws.

As a more general note, limiting the use, availability and manufacturing of certain dangerous tools, including nuclear and chemical weapons, has proven to be quite a successful strategy in preventing these types of terrorist attacks before they even become possible. However, this strategy cannot be applied to the same degree in the cyberterrorism sector, where even the most sophisticated and wide-reaching attacks could potentially be committed by practically anyone with internet access, a laptop and the necessary expertise. Acts of cyberterrorism mainly rely on information, which is often readily available on the internet, whereas the materials used to manufacture weapons of mass destruction (WMDs) are difficult to acquire and their inherent scarcity make them an easier target for restrictive measures. Furthermore, the manufacturing of a stable and effective WMD requires a level of expertise that only a relatively small group of people possess.[37]

Through the years, states have adopted numerous multilateral treaties to combat new types of terrorist threats as their viability and potential scale have become clear. The global counter-terrorism response has been driven by these various "sectoral" treaties since the early 1970s after the terrorist attack during the Munich Olympics of 1972 had resulted in strong calls for

[37] David P. Fidler, *Cyberspace, Terrorism and International Law*, 21(3) Journal of Conflict and Security Law (2016) 475, 481–482.

action to combat international terrorism.[38] It was during the following negotiations in the UN concerning potential counter-terrorism measures that the "definitional" issue of terrorism, that continues to be one of the most complex problems in the field of counter-terrorism, first arose. The crux of this issue is summarized well in the widely used phrase "one person's terrorist is another person's freedom fighter".[39] Although this expression can also be a bit problematic since it can be explained and justified in countless ways by various actors, each with their own motives, it emphasizes the fact that any definition of terrorism must be sufficiently broad in scope in order to be effective while simultaneously protecting the right of freedom fighters to perform certain – even controversial – acts in exercising their right of self-determination.[40]

In order to largely avoid the political debates related to the definition of terrorism, the UN decided to confront the threat of terrorism through the aforementioned sectoral treaties. These conventions share certain key elements. Firstly, while they do not establish new international crimes of terrorism, they instead usually oblige the states to domestically criminalize the acts described in the treaty as well as impose punishments proportional to the seriousness of the acts in question. Secondly, the states must create extrajudicial jurisdiction over the acts, thus broadening the usually accepted scope of criminal jurisdiction in international law, which is mainly based on the perpetrator's nationality or on which state's territory the crime was committed. Thirdly, the states must either prosecute or extradite suspected offenders that they come across in their territories (*aut dedere aut iudiciare*). This particularly strict requirement has no exceptions and is further strengthened by several complementary measures aimed at broadening the potentially narrow scope of extraditable offences under the state parties' domestic laws to those described in the treaties.

The most central objective of the extradite or prosecute principle is to ultimately eliminate the still existing safe haven states for terrorists as more and more states become parties to these conventions.[41] Regardless of its admirable and notable aims, I would retain at least some degree of skepticism about the practical application of this regime. Even though the state parties cannot directly provide protection for suspected terrorists, they might be able to effectively achieve this by opting to prosecute the offenders. The potential for these unfortunate secondary effects can be derived from the language used in the sectoral treaties regarding the requirements for

[38] Amrith Rohan Perera, "The draft United Nations Comprehensive Convention on International Terrorism" in Ben Saul (ed), *Research Handbook on International Law and Terrorism* (Edward Elgar Publishing 2020) 121.
[39] For example, *ibid* 122.
[40] The right of self-determination also covers situations related to foreign occupation.
[41] *Supra* Saul (2020) 121–123.

prosecution. For example, Article 8(1) of the 1997 International Convention for the Suppression of Terrorist Bombings states that the competent authorities obligated to prosecute an alleged offender must "take their decision in the same manner as in the case of any other offence of a grave nature under the law of that State"[42]. This rule is rational from a normative standpoint since the method utilized in the sectoral treaties centers around the domestic criminalization and prosecution of the relevant acts. However, Article 8(1) – and comparable articles in other sectoral treaties – can create problematic inconsistencies in practice since it only vaguely refers to the respective criminal procedures of the states ("the same manner" --- "under the law of that State"). As a result, the current safe havens based on a lack of jurisdiction or of domestic criminalization could effectively transform into procedure-based ones.[43] While a clear abuse of the interpretative space provided by the article would certainly be construed by the wider community as a breach of the treaty obligation, a certain level of inconsistency could nevertheless emerge if, for example, a particular state required a higher standard of proof for the set of crimes that includes the offence described in the treaty.

A similar issue relates to the level of punishment required by the treaty. Article 4(b) states that the states must make the offences described in the treaty "punishable by appropriate penalties which take into account the grave nature of those offences"[44]. What are considered "appropriate penalties" can vary from state to state regardless of the fact that the states must "take into account" the seriousness of the behavior. This could ultimately result in a *prima facie* comprehensive and seemingly uniform legislative framework whose application is nevertheless driven by a potentially varied collection of domestic procedural rules and levels of punishment. This variance could, in turn, create the possibility that a large part of terrorist attacks are committed in a particular state or that perpetrators flee to that state after having committed attacks in another state due to the – comparatively – more lenient legislation of the "receiving" state.[45]

[42] 1997 UN International Convention for the Suppression of Terrorist Bombings, Art. 8(1).
[43] This transformation would, of course, also require that the states currently providing effective safe havens for terrorists would become parties to the sectoral treaty, which, in itself, is in no way certain.
[44] 1997 UN International Convention for the Suppression of Terrorist Bombings, Art. 4(b).
[45] It must be noted, however, that the negative "guiding" effects caused by the possibility of potential perpetrators to "choose" the state with the most favorable domestic counter-terrorism legislation might be more limited in the field of terrorism than it is in other fields of law such as tax legislation due to the fact that terrorists might often not carefully consider the potential legal consequences of the act. Some perpetrators also effectively "avoid" punishment by committing suicide either right before they are taken into custody by the authorities or as an intentional part of the attack.

The issues related to the discrepancies in national legislations presented in the previous two paragraphs are not exclusive to counter-terrorism regulation since they are inherent in practically all fields of international law in which a combination of treaty law and domestic law is utilized in order to try and solve a complex legal dilemma. Nonetheless, it is important to recognize and remember the disadvantages and potential weaknesses of the sectoral approach. Furthermore, it must also be highlighted that these issues are heightened in the cyberterrorism field due to the significant difficulties in applying inflexible or overly broad domestic laws to new, unique acts that are rendered possible through the rapid development of advanced technologies such as 5G networks and all of their various applications. Despite these concerns, I believe that the sectoral approach can have a role in abolishing some of the still remaining terrorist safe havens or at the very least weaken their impact and harmful effects.

Through the wide use of these sectoral treaties, states have been able to avoid defining the general crime of terrorism by merely reacting to emerging threats through new, narrow pieces of legislation. While the states may find it relatively easy to adopt these types of treaties due to their limited scope and seemingly dynamic nature, the result is an overlapping mosaic of sectoral and more comprehensive counter-terrorism treaties which still fails to provide a sufficiently clear answer to even the most fundamental question of counter-terrorism legislation; what constitutes a terrorist act, let alone an act of cyberterrorism?[46] Furthermore, even the states' willingness to adopt additional sectoral treaties may quite possibly be weakened by the fact that the newer treaties expressly define the acts described in the treaties as non-political.[47] As a result, the states that advocate for a definition of terrorism that excludes certain – often political – acts committed, *inter alia*, in the practice of a right to self-determination, could be hesitant to adopt future sectoral treaties that include the "political offence exception"[48] regarding the extradition of suspected offenders. Of course, the definition of a "political offence" is in itself ambiguous and often guided by and interpreted through the political interests of the interpreter.

[46] Ben Saul and Kathleen Heath, "Cyber terrorism" in Nicholas Tsagourias et al. (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 152.
[47] 1997 UN International Convention for the Suppression of Terrorist Bombings, Art. 15; 1999 UN International Convention for the Suppression of the Financing of Terrorism, Art. 14; 2005 UN International Convention for the Suppression of Acts of Nuclear Terrorism, Art. 15. The core of these articles is that denying the extradition of suspected offenders based on the political motives connected to the acts described in the treaties is explicitly prohibited.
[48] *Supra* Saul (2020) 123.

The sectoral UN treaties originally adopted to deal with conventional and emerging terrorist threats including, inter alia, the unlawful seizure of aircrafts[49], the taking of hostages[50] and the targeting of nuclear power plants and reactors[51] described above remain the most influential sources of law in the cyberterrorism field and will most likely also remain so at least in the near future, since a sudden breakthrough in either customary international law or in the deadlocked negotiations over the Draft Comprehensive Convention seem unlikely. The prevalent adopting of all types of counter-terrorism treaties is certainly also guided by the principles and objectives laid down in the UN Charter, whose very first article states the Charter's primary objectives of maintaining international peace and security.[52] Due to terrorism's manifest border-crossing nature, a joint response is vital in ensuring not only regional but global peace and social justice.[53] This common, multilateral approach to terrorism is strengthened by Article 2 of the Charter, which includes the "good faith"[54] and peaceful resolution of disputes[55] principles as well as the general presumption against threat or use of force[56] by states towards other states.

While none of the various sectoral counter-terrorism conventions specifically target cyberterrorism, certain terrorist acts committed in cyberspace do fall within the scope of the treaties even though this is in large part due to the broadness of some of the conventions instead of a specific intention on behalf of the drafters to also include cyber-based acts.[57] Perhaps the most notable of these broader treaties is the 2005 Convention on Acts of Nuclear Terrorism whose Article 2(1)(b) states that anyone who "(u)ses in any way radioactive material or a device, or uses or damages a nuclear facility in a manner which releases or risks the release of radioactive material"[58] with, for example, the specific intention of causing serious bodily injury or substantial damage to property, has committed an act of nuclear terrorism. Since the text of the article does not specify the manner in which the act must be performed, the language

[49] 1970 UN Convention for the Suppression of Unlawful Seizure of Aircraft and 2010 UN Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft. Several other UN conventions have been adopted relating to other sectors of terrorism in the field of civil aviation.
[50] 1979 UN Convention against the Taking of Hostages.
[51] 2005 UN International Convention for the Suppression of Acts of Nuclear Terrorism.
[52] Art. 1(1) of the UN Charter. All states also have a general obligation under international law to prevent and repress terrorist acts emanating from their territory: "Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations", annex to UN General Assembly resolution 2625 (XXV) [2] and [8-9].
[53] I have opted here for the use of the term "peace and social justice" instead of the more traditional "peace and security", since "social justice" is a more inclusive term that encompasses both global security and social justice. This more recent approach is utilized, inter alia, in the preamble of the UN Convention on the Law of the Sea.
[54] Art. 2(2) of the UN Charter.
[55] Art. 2(3) of the UN Charter.
[56] Art. 2(4) of the UN Charter with the exception of self-defense laid down in Art. 51 of the Charter and the principle of non-intervention by the UN in the essentially domestic matters of any state (Art. 2[7] of the Charter).
[57] *Supra* Tsagourias et al. (2015) 152.
[58] 2005 UN International Convention for the Suppression of Acts of Nuclear Terrorism, Art. 2(1)(b)

effectively also includes cyber-based instances of nuclear terrorism. In addition to Article 2(1)(b) of the nuclear treaty, the language used certain articles of the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation and the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation might be broad enough to be applied to acts in cyberspace.[59]

An example of a cyberterrorist act potentially falling inside the scope of the nuclear treaty is the "Stuxnet" attack of 2010 which targeted Iranian uranium enrichment centrifuges.[60] The attack, reportedly a joint operation of U.S. and Israeli experts,[61] was performed through a highly sophisticated computer bug that caused significant damage to the targeted centrifuges.[62] This attack demonstrates that nuclear facilities can be targeted through cyber attacks with potentially disastrous consequences. Solely judging by the nature and effects of the act, the Stuxnet attack could also fall within the scope of the sectoral nuclear treaty. However, since it was seemingly committed by states, it cannot be characterized as nuclear terrorism under the treaty and is instead interpreted under international humanitarian law.[63]

Despite certain exceptions such as those highlighted above, the clear majority of the sectoral treaties cannot be applied to cyberterrorist acts due to the general requirement of a physical attack of one type or another.[64] Nevertheless, the terms used in the treaties such as "violence" or use of "force" raise the question of whether acts committed through cyberspace can be considered "violence" or as use of "force" in the context of the treaties. Yet another example of an unresolved term regarding cyberspace is whether the use of a cyber tool constitutes "placing" a dangerous "device" on an aircraft.[65] In the lack of international case law, these complicated interpretative issues are still up for debate.[66]

---

[59] 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Art. 1(d); 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Arts. 3(e) and 3(f).
[60] Peter Beaumont, "Iran nuclear experts race to stop spread of Stuxnet computer worm", The Guardian (26 September 2010) <https://www.theguardian.com/world/2010/sep/26/iran-stuxnet-worm-nuclear> accessed 21 March 2021.
[61] Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say", The Washington Post (2 June 2012) <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html> accessed 21 March 2021.
[62] *Ibid*; David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", The New York Times (1 June 2012) <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> accessed 21 March 2021.
[63] 2005 UN International Convention for the Suppression of Acts of Nuclear Terrorism, Art. 4(2).
[64] *Supra* Tsagourias et al. (2015) 153.
[65] 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Art. 1(c); *supra* Tsagourias et al. (2015) 154.
[66] *Supra* Tsagourias et al. (2015) 154.

One additional issue that must be considered briefly is the difficulty of attribution, which is equally significant in the application of both the sectoral treaties and the Draft Comprehensive Convention to cyberterrorism – as well as in all other types of cybercrime. Applying the criminal law approach adopted in the sectoral treaties and the Draft Convention requires identifying the perpetrators of the terrorist acts.[67] Even identifying conventional terrorist actors is certainly not an easy task but trying to perform it in cyberspace poses certain unique challenges.[68] This issue is exacerbated further by the fact that states are extremely reluctant to admit to having taken part – either directly or indirectly – in cyber attacks both due to the political considerations related to the potentially unethical nature of the acts and their reluctance to reveal information about, often highly classified, strategic military operations and their objectives.

3.2 THE UN DRAFT COMPREHENSIVE CONVENTION ON TERRORISM

As has already been mentioned in the introduction of this thesis, the negotiations over the UN Draft Comprehensive Convention on Terrorism have been at an impasse for several years.[69] The central aim of the Comprehensive Convention was to fill up the normative gaps still remaining in the sectoral treaties and the broader counter-terrorism framework by finally agreeing on a general definition of terrorism. After the early debates concerning the definitional issue, the current gridlock in the negotiations mainly centers on the treaty's stance on state terrorism and the right to self-determination.[70] This chapter touches on all three issues, but certain questions related to statehood are analyzed in more detail in chapter 5 of this thesis.

The core definition of terrorism under the Draft Convention which has remained unchanged since 2001 is described in Article 2 of the proposed treaty as follows:

> 1. Any person commits an offence within the meaning of the present Convention if that person, by any means, unlawfully and intentionally, causes:
>
> a) Death or serious bodily injury to any person; or
>
> b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or to the environment; or

[67] *Supra* Fidler (2016) 479.
[68] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution" (2012) 17(2) Journal of Conflict and Security Law 229.
[69] Generally on the long journey from 1930s to present day to define and criminalize terrorism internationally see, for example, Ben Saul, *Defining Terrorism in International Law* (2006 OUP).
[70] *Supra* Saul (2020) 125.

(c) Damage to property, places, facilities or systems referred to in paragraph 1 (b) of the present article resulting or likely to result in major economic loss,

when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.[71]

This quite broad definition demonstrates the drafters' willingness to address the gaps left by the sectoral treaties. Although the main focus of the Draft Convention is quite clearly on providing an accepted definition of conventional terrorism, the proposed definition is sufficiently broad to also cover the majority of cyberterrorist acts, since the use of cyberspace is obviously included in the Article's "by any means" requirement.[72]

In summation, the definition encompasses acts that cause 1) death or serious personal injury, 2) "serious" property damage or 3) "major economic loss". The terms "serious" (in both instances) and "major" are both highly subjective and vague, which means that one can mostly only speculate about their exact scope until the Draft convention is adopted and a significant body of international case law emerges. Nevertheless, it is useful to demonstrate some of the difficulties that might arise in the future if this definition is to be applied to certain cyberterrorist acts. First of all, actors performing acts of "hacktivism" by, for example, seizing websites, disseminating viruses, overloading servers through denial-of-service attacks or utilizing automated "email bombs"[73], would most likely not be considered cyberterrorists under the Draft Convention, since their acts would not ordinarily fulfil the requirement of "serious" property damage or personal injury. However, these attacks could potentially fall into the third category of attacks, namely by causing significant economic losses through the loss of revenues, provided that the act also includes one of the specific intent requirements of Article 2.[74]

Another factor limiting the scope of the Article 2 definition is the additional requirement of "purpose". Thus, an act that fulfils one or more of the three requirements described above does

[71] U.N. Report of the Working Group, "Measures to Eliminate International Terrorism", (3 November 2010) U.N. Doc A/C.6/65/L.10, Annex I, 16.
[72] *Supra* Tsagourias et al. (2015) 155.
[73] Dorothy Denning, "Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy" in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime and Militancy* (2001 RAND) 263.
[74] The so-called "Operation Avenge Assange" carried out by the well-known "hacktivist" group known as Anonymous could have been characterized as a cyberterrorist attack under Article 2 of the Draft Convention since it included a coercive element. See, for example, Mark Townsend, Paul Harris, Alex Duval Smith, Dan Sabbagh and Josh Halliday, "Wikileaks backlash: The first global cyber war has begun, claim hackers", The Guardian (11 December 2010) <https://www.theguardian.com/media/2010/dec/11/wikileaks-backlash-cyber-war> accessed 23 March 2021. However, these types of attacks are not necessarily even referred to as terrorism in the media and I believe that only in exceptionally grave cases should counter-terrorism legislation apply to acts that cause mainly monetary losses.

nevertheless not constitute a terrorist act under the Draft Convention if it does not include the specific aim of intimidating a population or coercing a government or an international organization to do or to abstain from performing a certain act. Thus, an actor demanding money from a government for ceasing to inflict damage to public property would fall within the Article's scope[75], whereas the sole act of severely damaging public property would not. Additionally, perpetrators whose only motivation is, for example, revenge or personal satisfaction are excluded from the Article's scope. It must also be noted, however, that the Draft Convention's definition does not require any additional motivation-related factors such as religious or political intentions, which broadens the definition's scope.[76] Then again, demonstrating the specific purpose of, for example, "intimidating a population" can often be extraordinarily difficult in practice due to the requirement's inherently subjective and vague nature.

Drawing the line between cyberterrorist acts and other types of cybercrime under the Draft Convention is no easy task, but the same holds true for practically any counter-terrorism treaty, although it is particularly difficult under a treaty that aims to provide a comprehensive definition of terrorism. However, the potential overreach of the Draft Convention's definition can be demonstrated through a few examples. First of all, the aforementioned act of extorting money from the government does not, in my opinion, warrant the label of (cyber)terrorism since the act itself could effectively mount to a mere nuisance for the government and should therefore be regulated under other bodies of law such as relevant cybercrime legislation and international criminal law.[77]

Certain types of political or ideological acts such as industrial action or environmental protests could also effectively be within the Draft Convention's scope since they can combine property damage and/or the potential of major economic losses with a concrete demand of, for example, better working conditions (labor negotiations) or the protection of a certain element of the environment (environmental protest).[78] In order to prevent the possible suppression of political and ideological debate by domestic legal actors under the Article 2 definition, an exclusion

[75] *Supra* Tsagourias et al. (2015) 158.
[76] *Ibid*.
[77] The effects of these types of attacks could, of course, be quite severe to the government from a monetary perspective due both to the potential "ransom" payments and the significant property damages but, as noted above, my view is that acts resulting in even significant monetary losses could only be regarded as terrorism in exceptionally serious cases.
[78] *Supra* Tsagourias et al. (2015) 159–160.

concerning legitimate democratic dissent and protest might prove necessary at least regarding instances where the damages are of a purely monetary nature.[79]

Despite its flaws, the core definition of terrorism under the Draft Convention is quite widely agreed upon, whereas certain heated debates remain about the exact scope of the Convention. As a result of recent technological advancements and the global population's relatively broad access to the internet's vast resources and tools, cyberterrorist acts may be perpetrated by a large group of potential actors ranging from self-taught individuals and groups with extremist ideologies to state actors themselves. The term "state terrorism" itself is a controversial one, since the majority of states do not seemingly recognize states as potential perpetrators of external state terrorism (state terrorism that targets foreign populations).[80]

As has been referred to above, the issues of state terrorism, foreign occupation and the right of peoples to self-determination are one of the main points still contended by the state parties negotiating over the Draft Convention. The western wording rejects direct state responsibility, whilst the Organization of Islamic Cooperation (OIC) – and the states supporting it – seeks to incorporate an opposite approach.[81] Under the western proposal, acts committed in armed conflict by the armed forces of states or States are not included in the Convention's scope if the acts are covered by international humanitarian law.[82] While the exact scope of "armed forces" can be debated[83], it is clear that armed forces committing cyberattacks in the course of an armed conflict would not be considered terrorists under the western proposal of the Draft Convention. Instead, these acts are regulated by the rules of international humanitarian law such as the principles of distinction and proportionality.

As a result, it would appear that the majority of actions resembling terrorist acts are already prohibited under humanitarian law[84], although the western proposal overlooks two significant factors. Firstly, armed resistance groups acting against foreign occupation would be considered terrorists under this proposal, even though these acts are lawful under the Additional Protocol

[79] *Ibid* 160.
[80] *Supra* Shiryaev, 2012, pp. 150–151.
[81] U.N. Report of the Ad Hoc Committee, 6th Session (28 January–16 October, 2002) U.N. Doc A/57/37, Annex IV; U.N Report of the Ad Hoc Committee, 14th Session (12–16 April, 2010) U.N. Doc A/65/37.
[82] *Ibid*.
[83] Generally on the definition of armed forces and the broader principle of distinction see, for example, Nils Melzer, "The Principle of Distinction Between Civilians and Combatants" in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (2014 OUP) 296–331.
[84] *Supra* Tsagourias et al. (2015) 160–161, especially footnote 67.

1 of the Geneva Conventions[85]. Secondly, the Convention would also apply to the actions of "unprivileged combatants" performed against "a party to a conflict not belonging to a state's army".[86] These acts are also effectively considered lawful under international humanitarian law.[87] The IOC's proposal aims to solve these two problems by referring to "parties to an armed conflict" instead of the "armed forces" described in the western proposal. Combined with the reference to the definition of "parties to an armed conflict" as it is understood in international humanitarian law[88], the IOC's response effectively overcomes both of the issues caused by the western proposal. [89] I am a strong advocate of the IOC's wording, since it is in my view the only way to ensure that the rights under international humanitarian law – especially the right of liberation movements to legally resist foreign occupation – are not diluted by the adopting of the Comprehensive Convention.

According to the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, cyber-based acts are also included in the definition of the war crime of spreading terror amongst a civilian population.[90] Nonetheless, the neutrality of the Tallinn Manual, which is a publication of the NATO Cooperative Cyber Defence Centre of Excellence, can, quite justifiably, be questioned since several NATO members such as the U.S. would most certainly want to avoid being labelled (state) (cyber)terrorists if the OIC's proposal prevailed in the negotiations.

Another problematic element of the western proposal also relates to the actions of armed forces. In addition to acts committed in the course of an armed conflict, under the western proposal the activities of State armed forces during peacetime would also fall outside the scope of the Comprehensive Convention.[91] While the armed forces of a state could potentially commit numerous types of seemingly terrorist cyberattacks such as "crashing the computer systems of a foreign central bank" or "interfering in dangerous manufacturing processes", only in very rare instances would these acts activate individual criminal liability.[92] In contrast, similar acts

[85] 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.
[86] *Supra* Hmoud (2006) 1037.
[87] *Ibid*.
[88] U.N. Report of the Ad Hoc Committee, 6th Session (28 January–16 October, 2002) U.N. Doc A/57/37, Annex IV, Art 18(2).
[89] Some of the negotiating state parties rejected the IOC's proposal based on the argument that the term "parties to a conflict" was ambiguous under international humanitarian law. However, this is a weak argument since the term "parties to a conflict" appears to already be a "known concept". See, *supra* Hmoud (2006) 1039.
[90] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereinafter Tallinn Manual) (CUP 2017) Rule 98.
[91] U.N. Report of the Ad Hoc Committee, 6th Session (28 January–16 October, 2002) U.N. Doc A/57/37, Annex IV, Art 18(3).
[92] *Supra* Tsagourias et al. (2015) 161–162.

committed by non-military state officials are within the scope of the Draft Convention according to the western proposal.

As a result, the military forces of states can effectively act with impunity against both foreign states and private persons as regards certain types of cyberattacks that do not rise to the level of cyberterrorism[93]. The clear division of rules between non-military state officials and state armed forces could also incentivize the states to redefine or recategorize, for example, their intelligence agents as part of their armed forces, thus effectively circumventing the Comprehensive Convention. The IOC has sought to include the acts of state armed forces in the Convention's scope through a slight modification of the wording of Article 18(3) of the Draft Convention.[94] The main reason why the IOC supports the inclusion of acts by state militaries during peacetime is that the only international body handling those types of acts is the inherently political Security Council.[95] I agree with the IOC's position since the Security Council, mainly due to the often paralyzing effect of the veto powers of the five permanent members, has shown time and time again that its decisions are guided strongly by national interests and politics instead of more objectively justifiable interpretations of international law.[96]

Similarly to Shiryaev, I tend to believe that the current western interpretation is an unsatisfactory one and seems to be driven mainly by the U.S. and its desire to keep practicing its highly questionable, preventive "self-defense" operations against potential terrorist threats.[97] This unambiguous and problematic state of affairs causes additional problems in cyberspace, where states could potentially justify ever-broader acts of state cyberterrorism under the auspices of proactive "self-defense". Although it appears that indirect state involvement such as state-sponsored acts of cyberterrorism could potentially be partly dealt with through various declarations and conventions such as the International Convention for the Suppression of the Financing of Terrorism[98], the problem of attribution of terrorist acts in cyberspace makes it

[93] *Supra* Hmoud (2006) 1040.
[94] U.N. Report of the Ad Hoc Committee, 6th Session (28 January–16 October, 2002) U.N. Doc A/57/37, Annex IV, Art 18(3).
[95] *Supra* Hmoud (2006) 1040.
[96] Leaving the issues regarding potential terrorist acts by state militaries to the discretion of the Security Council seems even more questionable in light of the reports about the U.S.'s surveillance and influence campaign inside the Security Council to gain sufficient support for the war against Iraq. See, for example, Martin Bright, Ed Vulliamy and Peter Beaumont, "Revealed: US dirty tricks to win vote on Iraq war", The Guardian (2003) <https://www.theguardian.com/world/2003/mar/02/usa.iraq> Accessed 24 March 2021.
[97] *Supra* Shiryaev, (2012), 173–178.
[98] *Supra* Shiryaev, (2012), 151.

difficult to point out even the direct perpetrators of the attacks, let alone the indirect actors or sponsors behind the activities.

3.3 JUS COGENS AND GENERAL PRINCIPLES OF LAW

In addition to the aforementioned sources, several peremptory (*jus cogens*) obligations such as the prohibitions against the threat or use of force, genocide, and crimes against humanity are relevant in the counter-terrorism sphere and, due to their prevailing effect over non-peremptory norms, should at least be considered whenever terrorism legislation is drafted. While the prohibition on use of force and the right of peoples to self-determination are connected to certain counter-terrorism debates at least in the broader context, their direct influence in the current field of international counter-terrorism law is mainly subsidiary.[99]

Another binding source of international law which can be used to cover up potential gaps in the counter-terrorism framework are the general principles of law referred to in Article 38(1)(c) of the Statute of the International Court of Justice. The exact scope of the general principles of law is not universally agreed upon and while they do sometimes overlap with certain customary law norms, several international cases have eventually been decided based on them in situations where a clear answer could not be easily derived from other sources of law.[100] For example, the principle known as *sic utere tuo, ut alienum non laedas*, first applied in the *Trail Smelter*[101] case, is the core foundation of international environmental law.[102]

3.4 SOFT LAW AND SECONDARY SOURCES OF INTERNATIONAL LAW

Non-formally binding or "soft law" sources form yet another part of the global counter-terrorism framework. Regardless of their characterization and practical legal effects, soft law instruments can at times prove even more influential in developing a particular field of international law than formally binding sources, especially in cases where the states are reluctant to formally agree on a particular course of action or when the topic is particularly

---

[99] Generally on *jus cogens* norms see, for example, Christian Tomuschat and Jean-Marc Thouvenin (eds), *The Fundamental Rules of the International Legal Order: Jus Cogens and Obligations Erga Omnes* (Martinus Nijhoff Publishers 2005).

[100] United Nations Office on Drugs and Crime, *Legal sources and the United Nations Counter-Terrorism Strategy*, <https://www.unodc.org/e4j/en/terrorism/module-3/key-issues/legal-sources-and-un-ct-strategy.html> accessed 9 December 2020; Cherif M. Bassiouni "A Functional Approach to 'General Principles of International Law'" (1990) 11(3) Michigan Journal of International Law 768.

[101] Trail Smelter Case (United States, Canada) (16 April 1938 and 11 March 1941) 3 U.N. Rep. International Arbitration Awards 1905.

[102] Leslie-Anne Duvic-Paoli, *The Prevention Principle in International Environmental Law* (CUP 2018).

politically controversial. Under these circumstances the states could nevertheless be more than willing to commit to a non-binding norm.[103] However, even agreeing on a non-binding instrument can often prove politically difficult for a state's politicians if they anticipate strong criticism from, for example, the more nationalist or protectionist parties or movements within their state. As regards cyberterrorism, the technology sector could, for example, recognize that a certain, less-used business practice could also protect the whole sector from massively harmful cyberterrorist attacks in the future and, as a result, decide to create a soft law instrument around that effective business practice. Furthermore, soft law instruments could also guide broader efforts in protecting critical infrastructure from cyberterrorist attacks, since these protections would not only guard states from terrorist attacks but also from intrusions and other interferences committed by state actors such as militaries and intelligence agents.[104]

The soft law sources most relevant to the international counter-terrorism strategy are namely the various non-binding UN General Assembly and Security Council resolutions, UN special mandates and procedures and certain other instruments such as general codes of practice and guidelines.[105] While most of these soft law instruments are regarded as being only supplementary to the formally binding sources, together they can have a significant influence in guiding the larger terrorism conversation, crystallizing the counter-terrorism response, providing dynamic solutions from various professional fields and filling some of the legislative holes that are still left open by the plethora of binding sources of international law both now and in the future in accordance with the further development of various types of advanced technologies. Additionally, the longer the deadlock regarding the definition of terrorism goes on, the more influential the various, more easily agreed-upon soft law instruments could become in defining acts of cyberterrorism and conventional terrorism.

When addressing the influence and legal significance of the various sectoral counter-terrorism conventions, one must also take into account the general principles of treaty making such as the doctrine on reservations. Under the 1969 Vienna Convention on the Law of Treaties, states may "opt-out" of a part of a treaty's obligations through the entering of a reservation[106], although these exceptions are subject to certain restrictions listed in Article 19 of the Vienna Convention. Reservations have also been utilized in counter-terrorism treaties, an example of which are the reservations entered by several states to the 1979 International Convention against the Taking

[103] *Ibid*.
[104] *Supra* Fidler (2016) 483.
[105] *Id.*
[106] Articles 2(d) and 34 of the 1969 Vienna Convention on the Law of Treaties.

of Hostages. In that particular case, states such as China and India did not accept the compulsory jurisdiction or adjudication of the International Court of Justice regarding the interpretation of implementing provisions between states.[107]

Although reservations are but a small part of the larger framework of counter-terrorism legislation, they could potentially bring a certain degree of flexibility into the negotiations by enabling the states to reject certain non-essential parts of a comprehensive counter-terrorism treaty, thus potentially leading to the acceptance, for example, of a compromise treaty that finally includes a clear definition of cyberterrorism. However, I am not very optimistic about this possibility, since the most fundamental issues preventing the adoption of a comprehensive counter-terrorism treaty such as the disagreements over the exact definition of terrorism are so deeply intertwined with international and regional politics that any practical attempt at a compromise over these issues would most likely lead to either an ineffectively narrow treaty or one rendered useless by the sheer amount of reservations made to it by the contracting states.

My pessimism regarding this approach stems from both the length of the deadlock over the Draft Comprehensive Convention and the reasons behind it. As I have expressed above, I believe that the adopting of the IOC's wording is essential in order to ensure the right of peoples to self-determination, whereas the majority of negotiating states are not prepared to accept this approach. The substantial length of the negotiations further demonstrates the parties' apparent inability to come to an agreement over this fundamental issue. The field of international counter-terrorism has also always involved certain clearly political elements, but I believe that those elements have reached an entirely new level in the 21st century after the 9/11 attacks. This, combined with the rise of – explicitly or implicitly – islamophobic political movements in several Western states, has made it nearly impossible to envision the universal or even broad adopting of a comprehensive counter-terrorism treaty in the near future. Various regional treaties could eventually provide a way to handle current and future terrorist threats at least within regions, although the differences between the regulations of different regions could cause many of the same complicated issues that the sectoral treaties have tried to address.

[107] UN Treaty Series Vol. 1704 (China), document available at <https://treaties.un.org/doc/Publication/UNTS/Volume%201704/volume-1704-A-21931-English.pdf> accessed 9 December 2020 and UN Treaty Series Vol. 1821 (India), document available at <https://treaties.un.org/doc/Publication/UNTS/Volume%201821/volume-1821-A-21931-English.pdf> accessed 9 December 2020.

4 CUSTOMARY INTERNATIONAL LAW AND TERRORISM

4.1 CUSTOMARY LAW AND INTERNATIONAL CRIMINAL LAW

The dominant role of the UN Charter and of the large collection of various multilateral treaties which includes the 19 UN sectoral treaties and specific parts of international human rights law, international refugee law and international humanitarian law shows that the field of international counter-terrorism (and cyberterrorism) regulation is strongly guided through the primary source of international law, international treaties. However, despite their strong legislative and political role, these treaties are not the only relevant source of international law in the area of counter-terrorism.

An interesting discussion around the issue of counter-terrorism is currently being had around another primary source of international law; custom. There is some debate about whether a definition of terrorism already exists under customary international law, which would effectively solve the issue that has plagued this legislative sector for far too long, since customary international law and international conventions are – in addition to the general principles of law – separately but equally authoritative, primary sources of international law.[108] As a result, the customary international law definition could become the authoritative definition of terrorism at least until the international community can come to an agreement on how the definition should ultimately be formulated in a comprehensive, multilateral treaty. An additional question in the field of cyberterrorism is whether the potential customary law definition of terrorism could also be analogically applied to acts of terror in cyberspace.

Before considering whether the specific crime of terrorism has effectively become binding international law, it is necessary to consider the general legal mechanism through which a certain behavior or certain acts transform into international crimes under customary international law. According to Art. 38(1)(b) of the Statute of the ICJ, binding customary law is "a general practice accepted as law".[109] This, on its face, quite vague definition has been accepted over the years to generally encompass two somewhat separate but equally important elements: 1) a general practice of states performed under 2) a sufficiently broad recognition by the international community that the practice in question is binding as law (*opinio juris*). The

[108] Judgment of 27 June 1986 of the ICJ in the case of Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).
[109] For perhaps the most well-known judgment regarding the creation of a binding rule of customary law see *North Sea Continental Shelf (Federal Republic of Germany v Denmark) (Merits)* [1969] ICJ Rep 3 [77].

acceptance of the behavior's binding nature (*opinio juris*) can be derived from various different sources, the most notable of which include statements made by representatives of a state, the decisions of high courts and – under certain circumstances – UN General Assembly resolutions[110]. Related to the connection between the two elements of customary law, there is also some debate about whether state practice is in itself a distinct requirement or merely evidence of an already existing *opinio juris*.[111]

Utilizing the votes given by states on a UN resolution to infer their opinion on the bindingness of the practice voted on in that resolution can seem very useful, since all member states take part in the voting process. However, a state's vote on a UN resolution is often influenced by various political considerations and thus should not be lightly interpreted as the state's official opinion regarding the international legal status of the subject of the vote. Due to the numerous biases and power dynamics of international law and global politics, I am generally wary of accepting UN resolutions as a basis for the formation of *opinio juris* and believe that it should only be allowed in cases where it is clear from the context of the vote that the voting state intended to also express its legal opinion on the issue. This "clear context" would be strengthened by earlier, extensive legislation, a sufficient amount of relevant decisions of high courts and/or precise and repeated statements from a diverse group of states regarding the conduct at hand.

I recognize that this approach further undermines the independent role of General Assembly resolutions in the formation of *opinio juris* but, in my opinion, this is justified in order to prevent – or at the very least limit – the undue influence of complex and often majority-driven (and West-centered) global politics in the creation of international law. This might generally be too limiting an approach to customary international law, since most issues of international law have a political element, but the stricter method that I have described above is essential at least on the most politically contentious issues of international law such as terrorism.

In addition to the general elements presented above, the creation of customary law is subject to certain unique requirements in the field of international criminal law. The principle of legality (*nullum crimen sine lege*)[112] is one of the most fundamental rules of criminal law and it plays an equally vital role in international criminal law. This principle includes three requirements

[110] *Nicaragua Case* (1986) ICJ 14, [188].
[111] Kai Ambos and Anina Timmermann, "Terrorism and customary international law" in *supra* Saul (2020) 17.
[112] On the principle's evolution in international criminal law see, for example, Héctor Olásolo, "A Note on the Evolution of the Principle of Legality in International Criminal Law" (2007) 18(3–4) Criminal Law Forum 301.

that must be met before a rule of customary international law would create criminal responsibility: the behavior 1) "must be the object of a written (*lex scripta*) criminal prohibition 2) at the time of commission to be prosecuted afterwards (*lex praevia*)".[113] Additionally, 3) the content of the behavior must be clearly and unambiguously defined (*lex certa*). It is quite obvious that a rule of customary international law cannot fulfil the *lex scripta* requirement, but it is also very rare for a behavior to be of such an unambiguous nature that it could be considered *lex certa*. As a result, rules of customary international law cannot generally create criminal responsibility.[114] This does not mean, however, that customary law cannot have other effects in the field of international criminal law especially in conjunction with written international law.

4.2 CORE INTERNATIONAL CRIMES AND TREATY-BASED CRIMES

Before inspecting the specific issues of terrorism and cyberterrorism in customary international law, one additional factor of international criminal law must be considered, namely the separation of treaty-based crimes and core international crimes (international crimes *stricto sensu*).[115] Included in the more limited set of core international crimes are most clearly the acts described in Articles 5–8 of the ICC Statute such as genocide[116] and crimes against humanity[117], whereas the already mentioned various sectoral counter-terrorism conventions are relevant examples of the international community agreeing to create new treaty-based crimes to handle emerging or heightened harmful acts.

As has been briefly described regarding the sectoral counter-terrorism treaties in Chapter 2 of this thesis, the central aims and legal effects of conventions creating new treaty-based crimes are the domestic criminalization of the behavior described in treaty and the establishing of domestic jurisdiction[118] related to that specific crime. This domestic-centered approach is – at least by itself – of limited use in solving the remaining issues of the current counter-terrorism framework, since it may often run into complicated additional questions related to jurisdiction. Another defect of this legislative approach is the fact that since only states as subjects of public international law can directly violate the treaty under international law, individuals are not

[113] See, for example, Robert Cryer, "Introduction: What is international criminal law?" in Cryer et al. (eds), *An Introduction to International Criminal Law and Procedure* (CUP 2019) 18 and M. Cherif Bassiouni, *Introduction to International Criminal Law* (2nd edn, Martinus Nijhoff Publishers 2012) 246–247.
[114] *Supra* Saul (2020) 18.
[115] *Supra* Cryer (2019) 4–5; Paola Gaeta, *International criminalization of prohibited conduct* in Antonio Cassese (ed), *The Oxford Companion to International Criminal Justice* (OUP, 2009) 63, 69.
[116] Article 6 of the Rome Statute of the International Criminal Court (hereinafter the ICC Statute)
[117] Article 7 of the ICC Statute.
[118] Robert Cryer, "Transnational crimes, terrorism and torture" in *supra* Cryer (2019) 319–320.

subject to any criminal liability for the crime described in the treaty if the state in whose territory the crime is committed has not yet fulfilled its obligation to nationally criminalize the behavior.[119] Neither the jurisdictional nor liability problems exist as regards core international crimes, since the creation of a core international crime automatically creates both global, individual criminal liability – and the crime is thus directly binding on individuals – and universal jurisdiction.[120]

Based on the interconnected relationship between treaty-based and core international crimes described above, customary international law can "either directly provide for true [i.e. core] international crimes or form the basis for or modify treaty-based crimes" (brackets and clarification added).[121] Customary international law may also cause the transformation of a treaty-based crime into a core international crime. Given the significance – in this context – of whether certain behavior is considered a crime under international law, it is quite surprising that no broadly accepted set of requirements have yet been formally agreed to. However, at least a few general conditions can be jointly derived from the *Tadić* decision of the International Criminal Tribunal for the former Yugoslavia[122] and relevant academic literature.[123] When applied to customary law, the conditions can be described as follows: 1) the behavior in question must be prohibited under an unambiguous and universally agreed upon definition, 2) breaching the prohibition in question is considered a grave "violation of universal values" and causes wide concern in the global arena, and 3) the prohibition is directly binding on individuals and has universal jurisdiction.[124]

The criteria required for a conduct to be transformed into a core[125] international crime through customary law might appear excessively narrow and unnecessarily difficult to meet, but it must be remembered that when a conduct becomes an international crime *stricto sensu*, it possesses instant individual criminal liability as well as universal jurisdiction. These two global legal consequences are enormously powerful in practice, since the international prosecution and conviction of even some of the most reprehensible and widely condemned acts can often run

[119] *Supra* Saul (2020) 19.
[120] *Supra* Cryer (2019) 7–8.
[121] *Supra* Saul (2020) 20.
[122] International Criminal Tribunal for the former Yugoslavia, *Prosecutor v Tadić* (*Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*), IT-94–1 (2 October 1995) [94].
[123] For example, *supra* Cassese (2013) 20; *supra* Bassiouni (2013) 142–143.
[124] *Supra* Saul (2020) 21.
[125] The terms "core" and "true" international crimes can be misleading, since they would seem to imply that treaty-based crimes are somehow "untrue" or of limited importance. However, despite their linguistic weaknesses, the use of these terms is quite justified due to the two significant elements only included in these types of international crimes: individual criminal liability and universal jurisdiction.

into issues related to overlapping or unclear jurisdictions or the differences in the domestic laws of two or more states regarding the act's criminal liability.

However, the opportunity to globally prosecute individuals of core international crimes regardless of the potential conflicts between the domestic laws of several states related to jurisdiction or individual criminal liability, the status of *stricto sensu* crimes must be reserved for only the most morally unacceptable and indefensible actions that are also recognized as such across the globe. As a result, the process of creating a new core international crime should be as far removed from political considerations as possible, although this may not be entirely realistic given the complex political dynamics that have managed to infiltrate practically every major point of contention in international law. When debating the possible emergence or creation of a core international crime, it would appear that often the most politicized *stricto sensu* requirement is the one related to an unambiguous and universal definition – as has been the case in the field of counter-terrorism.

While the considerations related to specific definitions might, at times, seem bureaucratic and the differences between the words being debated may appear minute, these debates are of great significance as they can sometimes be the last barrier preventing the majority of the international community (and its various biases) from effectively overruling the will and interests of the global minority. This implicit, legal form of neoimperialism could manifest itself in the counter-terrorism sector through, for example, the acceptance of an overly broad definition of terrorism which could be applied analogically to acts in cyberspace, thus further exacerbating the extraordinary legal reach of the definition.

The hypothetical that I've posed here touches upon another issue related to the formation of a new *stricto sensu* crime, namely the issue of time. Since core international crimes are seen as offences that are unequivocally unacceptable regardless of time or place, their definition must also – at least on some level – account for future behaviors that might unintentionally fall inside the scope of the definition due to – for example – certain previously unforeseen technological advancements. While this problem applies to all crimes that have the potential to reach *stricto sensu* status, it is quite significant in the terrorism field in which the influence of cyberspace may transform our understanding of terrorism and its many potential forms even in the next few decades. Considering the extraordinary legal status of core international crimes and the complex political considerations related to it, it is not surprising that only the crimes described in Articles

5–8 of the ICC Statute are generally considered to meet the strict criteria of a *stricto sensu* crime[126], although some[127] scholars disagree.

4.3 CURRENT CUSTOMARY LAW AND THE AYYASH ET AL. CASE

One of the most significant – and controversial – cases concerning the potential status of terrorism as a crime under customary international law comes from the Appeal Chamber (hereinafter Chamber) of the Special Tribunal for Lebanon (hereinafter Tribunal) as part of its judgment concerning the assassination of Rafik Hariri, the former Prime Minister of Lebanon.[128] While the definition of terrorism in general and its legal effects could have been addressed under Lebanese law by the Chamber in relation to the crime at hand, the decision's consequential and broader effect stems from the fact that the court effectively took it upon itself to consider the issue more thoroughly through an international law perspective after the pre-trial judge formulated and confirmed a specific question related to it under an interlocutory procedure.[129]

As a prologue to the discussion regarding the Chamber's actual decision, it is worth reflecting on the – in and of themselves quite dubious – procedural mechanisms that led to the Chamber's legal deliberations around the definition of terrorism under customary international law. The Special Tribunal for Lebanon was established in 2007 under a Security Council Resolution which granted the Tribunal, under its Statute, jurisdiction over the assassination of Hariri and cases connected to it.[130] The Statute of the Tribunal (hereinafter Statute) specifically states that the Special Tribunal's jurisdiction as regards the crime of terrorism is solely based on and limited by the Lebanese Criminal Code[131] despite earlier "suggestions" advocating for the application of international criminal law.[132] The Chamber's debate and eventual decision regarding the international crime of terrorism preceded the actual trial of the case and were done under a rule of procedure that was not included in the original Statute but was instead added to

[126] *Supra* Cryer (2019) 4; Paola Gaeta (ed), *The UN Genocide Convention: A Commentary* (OUP 2009) 66–68.
[127] For example, *supra* Cassese (2013) 21. Cassese advocates for a longer list that would also include torture and international terrorism.
[128] The *Ayyash et al. Case* (STL-11-01).
[129] Rule 68(G) of the Tribunal's *Rules of Procedure and Evidence* (STL/BD/2009/01/Rev. 6). Compare to the Tribunal's *Order on Preliminary Questions Addressed to the Judges of the Appeals Chamber Pursuant to Rule 68, Paragraph (G) of the Rules of Procedure and Evidence*, 21 January 2011 (STL-11-01-/I/AC/R176bis).
[130] UN Security Council Resolution 1757 (30 May 2007) and Statute of the Special Tribunal for Lebanon, attachment to UN Security Council Resolution 1757 (30 May 2007), Art 1. The Resolution was based on an unratified agreement negotiated on the issue between the UN and the government of Lebanon.
[131] Statute Art 2(a).
[132] Guénaël Mettraux, "The United Nations Special Tribunal for Lebanon: defining international terrorism" in *supra* Saul (2020) 588.

it as part of an amendment by the Tribunal. The new procedure granted the pre-trial judge the right to submit to the Chamber preliminary questions regarding, inter alia, the applicable law.[133] What makes this a peculiar part of the process is that the procedure in question is foreign to other international criminal tribunals.[134] This type of "law-making", even in procedural matters, can – quite justifiably – raise questions about the legitimacy of the legal process itself, especially when it is seemingly driven by the court's intent to take a more active role in defining and guiding the object of the trial.

Under the amended process, one of the fifteen preliminary questions submitted to the Chamber by the pre-trial judge was related to issue of whether an international definition of terrorism already existed and, if this was in fact the case, how it should be applied.[135] In a bizarre move that appears to – at least to a certain extent – violate the defendants' right to a fair trial, the Chamber then requested the Prosecutor's and Head of the Defence Office's written opinions regarding the questions, but the Chamber did not extend this request to the defendants' representatives, thus effectively blocking them from participating in this part of the process. Additionally, the parties did not have a right to appeal the questions put forward by the pre-trial judge. It certainly seems, as Mettraux – a counsel of the Defence Office – has argued, that the introduction of the specific questions and the related procedure were mainly designed to create room for additional "judicial activity" and to firmly establish the "legal and judicial" framework within which the Chamber would be allowed to operate.[136]

In addition to amending the actual procedural rules, the Tribunal also largely rejected both the Prosecution and the Defence Office's views on the state of a universal definition of terrorism in customary international law, since the parties generally agreed that such a definition had not been clarified under prevailing customary law. The parties also argued that any definition of terrorism that would be applied to the Tribunal's proceedings should be derived solely from Lebanese criminal law, completely detached from customary international law – as was originally laid down in the Tribunal's own Statute.[137]

---

[133] *Order on Preliminary Questions Addressed to the Judges of the Appeals Chamber Pursuant to Rule 68, Paragraph (G) of the Rules of Procedure and Evidence*, 21 January 2011 (STL-11-01-/I/AC/R176bis) [2].
[134] *Supra* Saul (2020) 590.
[135] *Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging* (hereinafter "Decision"), STL-11-01/I/AC/R176bis, 16 February 2011, 1 (Headnote: first question).
[136] *Supra* Saul (2020) 589–590.
[137] *Defence Office's Submissions Pursuant to Rule 176 bis (B)* (hereinafter "Defence's Submission"), 31 January 2011 (STL-11–01/I) [75–141]; *Prosecutor's Brief Filed Pursuant to the President's Order of 21 January 2011 Responding to the Questions Submitted by the Pre-Trial Judge (Rule 176 bis)* (hereinafter "Prosecutor's Submission"), 31 January 2011 (STL-11–01/I) [14] *et seq*.

The Prosecutor led the comprehensive considerations by noting that all previous attempts to "establish a universal definition of 'terrorism'" had failed and that Lebanese criminal law was not vague enough to require the application of international law.[138] The Defence Office agreed with the Prosecutor's arguments and referred to both state practice and the practice of international organizations to demonstrate the absence of a universal definition.[139] The Prosecutor also underlined that if a gap existed in the definitions of the relevant crimes under Lebanese law, the Tribunal could fill it "by relying on, *inter alia*, general rules and principles of Lebanese criminal law and Lebanese case law"[140]. While the prosecution and defense of a criminal case may quite frequently find common ground on certain, minor elements of an offence or of the legal process itself, it is much rarer to encounter a situation in which both parties[141] are in complete agreement over a procedural factor as significant as that of the body of law that should be applied to the case.

The Chamber disagreed wholeheartedly with both sides' arguments and instead made the claim that while the Tribunal could not base the definition of terrorism directly on international law, it could nevertheless use customary international law to interpret Lebanese criminal law.[142] Quite conveniently, the Chamber then stated that the use of customary law as an interpretative tool was necessary due to the ambiguous definition of terrorism in Lebanese criminal law.[143] These arguments were not supported by the Tribunal's Statute or prevailing Lebanese law. The Statute explicitly held that the Tribunal's rulings should be based on and interpreted under Lebanese law and that international law should not be used even in interpreting the relevant law. [144]

Furthermore, the Chamber's claim that Lebanese law was too ambiguous to be relied upon as such in the proceedings was apparently not supported by the Lebanese judiciary.[145] Accordingly, since the definition of terrorism under Lebanese law was already sufficiently unambiguous to be used in the present case, the Tribunal's insistence on applying customary

[138] Prosecutor's Submission [16–18] and [42].
[139] Defence's Submission [90–125].
[140] Prosecutor's Submission [6].
[141] I refer in this chapter to the Prosecutor and the Defence Office as the "parties" of this case, although it must be remembered that the actual defendants of the case were effectively left out of this preliminary part of the Tribunal's process and the Defence Office had to effectively represent the collect interests of each individual defendant.
[142] Decision [45].
[143] *Ibid* [46].
[144] *Supra* Saul (2020) 591.
[145] *Sabra Motion for Reconsideration of Rule 176bis Decision – 'International Terrorism'*, 13 June 2012 (STL-11–01/PT/AC) [14–17] and Defence's Submission [62] *et seq*.

international law to bridge a nonexistent interpretative gap appears quite odd. Strong arguments were also presented in favor of the claim that applying customary international law to resolve any potential definitional inconsistencies in Lebanese law was strongly discouraged or even prohibited under Lebanese criminal law. The Chamber's arguments justifying this unusual application of Lebanese law were also quite uncompelling.[146]

Mettraux has argued that, in bringing the definition of terrorism inside the scope of its competence, the Tribunal relied on "questionable legislative authority", ruled on significant normative questions "without a truly adversarial process", acted *ultra vires* in relation to the Tribunal's Statute and effectively misinterpreted Lebanese law for its own aims.[147] All of these dubious procedural abnormalities together may even cast doubt on the substantive decision of the court.[148] I wholly agree with his analysis, but I would also like to address another, perhaps even more unsettling characteristic of the Tribunal's approach to Lebanese criminal law, namely its neocolonialistic tone.

On a general note, various types of deliberations and the weighing of competing interests are at the heart of practically any judicial process in its different stages. The vast majority of these considerations are performed by a court under the independent judicial authority granted to it through another, normative authority. It is when these interpretations or deliberations reach outside the actual scope of the court's authority that issues arise, which become apparent in the case at hand. By seemingly overruling the commonly held practice of the Lebanese judicial branch, the Tribunal appears to effectively present the highly problematic view that it is better equipped to interpret Lebanese law than the Lebanese legal system itself. Despite the fact that the Tribunal would never expressly state it, I believe that the court's argument represents a form of legal neocolonialism[149] in which it replaces a legitimate, widely recognized domestic judicial authority with it its own and does so against both the convincing arguments of the parties to the case and – through the amendment procedure – the specific provisions of the Tribunal's Statute.

[146] Defence's Submission [67] and [70].
[147] *Supra* Saul (2020) 592.
[148] *Ibid*.
[149] Generally on neocolonialism in international criminal law see, for example, Res Schuerch, *The International Criminal Court at the Mercy of Powerful States*, (T.M.C. Asser Press, 2017).

As regards the actual decision, the Chamber concluded, basing its arguments on treaty law[150], UN resolutions[151] and the domestic legislations[152] and case law[153] of various states, that a customary rule of international law regarding terrorism already exists.[154] The Chamber begins its argument by stating that there is "a settled practice concerning the punishment of acts of terrorism" and that "this practice is evidence of a belief of States that the punishment of terrorism responds to a social necessity (*opinio necessitatis*) and is hence rendered obligatory by the existence of a rule requiring it (*opinio juris*)".[155] The Chamber then goes on to describe the obligations (and one right) that are imposed on both states and non-state actors under the customary rule. Firstly, the actors are obligated to refrain from performing terrorist acts. Secondly, they must "prevent and repress terrorism" and, particularly, prosecute and try alleged terrorist actors. Thirdly, they have a right to prosecute and repress terrorist acts that have been committed on their territory by either nationals or foreigners and third states must recognize and accept this right without objection, even if this right is being used against their nationals.[156]

The Chamber also argues that a sufficiently clear definition of terrorism, consisting of three elements, has already been established in customary law through treaty law and state practice. Going against the widely held stance of academia that no universally agreed definition of terrorism exists[157], the Chamber describes the three elements of terrorism under customary law as (1) the perpetration or threatening of a criminal act with (2) the intent to spread fear among the population *or* to directly or indirectly coerce a national or international authority to take some action or to refrain from taking it, and, finally, (3) the act must contain a transnational element.[158] As has been already noted above, the general reaction of the wider international legal community to the Chamber's holding and its supporting arguments was highly critical.[159]

[150] Decision [88–89].
[151] *Ibid* 92 and [110].
[152] *Ibid* 93–97.
[153] *Ibid* [99–100].
[154] *Ibid* [85], [102].
[155] *Ibid* [102].
[156] *Ibid* [102].
[157] *Ibid* footnote 127; *supra* Cryer (2019) 326–330; *supra* Cassese (2013) 146–158.
[158] Decision [85], [111].
[159] See, for example, Ben Saul, "Legislating from a radical Hague: The United Nations Special Tribunal for Lebanon invents an international crime of transnational terrorism" 24(3) Leiden Journal of International Law (2015) 677; Kai Ambos, "Judicial creativity at the Special Tribunal for Lebanon: Is there a crime of terrorism under international law" 24(3) Leiden Journal of International Law (2015) 655; Matthew Gillett and Matthias Schuster, "Fast-track justice: The Special Tribunal for Lebanon Defines Terrorism" 9(5) Journal of International Criminal Justice (2011) 989–1020. Cf, Manuel Ventura, "Terrorism according to the STL's Interlocutory Decision on the applicable law: A defining moment or a moment of defining?" 9 Journal of International Criminal Justice (2011) 1021.

The controversy related to the substantive decision of the Chamber does not revolve around the Chamber's acknowledgement of a customary rule of international law as regards the prohibition of terrorism and the obligations to prevent and repress terrorist acts, since these types of actions have already come to form an integral part of the global counter-terrorism response through the numerous sectoral, suppression-style counter-terrorism treaties. The Chamber, however, goes even further by confirming the existence of a core international crime of terrorism based on the *Tadić* criteria through the use of questionable legal methodology. Although the Chamber does admit that the process of transforming a customary law rule centered on outlawing and suppression into a true international crime cannot be automatic, it does not appear to fully follow its own advice on this point in its final decision.

First, the Chamber states that the "individual criminal responsibility" of an actor committing an international crime is already inherently included in the "individual criminal liability at the international level" portion of the *Tadić* requirements.[160] This argument, by itself, has been accused of nearly amounting to the level of circular logic, since it mixes an assumption with a conclusion[161]. The Chamber continues, stating that, according to *Tadić*, the intention to criminalize the prohibition of an act "must be evidenced by statements of government officials and international organizations" and by "punishment of such violations by national courts".[162] Then the Chamber states that demonstrating this intention and state practice is "relatively easy" and, contrasting counter-terrorism with the criminalization of war crimes, highlights the wide domestic criminalization of terrorism, the Security Council's strong public position against terrorist acts and the collection of international counter-terrorism treaties as evidence that the *Tadić* requirement has indeed been met in the case of terrorism.[163] Through its reasoning, the Chamber seems to also effectively merge the two separate requirements of customary international law, state practice and *opinio juris*, into one.[164] This is only one of the several instances in which the Chamber appears to either bend or amend the long-held principles and legal traditions of customary international law.

Based on this evidence, the Chamber concludes that terrorism "is an international crime classified as such by international law, including customary international law, and also involves

[160] *Ibid* [103].
[161] *Supra* Saul (2020) 22–23.
[162] Decision [103].
[163] Decision [103–104].
[164] *Supra* Saul (2020) 596 and its footnotes.

the criminal liability of individuals".[165] Interestingly, the Chamber adds that the states "still insisting on an exception for 'freedom fighters' --- could, at most, be considered persistent objectors".[166] This seemingly off-handed remark seems quite dismissive and even patronizing considering the effect of that exception and its importance to the states still advocating for it. It appears to also directly contradict several formal human rights agreements such as the 1977 Geneva Conventions Additional Protocol 1, which grants freedom fighters combatant and prisoner-of-war status. Adopting the Chamber's approach would also create additional complications regarding cyber-freedom fighters if the customary law definition supported by the Chamber was also applied to acts in cyberspace.[167]

The most central – and in my opinion, well justified – critiques of the decision relate to the Chamber's flawed interpretation of prevailing state practice, its selective use of sources and its methodological creativity in reaching a universal definition of terrorism.[168] I believe the latter of these issues to be the most problematic and perplexing. The Chamber reached a definition of terrorism under customary law by arguing that the common elements of the varied definitions found in numerous statutes effectively formed the accepted customary law definition of terrorism.[169] While this approach is useful in identifying the elements of terrorism that are widely recognized as forming the basis of practically all legislative definitions of terrorism, I believe that it can only be used in the law-creation process as a starting point for drafting future legislation and its application in the Chamber's particular context can lead to truly bizarre results.

The Chamber's argument regarding the common definition of terrorism unravels quite effortlessly when considered through a simplified hypothetical. Let us assume that we want to indicate the existence of a customary law definition for the crime of murder for which state A and state B's legislations offer differing definitions. In both states the crime's definition includes "the unlawful killing of a human being by another" but the additional elements of the crime are different. State A's definition requires premeditation while in state B performing the

[165] *Ibid* [110]. The Chamber also placed additional weight on the fact that the Security Council has described terrorism as a "threat to peace and security", while similar transnational crimes such as drug trafficking had not been denoted as such by the Security Council (*ibid* [104]).
[166] *Ibid*.
[167] For more on the issues regarding cyber-freedom fighters, see Chapter 4 of this paper regarding statehood and cyberterrorism.
[168] *Supra* Saul (2020) 592.
[169] For additional criticism of the general method applied by the Chamber see, for example, Martin Scheinin, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, E/CN.4/2006/98 (28 December 2005) [37–38] and [40–41].

killing in an "exceptionally cruel or unusual manner" is sufficient to meet the law's definition.[170] Following the Chamber's logic, the common core of the customary law crime of murder based on state A and B's criminal laws would consist solely of "the unlawful killing of a human being by another", since the additional elements of the crime are in dispute. This thought experiment demonstrates the absurdity of the Chamber's method, since its application to the given example would distort the actual definition of murder by effectively equating it with the crime of manslaughter which is universally understood to be a less severe act than murder.

As regards the issue of consistent and uniform state practice, the Chamber appeared to ignore case law that went against its broader argument in favor of highlighting and primarily relying on the specific precedents that appeared to confirm the existence of an accepted definition of terrorism.[171] Perhaps the most notable exclusion from the list of cases cited in the Chamber's decision was the, at the time, only judgment of an international court that had specifically addressed the definition of terrorism, *Prosecutor v Stanislav Galić*, in which the International Criminal Tribunal for the Former Yugoslavia held that "'terrorism' has never been singly defined under international law".[172] The Chamber's selective habit regarding its references was by no means purely limited to state practice. As has already been mentioned above, the Chamber's recognition of an already existing customary law definition of terrorism was not supported by the majority of the academic community of international law[173], although the Chamber's use of sources makes it quite difficult to recognize that its stance contradicts the

[170] I have used the crime of murder as an example because it is one of the most widely recognized and known multi-element crimes and I am aware that while there might be some variance in the elements of the definition between states, they most likely overlap much more comprehensively than I have indicated here.
[171] *Supra* Saul (2020) 593, especially footnote 21.
[172] *Prosecutor v Stanislav Galić (Trial Judgment)*, International Criminal Tribunal for the Former Yugoslavia (ICTY, Case no. IT-98-29-T, 5 December 2003) footnote 150.
[173] See, for example, Ben Saul, *Defining Terrorism in International Law* (OUP 2008) 270; *supra* Saul (2018), 677–700; M Cherif Bassiouni, International Terrorism: Multilateral Convention (Transnational Publishers 2001) 3, 8, 9, 15; Pierre-Marie Dupuy, "State sponsors of terrorism: International responsibility enforcing international law norms against terrorism", in Andrea Bianchi (ed), *Enforcing International Law Norms Against Terrorism* (Hart Publishing 2004); George Fletcher, "Responding to terrorism: The quest for a legal definition. The indefinable concept of terrorism" (2006) 4 Journal of International Criminal Law 894, 900; Marco Sassòli, "Terrorism and war" (2006) 4 Journal of International Criminal Law 960; William Schabas, "The Special Tribunal for Lebanon: Is a Tribunal of an international character equivalent to an international criminal court?" (2008) 21 Leiden Journal of International Law 513,520; Beth Van Schaak, "Crimen sine lege: judicial law-making at the intersection of law and morals" (2008) 97 Georgetown Law Journal 119, 191; Thomas Weigend, "The universal terrorist: The international community grappling with a definition" (2006) 4 Journal of International Criminal Law 912, 914–5; Marko Milanovic, "An odd couple – Domestic crimes and international responsibility in the Special Tribunal for Lebanon" (2007) 5 Journal of International Criminal Law 1139, 1141; Elizabeth Wilmshurst, "Transnational crimes, terrorism and torture" in Robert Cryer et al. (eds), *An Introduction to International Criminal Law and Procedure* (CUP 2010); Alex Schmid, "Terrorism: The definitional problem" (2004) 36 Case Western Reserve Journal of International Law 375; Yoram Dinstein, "Terrorism as an international crime" (1989) 19 Israel Yearbook on Human Rights 55.

majority of scholarly literature on the matter. What makes the Chamber's decision to effectively disregard the vast collection of authoritative sources even more interesting is the fact that one of the few prominent scholars that had taken a strong position in favor of the minority's view[174], Antonio Cassese, also acted as the presiding judge in the case. Although it is quite understandable that a scholar as notable in the field of international criminal law as Cassese would at least partly rely on their own writings while presiding over a case in an international criminal court, the referencing should be expressly and unequivocally justified, especially if the sources cited represent a minority's view on the issue, as was the case in the Chamber's decision.

In addition to the various, significant problems related to both the procedural and substantive elements of the Chamber's decision described above, by identifying terrorism as a true international crime that is directly binding on individuals, the Chamber, in my opinion, also overlooked the politically complex, substantive issues regarding the definition of terrorism and instead relied heavily on UN Resolutions that are most often – as has already been mentioned earlier – driven by highly political, underlying motives and do not necessarily reflect a state's true view on the legal aspect of the issue being voted on. Furthermore, the two General Assembly Declarations most relevant to the issue of terrorism, the "Declaration on Measures to Eliminate International Terrorism" of 9 December 1994[175] and the Supplementary Declaration of 17 December 1996[176], advocate for cooperation[177] and the extradite or prosecute principle[178] instead of the universal jurisdiction and prosecution approach described in the Chamber's decision. The extradite or prosecute principle is the approach also taken in the UN Comprehensive Convention described earlier in this thesis. All in all, the Chamber's unusual procedural mechanisms, limited reasoning and questionable use of legal methodology point to its eagerness to be the international body that finally resolves the issues related to the international crime of terrorism, but the gaps in its legal deduction of the existence of a universal criminalization and its limited analysis of the definition of terrorism result in an unconvincing

[174] For his views on the issue see, for example, Antonio Cassese, International Criminal Law (2nd edn, OUP, 2008) 162–78; Antonio Cassese, 'Terrorism as an international crime', in Andrea Bianchi (ed), Enforcing International Law Norms Against Terrorism (Hart Publishing, 2004).
[175] Declaration on Measures to Eliminate International Terrorism of 9 December 1994, Annex to UN General Assembly Res 49/60 (9 December 1994).
[176] Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, Annex to UN General Assembly Res 51/210 (17 December 1996).
[177] Declaration on Measures to Eliminate International Terrorism of 9 December 1994, Annex to UN General Assembly Res 49/60 (9 December 1994). [6–8].
[178] Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, Annex to UN General Assembly Res 51/210 (17 December 1996) [5].

and overly simplified definition of terrorism. These issues are heightened by the fact that specifically Cassese was appointed as the President of the Tribunal.[179]

In conclusion, it appears that only one of the three *Tadić* requirements is fully met in the case of terrorism. Although terrorism clearly affects important universal values (second requirement), it does not have an unambiguous definition (first requirement) in international law nor is it subject to universal jurisdiction (third requirement). While I admit that a certain, elemental definition of terrorism does already exist[180], the parts of the definition still under debate are so significant in relation to the right of states to self-determination that I cannot agree that an unambiguous, global definition of terrorism exists at the moment.[181] Moreover, as has been demonstrated above, the requirement of universal jurisdiction is even further from being fulfilled, which makes the emergence of a core international crime of terrorism under customary law unlikely at least in the near future. However, the importance of the Chamber's decision should not be underestimated, either, since the decision could effectively pave the way towards a wider acceptance of the Chamber's approach regardless of the fact that I would find that development problematic.[182]

[179] The Permanent Mission of Italy to the U.N., "Antonio Cassese appointed as President of Special Tribunal for Lebanon <https://italyun.esteri.it/rappresentanza_onu/en/comunicazione/archivio-news/2009-03-24-cassese.html> accessed 28 April 2021.

[180] For example, the undisputed parts of the definition described in the Draft Comprehensive Convention.

[181] Compare, for example, *supra* Saul (2020) 27–30, in which Ambos and Timmermann argue that only the third *Tadić* requirement remains unfulfilled.

[182] The broader international legal community seems to have agreed with me on this point, since the Chamber's decision has seemingly been viewed as merely a singular case instead of as a strong precedence reflecting the current consensus in international law. See, for example, Commission on Human Rights, 27 February 2018, A/HRC/37/52, Promotion and Protection of Human Rights – Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism [2]; Commission on Human Rights, 21 February 2017, A/HRC/34/61, Promotion and Protection of Human Rights – Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism.

5 STATEHOOD IN THE COUNTER-TERRORISM FIELD AND CERTAIN POLITICAL ASPECTS OF COUNTER-TERRORISM

In drafting and adopting counter-terrorism legislation, states must also take into account the fundamental doctrine of state sovereignty and the various Charter articles and other treaties regarding human rights and fundamental freedoms.[183] As has been mentioned earlier in this paper, certain governments have come under criticism for enacting domestic terrorism laws that limit the fundamental rights of their citizens through overreaching definitions of terrorism. It is feared that these broad definitions of terrorism could effectively allow the characterization and subsequent prosecution of various types of legitimate political activities as acts of terrorism. This development would enable these governments to utilize domestic terrorism legislation as a tool for suppressing political opposition and other forms of legitimate expression while simultaneously appearing as a mere enforcer of the democratically adopted domestic laws of that state.

The issues regarding state or state-sponsored terrorism have already been mentioned above, but that very debate is tangentially connected to yet another fundamental doctrine of international law, the creation and recognition of statehood. This is because the legal classification of the actor can affect the actual determination and legal consequences of the harmful act itself. If an apparent act of cyberterrorism is determined to have been committed by a state, the state can generally try and justify its actions under the *jus ad bellum* or *jus in bello* frameworks, for example, by arguing that it acted in "self-defense" by preventing a potential terrorist attack.[184] Many of these legal instruments and their significant political and legal protections are not, however, available to non-state actors committing similar acts.

The on-off approach in the terrorism field described above creates a situation where the primary focus of international law appears to be on determining the legal effects of a terrorist act through the classification of the perpetrator as guided by international law. As a consequence, the harmfulness of an act (from a legal standpoint) seems to mainly turn on the nature of the perpetrator instead of the concrete elements or scale of the act itself. The question regarding the creation and recognition of statehood is one of the most contentious and politically sensitive topics of international law.[185] One of the most significant examples related to the recognition

[183] Inter alia, Articles 1(3), 55 and 56 of the UN Charter.
[184] On the issue in connection to Israeli activities see, eg, Christine Gray, *International Law and the Use of Force* (OUP 2000) 116.
[185] See, for example, *supra* Crawford (2019), 117–133.

of statehood is the ongoing situation between Israel and Palestine. The two parties have not been able to reach an agreement on how to achieve the originally envisioned goal of a two-state solution despite the fact that, as of July 1st of 2018, some 137 states had recognized Palestine as a state.[186]

The issue of statehood ties into terrorism legislation especially through the *jus in bello* norms of international law. Under the 1977 Geneva Conventions Additional Protocol 1, freedom fighters that are "fighting against colonial domination, alien occupation or racist regimes in the exercise of their right of self-determination" are guaranteed combatant and prisoner-of-war status. In cyberspace these actors would include, for example, the group known as the Islamic Jihad, who have committed minor cyber attacks with the ultimate goal of liberating Palestine. It is possible to classify these groups as cyber-freedom-fighters under current humanitarian law, whereas they could be viewed as cyberterrorists under the western proposal of the Draft Comprehensive Convention. This categorical rejection of cyber-freedom-fighter status under the western Draft proposal further demonstrates the North-South divide of international law and the Northern bias of this proposed piece of legislation, since the already established Northern states might benefit from narrowing the scope of "legal" freedom fighters under international law, whilst a Southern state or movement fighting for its freedom under their right to self-determination would be interpreted as perpetrating acts of terrorism in cyberspace.[187]

Regardless of the fact that the aforementioned groups could nevertheless be classified as cyber-freedom-fighters under international humanitarian law, various aspects of the western approach are highly problematic. The sole act of adopting the western proposal of the Draft Convention would "create" more cyber terrorists as groups such as the Islamic Jihad could instantly be classified as such under the Convention. Furthermore, this broadening of the legal definition of cyberterrorism under international law could lead to the adopting of stricter domestic counter-

[186] *Supra* Crawford (2019) 128–129.

[187] The "North-South divide" of international law is understood in this context as the differences in the practice and application of international law between the "developed" states of the Global North (e.g. The United States, France and the United Kingdom) and the "developing" states of the Global South such as various African and Latin American states. For a general analysis of the North and South divide regarding international environmental, humanitarian and human rights law see, for example, Abdul Hamid Kwarteng & Thomas P. Botchway, "The North and South Divide in the Practice and Application of International Law: A Humanitarian and Human Right Law Perspective" (2018) 11 Journal of Politics and Law 79.

terrorism measures perhaps even mirroring those enacted by the United States in the aftermath of 9/11.[188]

While the explicit and implicit biases of international law such as the North-South divide can – and often do – negatively guide and influence the international regulatory response to terrorism, leaving more space for the states to pass their own, potentially further-reaching counter-terrorism regulations could enable even more severe human rights abuses at the domestic level. It is also quite safe to assume that it would become a lot easier for a domestic legislator to politically justify broader national counter-terrorism measures to his/her constituents if the targets of the legislation were already categorized as cyber terrorists instead of as freedom fighters under a multilateral treaty as a result of the adoption of the western proposal of the Draft Convention.

As Di Filippo has noted, the "language of terrorism" is often used by national legislators to both highlight the reprehensibility of certain types of violent acts and to "justify the application of a special regime".[189] This "special regime" is generally focused on criminal law in the form of, inter alia, harsher penalties and accelerated court procedures, but domestic counter-terrorism legislation can branch onto several other sectors of regulation such as administrative procedures, surveillance and immigration law. It is important to recognize that the two effects highlighted by Di Filippo are tightly connected as politicians frequently utilize the shock value of earlier, particularly terrifying acts of terrorism or the supposedly grave threat of subsequent attacks to justify the adoption of distinct rules regarding terrorism.

The actual and perceived threat of both traditional and cyberterrorist attacks is considered more closely in Chapter 5 of this thesis, but it nevertheless bears reminding even in this chapter's context that the justifications given for the drafting and adopting of ever-stricter counter-terrorism regulations are often driven by various formulations of the type of "Us vs. Them"

[188] One of the most glaring human rights abuses justified by the United States as part of its counter-terrorism strategy is the practically indefinite detention, likely torture and denying of due process practiced at the detainee center of Guantánamo Bay. For an overview of the human rights abuses of Guantánamo see, for example, Amnesty International, "Guantánamo A Decade of Damage to Human Rights" (December 2011), available at https://www.amnestyusa.org/reports/guantanamo-a-decade-of-damage-to-human-rights/ accessed 26 February 2021. For a brief comparative analysis of the isolationist approach of the United States legal system as regards Guantánamo see, for example, Johan, Steyn, "Guantanamo Bay: The Legal Black Hole" (2004) 53(1) The International and Comparative Law Quarterly 1, available at https://www.jstor.org/stable/3663134 accessed 26 February 2021. For an example of some of the human rights issues regarding counter-terrorism in certain other states see, for example, Report of the Committee against Torture, U.N. Doc. A/59/44 (2004), paras. 67, 126 and 144.

[189] Marcello di Filippo, "The definition(s) of terrorism in international law" in *supra* Saul (2020) 3.

mentality briefly described above. The prevalence of these harmful mindsets is most visible in domestic settings in the language used by – mostly right-wing – politicians in supporting stricter regulations. However, these attitudes can also indirectly become part of a broader counter-terrorism response if, for example, these same politicians used their voices in the European Parliament to aid the passage of a new piece of EU legislation.

The very same politicians that act as legislators to pass, often questionable, domestic counter-terrorism laws also commonly use the label of terrorism in a slightly different context, i.e., in a more politically exclusionary sense of the word. This is a hugely powerful political tool which is reflected in the fact that merely labeling certain groups as terrorists or certain acts – regardless of their wider context – as terrorism allows the "designator" to immediately suppress any further debate about the broader issues related to the behavior such as the motive (for instance, the liberation of an area or people) and aims of the act. All of the additional factors and elements of the act are, of course, highly relevant from a legal standpoint, since only certain, carefully defined behaviors can be justifiably characterized as terrorism. However, this does not prevent politicians and other actors from deliberately broadening the scope of terrorism in public discourse and even through official designations.

A perplexing example of the mental gymnastics described above concerns the organization known as the People's Mujahedin of Iran (MEK) which the George W. Bush administration still labeled a terrorist group in 2002 in a public document regarding "Saddam Hussein's Support for International Terrorism".[190] The EU removed the group from its official list of terrorist organizations in 2009[191] after the Council's earlier decisions were annulled[192] by the EU Court of First Instance and even the U.S. followed suit in 2012.[193] This quite a rapid change of mind by the U.S. is surprising considering the fact that some reports at the time of the delisting claimed that the Mujahedin had, in an attack (allegedly) orchestrated with Israel,

[190] The White House of George W. Bush, "Saddam Hussein's Support for International Terrorism" in "A Decade of Deception and Defiance" (12 September 2002), White House Background Paper on Iraq. Available at <https://2001-2009.state.gov/p/nea/rls/13456.htm> accessed 11 March 2021.
[191] 2009/62/EC: Council Decision of 26 January 2009 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing Decision 2008/583/EC.
[192] European Commission, "The Court annuls, for the third time, a Council decision freezing the funds of the People's Mojahedin Organization of Iran", press release (4 December 2008) <https://ec.europa.eu/commission/presscorner/detail/en/CJE_08_84> accessed 29 April 2021.
[193] U.S. Department of State, "Delisting of the Mujahedin-e Khalq", press release (28 September 2012) <https://2009-2017.state.gov/r/pa/prs/ps/2012/09/198443.htm> accessed 11 March 2021.

assassinated Iranian scientists.[194] This turn appeared even more questionable once it became clear that several prominent U.S. politicians had received campaign contributions from the MEK and accepted payments from it to hold speeches in favor of the organization's delisting.[195]

Although it might be difficult to ethically explain why these officials had accepted money from a literal terrorist group, the picture becomes much clearer when considered from the perspective of broader U.S. foreign policy. In the beginning of the 21st century, the MEK was, according to the U.S. government, supported by the regime of Saddam Hussein, the primary target of hostile U.S. foreign policy at the time. After the U.S. turned its focus from Iraq to Iran, it saw – and took – the opportunity to use the Mujahedin as a tool in its fight against Iran.[196] These developments point to the unfortunate fact that the MEK's lobbying efforts to delist it were eventually successful not because it had ceased to commit violent acts but instead due to its strong opposition of the Iranian government. It would also appear that the U.S. is ready to lend its support to even potentially hostile groups of freedom fighters but only if they happen to simultaneously promote the broader U.S. foreign policy agenda.[197]

I have not included the above example in order to criticize the delisting of the MEK, since I believe that the organization has demonstrated a stronger commitment to peaceful forms of opposition in recent years and does not necessarily deserve to be on terrorist blacklists. Instead, my criticism is aimed at the U.S. government and its tendency to suppress complex debates regarding the governments of other states by quickly labeling large opposition groups as terrorists only to turn around and praise them as freedom fighters when it fits its own political aims. This is a clear demonstration of the difficulties and political considerations inherent in the "freedom fighter or terrorist" dilemma. The U.S.'s approach is highly problematic from the perspectives of both international law and global politics, but it is also quite ironic when it could be argued that the people fighting on behalf of American independence in the Revolutionary

[194] Kevin Jon Heller, "NBC: Israel and MEK Responsible for Murdering Iranian Scientists", Opinio Juris (2 February 2012) <http://opiniojuris.org/2012/02/11/nbc-israel-and-mek-responsible-for-murdering-iranian-scientists/> accessed 11 March 2021. The original NBC article is unfortunately no longer available.
[195] Chris McGreal, "MEK decision: multimillion-dollar campaign led to removal from terror list", The Guardian (21 September 2012) <https://www.theguardian.com/world/2012/sep/21/iran-mek-group-removed-us-terrorism-list> accessed 11 March 2021; Elizabeth Rubin, "An Iranian Cult and Its American Friends, The New York Times (13 August 2011) <https://www.nytimes.com/2011/08/14/opinion/sunday/an-iranian-cult-and-its-american-friends.html?pagewanted=all> accessed 11 March 2021.
[196] Arron Merat, "Terrorists, cultists – or champions of Iranian democracy? The wild story of the MEK", The Guardian (9 November 2018), <https://www.theguardian.com/news/2018/nov/09/mek-iran-revolution-regime-trump-rajavi> accessed 12 March 2021.
[197] For a good example of the U.S.'s support of various types of dangerous paramilitary groups especially in Latin America during the Ronald Reagan administration and regarding some of the more recent involvements in states such as Iran see Noam Chomsky, *Culture of Terrorism* (2nd edn, Pluto Press 2015).

War may have also been labeled terrorists under recent U.S. foreign policy. [198] All in all, this underlines one of the many politicized aspects of the international counter-terrorism response. It is vital to understand that while clear terrorist acts must be condemned, labeling an entire group of dissidents as terrorists – often with little to no direct evidence – drowns out even the peaceful and legitimate actions of these organizations and the cultural, social, economic and political grievances driving them.

In recent years, one of the most controversial sectors of national counter-terrorism legislation has been the field of government surveillance particularly in the U.S. after the adoption of the "Patriot Act" in 2001 as a response to the 9/11 attacks.[199] International counter-terrorism regulation and international law in general is often based on and guided by harmful biases, stereotypes and political motives but the Patriot Act has demonstrated that domestic legislative solutions can lead to even more harmful effects on individual rights than multilateral regulation even in a state such as the U.S. that prides itself on ensuring broad individual freedom to its citizens.

Thus, I believe that, regardless of the inherent biases of international regulation, it is significantly easier and more effective to try and recognize and solve the broader issues of international counter-terrorism regulation than trying to coordinate and enforce an endless collection of the more or less unique counter-terrorism laws of each state. However, this viewpoint is not aimed at providing an answer to the age-old question of which types of multinational regulation are most effective at achieving the foundational goals of counter-terrorism, but instead merely advocates for the benefits of a truly global or at least multilateral approach to cyberterrorism regulation over a primarily domestic-based one. While the political and dynamic nature of terrorism and of cyberterrorism in particular means that certain elements of cyberterrorism are bound to require domestic legislation, the core of the cyberterrorism framework should be formed at the multinational level.

---

[198] John J Tierney Jr, "Terror at Home: The American Revolution and Irregular Warfare" (1977) 12 Stanford Journal of International Studies 1.

[199] H.R. 3162 and its subsequent modifications. The last provisions of the Patriot Act that were still in effect at the time expired in 2020 but several similar surveillance laws remain in force, many of which are not only problematic from a right to privacy perspective but also mostly ineffective at producing unique information, see, for example, Andrew Crocker and Cindy Cohn, "Don't Worry, the Government Still Has Plenty of Surveillance Power If Section 215 Sunsets", Electronic Frontier Foundation (31 May 2015) <https://www.eff.org/deeplinks/2015/05/dont-worry-government-still-has-plenty-surveillance-power-if-section-215-sunsets> accessed 28 February 2021, India McKinney, "Reform or Expire", Electronic Frontier Foundation (26 February 2020) <https://www.eff.org/deeplinks/2020/02/reform-or-expire> accessed 28 February 2021 and Charlie Savage, "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads", The New York Times (25 February 2020) <https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html> accessed 28 February 2021.

Furthermore, the complex field of international counter-terrorism regulation presents a rejection of the traditional distinction between dualism and monism in international law.[200] The basic premise of dualism, the independent and distinct influence and status of national and international law, is effectively refuted by the numerous overlapping domestic, regional and international counter-terrorism instruments that influence one another and that are applied at various levels of jurisdiction from domestic courts up to international tribunals. Additionally, the various non-binding norms within the global counter-terrorism response are very difficult to explain under the dualism theory. While monism appears to offer a more coherent explanation of the structure of international counter-terrorism regulation, its emphasis on the direct applicability of international law is not fully represented in current international law, since certain significant aspects of the global counter-terrorism effort depend on the domestic laws of states, despite the international community's unanimous rejection of terrorism as a concept. The seemingly ever-growing legislative and jurisdictional influence of the EU is further demonstration that the traditional, twofold division between national and international actors and law has long since developed into a collection of public and private sector actors operating within a complex and overlapping network of domestic, regional and international regulations.

Another issue related to the legal characterization of the aforementioned cyber-freedom fighters under the western proposal of the Comprehensive Convention is the fact the fighters in question would also fall inside the scope of the various sectoral counter-terrorism treaties, whereas the military forces of states are not subject to those same treaties. Thus, a significant part of the current counter-terrorism framework treats the military forces of states more favorably than freedom-fighters, even if the two parties would be engaged in an ongoing conflict against one another. In my opinion, this situation is highly problematic both from a legal and political viewpoint regardless of the fact that both of these actors are nevertheless equally liable for potential war crimes and archaic terrorism under the relevant international legislation.[201] The western proposal of the Draft Convention seems to also indicate that states such as the U.S. are advocating strongly for a very limited interpretation of state terrorism in order to keep justifying their actions under international law in, among other regions, the Middle East. The issues regarding statehood are already in themselves one of the most politically driven parts of international law and their controversial elements are only exacerbated when paired with the equally debated field of international counter-terrorism legislation.

[200] Generally on dualism and monism see, for example, *supra* Crawford (2019) 45–102.
[201] *Supra* Shiryaev, 2012, pp. 188–189.

6 THE PERCEIVED AND ACTUAL THREAT OF TERRORISM

As I have already described in various parts of this paper, the threat of terrorism – whether partly or largely exaggerated or not – seems to have taken a more or less permanent role in our public discussion through the media, popular culture and both domestic and international politics. First, after the 9/11 attacks, the topic was led by the U.S. as it declared its infamous "War on Terror", which also led to heightened security measures in the aviation sector. The second wave of debates about the threat of terrorism and about the necessity of additional legislative measures to combat it were focused on Europe after the abovementioned Paris attacks of 2015.

In recent years, Europe has been painted in the media and by right-wing politicians as a ticking time bomb of terrorism, whilst few articles have been written about the victims of terrorism in regions such as the Middle East, Africa and South Asia, whose victims together constitute 95% of all deaths from terrorism.[202] This is of course partly by design, since one of the main objectives of terrorism is, quite literally, to cause terror. Nevertheless, conventional terrorist attacks receive a disproportionate amount of media coverage relative to their frequency and share of total deaths.[203] Additionally, it is difficult to ignore the islamophobic elements of the news coverage of terrorist attacks when a recent study showed an average increase of 758% in the number of news stories that an attack receives in major U.S. media outlets if the perpetrator was Muslim.[204] It could be argued that the media merely reflects the broader opinions of the general public and is utilizing them for their own financial gain. In reality, the news media has a tremendous impact in forming, strengthening and otherwise influencing public opinion and even domestic legislative agendas.[205] All in all, it appears that almost everyone has an opinion on how large a problem terrorism is, who is perpetrating these horrific acts and how we should handle the issue.[206]

---

[202] Hannah Ritchie, Joe Hasell, Cameron Appel and Mike Roser, "Terrorism", Our World in Data (2013, last updated in 2019) <https://ourworldindata.org/terrorism#global-distribution-of-terrorism> accessed 10 December 2020.

[203] *Supra* Ritchie et al. (2013); *ibid.*

[204] Erin M. Kearns, Allison E. Betus and Anthony F. Lemieux, "Why Do Some Terrorist Attacks Receive More Media Attention Than Others?" (2019) 36(6) Justice Quarterly 985.

[205] Gary King, Benjamin Schneer and Ariel White, "How the news media activate public expression and influence national agendas" (2017) 358 Science 776.

[206] Another interesting statistic that might help in placing the threat of terrorism in a proportional context is the fact that during 2008–2015, an individual living in the U.S. was over 18 times more likely to die of an animal attack than of a terrorist act. Alex Nowrasteh, "More Americans Die in Animal Attacks than in Terrorist Attacks" (8 March 2018) the Cato Institute <https://www.cato.org/blog/more-americans-die-animal-attacks-terrorist-attacks> accessed 28 April 2021.

It is quite clear that terrorism has maintained its outsized role in our public debates during the last few years. While I believe that the threat of conventional terrorist attacks in Europe and in the U.S. has been exaggerated, cyberterrorism has mostly remained in the periphery of these debates. I, for one, find this oversight quite interesting since the media, business sector and even the general public seem to have an endless thirst for all of the various types of new, emerging technological breakthroughs and at least the business sector showers praise on the seemingly endless opportunities created by these inventions. There are, however, those who have remained skeptical about certain elements of these emerging technologies and have raised concerns about their potentially harmful human rights and sociological impacts.[207]

The blazing speed of technological development of the past few decades highlights the potential ability of nefarious actors to begin using these emerging inventions for terrorist purposes. Why would terrorist organizations with highly sophisticated online networks and operations such as ISIS[208] not be able to incorporate these emerging technologies into their cyberterrorism schemes? In fact, the Islamic State's "Cyber Caliphate" has already claimed responsibility for an attack that temporarily disrupted certain social media channels of U.S. Central Command.[209] In its statement regarding the attack, U.S. officials stated that they viewed the incident "purely as a case of cybervandalism".[210] The incident acts as a useful demonstration of the subjective element of terrorist acts. The U.S. has a strong political incentive to reject the attack as terrorism, since it does not want to be perceived as an easy target for terrorists nor as a weak companion to its allies. However, the incident might have effectively "intimidated the (U.S.) population" or at least caused a certain level of terror in the general public, which are easily amplified in the modern social media environment. While this particular attack is more likely to fall within the "hacktivist" activities instead of cyberterrorism, it demonstrates that powerful terrorist organizations do already possess the ability and resources to conduct at least certain types of cyberattacks, and potentially even cyberterrorist acts.

---

[207] See, e.g., Julia Bossmann, "Top 9 ethical issues in artificial intelligence", World Economic Forum (21 October 2016) <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/> accessed 10 December 2020.

[208] See, for example, Asma Shakir Khawaja and Asma Hussain Khan, "Media Strategy of ISIS: An Analysis" (2016) 36(2) Strategic Studies 104, available at <www.jstor.org/stable/48535950> accessed 10 December 2020; Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media" (2017) 54 Society 138.

[209] Helene Cooper, "ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts", The New York Times (12 January 2015) <https://www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html> accessed 29 April 2021.

[210] "Centcom Acknowledges Social Media Sites 'Compromised'", U.S. Central Command News Release (12 January 2015) <https://www.defense.gov/Explore/News/Article/Article/603906/> accessed 29 April 2021.

Certain legal scholars have argued that cyberterrorism does not pose an imminent threat[211], some of them even arguing that a great gap exists between the presumed danger of these attacks and the scale of known cyberattacks.[212] Then again, in a 2014 study, 58% of the 110 researchers that had responded to the survey saw cyberterrorism as a significant threat.[213] As regards state activities, the aforementioned Stuxnet attack was essentially the first (nuclear) cyberterrorism act in history.[214] Although the Stuxnet attack required a particularly high level of cyber expertise – a field in which the U.S. is one of the frontrunners – I believe that it is only a matter of time before the most influential global terrorist organizations such as ISIS possess the necessary skills to try and commit similar acts of cyberterrorism on vulnerable infrastructure targets. Furthermore, the next broader technological advances such as the decentralized internet, developments in AI and the overall further reliance of both states and private actors on complex informational systems create both additional tools for potential cyberterrorist and new, vulnerable targets for attacks. If these issues are not addressed soon, we might not have the legal framework needed to effectively combat future, potentially even more devastating attacks.

[211] Massimo Mauro, "Threat Assessment and Protective Measures: Extending the Asia-Europe Meeting IV Conclusions on Fighting International Terrorism and Other Instruments to Cyber Terrorism" in Edward Halpin et al. (eds), *Cyberwar, Netwar and the Revolution in Military Affairs* (Palgrave Macmillan UK 2016), 219 and 221.
[212] Anna-Maria, Talihärm, *Cyber Terrorism; in Theory or in Practice?* (2010) 3(2) Defence Against Terrorism Review 59, 62.
[213] Lee Jarvis, Stuart Macdonald and Lella Nouri, "The Cyberterrorism Threat: Findings from a Survey of Researchers" 37(1) Studies in Conflict & Terrorism (2014) 68.
[214] *Supra* Shiryaev (2012)

7 CONCLUSION

The global counter-terrorism framework of which cyberterrorism is a sub-category, is a collection of international conventions, customary law and various other sources of international law that has been – and likely always will be – heavily influenced by international, regional and domestic politics as well as the various biases of international law. The main issues that have plagued the international counter-terrorism field for decades are the lack of a general definition of terrorism in both treaty and customary law and the related debates concerning the possible inclusion in the normative instruments of the exceptions for state terrorism and for the right of freedom movements to resist foreign occupation under their right of self-determination. It is difficult to envision a clear solution to these issues due to their highly political aspects. In addition to the aforementioned factors, the issue of attribution is exacerbated in cyberspace, where tracing a terrorist act to its direct or indirect source is even more complicated than it is in conventional environments.

Since the various sectoral treaties have quite successfully addressed myriad new emerging terrorist threats throughout the years, it is not entirely unlikely that a sectoral convention concerning cyberterrorism would be drafted and eventually adopted by several states in the near future. However, the issues highlighted in this thesis such as the potential for new types of terrorist safe havens, the variances between the domestic laws of different states and the potentially limiting effect of a "non-political" clause on the states' willingness to sign the treaty might ultimately prevent the wide adopting of a sectoral cyberterrorism convention. After all, the sectoral treaties are only effective in combating terrorism if they are both adopted by a significant number of states and the measures prescribed in them are also effective in practice. As a result, the current sectoral approach could offer a useful model for adopting new sectoral treaties regarding cyberterrorism, but their ability to address the broader issue of international terrorism is severely hampered by the inclusion in the most recent treaties of the "political offence exception" regarding the extradition of suspected perpetrators.

Even though the negotiations over the Draft Comprehensive Convention on International Terrorism have been deadlocked for years, the language of Article 2 of the Draft Convention quite clearly represents the current consensus on the general definition of terrorism. My view is that amending the relevant Draft articles according to the proposal submitted and supported by the IOC is necessary in order to 1) protect the legality of the acts of freedom fighters committed in resistance to foreign occupation under their essential right to self-determination

both in cyberspace and in the real world and 2) prevent state actors from committing cyberattacks with impunity against foreign states or private persons. Based on the analysis that I have performed in this thesis, I believe that adopting the Comprehensive Convention according to the IOC's wording would provide the international community with an efficient, just and sufficiently dynamic tool for combating both conventional terrorist threats as well as current and future cyberterrorist attacks. However, given the strong opposition of the other negotiating parties to the IOC's proposal, I am not hopeful about the successful conclusion of the Comprehensive Convention.

The two above paragraphs form the core of my answer to my primary research question of "To what extent can – and should – the current international counter-terrorism framework be applied to cyberterrorism?". Despite its flaws and gridlocked negotiations, I believe that the Draft Comprehensive Convention is the legal instrument that has come closest to reaching a nearly universal agreement on the definition of terrorism while also attempting to resolve the highly political issues of the role of freedom fighters and that of state terrorism. However, as I have described above, I am not optimistic about the probability of the Draft Convention being adopted, especially under the IOC's proposal, in the next few years. Resultingly, drafting new sectoral treaties, despite their own drawbacks, to counter current and emerging cyberterrorist acts might ultimately prove to be the most practical medium-term solution to combating cyberterrorism on a global, or at the very least regional, scale. In order to gain broad acceptance, these new sectoral treaties might have to revert back to the older sectoral approach of not including a "non-political" clause in the text of the treaty.

The emergence of a customary law definition and eventual prohibition of the international crime of terrorism is another potential development in the global counter-terrorism field. At first glance, the Appeal Chamber for the Special Tribunal for Lebanon had seemingly achieved the impossible by both crystallizing the definition of international terrorism and confirming its existence as a core international crime in its interlocutory decision in the *Ayyash et al. Case*. However, the type of judicial activism, cherry-picking and corner-cutting apparent in the Tribunal's reasoning resulted in an unconvincing and widely criticized decision the role of which as the prevailing authority on the current status of terrorism in customary international law appears to have been rejected by the international legal community. While it remains entirely possible that a customary law definition, along with the creation of core international crime of terrorism, emerges in the relatively near future, it is not yet sufficiently supported by a general practice of states or a broad *opinio juris*. This development is also effectively slowed

down if the often political and bias-driven UN resolutions and General Assembly resolutions may only have a weak or subsidiary influence on the formation of *opinio juris*, as I believe they should.

My analysis of the perceived and actual threat posed by both conventional terrorism and cyberterrorism leads me to believe that while the fears over potential archaic terrorist attacks are exaggerated and often driven by islamophobia, the threat of cyberterrorism might have been underreported at least in relation to the potentially disastrous effects of even a singular, well-coordinated attack on the critical infrastructure of a specific city or even of an entire state. This analysis also underlined the complicated relationship between the subjective elements of terrorism and the general perception of the level of threat posed by terrorism.

What about my secondary research question regarding the prevalence of the various biases of international law in the field of counter-terrorism? As I had suspected even before beginning my research for this thesis, certain problematic biases have guided the global response to terrorism. The Tribunal's behavior in the *Ayyash et al. Case* quite clearly represented a form of neocolonialism which resulted in a widely criticized decision. Although most of the academic criticism aimed at the decision appeared to center on the substantive elements of the case, the Tribunal's highly questionable procedural actions alone should have been sufficient to reject the decision altogether. While the effects of islamophobia have remained relatively limited in the global counter-terrorism response, they have – with the aid of near-constant media coverage – reached extraordinary levels in national political debates, often resulting in domestic laws that, directly or indirectly, target Muslim communities.

Finally, the several political elements of international counter-terrorism culminate in the debates over the status of freedom fighters in relation to the right of peoples to self-determination and the interpretation of state terrorism. As I have described above, I believe that the only way to adequately address both of these issues is to adopt the Comprehensive Convention according to the IOC's wording. In relation to the various clear biases mentioned above, the analysis in this thesis has demonstrated that global, regional and even domestic politics play a significant, structural role in many of the debates regarding the international counter-terrorism response. While it may not be possible to provide a clear solution to addressing all of the biases and conflicting interests described in this thesis, I have hopefully been able to highlight some of these fundamental issues and thus helping international legislators accomplish the first step in eventually solving the issue: recognizing its existence.

The global threat of terrorism can only be successfully combated through significant coordination efforts between states through mainly multilateral regulations instead of conflicting domestic laws. No matter how unfeasible it may seem given the history and central actors of international law, the states must be able to reach a political and legal compromise in the next couple of years in their negotiations over the issues described in this thesis in order for the international community to have the necessary regulatory tools to combat ever more advanced forms of cyberterrorism in the future.