BIBLIOGRAPHY

Books:

Bigo, Didier, Engin F. Isin, and Evelyn Sharon Ruppert (eds.), 2019, *Data politics: worlds, subjects, rights*, Routledge studies in international political sociology, Routledge, Taylor & Francis Group, London ; New York.

Broeders, Dennis and Bibi van den Berg (eds.), 2020, *Governing cyberspace: behavior, power, and diplomacy*, Digital technologies and global politics, Rowman & Littlefield, Lanham.

Cameron, Lindsey and Vincent Chetail, 2013, *Privatizing War: Private Military and Security Companies Under Public International Law*, Cambridge University Press, New York.

Cavelty, Myriam Dunn and Andreas Wenger, 2022, *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Routledge, London.

Clough, Jonathan, 2010, *Principles of cybercrime*, Cambridge University Press, Cambridge, UK ; New York.

Crawford, James, 2013, *State Responsibility: The General Part*, Cambridge University Press, Cambridge.

Fang, Binxing, 2018, *Cyberspace Sovereignty*, Springer Singapore, Singapore.

Grimm, Dieter, 2015, *Sovereignty: The origin and future of a political and legal concept*, Columbia University Press.

International Law Commission (ed.), "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", United Nations *Yearbook of the International Law Commission 2001*, Vol. II, 2008.

International Law Commission (ed.), "Draft articles on the responsibility of international organizations, with commentaries", United Nations *Yearbook of the International Law Commission 2011*, Vol. II, 2011.

Jackall, Robert (ed.), 1995, *Propaganda*, Vol. 8, NYU Press.

Kittichaisaree, Kriangsak, 2017, *Public International Law of Cyberspace*, Law, Governance and Technology Series, Vol. 32, Springer International Publishing, Cham.

Noortmann, Math, August Reinisch, and Cedric Ryngaert (eds.), 2015, *Non-state actors in international law*, Bloomsbury Publishing.

Tonkin, Hannah, 2011, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge University Press, Cambridge.

Willisch, Jan, Manfred Feldsieper, Rudolf Meimberg, and Richard Gross, 2021, *State responsibility for technological damage in international law*, Veröffentlichungen des Walther-Schücking-Instituts Für Internationales Recht an der Universität Kiel, Vol. 97, Duncker & Humblot.

Papers:

Da San Martino, Giovanni, Seunghak Yu, Alberto Barrón-Cedeño, Rostislav Petrov, and Preslav Nakov, "Fine-Grained Analysis of Propaganda in News

Article", in Kentaro Inui, Jing Jiang, Vincent Ng, and Xiaojun Wan (eds.), 2019, *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing*, presented at the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Hong Kong, China.

Delerue, Francois, "Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace", in Taťána Jančárková, Lauri Lindström, Gábor Visky, and Philippe Mitsuya Zotz (eds.), 2021, presented at the 2021 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Kosseff, Jeff, "The Contours of 'Defend Forward' Under International Law", in Siim Alatalu, Stefano Biondi, Tomáš Minárik, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky (eds.), 2019, presented at the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Kraszewski, Kenneth, "SamSam and the Silent Battle of Atlanta", in Siim Alatalu, Stefano Biondi, Tomáš Minárik, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky (eds.), 2019, presented at the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Roguski, Przemyslaw, "Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment", in Siim Alatalu, Stefano Biondi, Tomáš Minárik, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky (eds.), 2019, presented at the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Stejskal, Petr and Martin Faix, "Legal Aspects of Misattribution Caused by Cyber Deception", in Henrik Beckvard, Marius Gheorghevici, Davide Giovannelli, Keiko Kono, Lauri Lindström, Piret Pernik, Kārlis Podiņš, Ann Väljataga, and Jan Wünsche (eds.), 2022, presented at the 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), Tallinn, Estonia.

Tehrani, Pardis Moslemzadeh, "Cyber Resilience Strategy and Attribution in the Context of International law", in Paulo Simoes (ed.), 2019, presented at the European Conference on Cyber Warfare and Security, Reading.

Wolff Heintschel von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace", in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds.), 2012, presented at the 2012 4th International Conference on Cyber Conflict (CYCON 2012).

Journal Articles:

Aravindakshan, Sharngan, "Cyberattacks: a look at evidentiary thresholds in International Law", *Indian Journal of International Law*, Vol. 59, Nos. 1–4, February, 2021.

Ashraf, Cameran, "Defining cyberwar: towards a definitional framework", *Defense & Security Analysis*, Vol. 37, No. 3, July, 2021.

Assaf, Alaa, Daniil Moshnikov, 'International Law in the Digital Age' Research and Study Group, and Alaa Assaf, "Contesting sovereignty in cyberspace", *International Cybersecurity Law Review*, Vol. 1, Nos. 1–2, October, 2020.

Banks, William C., "The Bumpy Road to a Meaningful International Law of Cyber Attribution", *AJIL Unbound*, Vol. 113, 2019.

Banks, William Charles, "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage", *Emory Law Journal*, Vol. 66, No. 3, 2017.

Benvenisti, Eyal, "Are There Any Inherently Public Functions for International Law?", *AJIL Unbound*, Vol. 115, 2021.

Bertram, Stewart Kenton, "'Close enough' – The link between the Syrian Electronic Army and the Bashar al-Assad regime, and implications for the future development of nation-state cyber counter-insurgency strategies", *Journal of Terrorism Research*, Vol. 8, No. 1, February, 2017.

Bhupinder Chimni, "Customary International Law: A Third World Perspective", *American Journal of International Law*, Vol. 112, No. 1, January, 2018.

Biller, Jeffrey, "Cyber operations and the Second Geneva Convention", *International Review of the Red Cross*, Vol. 100, Nos. 907–909, April, 2018.

Brown, Étienne, "Propaganda, Misinformation, and the Epistemic Value of Democracy", *Critical Review*, Vol. 30, Nos. 3–4, October, 2018.

Buchan, Russell, "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm", *Journal of Conflict and Security Law*, Vol. 21, No. 3, December, 2016.

Bunga, Dewi, "Legal Response to Cybercrime in Global and National Dimensions", *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, Vol. 06, No. 01, April, 2019.

Chircop, Luke, "A Due Diligence Standard of Attribution in Cyberspace", *International and Comparative Law Quarterly*, Vol. 67, No. 3, July, 2018.

Chircop, Luke, "Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0", Melbourne *Melbourne Journal of International Law*, Vol. 20, No. 2, 2019.

Clara Assumpção, "The Problem of Cyber Attribution Between States", E-International Relations *E-International Relations*, May, 2020.

Corn, Gary P. and Robert Taylor, "Sovereignty in the Age of Cyber", *AJIL Unbound*, Vol. 111, 2017.

Couzigou, Irène, "Securing cyber space: the obligation of States to prevent harmful international cyber operations", *International Review of Law, Computers & Technology*, Vol. 32, No. 1, January, 2018.

Crootoft, Rebecca, "International Cybertorts: Expanding State Accountability in Cyberspace", HeinOnline *Cornell Law Review*, Vol. 103, No. 3, 2018.

Daugirdas, Kristina, "Member States' Due Diligence Obligations to Supervise International Organizations", University of Michigan Law School *Economics Working Papers*, No. 167, 2020.

de Wet, Erika, "The invocation of the right to self-defence in response to armed attacks conducted by armed groups: Implications for attribution", *Leiden Journal of International Law*, Vol. 32, No. 01, March, 2019.

DeFabo, Vincent L, "Rethinking Cyberspace Operations: Widespread Electromagnetic Jamming by States Indicates Cyber Interference Is Not a Use of Force", *Journal of Air Law and Commerce*, Vol. 86, No. 2, 2021.

Delbert Tran, "The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack", HeinOnline *Yale Journal of Law and Technology*, Vol. 20, 2018.

Delerue, François, "Reinterpretation or Contestation of International Law in Cyberspace?", *Israel Law Review*, Vol. 52, No. 3, November, 2019.

Denton, Allison, "Fake news: The legality of the Russian 2016 Facebook influence campaign", *Boston University International Law Journal*, Vol. 37, 2019.

Doyle, Todd, "Cleaning up Anti-Money Laundering Strategies: Current FATF Tactics Needlessly Violate International Law", *Houston Journal of International Law*, Vol. 24, 2001.

Dunn Cavelty, Myriam and Andreas Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, Vol. 41, No. 1, January, 2020.

Durkee, Melissa J., "Introduction to the Symposium on Frédéric Mégret, 'Are There "Inherently Sovereign Functions" in International Law?'", *AJIL Unbound*, Vol. 115, 2021.

Egloff, Florian and Andreas Wenger, "Public Attribution of Cyber Incidents", ETH Zurich, Zürich *CSS Analyses in Security Policy*, No. 244, May, 2019.

Egloff, Florian J, "Public attribution of cyber intrusions", *Journal of Cybersecurity*, Vol. 6, No. 1, January, 2020.

Egloff, Florian J., "Contested public attributions of cyber incidents and the role of academia", *Contemporary Security Policy*, Vol. 41, No. 1, January, 2020.

Eichensehr, Kristen E, "Not Illegal: The SolarWinds Incident and International Law", University of Virginia School of Law *SSRN Electronic Journal*, 2022.

Elbahy, Raghda, "Deterring violent non-state actors: dilemmas and implications", *Journal of Humanities and Applied Social Sciences*, Vol. 1, No. 1, June, 2019.

Eoyang, Mieke and Chimène Keitner, "Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity", *Journal of National Security Law & Policy*, Vol. 11, 2021.

Fink, Melanie, "The Action for Damages as a Fundamental Rights Remedy: Holding Frontex Liable", *German Law Journal*, Vol. 21, No. 3, April, 2020.

Finlay, Lorraine and Christian Payne, "The Attribution Problem and Cyber Armed Attacks", *AJIL Unbound*, Vol. 113, 2019.

Finnemore, Martha and Duncan B Hollis, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity", *European Journal of International Law*, Vol. 31, No. 3, December, 2020.

Garrie, Daniel and Masha Simonova, "A Keystroke Causes a Tornado: Applying Chaos Theory to International Cyber Warfare Law", Vol. 45, No. 2, 2020.

Geiss, Robin and Henning Lahmann, "Protecting Societies: Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats", Geneva Academy, Geneva *SSRN Electronic Journal*, 2021.

Ghappour, Ahmed, "Tallinn, Hacking, and Customary International Law", *AJIL Unbound*, Vol. 111, 2017.

Gross, Jessica R, "Hack and be Hacked: A Framework for the United States to Respond to Non-state Actors in Cyberspace", HeinOnline *California Western International Law Journal*, Vol. 46, 2016.

Harknett, Richard J. and Max Smeets, "Cyber campaigns and strategic outcomes", *Journal of Strategic Studies*, March, 2020.

Hasanuddin University, Maskun, Achmad, Naswar, Hasbi Assidiq, Armelia Syafira, Marthen Napang, and Marcel Hendrapati, "Qualifying Cyber Crime as a Crime of Aggression in International Law", *Journal of East Asia and International Law*, Vol. 13, No. 2, November, 2020.

Hathaway, Oona A, Emily Chertoff, Lara Domínguez, Zachary Manfredi, and Peter Tzeng, "Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors", *Texas Law Review*, Vol. 95, 2017.

Hobbs, Renee, "Propaganda in an Age of Algorithmic Personalization: Expanding Literacy Research and Practice", *Reading Research Quarterly*, Vol. 55, No. 3, July, 2020.

Inaki Navarrete and Russell Buchan, "Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions", *Cornell International Law Journal*, Vol. 51, No. 4, 2019.

Jacob Azrilyant, "The Cyber Privatization Problem: Navigating the Law of Armed Conflict Implications of Outsourcing Offensive Cyber Operations", *Public Contract Law Journal*, Vol. 50, No. 4, 2021.

Jamnejad, Maziar and Michael Wood, "The Principle of Non-intervention", *Leiden Journal of International Law*, Vol. 22, No. 2, June, 2009.

Jiang, Chaoyi, "Decoding China's Perspectives on Cyber Warfare", *Chinese Journal of International Law*, Vol. 20, No. 2, October, 2021.

Johnson, Durward E and Michael N Schmitt, "Responding to Proxy Cyber Operations Under International Law", Army Cyber Institute *The Cyber Defense Review*, Vol. 6, No. 4, 2021.

Katagiri, Nori, "Why international law and norms do little in preventing non-state cyber attacks", *Journal of Cybersecurity*, Vol. 7, No. 1, February, 2021.

Keitner, Chimène I., "Attribution by Indictment", *AJIL Unbound*, Vol. 113, 2019.

Khanna, Pallavi, "State Sovereignty and Self-Defence in Cyberspace", *BRICS Law Journal*, Vol. 5, No. 4, December, 2018.

Klimburg, Alexander, "Mobilising Cyber Power", *Survival*, Vol. 53, No. 1, February, 2011.

Kong, Stephen, "The Right of Innocent Passage: A Case Study on Two Koreas", *Minnesota Journal of International Law*, Vol. 11, 2002.

Koziarski, Jacek and Jin Ree Lee, "Connecting evidence-based policing and cybercrime", *Policing: An International Journal*, Vol. 43, No. 1, March, 2020.

Kristen E. Eichensehr, "The Law and Politics of Cyberattack Attribution", *UCLA Law Review*, Vol. 67, 2020.

Kubo Mačák, "On the Shelf, but Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law", *American Journal of International Law*, Vol. 113, 2019.

Lahmann, Henning, "On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace", *Duke Journal of Comparative & International Law*, Vol. 32, 2021.

Lanovoy, Vladyslav, "The Use of Force by Non-State Actors and the Limits of Attribution of Conduct", *European Journal of International Law*, Vol. 28, No. 2, May, 2017.

Leal, Marcelo and Paul Musgrave, "Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks", Oxford Academic *Foreign Policy Analysis*, Vol. 18, No. 2, March, 2022.

Lotrionte, Catherine, "Countering State-Sponsored Cyber Economic Espionage under International Law", *North Carolina Journal of International Law*, Vol. 40, No. 2, 2015.

Lubin, Asaf, "The Liberty to Spy", *Harvard International Law Journal*, Vol. 61, No. 1, 2020.

Mačák, Kubo, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors", *Journal of Conflict and Security Law*, Vol. 21, No. 3, December, 2016.

Maddocks, Jennifer, "Outsourcing of Governmental Functions in Contemporary Conflict: Rethinking the Issue of Attribution", *Virginia Journal of International Law*, Vol. 59, 2019.

Maglaras, Leandros, Mohamed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, Helge Janicke, and Stylianos Rallis, "Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures", Cornell University *arXiv*, January, 2019.

Mahoney, Charles W., "United States defence contractors and the future of military operations", *Defense & Security Analysis*, Vol. 36, No. 2, April, 2020.

Mannan, Syed Hamza, "Projecting Power: How States Use Proxies in Cyberspace", *Journal of National Security Law & Policy*, Vol. 10, No. 2, December, 2019.

Mare, Admire, Hayes Mawindi Mabweazara, and Dumisani Moyo, "'Fake News' and Cyber-Propaganda in Sub-Saharan Africa: Recentering the Research Agenda", *African Journalism Studies*, Vol. 40, No. 4, October, 2019.

Martti Koskenniemi, "What Use for Sovereignty Today?", *Asian Journal of International Law*, Vol. 1, No. 01, January, 2011.

Maurer, Tim, "'Proxies' and Cyberspace", *Journal of Conflict and Security Law*, Vol. 21, No. 3, December, 2016.

Maurer, Tim, "Cyber Proxies and Their Implications for Liberal Democracies", *The Washington Quarterly*, Vol. 41, No. 2, April, 2018.

Maweu, Jacinta Mwende, "'Fake Elections'? Cyber Propaganda, Disinformation and the 2017 General Elections in Kenya", *African Journalism Studies*, Vol. 40, No. 4, October, 2019.

McKenzie, Simon, "Cyber Operations against Civilian Data", *Journal of International Criminal Justice*, Vol. 19, No. 5, February, 2022.

Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyberspace. The Evolving International Law of Attribution", The NATO Cooperative Cyber Defence Centre of Excellence *Fletcher Security Review*, Vol. 1, No. 2, 2014.

Mikanagi, Tomohiro, "Application of the Due Diligence Principle to Cyber Operations", *International Law Studies*, Vol. 97, 2021.

Moynihan, Harriet, "The vital role of international law in the framework for responsible state behaviour in cyberspace", *Journal of Cyber Policy,* Vol. 6, No. 3, September, 2021.

Mueller, Milton L, "Against Sovereignty in Cyberspace", *International Studies Review,* Vol. 22, No. 4, November, 2020.

Müllerson, Rein, "Self-defence against Armed Attacks by Non-State Actors", *Chinese Journal of International Law,* Vol. 18, No. 4, December, 2019.

Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict and Security Law,* Vol. 17, No. 2, July, 2012.

Nieto-Navia, Rafael, "State Responsibility in Respect of International Wrongful Acts of Third Persons: The Theory of Control".

Osula, Anna-Maria, Agnes Kasper, and Aleksi Kajander, "EU Common Position on International Law and Cyberspace", *Masaryk University Journal of Law and Technology*, Vol. 16, No. 1, June, 2022.

Patrick, Colin, "Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations", *Washington International Law Journal,* Vol. 28, No. 2.

Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law,* Vol. 14, 2013.

Peters, Allison and Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime", *Journal of National Security Law & Policy*, Vol. 10, 2019.

Pijpers, Peter and Bart van den Bosch, "The 'Virtual Eichmann': on Sovereignty in Cyberspace", *SSRN Electronic Journal*, 2020.

Pray, Corey, "It's the Principle: Defining Sovereignty in the Context of Cyber Operations", *National Security Law Journal*, Vol. 7, No. 2, 2021.

Radosław Fordoński and Wojciech Kasprzak, "WannaCry ransomware cyberattack as violation of international law", *Studia Prawnoustrojowe*, No. 44, 2019.

Ryngaert, Cedric, "Attributing Conduct in the Law of State Responsibility: Lessons from Dutch Courts Applying the Control Standard in the Context of International Military Operations", *Utrecht Journal of International and European Law*, Vol. 36, No. 2, July, 2021.

Ryngaert, Cedric and Otto Spijkers, "The End of the Road: State Liability for Acts of UN Peacekeeping Contingents After the Dutch Supreme Court's Judgment in Mothers of Srebrenica (2019)", *Netherlands International Law Review*, Vol. 66, No. 3, December, 2019.

Sander, Barrie, "Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections", *Chinese Journal of International Law*, Vol. 18, No. 1, March, 2019.

Sawmiller, Jonathan K, "Fighting Election Hackers and Trolls on Their Own Turf: Defending Forward in Cyberspace", *Idaho Law Review*, Vol. 56, No. 2, 2020.

Schmitt, Michael N, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law", HeinOnline *Virginia Journal of International Law*, Vol. 54, No. 3, 2014.

Schmitt, Michael N, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", *Chicago Journal of International Law*, Vol. 19, No. 1, 2018.

Schmitt, Michael N, "Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention", *International Law Studies*, Vol. 96, 2020.

Schmitt, Michael N. and Liis Vihul, "Sovereignty in Cyberspace: *Lex Lata Vel Non* ?", *AJIL Unbound*, Vol. 111, 2017.

Schmitt, Michael N. and Sean Watts, "Beyond State-Centrism: International Law and Non-state Actors in Cyberspace", *Journal of Conflict and Security Law*, Vol. 21, No. 3, December, 2016.

Schöndorf, Roy, "Israel's Perspective on Key Legal and", *International Law Studies*, Vol. 97, 2021.

Sigholm, Johan, "Non-State Actors in Cyberspace Operations", *Journal of Military Studies*, Vol. 4, No. 1, December, 2013.

Skinner, Christina Parajon, "An International Law Response to Economic Cyber Espionage", *Connecticut Law Review*, Vol. 46, No. 4, May, 2014.

Starski, Paulina, "Right to Self-Defence, Attribution and the Non-State Actor Birth of the 'Unable and Unwilling' Standard?", *SSRN Electronic Journal*, 2015.

Sun, Yirong, "The Future of Due Diligence in Cyberspace", HeinOnline *International Law and Politics*, Vol. 54, 2022.

Taichman, Elya, "Defend Forward & Sovereignty: How America's Cyberwar Strategy Upholds International Law", *Inter-American Law Review*, Vol. 53, No. 1, December, 2021.

Talmon, Stefan, "The Responsibility of Outside Powers for Acts of Secessionist Entities", JSTOR *International and Comparative Law Quarterly*, Vol. 58, No. 3, July, 2009.

Terry, Patrick C. R., "'Don't Do as I Do'—The US Response to Russian and Chinese Cyber Espionage and Public International Law", *German Law Journal*, Vol. 19, No. 3, June, 2018.

Tignino, Mara and Christian Bréthaut, "The role of international case law in implementing the obligation not to cause significant harm", *International Environmental Agreements: Politics, Law and Economics*, Vol. 20, No. 4, December, 2020.

Tsagourias, Nicholas and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges", *European Journal of International Law*, Vol. 31, No. 3, December, 2020.

Volk, Christian, "The Problem of Sovereignty in Globalized Times", *Law, Culture and the Humanities*, Vol. 0, No. 0, February, 2019.

Walden University and Sunday Ogunlana, "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies", *Journal of Strategic Security*, Vol. 12, No. 1, April, 2019.

Watts, Sean and Theodore Richard, "Baseline Territorial Sovereignty and Cyberspace", HeinOnline *Lewis & Clark Law Review*, Vol. 22, No. 3, 2018.

Westphal, Carter, "Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace", *Penn State Law Review*, Vol. 126, No. 3, 2022.

White, Nigel D., "Outsourcing Military and Security Functions", *AJIL Unbound*, Vol. 115, 2021.

Wicaksana Prakasa, Satria Unggul and Noviandi Nur P.E., "Analysist of Cyber Espionage in International Law and Indonesian Law", *Humanities & Social Sciences Reviews*, Vol. 7, No. 3, April, 2019.

Wieteke Theeuwen, "Attribution for the purposes of State responsibility", Ministerie van Defensie *Netherlands Military Review*, 2018.

Xiao, Alex, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election", *Duke Journal of Comparative & International Law*, Vol. 30, 2019.

Yao Dong, "The Jus Ad Bellum in Cyberspace: Where Are We Now and What next?", HeinOnline *New Zealand Journal of Public and International Law*, Vol. 17, 2019.

Essays in a Book:

Banks, William, "Who Did It? Attribution of Cyber Intrusions and the Jus in Bello", in Alcala, Ronald and Eric Talbot Jensen (eds.), 2019, *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford University Press.

Bantekas, Ilias, "Cybercrime and its sovereign spaces: an international law perspective", in Van der Wilt, Harmen and Christophe Paulussen (eds.), 2017, *Legal Responses to Transnational and International Crimes*, Edward Elgar Publishing.

Bellal, Annyssa, "What Are 'Armed Non-State Actors'? A Legal and Semantic Approach", in Heffes, Ezequiel, Marcos D. Kotlik, and Manuel J. Ventura (eds.), 2020, *International Humanitarian Law and Non-State Actors*, T.M.C. Asser Press, The Hague.

Boulos, Sonia, "Does Foreign Cyber Intervention in Electoral Processes Violate International Law?", in Ramírez, J. Martín and Bartolomé Bauzá-Abril (eds.), 2021, *Security in the Global Commons and Beyond*, Advanced Sciences and Technologies for Security Applications, Springer International Publishing, Cham.

Buchan, Russell, "Introduction", in Buchan, Russell (ed.), 2019, *Cyber Espionage and International Law*, Hart, Oxford ; New York.

Dinstein, Yoram and Arne Willy Dahl, "Section II: Cyber Operations", in Dinstein, Yoram and Arne Willy Dahl (eds.), 2020, *Oslo Manual on Select Topics of the Law of Armed Conflict*, Springer International Publishing, Cham.

Kleinlein, Thomas, "Customary International Law and General Principles: Rethinking Their Relationship", in Lepard, Brian D. (ed.), 2017, *Reexamining Customary International Law*, Cambridge University Press, Cambridge.

Li, Hui and Xin Yang, "Interpretation of Network Sovereignty", in Li, Hui and Xin Yang (eds.), 2021, *Co-governed Sovereignty Network*, Springer Singapore, Singapore.

Markus Wagner, "Non-State Actors", in Rüdiger Wolfrum (ed.), 2009, *Max Planck Encyclopedia of Public International Law*, Oxford University Press.

Schmitt, Michael N. (ed.), "Cyber operations not per se regulated by international law", 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge.

Schmitt, Michael N. (ed.), "Due diligence", 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge.

Schmitt, Michael N. (ed.), "Law of international responsibility", 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge.

Schmitt, Michael N. (ed.), "Sovereignty", 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge.

Tsagourias, Nicholas, "The legal status of cyberspace: sovereignty redux?", in Tsagourias, Nicholas and Russell Buchan (eds.), 2021, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing.

Online Reference:

Barth, Bradley, *Password found to rescue victims of malicious COVID-19 tracker app*, https://www.scmagazine.com/news/security-news/news-archive/coronavirus/password-found-to-rescue-victims-of-malicious-covid-19-tracker-app, accessed on February 5, 2022.

Cyber Law Toolkit (ed), *Industroyer – Crash Override (2016)*, https://cyberlaw.ccdcoe.org/wiki/Industroyer_%E2%80%93_Crash_Override_(2016), accessed on February 2, 2022.

Cyber Law Toolkit (ed), *Shamoon (2012)*, https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012), accessed on January 31, 2022.

Isabel San Martin, *Attribution*, https://jusmundi.com/en/document/wiki/en-attribution, accessed on May 23, 2022.

malpedia (ed), *Operation C-Major (Threat Actor)*, https://malpedia.caad.fkie.fraunhofer.de/actor/operation_c-major, accessed on April 5, 2022.

Michael N. Schmitt, *In Defense of Sovereignty in Cyberspace*, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/, accessed on February 15, 2022.

Michael N. Schmitt, *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/, accessed on August 26, 2022.

Michael N. Schmitt, *EJIL: Talk!*, https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-ii/, accessed on April 24, 2022.

Mueller, Milton, "Sovereignty and Cyberspace":, Indiana, 2018.

Newman, Lily Hay, "Security News This Week: North Korea's Lazarus Group Was Behind $540 Million Ronin Theft", *Wired*, 2022.

The National Radio Company of Ukraine (ed), *Ukraine power cut "was cyber-attack" | Новини | Українське радіо*, http://www.nrcu.gov.ua/en/news.html?newsID=42626, accessed on February 2, 2022.

attribution, *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/attribution, accessed on May 10, 2022.

Connect the Dots on State-Sponsored Cyber Incidents—APT 36, *Connect the Dots on State-Sponsored Cyber Incidents - APT 36*, https://www.cfr.org/cyber-operations/apt-36, accessed on April 5, 2022.

Hacks of OPM databases compromised 22.1 million people, federal authorities say, *Washington Post*, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/, accessed on June 21, 2022.

Juridical Decisions:

Alabama claims of the United States of America against Great Britain. Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, 14 September 1872.

D. Earnshaw and Others (Great Britain) v. United States (Zafiro case), 30 November 1925.

General Claims Commission, *Thomas H. Youmans (U.S.A.) v. United Mexican States*, 23 November 1926.

Charles S. Stephens and Bowman Stephens (U.S.A.) v. United Mexican States, 15 July 1927.

Permanent Court of International Justice, *The Case of the S.S. Lotus*, Case No. Series A.-No. 10, 7 September 1927.

Commission US-Germany, *Sabotage Cases, Lehigh Valley Railroad Company (U.S.A.) v. Germany*, 15 June 1939.

International Court of Justice, *Corfu Channel case*, 9 April 1949.

icj, *Reparation for injuries suffered in the service of the United Nations*, 11 April 1949.

icj, *Nuclear Tests (Australia v. France)*, 20 December 1974.

icj, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, 24 May 1980.

International Court of Justice, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua: (Nicaragua v. USA)*, 27 June 1986.

Case concerning the differences between New Zealand and France arising from the Rainbow Warrior affair, 6 July 1986.

Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair, 30 April 1990.

icty, *Prosecutor v. Tadic*, Case No. IT-94-1-A, 15 July 1999.

icj, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 9 July 2004.

United States—Countervailing Duty Investigation on Dynamic Random Access Memory Semiconductors (DRAMS) from Korea, 2005, Appellate Body Reports, WT/DS296/AB/R, Appellate Body Reports.

icj, *Case concerning armed activities on the territory of the Congo (Democratic Republic of the Congo v. Uganda)*, 19 December 2005.

echr~section.3, *Weber and Saravia v. Germany*, Case No. 54934/00, 29 June 2006.

icj, *Case concerning application of the Convention on the Prevention and Punishment of the Crime of genocide (Bosnia and Herzegovina v. Serbia and Montenegro): Judgment of 26 february 2007*, 26 February 2007.

International Court of Justice, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion*, 22 July 2010.

icty, *Prosecutor v Prlic and Others*, Case No. IT-04-74-T, 29 May 2013.

icj, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, 16 December 2015.

icj, *Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua v. Colombia)*, 21 April 2022.

Others:

Alain Pellet, "Verbatim record 2006/8 Public sitting held on Friday 3 March 2006, at 10 a.m., at the Peace Palace, President Higgins presiding", The Hague, 2006.

Anastasiya Kazakova, Ivan Kwiatkowski, Julia Ryng, and Kenddrick Chan, 2022, *'Unpacking' technical attribution and challenges for ensuring stability in*

cyberspace, Submission to 2021–2025 UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies.

Bergwik, Maja, 2020, *Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0*, Master Thesis, Uppsala Universitet, Uppsala.

Bilyana Lilly, Adam S. Moore, Quentin E. Hodgson, and Daniel Weishoff, 2021, *RAND's Scalable Warning and Resilience Model (SWARM): Enhancing Defenders' Predictive Power in Cyberspace*, RAND Corporation.

Botek, Adam, 2020, *The Application of the Due Diligence Principle in Cyberspace*, Master Thesis, Charles University, Prague.

Broeders, Dennis, Els De Busser, and Patryk Pawlak, 2020, *Three tales of attribution in cyberspace: Criminal law, international law and policy debates*, The Hague, The Hague Program For Cyber Norms Policy Brief.

Caroline Nordström, 2019, *The Regulation of Cyber Operations Below the Threshold of Article 2(4) of the Charter*, Master Thesis, Uppsala Universitet, Uppsala.

Davis, Brandon S, 2018, *State Cyber Operations and International Law: Russian and Western Approaches*, Master Thesis, Ohio State University, Ohio.

Francis, Jaclyn L, 2020, *International Governance of Non-State Actors In Cyberspace: Is a Single Entity Sufficient for Dispute Resolution*, Postgraduate Thesis, Naval Postgraduate School, Monterey, California.

Goldsmith, Jack and Alex Loomis, 2021, *"Defend Forward" and Sovereignty*, 2102, Hoover Institution, Stanford, Aegis Series Paper.

Grindal, Karl, Brenden Kuerbis, Farzaneh Badiei, and Milton Mueller, 2018, *Is It Time to Institutionalize Cyber-Attribution.*

Hollis, Duncan B, 2021, *A Brief Primer on International Law and Cyberspace*.

Joshua Taft, 2020, *Sea Dogs in Cyberspace: Exploring the Employment of Privateers in the Cyber Domain*, Master Thesis, United States Army Command and General Staff College, Fort Leavenworth.

MacNamara, Conor, 2019, *Power in Cyberspace—How States Operate in the Digital Domain*, Bachelor Thesis, Queens University Belfast, Belfast.

Mossberg, Sofia, 2020, *Self-Defence Against Non-State Cyber Attacks The Attribution Problem in Cyberspace*, Master Thesis, Uppsala Universitet, Uppsala.

Moynihan, Harriet, 2019, *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention*, Research Paper, Chatham House.

Prem Mahadevan, 2020, *Cybercrime Threats During the COVID-19 Pandemic*, Policy Brief, Geneva.

Rain Liivoja, Maarja Naagel, and Ann Väljataga, 2019, *Autonomous Cyber Capabilities under International Law*.

Roguski, Przemysław, 2020, *Application of International Law to cyber operations: a comparative analysis of States' views*, The Hague, The Hague Program For Cyber Norms Policy Brief.

Sam Safi, 2019, *Sovereignty in Cyberspace A Study on Customary International Law on the Principle of Sovereignty*, Master Thesis, University of Gothenburg, Gothenburg.

Shoshan, Ella, 2015, *Applicability of International Law on Cyber Espionage Intrusions*, Master Thesis, Stockholm University, Stockholm.

Uribe, Eva, Jeffrey Apolis, Benjamin Bonin, John Hinton, Andrew Kosydar, Christopher Mairs, Timothy Sa, and Mark Tucker, 2019, *Paradigms and Challenges for Deterrence in Cyberspace*, SAND--2019-4389, 1762337, 674830, United States Department of Energy, Albuquerque.

Charter of the United Nations and Statute of the International Court of Justice, 24 October 1945.

United Nations Security Council Resolution 138, 1960, S/4349, United Nations.

International Covenant on Civil and Political Rights, 1966.

United Nations Convention on the Law of the Sea, 1982.

United Nations Security Council Resolution 1373, 2001, S/RES/1373 (2001), United Nations.

Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001.

Fragmentation of International Law: Difficulties Arising From The Diversivication and Expansion of International Law: Report of the Study Group of the International

Law Commission - Finalized by Martti Koskenniemi, 2006, A/CN.4/L.682, United Nations, Geneva.

Draft articles on the responsibility of international organizations, 2011, International Law Commission, 2011.