Kevin Jon Heller

LOW-INTENSITY CYBER OPERATIONS AND STATE SOVEREIGNTY IN CYBERSPACE

DJØF PUBLISHING
IN COOPERATION WITH THE
CENTRE FOR MILITARY STUDIES

LOW-INTENSITY CYBER OPERATIONS AND STATE SOVEREIGNTY IN CYBERSPACE

Kevin Jon Heller

LOW-INTENSITY CYBER OPERATIONS AND STATE SOVEREIGNTY IN CYBERSPACE

Djøf Publishing
In cooperation with the
Centre for Military Studies
2022

Kevin Jon Heller
LOW-INTENSITY
CYBER OPERATIONS AND
STATE SOVEREIGNTY
IN CYBERSPACE

This publication is peer reviewed according to the standards set by the Danish Ministry of Higher Education and Science.

Cover: Kelly Chigozie Kjelsø Arazu
Print: Ecograf, Brabrand

Printed in Denmark 2022

ISBN 978-87-574-5446-8

Djøf Publishing
Gothersgade 137
1123 København K

Telefon: 39 13 55 00
e-mail: forlag@djoef.dk
www. djoef-forlag.dk

Editors' preface

The publications of this series present new research on defence and security policy of relevance to Danish and international decision-makers. This series is a continuation of the studies previously published as CMS Reports. It is a central dimension of the research-based services that the Centre for Military Studies provides for the Danish Ministry of Defence and the political parties behind the Danish defence agreement. The Centre for Military Studies and its partners are subject to the University of Copenhagen's guidelines for research-based services, including academic freedom and the arm's length principle. As they are the result of independent research, the studies do not express the views of the Danish Government, the Danish Armed Forces, or other authorities. Our studies aim to provide new knowledge that is both academically sound and practically actionable. All studies in the series have undergone external peer review. And all studies conclude with recommendations to Danish decision-makers. It is our hope that these publications will both inform and strengthen Danish and international policy formulation as well as the democratic debate on defence and security policy, in particular in Denmark.

The present publication is a result of the additional grant specifically aimed at research in the international legal challenges of the Danish Defence, which the parties to the Danish Defence Agreement have awarded to the Centre for Military Studies. The international legal research is conducted in collaboration with the Faculty of Law, University of Copenhagen, and the Royal Danish Defence College. Read more at: https://jura.ku.dk/icourts/research/intermil/.

The Centre for Military Studies is a research centre at the Department of Political Science, University of Copenhagen. The centre conducts research into security and defence policy as well as military strategy. Read more about the centre, its activities, and other publications at: https://cms.polsci.ku.dk/english/

Copenhagen, June 2022
Kristian Søby Kristensen, Kevin Jon Heller
and Astrid Kjeldgaard-Pedersen.

Table of Contents

Abstract and Recommendations

The final report of the United Nations Open-Ended Working Group on Security of and in the Use of Information and Communication Technologies (OEWG), adopted by consensus in March 2021, affirms that international law applies to cyberspace and calls upon states 'to avoid and refrain from taking any measures not in accordance with international law'. Significant differences nevertheless remain concerning how international law applies to cyberspace, as states have been unable to agree on what kinds of cyber operations international law prohibits.

States are particularly divided over the international wrongfulness of cyber operations that penetrate a computer system located on the territory of another state but do not rise to the level of a use of force or prohibited intervention –often referred to as 'low-intensity' cyber operations. Low-intensity cyber operations, which include most acts of extraterritorial law-enforcement (including counterterrorism) and espionage, are the most common form of cyber operation and are likely to become even more common over time given their relatively low cost and significant utility for states.

This report compares and assesses three very different positions concerning whether low-intensity cyber operations violate the sovereignty of the territorial state. The first position, endorsed by the UK and until recently by the US, is that low-intensity cyber operations are never wrongful because sovereignty is a principle of international law, not a primary rule that can be independently violated. The second position, defended most vigorously by France, is that low-intensity cyber operations are always wrongful because sovereignty is a primary rule of international law that is violated by any non-consensual penetration of a computer system located on the territory of another state – what has been called the 'pure sovereigntist' approach. And the third position, adopted by states such as the Netherlands and the Czech Republic, is that although sovereignty is a primary rule of international law, only low-intensity cyber operations

that cause some kind of physical damage to the territorial state or render its cyberinfrastructure inoperable are wrongful – what has been referred to as the 'relative sovereigntist' approach.

The report concludes that **Denmark should adopt either pure sovereignty or relative sovereignty,** because the 'sovereignty as a principle' approach is incompatible with international law, has been overwhelmingly rejected by the international community, and has little to offer a small state that is more concerned with defending itself against cyberattacks than using them for offensive purposes. Pure sovereignty, as the report demonstrates, is more consistent with the traditional understanding of how sovereignty functions in the physical world and would better protect Denmark against damaging cyber espionage than relative sovereignty. But the report acknowledges that relative sovereignty has been endorsed by Denmark's most important allies, including the US and Norway, making its adoption attractive from a diplomatic perspective.

The report recommends that, regardless of which position it adopts, Denmark should **issue a public statement** concerning its understanding of how international law applies in cyberspace. If it endorses pure sovereignty, saying so publicly would be sufficient. But if it endorses relative sovereignty, Denmark could make a significant contribution to the development of the relative-sovereigntist position by specifying, in a manner most previous public statements have not, precisely what kinds of low-intensity cyber operations Denmark believes violate its sovereignty. The report also recommends that Denmark should **participate actively in the new OEWG,** which will report its findings to the General Assembly in 2022. Participation in the OEWG is necessary to ensure that Denmark's sovereign interests are adequately represented while the international law of cyberspace continues to develop.

Resumé og anbefalinger

Den endelige rapport fra FN's arbejdsgruppe om sikkerhed i og ved brugen af informations- og kommunikationsteknologier (OEWG), som blev enstemmigt vedtaget i marts 2021, bekræfter, at folkeretten gælder i cyberspace, og opfordrer stater til at "undgå og undlade at træffe foranstaltninger, som ikke er i overensstemmelse med folkeretten." Ikke desto mindre er der fortsat betydelige uenigheder om, hvordan folkeretten finder anvendelse i cyberspace, eftersom stater ikke har været i stand til at blive enige om, hvilke typer af cyberoperationer folkeretten forbyder.

Stater er især splittede i spørgsmålet om, hvorvidt cyberoperationer, som trænger ind i computersystemer lokaliseret på en anden stats territorium, men som ikke kvalificerer som magtanvendelse eller ulovlig intervention i juridisk forstand – såkaldte lavintensive cyberoperationer – er i uoverensstemmelse med folkeretten. Lavintensive cyberoperationer, som inkluderer de fleste handlinger, stater foretager i forbindelse med retshåndhævelse uden for eget territorium (herunder terrorbekæmpelse) og spionage, er den mest almindelige type af cyberoperation, og de vil formentlig blive endnu mere udbredte med tiden pga. deres relativt lave omkostninger og høje nytteværdi for stater.

Denne rapport sammenligner og vurderer tre meget forskellige positioner med hensyn til, hvorvidt lavintensive cyberoperationer overtræder territorialstatens suverænitet. Den første position, som indtages af Storbritannien og indtil for nylig af USA, er, at lavintensive cyberoperationer aldrig er uretmæssige, eftersom suverænitetsbegrebet blot er et princip i international ret og ikke en primær regel, der selvstændigt kan blive overtrådt. Den anden position, som især Frankrig er fortaler for, er, at lavintensive cyberoperationer altid er uretmæssige, fordi suverænitetsprincippet udgør en bindende folkeretlig regel, som overtrædes ved enhver indtrængen uden samtykke i et computersystem lokaliseret på en anden stats territorium. Denne position kaldes den rene suverænitetstilgang. Den tredje position, som indtages af bl.a. Holland og Tjekkiet, er, at selvom suverænitetsprincippet er en bindende folkeretlig regel, er det kun den delmængde af lavintensive cyberoperationer, som forårsager en

form for fysisk skade på territorialstaten eller efterlader dens cyberinfrastruktur ude af funktion, der er uretmæssige. Denne position kaldes også den relative suverænitetstilgang.

Rapporten konkluderer, at **Danmark bør tilslutte sig enten den rene eller den relative tilgang til suverænitet,** fordi den første position – "suverænitet som princip"-tilgangen – er uforenelig med folkeretten, i overvældende grad er blevet afvist af det internationale samfund og grundlæggende ikke er attraktiv for en småstat som Danmark, der må forventes at være mere optaget af at forsvare sig mod cyberangreb end at anvende cybermidler til offensive formål. Rapporten viser, at den rene suverænitetstilgang er mere i overensstemmelse med den traditionelle forståelse af, hvordan suverænitet fungerer i den fysiske verden og bedre vil kunne beskytte Danmark mod ødelæggende cyberspionage end den relative tilgang. På den anden side anerkender rapporten, at Danmarks vigtigste allierede, herunder USA og Norge, har tilsluttet sig den relative tilgang, hvilket gør denne attraktiv ud fra et diplomatisk perspektiv.

Rapporten anbefaler, at Danmark, uanset hvilken position der vælges, **bør udsende en offentlig erklæring** om sin forståelse af, hvordan folkeretten finder anvendelse i cyberspace. Vælges den rene tilgang, vil det være tiltrækkeligt blot at erklære det offentligt. Vælges den relative tilgang, kan Danmark yde et væsentligt bidrag til udviklingen af denne position i internationalt henseende ved at specificere præcist, hvilke former for lavintensive cyberoperationer Danmark mener krænker dets suverænitet. Rapporten anbefaler også, at **Danmark deltager aktivt i den nye FN-arbejdsgruppe (OEWG),** som afrapporterer sine konklusioner til FN's Generalforsamling i 2022. Aktiv deltagelse i OEWG'en er nødvendig for at sikre, at Danmarks interesser for så vidt angår suverænitet bliver tilstrækkeligt repræsenteret, mens folkerettens anvendelse i cyberspace fortsætter sin udvikling.

ACKNOWLEDGEMENTS

The author is grateful for valuable input from an anonymous peer reviewer as well as colleagues from CMS and the Faculty of Law at the University of Copenhagen.

1

Introduction

Since 2016, more than two dozen states and NATO have issued public statements concerning how international law applies in cyberspace. In general, the statements focus on the rules applicable to two types of cyber operations: those that violate the prohibition of the use of force in Art. 2(4) of the UN Charter and possibly qualify as an armed attack that triggers the right of self-defence; and those that violate the principle of non-intervention in customary international law because they are intended to coerce a state regarding matters that fall within its domaine réservé (e.g., the conduct of elections).

These types of cyber operations, however, are exceedingly rare. To date, no state has ever publicly described a cyber operation as a use of force, much less an armed attack; not even the Stuxnet virus that targeted Iran's nuclear programme in 2010, which the International Group of Experts (IGE) responsible for Tallinn Manual 2.0 unanimously agreed violated Art. 2(4).[1] Similarly, no state has ever explicitly invoked the principle of non-intervention in the cyber context, although the US strongly implied that Russian interference in the 2016 presidential elec-

1. *See* Michael N. Schmitt (ed.), T*allinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 342. Iran acknowledged the computer worm but denied that it caused significant damage. *See* Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," *JFQ* 67 (2012): 40, 46.

tion violated the principle,[2] as did Georgia in response to Russian attacks on key Georgian government agencies in 2019.[3]

A third type of cyber operation, by contrast, has become increasingly common: those that involve penetrating a computer system located on the territory of another state without its consent but do not qualify as a prohibited intervention or use of force[4] – what are often referred to as 'low-intensity' cyber operations.[5] Such operations normally involve either law enforcement or espionage. Extraterritorial law-enforcement is nearly always low intensity because such cyber operations generally aim at obtaining digital evidence or removing information (e.g., terrorist propaganda videos) from computer systems located abroad, not at harming the territorial state or coercing its government with regard to its domaine réservé.[6] And cyber espionage is almost by definition low intensity, because it involves the clandestine 'use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information'.[7]

According to the Council on Foreign Relations (CFR), 34 states have engaged in low-intensity cyber operations since 2005, and the frequency of such cyber operations has increased over time (from nine operations in 2010 to 34 in 2015 and 120 in 2020).[8] This trend is likely to contin-

2. *See* Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law* 112, no. 4 (October 2018): 583, 642.
3. *See* Agenda.Ge, "Georgia Accuses Russia of Widespread Cyber Attack," *Agenda.GE*, 20 February 2020, available at https://agenda.ge/en/news/2020/535.
4. Michael N. Schmitt and Liis Vihul, "Sovereignty in Cyberspace: Lex Lata Vel Non?" *AJIL Unbound* 111, no. 1 (2017): 213-14 (noting that the 'vast majority of hostile cyber operations attributable to states' fall into this category); *see also* Sean Watts and Theodor Richard, "Baseline Territorial Sovereignty in Cyberspace," *Lewis & Clark Law Review* 22, no. 3 (2018): 771, 794 ('[T]he far more prevalent form of State-sponsored cyber exploitation involves consequences below the thresholds of use of force or even the coercive element required by the principle of non-intervention'); Harriet Moynihan, "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention," *Chatham House Research Paper* 3 (December 2020) ('[I]n practice, the vast majority of cyber operations by states take place below the threshold of use of force, instead consisting of persistent, low-level intrusions that cause harm in the victim state but often without discernible physical effects').
5. *See, e.g.*, Watts and Richard, "Baseline," 2018, 794.
6. *See, e.g.*, Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 68.
7. *Ibid.*, 168.
8. *See* Council on Foreign Relations, "Cyber-Operations Tracker," *Council on Foreign Relations*, available at https://www.cfr.org/cyber-operations/.

ue, as low-intensity cyber operations are 'an inexpensive and potentially anonymous way of degrading adversaries during conflict or peacetime'.[9]

In contrast to cyber operations that potentially implicate the prohibition of the use of force or the principle of non-intervention, where there is general agreement concerning the applicable legal framework,[10] states are deeply divided over when low-intensity cyber operations violate international law – a question that depends on whether state sovereignty is a primary rule of international law in cyberspace and, if so, how it applies. More specifically, states have adopted three different and generally irreconcilable positions on that question. The first position, endorsed by the UK and until recently the US, is that low-intensity cyber operations are never wrongful, because sovereignty is a principle of international law, not a primary rule that can be independently violated. The second position, defended most vigorously by France, is that low-intensity cyber operations are always wrongful, because sovereignty is a primary rule of international law that is violated by any non-consensual penetration of a computer system located on the territory of another state – what has been called the 'pure sovereigntist' approach.[11] And the third position, adopted by states such as the Netherlands and the Czech Republic, is that although sovereignty is a primary rule of international law, only low-intensity cyber operations that cause physical damage to the territorial state or render its cyberinfrastructure inoperable are wrongful – what has been called the 'relative sovereigntist' approach.[12]

The lack of consensus over how sovereignty functions in cyberspace reflects genuine disagreement over the creation and content of international law. But it also undoubtedly reflects important policy differences between states concerning the desirability of using low-intensity cyber operations for offensive purposes. Whatever the source, though, the lack of agreement over the international-law framework that applies to low-intensity cyber operations undermines the ability of states such as

9. *See, e.g.*, Luke Chircop, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0," *Melbourne Journal of International Law* 20, no. 2 (2019): 1, 18.
10. *See generally* Przemysław Roguski, "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views," *The Hague Program for Cyber Norms Policy Brief* (March 2020).
11. Moynihan, "The Application," 2020, 21.
12. *Ibid*., 45.

Denmark to develop and execute their cyber strategies. States have no right to engage in cyber operations that violate international law; when they do, they bear responsibility for their internationally wrongful act.[13] Moreover, a state targeted by a cyber operation that violates international law is entitled to engage in countermeasures[14] against the responsible state.[15] Disagreements over which kinds of low-intensity cyber operations are internationally wrongful thus make it significantly more likely that actual operations will cause legal and political conflict between states, because states contemplating an offensive operation will find it very difficult to predict whether the target state will deem the operation wrongful and respond with countermeasures.

This report provides a comprehensive analysis of the three positions that states have taken on whether non-consensual[16] low-intensity cyber operations violate sovereignty. Section I lays out the positions, notes which states adopt them, and identifies how they differ in practice. Section II critiques the 'sovereignty as a principle' position currently defended solely by the UK, agreeing with the overwhelming majority of states that sovereignty functions in cyberspace as a rule, not as a principle. Section III provides a legal analysis of the two 'sovereignty as a rule' positions: pure sovereignty and relative sovereignty. It concludes that the pure-sovereigntist position has a much stronger foundation in general international law than the relative-sovereigntist position. Section IV rejects the most common legal objection to pure sovereignty: the supposed permissibility of espionage under international law. Section V shows how a variety of policy considerations also favour pure sovereign-

13. International Law Commission, "Articles on Responsibility of States for Internationally Wrongful Acts," Art. 2, *UN General Assembly* Res. 56/83 (December 2000) (ARSIWA).
14. Countermeasures are 'State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions'. Michael N. Schmitt, "'Below the Threshold Cyber Operations': The Countermeasures Response Option and International Law," *Virginia Journal of International Law* 54 (2014): 698, 700.
15. International Law Commission, "Articles on Responsibilities," 2000, Art. 49(1).
16. Because it is uncontroversial that a state can consent to a low-intensity cyber operation, this article addresses only those operations that are non-consensual. The expression 'low-intensity cyber operation' thus refers to operations taking place without the territorial state's consent. For the sake of readability, the article will not constantly note that a low-intensity cyber operation is non-consensual.

ty over relative sovereignty. And finally, given Denmark's need to defend itself against cyberattacks and its interest in contributing to the creation of customary international law, Section VI recommends that the Danish government should issue a public statement concerning whatever position on low-intensity cyber operations it decides to adopt.

The analysis in this report, it is important to note, has two limitations. First, it addresses only low-intensity cyber operations that take place in peacetime. The legality of offensive cyber operations in armed conflict, whether international or non-international, is determined by international humanitarian law as the lex specialis, requiring a separate and quite different legal analysis. Second, the report applies only to low-intensity cyber operations that are attributable to a state under the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA). It thus excludes from consideration cyber operations conducted by non-state actors of their own accord.

2

State Positions on Sovereignty

When states first began discussing in multilateral fora how international law applies in cyberspace, the idea that sovereignty is a primary rule of international law, not simply a principle from which specific rules are derived, seemed uncontroversial. In 2013, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which had been created by the General Assembly in 2004, issued a consensus report that concluded 'state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.[17] Two years later, the GGE – having expanded from 20 states to 25 – reaffirmed that position.[18] The General Assembly adopted the GGE's 2015 report by consensus.[19]

In 2018, however, the United Kingdom publicly rejected the GGE position concerning the status of sovereignty, despite having been a member of the group in both 2013 and 2015. According to then-Attorney General Jeremy Wright, the official UK position is that sovereignty

17. General Assembly of United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations Digital Library*, A/68/98 (24 June 2013): 8.
18. General Assembly of United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)," *United Nations Digital Library*, A/70/174 (22 July 2015): 12.
19. General Assembly of United Nations, "Resolution 70/237," *United Nations Digital Library* (30 December 2015): § 1-2(a).

is a principle, not a rule, and thus cannot be directly violated by a cyber operation:

> *Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.*[20]

To date, states have uniformly rejected the British position. Most strikingly, NATO's Allied Joint Doctrine for Cyberspace clearly endorses the idea that sovereignty applies in cyberspace as a rule[21] – a position that forced the UK to issue a reservation to the contrary.[22] Moreover, nearly every state that has issued a public statement concerning international law and cyberspace since Wright's speech has taken the same position as NATO. Three of those states (Brazil,[23] France,[24] and Germany[25]) were

20. Government of United Kingdom, "Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General Jeremy Wright QC MP," *Gov.uk* (23 May 2018): 5-6, available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
21. North Atlantic Treaty Organization, "Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations," *North Atlantic Treaty Organization* (29 January 2020): 20, section 3.7 and note 26.
22. *Ibid*. at page v ('The AJP refers to cyberspace operations as being, dependent on the context, potential violations of international law as a breach of sovereignty … [T]he UK government does not consider that the current state of international law allows for a specific rule or additional prohibition for cyberspace operations beyond that of a prohibited intervention').
23. *See* Russell Buchan, "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2015), 168, 184.
24. France, Ministry of Defence, "International Law Applied to Operations in Cyberspace," *Ministry of Defence* (2019): 9, available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+-Cyberespace.pdf ('The principle of sovereignty applies to cyberspace. France exercises its sovereignty over the information systems located on its territory').
25. Germany, The Federal Government, "On the Application of International Law in Cyberspace," *The Federal Government* (March 2021): 2, available at https://www.auswaertiges-amt.

part of the 2015 GGE, making their affirmation unsurprising. But most were not, including Austria,[26] Bolivia,[27] the Czech Republic,[28] Finland,[29] Guatemala,[30] Guyana,[31] Iran,[32] New Zealand,[33] and Switzerland.[34]

The US position, it is important to note, has oscillated over time. At first, the US seemed squarely in the sovereignty-as-a-rule camp. Presi-

de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

26. Quoted in Przemysław Roguski, "The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States," *Just Security*, 11 May 2020, available at https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/ ('Austria has recently been the target of a severe cyber operation. In that context, we would like to refer to the principle of state sovereignty. A violation of this rule constitutes an internationally wrongful act – if attributable to a state – for which a target state may seek reparation under the law of state responsibility').
27. Organization of American States, "Improving Transparency — International Law and State Cyber Operations: Fourth Report" *(Presented by Prof. Duncan B. Hollis)*, *OEA/Ser.Q*, CJI/doc. 603/20 rev.1 (March 2020): 30.
28. Czech Republic, National Cyber and Information Security Agency, "Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace Director of Cybersecurity Department," *National Cyber and Information Security Agency* (February 2020): 3, available at https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.
29. Finland, Ministry of Foreign Affairs "International Law and Cyberspace – Finland's National Positions," *Ministry of Foreign Affairs* (October 2020): 3, available at https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=160309752272.
30. Organization of American States, "Improving Transparency," 2020, 30.
31. *Ibid*., 30. It is also worth noting that the IGE conducted consultations with more than '50 states and international organizations' over an early draft of Tallinn Manual, and not a single state objected to the idea, reflected in Rule 4, that sovereignty applies in cyberspace as a rule. *See* Michael N. Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," *Texas Law Review* 95 (2017): 1639, 1649.
32. Iran, "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace," *Nournews*, Art. 2(2), July 2020, available at https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat ('According to the armed forces of the Islamic Republic of Iran, the territorial sovereignty and jurisdiction of the states are also extended to all elements of the cyberspace').
33. New Zealand, Ministry of Foreign Affairs and Trade, "The Application of International Law to State Activity in Cyberspace," *Ministry of Foreign Affairs and Trade* (1 December 2020): 3, available at https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.
34. Switzerland, Federal Department of Foreign Affairs, "Position Paper on the Application of International Law in Cyberspace," *Federal Department of Foreign Affairs*, Annex UN GGE 2019/2021 (2021): 2, available at https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf ('Sovereignty is also applicable to cyberspace').

dent Obama's 2011 International Strategy for Cyberspace affirmed that the 'development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyberspace'.[35] The US also endorsed the GGE's 2013 and 2015 reports.

In March 2020, however, the General Counsel of the Department of Defense (DoD) explicitly rejected the idea that sovereignty is a primary rule of international law in cyberspace:

> *For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory ... Indeed, many States' public silence in the face of countless publicly known cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view that there is an international prohibition against all such operations (regardless of whatever penalties may be imposed under domestic law).*[36]

US endorsement of the UK position, however, was short-lived. Almost certainly as a result of the President Biden's election, the US recently stated – in response to the Final Report of the GGE, which was issued in May 2021[37] – that '[i]n certain circumstances, one State's non-consensual cyber operation in another State's territory, even if it falls below the threshold of a use of force or nonintervention, could also violate

35. U.S. President, "International Strategy for Cyberspace," *Obama White House* (May 2011): 12, available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
36. U.S. Department of Defense, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," *U.S. Department of Defense* (2 March 2020): 11, available at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.
37. United Nations, Office for Disarmament Affairs, "Report of the Group of Governmental Experts on Advancing State Behaviour in the Context of International Security," *UNODA*, advance copy, annex, bullet 71(b) (28 May 2021).

international law'.[38] This assertion implies that the US now believes sovereignty can indeed function as a rule in cyberspace (at least sometimes).

Many states hoped that the UN Open Ended Working Group (OEWG), which was created by the General Assembly in 2019 and was open (unlike the GGE) to 'all interested states', would help bring clarity to the status of sovereignty in cyberspace, as well as to a number of other contested international law issues. Unfortunately, states were ultimately unable to agree on binding international rules. The OEWG's Final Report thus simply affirms the applicability of international law in cyberspace[39] and articulates 11 'voluntary, non-binding norms of responsible State behaviour'.[40]

Because the OEWG was unable to reach consensus on binding rules, there is currently no international consensus concerning whether sovereignty functions in cyberspace as a rule or as a principle. Moreover, although the vast majority of states take the former position, they disagree among themselves over how sovereignty functions as a rule in cyberspace. Some states endorse pure sovereignty, believing that any low-intensity cyber operation that involves penetrating a computer system located on another state's territory violates the targeted state's sovereignty. Others, by contrast, adopt relative sovereignty, insisting that a low-intensity cyber operation violates sovereignty only if it causes some kind of harm to the territorial state.

In short, states currently endorse three different positions on how sovereignty applies in cyberspace: (1) sovereignty as a principle, (2) pure sovereignty, and (3) relative sovereignty.

38. General Assembly of United Nations, "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts," *United Nations Digital Library*, UN Doc. A/76/136* (13 July 2021): 140.
39. *See* United Nations, Office for Disarmament Affairs, "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," *UNODA*, Final Report A/AC.290/2021/CRP.2 (10 March 2021): 1, bullet 2.
40. Ibid., 2, bullet 8.

2.1. Sovereignty as a Principle

The 'sovereignty as a principle' position is straightforward: an extraterritorial cyber operation is internationally wrongful only if it violates the principle of non-intervention or the prohibition of the use of force.[41] This position, adopted to date only by the UK, gives states carte blanche to conduct low-intensity cyber operations on the territory of other states – for law-enforcement or for espionage – without fear of legal retaliation.[42] As noted earlier, states are entitled to engage in countermeasures only in response to internationally wrongful acts.

2.2. Pure Sovereignty

The pure-sovereigntist position rejects the idea that a low-intensity cyber operation is internationally wrongful only if it rises to the level of a prohibited intervention or prohibited use of force. On the contrary, it insists that all low-intensity cyber operations are internationally wrongful, because sovereignty prohibits a state from penetrating a computer system on another state's territory without that state's consent. Under pure sovereignty, therefore, a state targeted by a low-intensity cyber operation always has the right to engage in countermeasures against the state responsible for the operation.

At least three states have explicitly adopted the pure-sovereigntist position: France, Iran, and Switzerland. France's public statement about how international law applies in cyberspace says that '[a]ny cyberattack against French digital systems ... constitutes a breach of sovereignty'[43]

41. *See, e.g.*, Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *AJIL Unbound* 111 (2017): 210 ('Because the doctrine of sovereignty does not prevent all actions by one state that affect another state or even "encroachment on other sovereign jurisdictions", a state involved in operations against ISIS, such as the United States, is not precluded from taking action against ISIS's cyber facilities in other states, even without the consent of the host state, unless doing so constitutes a prohibited intervention or use of force').
42. *See* Michael Schmitt, "In Defense of Sovereignty in Cyberspace," *Just Security*, 8 May 2018, 5, available at https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/. To be sure, states targeted by a low-intensity cyber operation could legally respond with a low-intensity cyber operation of its own. As discussed below, however, that will not be an option for most states.
43. France, Ministry of Defence, "International Law Applied," 2019, 7.

and defines French digital systems to include all 'information systems located on its territory'.[44] Iran claims that '[a]ny utilization of cyberspace if and when involves unlawful intrusion to the (public or private) cyber structures which is under the control of another state, may be constituted as the violation of the sovereignty of the targeted state'.[45] And Switzerland asserts that 'state sovereignty protects information and communication technologies (ICT) infrastructure on a state's territory against unauthorised intrusion or material damage', including 'computer networks systems and software supported by the ICT infrastructure, regardless of whether the infrastructure is private or public'.[46]

A fourth state, Guatemala, has adopted a position that borders on pure sovereignty: 'a State participating in a specific cyber operation violates a country's sovereignty if, in the course of a cyberattack, it takes certain information from another State's cyber realm, even when no harm that could affect equipment or the human rights of a person or persons is caused'.[47] This position does not require a low-intensity cyber operation to cause harm – thus distinguishing it from the relative-sovereigntist position discussed below – but it requires more than merely penetrating a computer system located on another state's territory.

Six other states have endorsed a position similar to Guatemala's. In 2013, WikiLeaks revealed that the US National Security Agency (NSA) had systematically intercepted the email and telephone communications of dozens of governments (friend and foe), international organizations, and NGOs.[48] In response, Mercosur issued a statement on behalf of its five members (Argentina, Brazil, Paraguay, Uruguay, and Venezuela) '[s]trongly rejecting the interception of telecommunications and the acts of espionage carried out in our countries' on the ground that it 'violates our sovereignty'.[49] The Bahamas also protested, insisting that international law guarantees in cyberspace 'the primacy of sovereignty, maintenance

44. *Ibid*., 6.
45. Iran, "Declaration of General Staff," 2020, Art. 2(4).
46. Switzerland, Federal Department of Foreign Affairs, "Position Paper," 2021, 2.
47. Organization of American States, "Improving Transparency," 2020, 30.
48. *See, e.g*., Buchan, "Cyber Espionage," 2015, 184.
49. General Assembly of United Nations, "Note Verbale Dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations Addressed to the Secretary-General," *United Nations Digital Library*, A/67/946 (July 2013): 2, available at https://undocs.org/pdf?symbol=en/A/67/946.

of territorial integrity, [and] freedom from undue external intrusion and influence'.[50] Given that the NSA cyber espionage did not cause any kind of harm to the penetrated computer systems, these statements strongly suggest that Argentina, the Bahamas, Brazil, Paraguay, Uruguay, and Venezuela subscribe to some version of the pure-sovereigntist position.

Finally, NATO appears to believe at least some low-intensity cyber operations that do not result in physical damage or render cyberinfrastructure inoperable are capable of violating sovereignty. The NATO Allied Joint Command Doctrine says that cyber operations 'that create only temporary disruptions or denials of service, or those intended merely for disseminating or gathering information ... may nevertheless constitute a violation of international law as a breach of sovereignty'.[51] Although that statement does not explicitly endorse pure sovereignty, it is closer to the pure-sovereigntist position than to the relative-sovereigntist position discussed below. The fuzziness of NATO's position likely reflects the fact that its members are themselves divided over how territorial sovereignty functions in cyberspace.

2.3. Relative Sovereignty

The relative-sovereigntist position shares the pure-sovereigntist belief that a cyber operation can be internationally wrongful even if it does not violate the principle of non-intervention or the prohibition of the use of force. But it rejects the idea that merely penetrating a computer system located on another state's territory without its consent violates the targeted state's sovereignty. According to relative sovereignty, a low-intensity cyber operation is internationally wrongful – thus permitting countermeasures – only if it causes some kind of harm to the territorial state or interferes with or usurps one of its inherently governmental functions.

As this phrasing indicates, the relative-sovereigntist position focuses on two aspects of what has been called the 'internal dimension' of state sovereignty: territorial integrity and governmental exclusivity. Territo-

50. Quoted in Rashad Rolle, "Lawyers to Act in NSA Spy Row," *The Tribune* (5 June 2014): 242, available at http://www.tribune242.com/news/2014/jun/05/lawyers-act-ns-spy-row/.
51. North Atlantic Treaty Organization, "Allied Joint Publication-3.20," 2020, 20 n.26.

rial integrity refers to a state's right 'to exercise supreme authority over all persons and things within its territory'[52] without 'any form of interference' by other states.[53] Governmental exclusivity refers to the right of each state to freely choose its 'political, economic, social, and cultural system' and determine its own foreign policy.[54]

2.3.1. The Tallinn Manual 2.0

The relative-sovereigntist idea that a low-intensity cyber operation can be internationally wrongful by violating either aspect of sovereignty's internal dimensions (territorial integrity or governmental exclusivity) is specifically based on the Tallinn Manual 2.0.[55]

The International Group of Experts (IGE) responsible for the Manual debated whether three different kinds of low-intensity cyber operations violate a state's territorial integrity. The first is a cyber operation that causes physical damage, such as 'malware that causes the malfunctioning of the cooling elements of equipment, thereby leading to overheating that results in components melting down'.[56] The vast majority of the IGE agreed that such an operation violates sovereignty.[57] The second is a cyber operation that causes cyberinfrastructure in the territorial state to lose significant functionality, such as the 2012 Shamoon 1 virus, which rendered inoperable thousands of hard drives used by Saudi Aramco.[58] The IGE agreed that sovereignty prohibits 'a cyber operation necessitating repair or replacement of physical components of cyber infrastructure amounts to a violation because such consequences are akin to physical damage or injury'.[59]

The third kind of cyber operation is one that causes neither physical damage nor any equivalent loss of cyberinfrastructure functionality.

52. Robert Jennings and Arthur Watts eds., *Oppenheim's International Law: Peace* (Longman, 9th ed., 1996), 382.
53. Wolff Heintschel von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace," in 4th *International Conference on Cyber Conflict*, ed. Christian Czosseck et al. (NATO CCD COE Publications, 2012), 1, 8.
54. International Court of Justice, "Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)," Judgment, *ICJ*, Rep. 14 (27 June 1986): 98, bullet 205.
55. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 20.
56. *Ibid*.
57. *Ibid*.
58. *Ibid*., 21.
59. *Ibid*.

Non-harmful operations[60] the IGE debated include 'causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major [denial of service] operation'.[61] The IGE could not reach consensus on these kinds of operations.[62]

The IGE was less divided concerning governmental exclusivity, although it struggled 'definitively' to define the concept of an 'inherently governmental function'.[63] Most importantly, the experts agreed that, for cyber operations in this category, '[i]t matters not whether physical damage, injury, or loss of functionality has resulted or whether the operation qualifies in accordance with the various differing positions outlined above for operations that do not result in a loss of functionality'.[64] A cyber operation interferes with an inherently government function when it disrupts 'data or services' that are necessary for that function to operate normally. Examples include 'changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities'.[65] By contrast, usurpation refers to a remote cyber operation that involves engaging in an inherently governmental function that is 'exclusively reserved to another State on the latter's territory'[66] – the most important of which, according to the IGE, is law-enforcement.[67]

2.3.2. State Positions

Eight states currently endorse relative sovereignty: the Netherlands, the Czech Republic, Finland, New Zealand, Germany, Guyana, Norway, and (as of 2021) the US. With regard to governmental exclusivity, there

60. For the sake of readability, this report often refers to 'harmful' and 'non-harmful' cyber operations. Harmful cyber operations include both those that cause physical damage and those that cause loss of cyberinfrastructure functionality equivalent to physical damage. Non-harmful refers to all other low-intensity cyber operations.
61. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 21.
62. *Ibid*.
63. *Ibid*., 22.
64. *Ibid*.
65. *Ibid*.
66. *Ibid*., 23.
67. *Ibid*., 22-3.

appears to be no differences between the relative-sovereigntist states. Finland,[68] the Czech Republic,[69] New Zealand,[70] the Netherlands,[71] Norway,[72] and Guyana[73] have each made statements that effectively endorse the Tallinn Manual 2.0's position on usurpation and interference. New Zealand and the Netherlands have also publicly agreed with the IGE conclusion that governmental sovereignty prohibits a state from engaging in extraterritorial law-enforcement.[74]

With regard to territorial integrity, relative-sovereigntist states agree that a low-intensity cyber operation is not internationally wrongful unless it causes some kind of harm to the state targeted by the operation. 'Some kind of harm' is obviously a rather vague expression. Unfortunately, the eight states that have endorsed relative sovereignty have not coalesced around a common understanding of what kind of harm separates a lawful low-intensity cyber operation from an unlawful one. The Czech Republic seems to set the bar the highest, limiting violations of sovereignty to cyber operations involving 'damage to or disruption of cyber or other infrastructure' that has 'a significant impact on national security,

68. Finland, Ministry of Foreign Affairs, "International Law," 2020, 2 ('[A]n unauthorized intrusion by cyber means may be seen as a violation of the target State's territorial sovereignty if it interferes with data or services that are necessary for the exercise of inherently governmental functions').
69. Czech Republic, National Cyber and Information Security Agency, "Statement by Mr. Richard Kadlčák," 2020, 3 (arguing that a low-intensity cyber operation violates sovereignty if its interference with 'data or services' has a 'significantly disrupting' effect on 'the exercise of inherently governmental functions').
70. New Zealand, Ministry of Foreign Affairs and Trade, "The Application," 2020, 2 ('The principle of sovereignty prohibits the interference by one state in the inherently governmental functions of another').
71. The Netherlands, Ministry of Foreign Affairs, "Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace — Appendix: International Law in Cyberspace," *Government of the Netherlands* (2019): 3, available at https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (claiming that sovereignty has been violated if 'there has been an interference with or usurpation of inherently governmental functions of another state').
72. *See* Statement of Norway in General Assembly of United Nations, "Official Compendium," 2021, 68.
73. *See* Organization of American States, "Improving Transparency," 2020, 30 (insisting that whether a low-intensity cyber operation violates sovereignty depends not only on territorial intrusion, but also on 'the degree of infringement and whether there has been an interference with government functions').
74. The Netherlands, Ministry of Foreign Affairs, "Letter of 5 July 2019," 2019, 2; New Zealand, Ministry of Foreign Affairs and Trade, "The Application," 2020, 2.

economy, public health or environment'.[75] The Netherlands simply endorses Rule 4 of the Tallinn Manual,[76] thereby requiring the cyber operation to cause physical damage or equivalent loss of cyberinfrastructure functionality – a position echoed by Norway.[77] And according to Finland, a cyber operation that causes 'material harm' violates sovereignty.[78]

Four other states that endorse the relative-sovereigntist position have provided almost no indication of what kind of harm is required. Germany says only that 'negligible physical effects and functional impairments below a certain impact threshold cannot – taken by themselves – be deemed to constitute a violation of territorial sovereignty',[79] while the US simply insists that sovereignty cannot be violated when a cyber operation has 'no effects or de minimis effects'.[80] Guyana is similarly unhelpful, asserting that whether a low-intensity cyber operation violates sovereignty depends on 'the degree of infringement' involved in the operation.[81] And New Zealand is the least helpful of all, noting only that 'there is a range of circumstances – in addition to pure espionage activity – in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful'.[82]

2.4. Practical Differences

In practical terms, the UK 'sovereignty as a principle' position differs substantially from the two positions that view sovereignty as a rule.

75. Czech Republic, National Cyber and Information Security Agency, "Statement by Mr. Richard Kadlčák," 2020, 3.
76. The Netherlands, Ministry of Foreign Affairs, "Letter of 5 July 2019," 2019, 3.
77. Statement of Norway in General Assembly of United Nations, "Official Compendium," 2021, 67.
78. Finland, Ministry of Foreign Affairs, "International Law," 2020, 2. Finland also suggests that a 'relevant consideration' in determining a violation of sovereignty is whether a low-intensity cyber operation 'modifies or deletes information'. *Ibid*. It is unclear, however, whether Finland believes that modification or deletion of information, standing alone, is sufficient for a sovereignty violation.
79. Germany, The Federal Government, "On the Application," 2021, 4.
80. Statement of the United States in General Assembly of United Nations, "Official Compendium," 2021, at 140.
81. Organization of American States, "Improving Transparency," 2020, 30.
82. New Zealand, Ministry of Foreign Affairs and Trade, "The Application," 2020, at 3.

Whereas the latter impose limits on what kinds of low-intensity cyber operations a state can lawfully engage in, the former views all such operations as lawful. For the UK, a cyber operation is internationally wrongful – thus entitling the targeted state to engage in countermeasures – only if it violates the principle of non-intervention or the prohibition of the use of force.

In addition to viewing sovereignty in cyberspace as a rule and not a principle, the pure-sovereigntist and relative-sovereigntist positions agree that extraterritorial law enforcement (including counterterrorism) violates the sovereignty of the territorial state. According to pure sovereignty, low-intensity law-enforcement operations are internationally wrongful simply because they involve penetrating a computer system located on another state's territory. According to relative sovereignty, low-intensity law-enforcement operations violate sovereignty because they usurp one of the targeted state's inherently governmental functions – a type of violation that does not require causing any kind of harm to the penetrated computer system.

The most significant difference between the pure-sovereigntist and relative-sovereigntist positions, therefore, concerns the legality of cyber espionage. Pure sovereignty deems all cyber espionage unlawful because it necessarily involves non-consensually penetrating a computer system on another state's territory.[83] By contrast, despite their differences, the eight states that have adopted relative sovereignty agree that the mere penetration of a computer system is not enough. That means that they all accept that cyber espionage is lawful – from installing backdoors to exfiltrating information – as long as it does not cause any harm to the targeted state's cyberinfrastructure.

83. Interestingly, France's statement on international law in cyberspace includes a footnote stating, '[t]his document does not contain any specific analysis or treatment of cyberespionage, which is not illegal in international law, though it may infringe such law when linked with an internationally wrongful act'. France, Ministry of Defence, "International Law Applied," 2019, 4, n. 2. Unless France believes that there is an exception in customary international law specifically permitting espionage (a possibility considered and rejected in the next section), the pure-sovereigntist French approach would deem all acts of cyber espionage on its territory internationally wrongful, because cyber espionage by definition involves non-consensually penetrating a French computer system.

3

The UK Position

Read closely, the British statement on cyberspace does not deny that, under general international law, sovereignty is a primary rule distinct from the prohibition of the use of force and the principle of non-intervention. That is unsurprising, because the idea that sovereignty is a primary rule is supported not only by International Court of Justice (ICJ) jurisprudence,[84] but also by multilateral treaties,[85] General Assembly resolutions,[86] and a vast amount of state practice and opinio juris

84. See, e.g., International Court of Justice, "Corfu Channel Case (United Kingdom v. Albania)," Judgment, *International Court of Justice* Rep. (9 April 1949): 35 (holding that '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations'); International Court of Justice, "Military and Paramilitary Activities," 1986, 118, bullet 251 (noting that although '[t]he effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of nonintervention', sovereignty remains an independent rule); International Court of Justice, "Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica Along the San Juan River (Nicar. v. Costa Rica)," Judgment, *International Court of Justice*, Rep. 1, 2-4 (16 December 2015): 79, bullet 229 (holding that Nicaragua 'violated the territorial sovereignty of Costa Rica' by using its military to dredge a river on Costa Rican territory without its consent).
85. Examples include the UN Convention Against Transnational Organized Crime, which provides that 'States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of nonintervention in the domestic affairs of other States', United Nations, Office on Drugs and Crime, "United Nations Convention Against Transnational Organized Crime," *General Assembly resolution*, Res. 55/25, Annex, Art. 4 (15 November 2000) and the Helsinki Accords, which contain separate provisions on sovereignty, the use of force, and intervention. Final Act of the Conference on Security and Cooperation in Europe, Arts. 1, 2, 6, 14 ILM 1292, *OSCE* (August 1975).
86. The best example is the Friendly Relations Declaration, adopted by consensus by the General Assembly in 1970, which specifically distinguishes between the prohibition of the use of force, the principle of non-intervention, and sovereignty when itemizing the rules of international law that govern cooperation between states. General Assembly of United

concerning actions on land,[87] in the air,[88] and at sea.[89] Instead, the UK position is based on the idea that – to quote the now-superseded statement by the DoD General Counsel in 2020 – 'there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits ... non-consensual cyber operations in another State's territory'.[90] In other words, the argument is that although sovereignty functions as a primary rule of international law in the physical world, that rule does not apply in cyberspace.

There are two significant problems with the UK position. The first is that it significantly overstates the extent of international disagreement concerning whether sovereignty applies in cyberspace in the same way as it applies in the physical world.[91] As we have seen, no other state current-

Nations, "Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations," Annex, 4, *UN General Assembly* Res. 2625 (XXV) (October 1970).

87. For example, in response to Israel's abduction of Adolph Eichmann from Argentina, the Security Council adopted Res. 138, which affirms that 'violation of the sovereignty of a Member State is incompatible with the Charter of the United Nations'. UN Security Council, "Security Council Resolution 138 (Question relating to the case of Adolf Eichmann)," *United Nations Digital Library*, S/RES/4349 (30 June 1960).
88. Notable examples include the Chinese claim in 2003 that the distressed landing of a US reconnaissance plane on a Chinese island violated its territorial sovereignty (a claim the US implicitly accepted); Schmitt and Vihul, "Respect for Sovereignty," 2017, 1657, and Pakistan's repeated denunciation of US drone operations as 'a violation of Pakistani sovereignty and territorial integrity'. *Ibid*.
89. Two incidents in which Iran detained sailors they believed had violated the state's 'sovereign boundaries' are particularly illuminating: the capture of personnel from Britain's HMS Cornwall in 2007, *ibid*. 1658, and the unprotested detention of two U.S. Navy vessels that had mistakenly entered Iran's territorial waters. *Ibid*. In each situation, although the disputed actions could at least arguably have been characterized as uses of force, the states in question debated them using the language of sovereignty.
90. U.S. Department of Defense, "DOD General Counsel Remark," 2020, 11. Israel has questioned the idea that sovereignty necessarily applies in cyberspace in the same way that it does in the physical world, though it has refrained from concluding that sovereignty is a principle and not a rule in cyberspace. *See* Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *International Law Studies* 97 (2021): 396, 397 ('It cannot be automatically presumed that a customary rule applicable in any of the physical domains is also applicable to the cyber domain. The key question in identifying State practice is whether the practice which arose in other domains is closely related to the activity envisaged in the cyber domain. Additionally, it must be ascertained that the *opinio juris* which gave rise to the customary rules applicable in other domains was not domain-specific').
91. As noted above, at the time the UK adopted the sovereignty-as-a-principle position, few states had weighed in on the sovereignty debate. Later rejections of the UK position, how-

ly endorses the UK position, and at least two dozen states have explicitly rejected it.

The second and more important problem is that there is actually no need to find a rule of customary international law that 'extends' sovereignty into cyberspace, because general rules of international law have long been understood to apply in a technologically neutral manner. In the landmark Legality of the Threat or Use of Nuclear Weapons case, for example, nuclear states argued that generally applicable rules of international humanitarian law (IHL), such as distinction and proportionality, could not be applied to nuclear weapons because those weapons did not exist at the time the general rules were created. The ICJ disagreed:

> *[T]here is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.*[92]

The Court reached a similar conclusion concerning three conventional rules of the jus ad bellum – the prohibition of the use of force, the right of self-defence against an armed attack, and the power of the Security Council to authorize military action in response to a breach of the peace or an act of aggression. 'These provisions', the Court noted, 'do not refer to specific weapons'. The Court thus held that, as general rules, they apply 'to any use of force, regardless of the weapons employed'.[93]

---

ever, have not led the UK to rethink it. On the contrary, in its 2021 submission of the GGE, the UK again insisted that it 'does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention'). *See* United Kingdom, "Application of International Law to States' Conduct in Cyberspace," *Government of United Kingdom* (3 June 2021): bullet 10, available at https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

92. International Court of Justice, "Legality of the Threat or Use of Nuclear Weapons," Advisory Opinion, *International Court of Justice* Rep. 226 (8 July 1996): bullet 86.
93. *Ibid*., bullet 38.

The idea that it is unnecessary to find sufficient state practice and opinio juris for specific applications of a general rule of international law should not be controversial – even in the context of cyberspace. After all, states overwhelmingly agree that the basic rules of IHL, including the principle of distinction, apply equally to cyber and kinetic attacks. That position has been taken, inter alia, by the GGE,[94] NATO,[95] the EU,[96] and nearly the entirety of the OAS.[97] Those rules long predated the cyber era, yet no state suggested in those fora (or has suggested since) that sufficient cyber-specific state practice and opinio juris is required to extend them to cyberattacks.

The UK position on sovereignty in cyberspace makes sense, in short, only if the primary rule of sovereignty in international law is limited to kinetic activities. Applying the rule to cyberspace would then require sufficient state practice and opinio juris to justify the extension. But that is not the case: like the basic rules of the jus in bello and jus ad bellum, sovereignty is a general rule that is not limited to particular means of interfering with a state's exclusive right to control its territory and determine its foreign policy. As the Permanent Court of International Justice (PCIJ) said in the seminal Lotus case:

> *[T]he first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another*

94. United Nations, Office of Disarmament Affairs, "Report of Governmental Experts," 2021: bullet 71(f) (noting the applicability in cyberspace of 'established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction').
95. NATO, "Allied Joint Publication-3.20," 2020, 19 ('NATO COs must be conducted in accordance with international law, including the United Nations (UN) Charter, Law of Armed Conflict (LOAC) and human rights law, as applicable').
96. *See* EU Council Conclusions, "General Affairs Council Meeting," *Council of the European Union*, Doc. No. 11357/13, Annex (21 June 2013): 4, available at https://data.consilium.europa.eu/doc/document/ST%2011357%202013%20INIT/EN/pdf ('Recognising that international law, including ... relevant conventions on international humanitarian law and human rights ... provide a legal framework applicable in cyberspace').
97. *See* Laurent Gisel et al., "Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts," *International Review of the Red Cross* 913 (March 2021): nn. 56-7, available at https://international-review.icrc.org/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913#footnote59_ilkhhlq. The exceptions are Cuba and Nicaragua. *Id*. at n. 58.

> *State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.*[98]

Because sovereignty is a general rule, the UK is wrong to insist that state practice and opinio juris must establish that sovereignty applies in cyberspace. On the contrary, the default position is that sovereignty applies in cyberspace no less than in the physical world, with the burden of proof on the UK to show otherwise.[99] That is a burden it cannot satisfy, given that other states uniformly believe that sovereignty is a general rule of international law.

98. The Permanent Court of International Justice, "The Case of the S.S. Lotus," *The Permanent Court of International Justice* Series A, No. 10 (7 September 1927): 18-19 (emphasis added).
99. *See* Dapo Akande et al., "Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond," *Just Security* (5 January 2021), available at https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

4

Pure Sovereignty vs. Relative Sovereignty

The fundamental issue concerning the legality of non-consensual, low-intensity cyber operations is thus not whether sovereignty applies to them but how. Given how sovereignty functions in the physical world, the pure-sovereigntist position has a much stronger legal foundation than the relative-sovereigntist one.

4.1. Extraterritorial Power and the Lotus Case

The argument for the pure-sovereigntist position is straightforward: the first Lotus principle prohibits a state from exercising 'any form' of power on the territory of another state in the absence of an international rule permitting it to do so; penetrating a computer system in another state is a form of exercising power on that state's territory; no permissive rule of international law authorises such penetration. All low-intensity cyber operations, therefore, violate the territorial state's sovereignty, even those that do not cause any harm.

The first Lotus principle is widely considered to accurately reflect how customary international law understands territorial sovereignty.[100] Indeed, even the Tallinn Manual 2.0 takes the position that the princi-

100. *See, e.g.*, Simon Chesterman, "The Spy Who Came in from the Cold War: Intelligence and International Law, *Michigan Journal of International Law* 27, no. 4 (2006): 1071, 1081 ('The foundational rules of sovereignty ... provide some guidance on what restrictions, if any, might be placed on different forms of intelligence gathering that do not rise to the

ple is customary: 'The Experts agreed that a violation of sovereignty occurs whenever one State physically crosses into the territory or national airspace of another State without either its consent or another justification in international law'.[101] The Manual specifically cites Lotus for that point.[102]

More importantly, the first Lotus principle is consistent with state practice. In terms of airspace, for example, the U.S. Department of Defense has noted that aerial warfare has led to the creation of 'a highly restricted regime of air law in which any entry into a nation's airspace without its permission [is] to be regarded as a serious violation of its sovereignty and territorial integrity'.[103] That highly-restricted regime is explicitly embraced by the Chicago Convention on International Civil Aviation, which 'affirms that every state enjoys complete and exclusive sovereignty over the airspace above its territory'[104] and categorically prohibits all state aircraft from entering another state's airspace without its consent.[105] And states have routinely invoked their territorial sovereignty to condemn even the most minor and harmless incursions into their airspace as sovereignty violations (e.g., Estonia's formal complaint to Russia when a Russian jet entered its airspace for less than 60 seconds).[106]

States also view unauthorized entry into their territorial sea as a violation of sovereignty, even when that entry does not cause any harm.[107] To be sure, that inviolability is limited by a variety of rights of passage and entry. But as Schmitt and Vilhul note, '[t]he regimes of innocent, transit, and archipelagic passage developed as customary and treaty-law

level of an armed attack or violate other specific norms. The basic rule was articulated by the Permanent Court of International Justice in the 1927 *Lotus* case').

101. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 19.
102. *Ibid*., 67, n. 82.
103. U.S. Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., November 1999): 2.
104. United Nations Specialized Agency, "Convention on International Civil Aviation," *ICAO*, 61 Stat. 1180, 15 UNTS 295 (7 December 1944): Art. 1.
105. *Ibid*. Art. 3(c).
106. Radio Free Europe/Radio Liberty, "Estonia Says Russian Aircraft Violated Airspace Again," *Radio Free Europe/Radio Liberty*, 6 September 2016, available at http://www.rferl.org/a/russia-estonia-airspace-violated/27970888.html.
107. Schmitt and Vihul, "Respect for Sovereignty," 2017, 1657-59.

exceptions to the territorial sea's inviolability; they modify the baseline principle that maritime borders may not be pierced by other States'.[108]

State practice on land generally concerns abduction, which normally involves no harm. States have routinely protested abductions from their territory as inconsistent with their sovereignty.[109] We have already noted the most famous example, Israel's kidnapping of Eichmann in Argentina, which was explicitly condemned on sovereignty grounds by the Security Council. A more recent example is the US kidnapping of Abu Omar from the streets of Milan, which led Italy to insist that the US had a legal duty to 'fully respect Italian sovereignty'.[110]

4.2. Lotus in Cyberspace

Two propositions, in short, have a strong basis in international law. The first is that sovereignty functions in cyberspace as a rule, not as a principle, because it is a general rule of international law that applies to all forms of exercising power on another state's territory. The second is that the general rule of sovereignty in the physical world prohibits any penetration of a state's territory, even penetration that is completely harmless.

Taken together, those propositions suggest that, in terms of low-intensity cyber operations, the pure-sovereigntist position is correct: any remote penetration of a computer system, even penetration that does not cause any harm, violates the territorial sovereignty of the state in which the computer system is located. Simply put, there is no reason to believe that sovereignty functions any differently in cyberspace than in the physical world: 'the same rules regarding violation of sovereignty apply whether the exercise of authority by the perpetrating state is carried out through a physical presence on the territory of the affected state or remotely from outside the affected territory'.[111]

108. *Ibid*., at 1645.
109. *See, e.g*., L.C. Green, "The Eichmann Case," *Modern Law Review* (1960): 507, 509.
110. The Irish Times, "Italy Tells US to Respect Sovereignty After Kidnap," *The Irish Times* (1 July 2005), available at https://www.irishtimes.com/news/italy-tells-us-to-respect-sovereignty-after-kidnap-1.1179451.
111. Moynihan, "The Application," 2020, 17; *see also* Chircop, "Territorial Sovereignty in Cyberspace," 2019, 20 ('[T]he strongest argument in favour of the strict inviolability approach is that an equivalent standard of territorial sovereignty has long been accepted by states in

This conclusion is supported by the ICJ's insistence in the Legality of the Threat or Use of Nuclear Weapons case that general rules of international law are normally technologically neutral. When a state uses a low-intensity cyber operation to obtain evidence of a crime, delete terrorist recruiting videos, or steal corporate IP, it is still engaging in law enforcement, counterterrorism, or espionage. Only the means of carrying out those traditional state functions are different. The idea that sovereignty functions differently in cyberspace than in the physical world is thus no more compelling than the idea that key rules of IHL function differently for nuclear weapons than for conventional ones.

Moreover, despite its seeming virtuality, cyberspace is no less a territorial domain than air, sea, or land. As the Tallinn Manual 2.0 points out, '[c]yber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives'.[112] This means that a state's sovereign right to protect data is no different than its sovereign right to protect brick-and-mortar objects.[113] There is no reason why the general rule of sovereignty would provide a state's cyberinfrastructure with less protection than its physical infrastructure.[114]

4.3. Are Low-Intensity Cyber Operations an 'Exercise of Power'?

The first Lotus principle applies to remote low-intensity cyber operations only if they qualify as a state 'exercis[ing] its power ... in the territory of another state'. But that is clearly the case. As we have seen, in the physical world, the mere penetration of a state's airspace, territorial

respect of physical space, and that the content of the principle should not differ across the physical and cyber domains').

112. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 12.

113. Chircop, 2019, 17 ('The critical next step is to recognise that states also exercise territorial sovereignty over data emanating from their cyber infrastructure. The basis of a state's claim to territorial sovereignty over data remains physical, in that it is limited to data that emanates from infrastructure located on its territory').

114. *See, e.g.*, *ibid.*, 23 (pointing out that 'it would be curious if the rule of territorial sovereignty provided a state's sovereign cyber infrastructure with less protection from intrusion than a state's sovereign physical territory').

sea, or land qualifies as an exercise of power that violates the first Lotus principle in the absence of a conventional or customary exception allowing it; no physical effects, much less actual harm, is required. Mutatis mutandis, merely penetrating a computer system located on another state's territory, should also qualify as an exercise of power.[115] In both contexts, the salient characteristic of the act is that a state is exercising its sovereign authority on the territory of another state without its consent.

Such 'mere penetration', it is important to note, is distinguishable from situations in which a state intercepts wireless signals emanating from another state without penetrating a computer system located on its territory. That kind of interception does not violate sovereignty, because the interception is not considered extraterritorial. In Weber and Saravia v. Germany, for example, the European Court of Human Rights (ECHR) affirmed the legality of a program in which '[s]ignals emitted from foreign countries are monitored by interception sites situated on German soil'.[116] The ECHR held that such 'strategic monitoring measures' did not violate Uruguay's territorial sovereignty because they involved 'international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links'.[117]

These kinds of cyber operations, which also include using spy satellites to intercept wireless signals,[118] do not violate territorial sovereignty for two reasons: (1) the state agents intercepting the information are located outside of the targeted state; and (2) the interception does not require penetrating cyber infrastructure located on the targeted state's territory. A low-intensity cyber operation satisfies (1) but not (2): although the operation is conducted remotely, obtaining the information

115. *See*, *e.g.*, Patricia L. Bellia, "Chasing Bits Across Borders," *The University Chicago Legal Forum* (2001): 35, 77 (rejecting the argument that 'a remote search is less invasive than a physical search' because '[i]f the sovereignty interest at issue is the target state' power to protect persons and property within its borders, it does not matter whether interference with that power comes from inside or outside of the target state'); Moynihan, "The Application," 2020, 19-20 ('There seems to be no reason in principle to distinguish physical violations (i.e. activity carried out by a state agent physically on the territory of the victim state) and remote violations (i.e. activity carried out from outside the affected state's territory)').
116. European Court of Human Rights, "Weber and Saravia v. Germany," *European Court of Human Rights*, Decision, App. No. 54934/00 (29 June 2006): bullet 88.
117. *Ibid*.
118. *See*, *e.g.*, Chesterman, "The Spy," 2006, 108.

requires penetrating computer systems located on the territory of the targeted state.[119] Such low-intensity cyber operations thus involve precisely the 'exercise [of] power ... in the territory of another state' that the first Lotus principle prohibits.[120]

This analysis is supported by the Tallinn Manual 2.0 itself. The Manual specifically distinguishes between remote cyber operations that simply intercept wireless signals and remote cyber operations that involve penetrating computer systems located on the territory of another state. In the IGE's view, the former cannot violate sovereignty 'because the cyber operation does not manifest in cyber infrastructure on the target State's territory'.[121] By contrast, the latter at least potentially violates sovereignty, because such operations do territorially manifest.[122] In other words, the IGE does not deny that low-intensity cyber operations are an 'exercise [of] power ... in the territory of another state'. Instead, it suggests that the 'precise legal character' of such operations 'is somewhat unsettled in international law'.[123]

119. See, e.g., Katharina Ziolkowski, "Peacetime Cyber Espionage: New Tendencies in International Law," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, ed. Katharina Ziolkowski (NATO CCD COE Publications, 2013): 425, 429 (arguing that cyber espionage does not include 'electronic reconnaissance and surveillance methods ... using, for example, satellites, long-range cameras and acoustic devices, as such methods do not include copying of data from IT-systems or computer networks').
120. *See, e.g.*, Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," *Baltic Yearbook of International Law* 14 (2017): 137, 145 ('[I]t could well be argued that the intrusion by US officials into data stored on servers located on German soil amounts to a violation of Germany's territorial sovereignty because they are hereby, albeit remotely, exercising US governmental authority on German territory without German consent'); Przemyslaw Roguski, "Violations of Territorial Sovereignty in Cyberspace: An Intrusion-based Approach." *In Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield, 2020): 75 ('If the agents of a state perform cyber operations within the cyber infrastructure of another state in ways other than the intended use of said cyber infrastructure, that is, by violating the information security of computer systems, they exercise state power vis-à-vis cyber infrastructure under the jurisdiction of another state').
121. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 19-20.
122. *Ibid*., 20.
123. *Ibid*.

4.4. Does a Permissive Rule Apply to Low-Intensity Cyber Operations?

Because remotely penetrating a computer system involves the 'exercise [of] power ... in the territory of another state', all low-intensity cyber operations violate the first Lotus principle unless there is either a conventional or customary rule that permits such penetration. There are numerous conventional rules that explicitly permit states, on an exceptional basis, to violate another state's territorial sovereignty. An obvious example is Art. 17 of UNCLOS, which provides that, '[s]ubject to this Convention, ships of all States, whether coastal or land-locked, enjoy the right of innocent passage through the territorial sea.'[124] By contrast, no convention explicitly or even implicitly permits states to engage in low-intensity cyber operations on the territory of another state as long as they are not harmful.

There is also no persuasive argument that customary international law imposes a de minimis test on low-intensity cyber operations that it does not impose on physical violations of territorial sovereignty. Even if ratifications of the Budapest Convention do not count as evidence to the contrary,[125] the state practice discussed above indicates that, at best, states are nearly equally divided between the pure-sovereigntist and relative-sovereigntist positions. That is far from the 'general practice' that the creation of a customary cyber exception to the first Lotus principle requires.

124. United Nations, "United Nations Convention on the Law of the Sea," *United Nations*, 1833 UNTS 397 (10 December 1982): Art. 17.

125. The ILC Draft Conclusions on the Identification of Customary International Law contemplate the ratification of treaties qualifying, in certain circumstances, as opinio juris. *See* General Assembly of United Nations, "Report of The International Law Commission on the work of its sixty-sixth session," *United Nations Digital Library*, A/69/10 (2014): Draft Conclusion 10(2).

5

The Question of Espionage

Despite some members of the IGE defending the pure-sovereigntist position, the Tallinn Manual 2.0 insists that '[t]he precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law'.[126] The IGE's reluctance to endorse pure sovereignty appears to be based on the supposed lawfulness of espionage under international law: given the nature of general rules, if sovereignty does not prohibit espionage in the physical world, there is no reason to assume it prohibits espionage in cyberspace. And if cyber espionage is lawful, the pure-sovereigntist position cannot be correct.

The espionage argument takes two very different forms: (1) espionage is affirmatively permitted by international law; and (2) international law does not regulate espionage, so it is neither affirmatively lawful nor affirmatively unlawful. Neither argument is persuasive.

5.1. Is Espionage Lawful?

A minority of scholars make the more assertive claim that state practice and opinio juris have created a customary exception to territorial sovereignty that permits states to engage in espionage, whether kinetic or cyber. Brown and Poellet argue, for example, that '[y]ears of state practice accepting violations of territorial sovereignty for the purpose of espionage have apparently led to the establishment of an exception

126. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 20.

to traditional rules of sovereignty – a new norm seems to have been created'.[127]

This argument, however, suffers from a glaring problem: although states clearly engage in espionage in the physical world and in cyberspace, they rarely, if ever, argue that international law entitles them to do so.[128] The creation of customary international law requires both state practice and opinio juris; state practice is not enough.[129] The brute fact that espionage is commonplace is thus incapable on its own of creating a customary exception to territorial sovereignty.[130] Moreover, numerous states have denounced espionage as unlawful – opinio juris that cuts precisely the other way. A particularly powerful example is Mercosur's five-party statement 'strongly rejecting the [NSA's] interception of telecommunications and the acts of espionage carried out in our countries' on the ground that such 'unacceptable behaviour ... violates our sovereignty'.[131]

The idea that international law prohibits espionage is supported by the fact that most states criminalize espionage conducted on their ter-

127. Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (2012): 126, 134; *see also* Jeffrey H. Smith, "Symposium: State Intelligence Gathering and International Law: Keynote Address," *Michigan Journal of International Law* 28, no. 3 (2007): 543, 544 ('[B]ecause espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law').

128. *See, e.g.*, Buchan, "Cyber Espionage," 2015, 162 (noting that, although 'on rare occasions states have publicly acknowledged their espionage activities and, in doing so, have sought to provide justifications for this conduct ... these states have steadfastly refused to justify their conduct on the basis that it is lawful under customary international law'); Pål Wrange, "Intervention in National and Private Cyberspace and International Law," in *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, eds. Jonas Ebbesson et al. (Brill/Nijhoff, 2014): 307, 321 ('I know of no state that has publicly claimed that espionage in all its forms is legal. On the contrary, states generally deny being involved in illegal espionage, and admit only when there is full proof').

129. *See, e.g.*, International Court of Justice, "North Sea Continental Shelf Cases (Ger./Den.; Ger./Neth.)," Judgment, *International Court of Justice* Rep. 3 (20 February 1969): bullet 77 ('Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it').

130. *See, e.g.*, Craig Forcese, "Spies Without Borders: International Law and Intelligence Collection," *Journal of National Security Law and Policy* 5 (2011): 179, 202 ('Even if it is commonplace, spying is a poor candidate for a customary international law exception to sovereignty – whatever state practice exists in the area is hardly accompanied by opinio juris').

131. General Assembly of United Nations. "Note Verbale Dated 22 July," 2013, 2.

ritory, which indicates that they do not view espionage as affirmatively lawful.[132] If customary international law permitted espionage, a state would commit a wrongful act by prosecuting a foreign national for engaging in it. This is the second Lotus principle, which holds that, for actions that take place on its own territory, 'all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty'.[133] In other words, because international law is superior to domestic law, a state cannot prohibit what international law specifically permits. A useful analogy is the combatant's privilege to kill in an international armed conflict. That privilege is specifically guaranteed by international humanitarian law,[134] so it would be internationally wrongful for a state to bring murder charges against an enemy soldier who killed in the heat of battle.

5.2. Is Espionage Unregulated?

The weakness of the idea that espionage is affirmatively permitted by international law likely explains why the IGE takes the position that espionage is simply unregulated by international law; neither permitted nor prohibited.[135] This position has the advantage of making the widespread domestic criminalization of espionage irrelevant to whether international law prohibits committing espionage on the territory of another state. If the baseline position is that espionage is unregulated by international law, the fact that states choose to criminalize espionage domestically does not count – at least without more – as either state

132. *See, e.g.*, Catherine Lotrionte, "Countering State-Sponsored Cyber Economic Espionage Under International Law," North Carolina Journal of *International Law and Commercial Regulation* 40 (2014): 443, 479.
133. The Permanent Court of International Justice, "The Case of the S.S. Lotus," 1927, 19.
134. United Nations Human Rights, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts," *United Nations Human Rights* Art. 43(2), 1125 (8 June 1977): 3.
135. Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 169 (arguing that 'cyber espionage itself, that is, the collection of information vital to the protection of the State, does not breach international law irrespective of whether it is conducted for economic purposes or for more traditional military/political purposes').

practice or opinio juris toward a customary rule prohibiting its extraterritorial commission.

Notably, the U.S. Department of Defense has made precisely this argument:

> *Of course, most countries, including the United States, have domestic laws against espionage, but international law, in our view, does not prohibit espionage per se even when it involves some degree of physical or virtual intrusion into foreign territory. There is no anti-espionage treaty, and there are many concrete examples of States practicing it, indicating the absence of a customary international law norm against it.*[136]

The DoD argument assumes that extraterritorial espionage is lawful as long as there is no specific customary rule prohibiting it. But that assumption is based on the second Lotus principle, which applies only to legislative and adjudicative jurisdiction:

> *Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable.*[137]

As the quote makes clear, the second Lotus principle is that states are free to apply their laws to acts committed outside of their territory unless a rule of customary international law specifically prohibits them from doing so. That principle, however, does not extend to extraterritorial enforcement jurisdiction – where a state exercises power on the territory of another state. That is the domain of the first Lotus principle, which (again) provides that 'the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive

136. U.S. Department of Defense, "DOD General Counsel Remarks," 2020, 11-12.
137. The Permanent Court of International Justice, "The Case of the S.S. Lotus," 1927, 19.

rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial'.[138]

It is self-evident that, like remote cyber operations more generally, remote cyber espionage represents 'the exercise of power' on the territory of another state. After all, remote cyber espionage is simply a type of remote low-intensity cyber operation, one distinguished from other types – particularly law-enforcement – solely by its purpose. In terms of territorial sovereignty, that is a distinction without a difference.[139] We have already seen that states, scholars, and even the IGE agree that sovereignty categorically prohibits extraterritorial law-enforcement in the absence of the territorial state's consent. States are thus equally prohibited from committing espionage on the territory of another state 'except by virtue of a permissive rule derived from international custom or from a convention';[140] and no such permissive rule exists.

138. *Ibid*., 18-19.

139. *See, e.g*., Wrange, "Intervention in National," 2014, 320 (noting that nothing in international law suggests 'measures undertaken for security and intelligence purposes should be treated differently from measures undertaken to punish and prevent crime').

140. The Permanent Court of International Justice, "The Case of the S.S. Lotus," 1927, 19.

6

Policy Considerations

The pure-sovereigntist position, in short, has a stronger foundation in general international law than either sovereignty as a principle or relative sovereignty. Fidelity to international law thus suggests that Denmark should adopt the pure sovereignty approach to low-intensity cyber operations, joining fellow European states such as France and Switzerland.

That said, because a number of states endorse relative sovereignty (including traditional Danish allies like Norway, Finland, and the US), it is important to consider which position – sovereignty as a principle, pure sovereignty, or relative sovereignty – makes the most sense for Denmark from a policy perspective. As this section demonstrates, a variety of policy considerations support pure sovereignty as well.

6.1. Sovereignty as a Principle

The 'sovereignty as a principle' position defended by the UK and until recently by the US clearly maximises the legal right of states to engage in low-intensity cyber operations. Simply put, if sovereignty does not apply in cyberspace as a rule, states are free to conduct any low-intensity cyber operation without fear of the targeted state engaging in countermeasures.[141] As discussed earlier, states are entitled to engage in countermeasures only in response to internationally wrongful acts.

To be sure, the unavailability of countermeasures would not leave a state targeted by a low-intensity cyber operation powerless to defend

141. *See* Schmitt, "In Defense of Sovereignty," 2018, 5.

itself. The targeted state would be free to engage in a retaliatory low-intensity cyber operation of its own. That freedom, however, is not an adequate substitute for the legal right to engage in countermeasures. Not all states (indeed, relatively few[142]) have the technological ability to respond to a low-intensity cyber operation with a counter- low-intensity cyber operation. For states that do not, the freedom to engage in such operations would be illusory: they would simply have to tolerate low-intensity cyber operations on their territory; even when those operations caused physical damage or rendered cyberinfrastructure inoperable. International law would only prohibit other states from engaging in (rare) cyber operations that rose to the level of a prohibited intervention or use of force.

This is why countermeasures are so important for less powerful states: they do not have to be in kind. A state targeted by a low-intensity cyber operation that violates its sovereignty does not have to respond with its own cyber operation; it can engage in any proportionate response to that internationally wrongful act, such as by 'denying the state launching [the cyber operation] overflight or landing rights provided for in a respective treaty'.[143] The availability of countermeasures thus ensures that each and every state, no matter its technological capabilities, has both the right and the ability to defend itself against an unlawful cyber operation.

From a policy perspective, then, sovereignty as a principle is attractive only for states that want the legal right to engage in offensive low-intensity cyber operations and have the technological capability to defend themselves against such operations with low-intensity cyber operations of their own.[144] For less technologically sophisticated states or states that are simply in favour of greater regulation of cyberspace by international law, that position makes little sense. It is thus not surprising that so few states have endorsed the sovereignty-as-a-principle position; or that some states, including Finland, have specifically condemned it.[145]

142. As noted earlier, data compiled by the Council on Foreign Relations indicates that only 34 states have engaged in low-intensity cyber operations over the past 16 years. *See* Council on Foreign Relations, "CFR Tracker."
143. Schmitt, "In Defense of Sovereignty," 2018, 6.
144. Efrony and Shany, "A Rule Book," 2018, 648-49.
145. *See* Finland, Ministry of Foreign Affairs, "International Law and Cyberspace," 2020, 3 ('Agreeing that a hostile cyber operation below the threshold of prohibited intervention

It is also worth noting that even technologically sophisticated states have reason to endorse sovereignty as a rule. The first reason is reputational: '[s]tates that do not intend to conduct offensive cyber operations or see themselves as likely victims will understandably perceive the approach as threatening, particularly if espoused by states wielding substantial cyber capability'.[146] The second reason is more pragmatic. Advocates of sovereignty as a principle often invoke the need for states like the US to be able to engage in law-enforcement and counterterrorism on the territory of hostile states without fear of lawful countermeasures. Leaving low-intensity cyber operations unregulated by international law, however, empowers all states with offensive capability to engage in extraterritorial low-intensity cyber operations under the guise of fighting 'terrorism' – not just those who will ostensibly use their power wisely.[147] China and Russia are the most obvious examples here.

6.2. Sovereignty as a Rule

Every state, in short, has an interest in promoting the idea that sovereignty applies in cyberspace as a rule, not as a principle. The question is which position they should endorse: pure sovereignty or relative sovereignty. As explained earlier, because both categorically prohibit low-intensity cyber operations that involve extraterritorial law enforcement (including counterterrorism), the critical difference between them is the legality of cyber espionage: whereas the pure-sovereigntist position deems all cyber espionage a violation of sovereignty, the relative-sovereigntist position permits cyber espionage as long as it does not cause physical damage or render cyberinfrastructure inoperable.

Which position to favour thus depends on whether a state wants the freedom to engage in cyber espionage. If a state does not want that

cannot amount to an internationally wrongful act would leave such operations un-regulated and deprive the target State of an important opportunity to claim its rights').

146. Schmitt, "In Defense of Sovereignty," 2018, 7.

147. Schmitt and Vihul, "Sovereignty in Cyberspace," 2017, 217. This is not to say that voluntary norms of state behaviour of the kind endorsed by the GGE in its Final Report have no utility. Such norms, however, are unlikely to influence the behaviour of states that view offensive low-intensity cyber operations as an integral part of their overall cyber strategy.

freedom – whether out of principle or (more likely) because it lacks the technological ability – pure sovereignty is obviously the more desirable position: any act of cyber espionage will be an internationally wrongful act that entitles the state to respond with proportionate countermeasures. The pure-sovereigntist position maximizes the ability of a state to defend itself against cyber espionage – and likely helps deter cyber espionage in general, because would-be perpetrator states will have no 'grey zone' concerning the legality of a particular operation to exploit.[148]

For the same reasons, a state that wants to engage in cyber espionage and has the requisite technological ability should prefer the relative-sovereigntist position. That position would permit the state to engage in cyber espionage as long as it was not harmful. And although the state would lose the right to engage in countermeasures against non-harmful cyber espionage that targeted its computer systems, it would still have the freedom to respond to such cyber espionage with low-intensity cyber operations of its own.

The relative-sovereigntist position would seem particularly attractive for technologically sophisticated states that respect international law. Those states would presumably be uninterested in engaging in cyber espionage that causes physical damage to the territorial state or renders its cyberinfrastructure inoperable. Their interest would lie in non-harmful forms of cyber espionage, such as the NSA surveillance revealed by WikiLeaks: monitoring communications, exfiltrating information, deleting or amending data. For them, relative sovereignty would appear to strike the perfect balance between offence and defence; neither too restrictive nor too permissive.[149]

That said, even states with the ability to engage in cyber espionage have reason to prefer an international legal regime that categorically pro-

148. *See* Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *Yale Journal of International Law Online* 42, no. 2 (2017): 21 ('Certitude that a cyber operation can risk consequences at a set level can deter the taking of that operation, because the State concerned cannot act in the hope that the target State will hesitate to respond out of concern that its response might be viewed as unlawful').

149. *See, e.g.*, Moynihan, "The Application," 2020, 23 ('An approach based on quantitative and/or qualitative effects in the target state, or some other form of de minimis threshold, is attractive from a practical and pragmatic point of view as it enables states to take action in relation to cyber intrusions that may not reach the threshold of intervention but that nevertheless cause harmful effects within the territory').

hibits, and thus helps deter, such espionage even when it is not harmful. Simply put, many types of 'harmless' cyber espionage – both public and private – pose a threat to even the most powerful and technologically sophisticated states.

This is most obvious in terms of espionage against corporations. It is uncontroversial that a state's territorial sovereignty extends to both private and public cyberinfrastructure,[150] and there may well be acts of cyber espionage that satisfy the relative-sovereigntist position by causing significant harm to private cyberinfrastructure.[151] Most private cyber espionage, however, will not cause physical damage or the equivalent loss of cyberinfrastructure functionality.[152] China's theft of intellectual property from Lockheed-Martin in 2009 and Google in 2010 are examples,[153] as is the notorious Flame virus, believed to be the work of the US and Israel, which targeted Iranian oil companies and had the ability to 'activate computer microphones and cameras, log keyboard strokes, take screen shots, extract geolocation from images, and send and receive commands and data through Bluetooth wireless technology'.[154] The pure-sovereigntist position would deem all of these acts of private cyber espionage internationally wrongful simply because they involved non-consensually penetrating computer systems located on another state's territory. But they would be entirely lawful under the relative-sovereigntist position because they did not harm the computer systems from which the information was exfiltrated.

150. *See, e.g.*, Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 13-14 ('With respect to a State's internal sovereignty, it is irrelevant as a matter of international law whether the cyber infrastructure in question is public or private in character, or whether the cyber activities concerned are engaged in by the State's organs or by private individuals or entities').
151. An example is the Shamoon 1 malware attack on Saudi Aramco, widely attributed to Iran, which wiped out the memory of at least 30,000 computers. Not only was Saudi Aramco's entire computer network inoperable for 10 days, the corporation needed months to replace all of the affected computers. Efrony and Shany, "A Rule Book," 2018, 621.
152. *See, e.g.*, Edwin Djabatey, "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part 1," *Just Security* (11 July 2019): 5, available at: https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/ ('[T]he creation of a backdoor to access commercial or technological information is unlikely to be of a scale equivalent to the emplacement of malware capable of significantly impairing or damaging critical infrastructure').
153. *See, e.g.*, Moynihan, "The Application," 2020, 3.
154. Buchan, "Cyber Espionage," 2015, 169.

Private cyber espionage is extraordinarily costly,[155] and it seems safe to assume that law-abiding states are far less likely to engage in it than lawless ones. Law-abiding states thus have little incentive to accept a conception of sovereignty that does not deem private cyber espionage internationally wrongful and prohibits them from taking countermeasures against the responsible state. Yet that is precisely what the relative-sovereigntist position does.

The policy calculus is more complicated for public cyber espionage, because the relative-sovereigntist position prohibits low-intensity cyber operations that interfere with or usurp inherently governmental functions regardless of whether they cause harm. A number of states claim the exclusive right to regulate cyber activity that takes place on their territory, including China,[156] Finland,[157] Germany,[158] and the Netherlands.[159] If states have that exclusive right (what is often referred to as 'cyber sovereignty'), it is difficult to understand how any act of cyber espionage does not interfere with a state's governmental exclusivity. By

155. The IP Commission Report, for example, states that the theft of intellectual property from American companies alone amounts to 'hundreds of billions of dollars per year'. Quoted in Lotrionte, "Countering State-Sponsored," 2014, 451.
156. China, Department of Arms Control, "International Strategy of Cooperation on Cyberspace," Xinhuanet.com (1 March 2017): 2, available at http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm ('National governments are entitled to administer cyberspace in accordance with law. They exercise jurisdiction over ICT infrastructure, resources and activities within their territories, and are entitled to protect their ICT systems and resources from threat, disruption, attack and destruction ... National governments are entitled to enact public policies, laws and regulations with no foreign interference').
157. Finland, Ministry of Foreign Affairs, "International Law and Cyberspace," 2020, 1 ('While cyberspace as a whole cannot be subject to appropriation by any State, each State has jurisdiction over the cyber infrastructure and the persons engaged in cyber activities within its territory. Sovereignty confers each State the exclusive right to exercise the functions of a State within a certain territory').
158. Germany, The Federal Government, "On the Application," 2021, 3 ('Within its borders, a State has the exclusive right – within the framework of international law – to fully exercise its authority, which includes the protection of cyber activities, persons engaging therein as well as cyber infrastructures in the territory of a State against cyber and non-cyber-related interferences attributable to foreign States').
159. The Netherlands, Ministry of Foreign Affairs, "Letter of 5 July," 2019, 2 ('States have exclusive authority over the physical, human and immaterial (logical or software-related) aspects of cyberspace within their territory. Within their territory they may, for example, set rules concerning the technical specifications of mobile networks, cybersecurity and resilience against cyberattacks, take measures to combat cybercrime, and enforce the law with a view to protecting the confidentiality of personal data').

definition, cyber espionage makes it more difficult for a state to ensure that only legally authorized cyberactivity takes place on its territory.[160]

The conclusion that relative sovereignty prohibits all public cyber espionage is complicated, however, by the Tallinn Manual 2.0's extremely restrictive approach to 'interference'. According to a majority of the IGE, the exfiltration of information from a government computer system can never qualify as interference – not even when the loss of the information is capable of crippling an inherently governmental function like national security, such as the theft of nuclear launch codes.[161] If the Manual's approach to interfering with an inherently governmental function becomes generally accepted by states, the relative-sovereigntist position would permit a great deal of public-cyber espionage. Consider, for example, the US's 'Cyber Pearl Harbor', in which China allegedly stole the personal data of millions of past and present US government employees. That cyber espionage would not violate the Tallin Manual 2.0's approach to governmental exclusivity, because it was limited to the exfiltration of information from the Office of Personnel Management.

States defending the relative-sovereigntist position have not explained why they are willing to tolerate public cyber espionage. Some, like France, might be able to compensate for the unavailability of countermeasures in such situations by responding with a low-intensity cyber operation of their own. Once critical information is stolen through espionage, however, counter-espionage cannot 'unsteal' it. All the targeted state can do is punish the responsible state, hoping to deter it from engaging in similar acts in the future.

That potential response might be sufficient to justify relative sovereignty if the threat of retaliation would be more likely to deter public cyber espionage than the threat of countermeasures. But that is almost certainly not the case. A cyber operation launched in response to lawful public cyber espionage would have to remain within the limits imposed

160. Such cyber sovereignty obviously carries with it significant risk of human-rights abuse – regarding privacy, freedom of expression, etc. The exercise of cyber sovereignty is, however, always limited by prohibitive rules of international law. *See* Schmitt (ed.), *Tallinn Manual 2.0*, 2017, 14 (noting that although 'a State may regulate the cyber activities of those on its territory, including both natural and legal persons ... State censorship of, or restrictions on, online communications and activities are subject to applicable international human rights law').

161. *Ibid*., 171.

by international law. That means the operation could not involve a use of force against the targeted state, could not intervene in the targeted state's internal affairs, could not damage or render inoperable the targeted state's cyberinfrastructure, and could not usurp or interfere with the targeted state's inherently governmental functions. The deterrent value created by the threat of such retaliation would likely be limited – particularly in contrast to the threat of countermeasures, which could involve any proportionate response to the public cyber espionage, including responses in the physical world.

Moreover, few states have Germany's cyber capabilities. For states that cannot credibly threaten cyber retaliation, the relative-sovereigntist position removes the one deterrent and the one potentially effective response they have against cyber espionage. They must simply accept non-harmful cyber espionage, public and private. Indeed, they must accept it even when non-harmful cyber espionage has the potential to become extremely damaging later on – such as Operation Nitro Zeus, which involved 'the US penetrating deeply into Iran's infrastructure before the 2015 nuclear accord [and] placing digital "implants" in systems that would enable it to bring down power grids, command-and-control systems and other infrastructure in case a conflict broke out'.[162] According to the relative-sovereigntist position, Iran had no right to engage in countermeasures unless and until the US decided to activate the digital implants and actually caused physical damage or equivalent loss of cyberinfrastructure functionality. That is a problematic limitation,[163] akin to prohibiting the police from arresting a suspect who is pointing a gun at someone until he pulls the trigger.

162. *Cybersecurity Observatory*, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," Cybersecurity Observatory, 16 March 2018, available at https://www.cybersecobservatory.com/2018/03/16/cyberattacks-put-russian-fingers-switch-power-plants-u-s-says/.
163. *Cf.* Roguski, "Violations of Territorial Sovereignty," 2020, 76 (noting that 'this freedom to act ... in effect create[s] a freedom to install malware on foreign computer systems').

7

Recommendations

Since the release of the Tallinn Manual 2.0 in 2017, more than a dozen states have taken a public position on how sovereignty applies in cyberspace. One state, the UK, claims that sovereignty functions solely as a principle, thereby deeming all low-intensity cyber operations lawful. All of the other states agree that sovereignty applies in cyberspace as a rule, but they are divided between pure sovereigntists, who believe that sovereignty prohibits all low-intensity cyber operations, and relative sovereigntists, who believe that sovereignty prohibits only low-intensity cyber operations that cause some kind of harm to the territorial state. Those differences matter, because low-intensity cyber operations are by far the most common type of cyber operation and international law permits a state to engage in countermeasures only in response to internationally wrongful acts.

Despite the legal and practical importance of the issue, Denmark has yet to take a position on how sovereignty applies in cyberspace. This report thus concludes by answering two questions. The first is which position on sovereignty Denmark should adopt. The second is whether it is in Denmark's interest to issue a public statement announcing its position.

7.1. Denmark's Position

Denmark's decision concerning which position on sovereignty to adopt should be informed both by law and policy.

7.1.1. Sovereignty as a Principle

Of the three positions, sovereignty as a principle is the most difficult to reconcile with black-letter international law. It is uncontroversial, even for the UK, that sovereignty is a primary rule of international law that protects a state's territory from physical intrusion. The only difficult issue is whether that primary rule applies in cyberspace as well – and as we have seen, the ICJ's approach to nuclear weapons and the widespread state acceptance of IHL's applicability in cyberspace make it difficult to defend the UK position. It is thus hardly surprising that more than two dozen states reject the idea that sovereignty functions in cyberspace as nothing more than a principle – including the US as of May 2021.

The 'sovereignty as a principle' position should also hold little appeal to Denmark as a matter of policy. Because the position views all low-intensity cyber operations as lawful, it makes sense only for states that want to make offensive use of such operations and are willing to accept having no legal right to take countermeasures in response to low-intensity cyber operations that target them – not even espionage.

Denmark has had the ability to engage in offensive cyber operations since the end of 2019,[164] but it is clear from its 2018-2023 Cyber and Information Security Strategy (CISS) that it is primarily concerned with defending itself against cyber threats.[165] CISS's emphasis on defence makes sense, because Denmark's status as 'one of the most digitized countries in the world'[166] – public sector and private sector alike – makes it a rich target for cyber espionage. Indeed, the Centre for Cyber Security's 2020 report assesses that threat as 'very high':

> *Danish public authorities and private companies will highly likely become targets of attempted cyber espionage over the next two years. Denmark is the target of both politically and commercially motivated cyber*

164. Tobias Liebetrau, "Dansk Offensiv Cybermagt Mellem Angreb, Spionage og Forsvar: En Komparativ Analyse på Tværs af Europa," *Centre for Military Studies* (May 2020): 5.
165. Denmark, Ministry of Finance, "Danish Cyber and Information Security Strategy 2018-2021," *Agency for Digitization* (2018): 6, available at https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/ ('In its national cyber and information security strategy, together with a series of sub-strategies targeting the most critical sectors in society, the Danish government has set out an ambitious plan for the coming years' work of ensuring that Denmark is digitally secure').
166. *Ibid*.

> *espionage by foreign states. The threat from cyber espionage is persistent. It is particularly directed at Danish public authorities involved in foreign and security policy, and Danish private companies whose knowledge is of interest to foreign states.*[167]

Denmark's emphasis on protecting its public and private sectors against cyber threats suggests that its position on sovereignty in cyberspace should be based primarily on considerations of deterrence. Information stolen through cyber espionage cannot be 'unstolen', so the only effective counter-espionage strategy is to deter other states from engaging in cyber espionage in the first place. Empirical research has shown, perhaps counterintuitively, that the likelihood of a state suffering a cyberattack is not correlated with the security of its cyberinfrastructure.[168] This means that a state must be more proactive in deterring threats from other states; and as we have seen, the threat of countermeasures will almost always have greater deterrent value than the threat of a counter-cyber operation, especially for a state like Denmark whose offensive capacity is relatively undeveloped. Denmark thus has little to gain by adopting a view of how sovereignty applies in cyberspace that takes countermeasures completely off the table.

The other relevant policy consideration is whether Denmark wants to maintain the right to use low-intensity cyber operations to combat transnational crime, whether organised or terrorism-related. Both pure and relative sovereignty categorically prohibit law-enforcement operations that take place without the territorial's consent. Only the UK position permits it.

A complete analysis of the threat transnational crime poses to Denmark is beyond the scope of this report. No matter how serious that threat, however, there is no indication that Denmark would not be able to obtain the cooperation it needed to conduct extraterritorial law-enforcement effectively. With the exception of a small number of hostile

167. Centre for Cyber Security, "Threat Assessment 2020: The Cyber Threat Against Denmark," *Centre for Cyber Security* (2020): 15, available at https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-denmark-2020.pdf.

168. Anthony John Stuart Craig, "Capabilities and Conflict in the Cyber Domain: An Empirical Study" (dissertation submitted to the School of Law and Politics, Cardiff University, January 2020): 147.

states (e.g., Russia, China, Syria), most states would likely consent to Denmark accessing a computer on their territory to obtain incriminating evidence or remove terrorist information. Indeed, if that was not the case, other small European states (e.g., Finland, Switzerland) would almost certainly have rejected the idea that sovereignty functions in cyberspace as a rule. Yet those similarly-situated states have adopted either relative sovereignty (Finland) or pure sovereignty (Switzerland) instead of the 'sovereignty as a principle' position.

7.1.2. Pure Sovereignty vs. Relative Sovereignty

Both law and policy, then, suggest that Denmark should endorse either pure sovereignty or relative sovereignty. Viewed solely through the lens of Denmark's traditional alliances, the relative-sovereigntist position is clearly more desirable, given that it has been endorsed by the only two Nordic states – Norway and Finland – that have issued public statements concerning how international law applies in cyberspace. The US has also recently endorsed relative sovereignty, and Denmark has traditionally been loath to publicly disagree with the Americans, particularly on matters of foreign policy.[169]

Viewed in terms of larger policy concerns, the decision between pure and relative sovereignty turns on whether Denmark wants to maintain the legal right to engage in cyber espionage even if doing so means it will not be entitled to take countermeasures against states that use cyber espionage to target it. As we have seen, the pure-sovereigntist and relative-sovereigntist positions agree that sovereignty categorically prohibits using low-intensity cyber operations for law enforcement; the only difference between them is that pure sovereignty prohibits all cyber espionage, while relative-sovereignty permits it as long as it does not cause physical damage or render cyberinfrastructure inoperable.

Whether Denmark wants to maintain the legal right to engage in public or private cyber espionage is difficult to assess. Nevertheless, it

169. Anders Wivel and Matthew Crandall, "Punching above Their Weight, but Why? Explaining Denmark and Estonia in the Transatlantic Relationship," *Journal of Transatlantic Studies* 17 (2019): 392, 398 (noting that 'Danish foreign policy is characterized by strong and unwavering support for the American world order and specific US policies'). There is no guarantee, of course, that a future Republican administration would not reverse course once again and endorse the sovereignty-as-a-principle position.

is worth noting that neither the Council for Foreign Relations Cyber Tracker nor the Center for Strategic & International Studies' list of significant cyber incidents[170] identifies even one act of cyber espionage – public or private – attributed or attributable to Denmark since 2005.[171] This suggests that Denmark is not interested in directly engaging in cyber espionage – although that may change as its offensive cyber capacity increases. Regardless, as noted above, the threat of cyber espionage against Denmark remains extremely high, giving it little reason to abandon the right to respond to cyber espionage with countermeasures.

Alliances aside, then, pure sovereignty appears superior to relative sovereignty from a policy perspective. The pure-sovereigntist position would prohibit Denmark from engaging in cyber espionage – at least insofar as it wanted to comply with international law – but it would permit Denmark to respond to any act of cyber espionage by taking countermeasures against the offending state. Whether the threat of countermeasures is capable of deterring other states from engaging in cyber espionage against Denmark is, of course, an open question. But insofar as deterrence is possible, pure sovereignty will maximise it by deeming all cyber espionage unlawful. Relative sovereignty, by contrast, can only deter cyber espionage that causes harm or renders cyberinfrastructure inoperable; which is rarely the case, as noted earlier.

7.2. Actions by Denmark

Whether Denmark should publicly announce its position on how sovereignty applies in cyberspace is a separate question. No matter which position it decides to adopt, a public statement would run the risk of

170. Centre for Strategic and International Studies, "Significant Cyber Incidents," *Centre for Strategic and International Studies*, 2021, available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

171. Recent reports indicate that the Danish Defence Intelligence Service actively assisted the United States in spying on Danish companies and a number of Denmark's close European allies. That espionage, however, appears to have relied on accessing Danish internet cables with Denmark's consent – not on accessing computer systems in the countries the NSA surveilled. *See, e.g.*, Amelie Theussen, "Why Did Denmark Help the US Spy on Its European Allies?" *The Conversation* (8 June 2021), available at https://theconversation.com/why-did-denmark-help-the-us-spy-on-its-european-allies-161959. Though obviously problematic, the espionage thus does not involve the kinds of sovereignty violations discussed in this report.

alienating states with a different position: powerful European states like France if Denmark endorsed relative sovereignty; important allies like Norway, Finland, and the US if it endorsed pure sovereignty. Indeed, an interest in not being seen as taking sides on such a contested issue likely explains why some states have issued public statements concerning international law in cyberspace that are conspicuously silent on the question of sovereignty. Australia's statement, for example, addresses every contested legal issue other than the international wrongfulness of low-intensity cyber operations.[172]

Denmark would nevertheless benefit in at least two ways from publicly endorsing either pure or relative sovereignty. The first would be deterrence: states will not be deterred from engaging in any kind of cyber espionage unless they know that Denmark believes it is internationally wrongful and entitles Denmark to respond with countermeasures. The second benefit is more narrowly legal: Denmark can contribute to the formation of customary international law regarding the legality of low-intensity cyber operations only by making its position on that issue publicly known. Publicity is inherent in the concept of opinio juris. A desire to influence international law almost certainly explains why states as varied as the Netherlands, Brazil, and Iran have each released statements concerning how international law applies in cyberspace.

At a minimum, therefore, Denmark should follow suit and issue a public statement that makes clear whether it endorses pure or relative sovereignty in the context of low-intensity cyber operations. Moreover, if it endorses relative sovereignty, Denmark could maximise the impact of its statement by making clear – in a manner that most other relative-sovereigntist states have not – what kind of harm it considers sufficient to violate territorial sovereignty.

As noted above, both the GGE and the OEWG have each completed their work on how international law applies in cyberspace and submitted their final reports. In early 2021, however, the General Assembly

172. *See* Australian Government, "Australian Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," *Australian Government*, Annex A, September 2019, available at https://www.internationalcybertech.gov.au/node/72.

voted to create a second OEWG that will report back to it in 2025.[173] Given the important uncertainties that remain regarding the status of sovereignty, Denmark would be well advised not only to issue a public statement on the topic, but also to participate actively in OEWG II.

173. *See* General Assembly of United Nations, "Resolution Adopted by the General Assembly on December 31 2020," *United Nations Digital Library*, Res. 75/240 (4 January 2021): 3.

Bibliography

Agenda.Ge. "Georgia Accuses Russia of Widespread Cyber Attack." *Agenda.Ge*, 20 February 2020, https://agenda.ge/en/news/2020/535.

Akande, Dapo, Antonio Coco and Talita de Souza Dias. "Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond." *Just Security*, 5 January 2021, https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

Australian Government. "Australian Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," *Australian Government*, Annex A, September 2019, https://www.internationalcybertech.gov.au/node/72.

Bellia, Patricia L. "Chasing Bits across Borders." *The University Chicago Legal Forum* (2001): 35-101.

Brown, Gary and Keira Poellet. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (2012): 126-45.

Buchan, Russell. "Cyber Espionage and International Law." In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan, 168-90. Edward Elgar, 2015.

Centre for Cyber Security. "Threat Assessment 2020: The Cyber Threat against Denmark." *Centre for Cyber Security*, 2020, https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-denmark-2020.pdf.

Centre for Strategic and International Studies. "Significant Cyber Incidents." *Centre for Strategic and International Studies*, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Chesterman, Simon. "The Spy Who Came in from the Cold War: Intelligence and International Law." *Michigan Journal of International Law* 27, no. 4 (2006): 1071-130.

China, Department of Arms Control. "International Strategy of Cooperation on Cyberspace." *Xinhuanet.com*, 1 March 2017, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

Chircop, Luke. "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0." *Melbourne Journal of International Law* 20, no. 2 (2019): 1-29.

Corn, Gary P., and Robert Taylor. "Sovereignty in the Age of Cyber." *AJIL Unbound* 111, (2017): 207-12.

Council on Foreign Relations. "Cyber-Operations Tracker." *Council on Foreign Relations*, https://www.cfr.org/cyber-operations/.

Craig, John Stuart. "Capabilities and Conflict in the Cyber Domain: An Empirical Study." Dissertation, School of Law and Politics, Cardiff University, January 2020.

Cybersecurity Observatory. "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says." *Cybersecurity Observatory*, 16 March 2018, https://www.cybersecobservatory.com/2018/03/16/cyberattacks-put-russian-fingers-switch-power-plants-u-s-says/.

Czech Republic, National Cyber and Information Security Agency. "Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace Director of Cybersecurity Department." *National Cyber and Information Security Agency*, 11 February 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.

Denmark, Ministry of Finance. "Danish Cyber and Information Security Strategy 2018-2021." *Agency for Digitization*, 2018, https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/.

Djabatey, Edwin. "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part 1," *Just Security*, 11 July 2019. https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/.

Efrony, Dan and Yuval Shany. "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." *American Journal of International Law* 112, no. 4 (October 2018): 583-657.

EU Council Conclusions. "General Affairs Council Meeting." *Council of the European Union*, Doc. No. 11357/13, Annex, 21 June 2013, https://data.consilium.europa.eu/doc/document/ST%2011357%202013%20INIT/EN/pdf.

European Court of Human Rights. "Weber and Saravia v. Germany." *European Court of Human Rights*, Decision, App. No. 54934/00, 29 June 2006.

Finland, Ministry of Foreign Affairs. "International Law and Cyberspace – Finland's National Positions." *Ministry of Foreign Affairs*, 15 October 2020, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=160309752272.

Foltz, Andrew C. "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate." *JFQ* 67, no. 4 (2012): 40-8.

Forcese, Craig. "Spies without Borders: International Law and Intelligence Collection." *Journal of National Security Law and Policy* 5 (June 2011): 179-210.

France, Ministry of Defence. "International Law Applied to Operations in Cyberspace." *Ministry of Defence*, 2019, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.

General Assembly of United Nations. "Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations." Annex, *UN General Assembly*, Res 2625 (XXV), 24 October 1970.

General Assembly of United Nations. "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts," *United Nations Digital Library*, A/76/136*, 13 July 2021.

General Assembly of United Nations. "Note Verbale Dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations Addressed to the Secretary-General," *United Nations Digital Library*, A/67/946, July 2013, https://undocs.org/pdf?symbol=en/A/67/946.

General Assembly of United Nations. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations Digital Library*, A/68/98, 24 June 2013.

General Assembly of United Nations. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)," *United Nations Digital Library*, A/70/174, 22 July 2015.

General Assembly of United Nations. "Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations Digital Library*, A/RES/70/237, 30 December 2015.

General Assembly of United Nations. "Report of The International Law Commission on the Work of Its Sixty-Sixth Session," Draft Conclusion 10(2), *United Nations Digital Library*. A/69/10, 2014.

General Assembly of United Nations, "Resolution Adopted by the General Assembly on December 31 2020," *United Nations Digital Library*, Res. 75/240, 4 January 2021.

Germany, The Federal Government. "On the Application of International Law in Cyberspace," *The Federal Government*, March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

Gisel, Laurent, Tilman Rodenhäuser and Knut Dörmann. "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts." *International Review of the Red Cross* 913 (March 2021): 287-334, https://international-review.icrc.org/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913#footnote59_ilkhhlq.

Government of United Kingdom. "Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General Jeremy Wright QC MP," *Gov.uk*, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Green, L.C. "The Eichmann Case." *Modern Law Review* (1960): 507-15.

Helsinki Accords. "Final Act of the Conference on Security and Cooperation in Europe," Arts. 1, 2, 6, 14 ILM 1292. *OSCE*, August 1975.

International Court of Justice. "Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica Along the San Juan River (Nicar. v. Costa Rica)." Judgment, *International Court of Justice*, Rep. 1, 2-4, 16 December 2015.

International Court of Justice. "Corfu Channel Case (United Kingdom v. Albania)," Judgment, *International Court of Justice*, 9 April 1949.

International Court of Justice. "Legality of the Threat or Use of Nuclear Weapons," Advisory Opinion, *International Court of Justice*, Rep. 226, 8 July 1996.

International Court of Justice. "Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)," Judgment, *International Court of Justice*, Rep. 14, 27 June 1986.

International Court of Justice. "North Sea Continental Shelf Cases (Ger./Den.; Ger./Neth.)." Judgment, *International Court of Justice*, Rep. 3, 20 February 1969.

International Law Commission. "Articles on Responsibility of States for Internationally Wrongful Acts," Art. 2, *UN General Assembly* Res. 56/83, December 2000 (ARSIWA).

Iran. "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace." *Nournews*, July 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

Jennings, Robert and Arthur Watts (eds.). *Oppenheim's International Law: Peace*, 9th edition. Longman, 1996.

Liebetrau, Tobias. "Dansk Offensiv Cybermagt Mellem Angreb, Spionage og Forsvar: En Komparativ Analyse på Tværs af Europa." *Centre for Military Studies*, May 2020, https://cms.polsci.ku.dk/publikationer/dansk-offensiv-cybermagt-mellem-angreb-spionage-og-forsvar-en-komparativ-analyse-paa-tvaers-af-europa/download-rapport/CMS_Rapport_-_Dansk_offensiv_cybermagt.pdf.

Lotrionte, Catherine. "Countering State-Sponsored Cyber Economic Espionage Under International Law." *North Carolina Journal of International Law and Commercial Regulation* 40 (2014): 443-541.

Moynihan, Harriet. "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention." *Chatham House Research Paper* 3 (December 2020): 1-59.

New Zealand, Ministry of Foreign Affairs and Trade. "The Application of International Law to State Activity in Cyberspace." *Ministry of Foreign Affairs and Trade*, 1 December 2020, https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.

North Atlantic Treaty Organization. "Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations," *North Atlantic Treaty Organization*, 29 January 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

Organization of American States. "Improving Transparency — International Law and State Cyber Operations: Fourth Report." *OEA/Ser*. Q, CJI/doc. 603/20 rev.1, March 2020 (*presented by Prof. Duncan B. Hollis*).

Radio Free Europe/Radio Liberty. "Estonia Says Russian Aircraft Violated Airspace Again." *Radio Free Europe/Radio Liberty*, 6 September 2016, http://www.rferl.org/a/russia-estonia-airspace-violated/27970888.html.

Roguski, Przemyslaw. "Violations of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach." In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg. London: Rowman & Littlefield, 2020. 65-84.

Roguski, Przemysław. "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views." T*he Hague Program for Cyber Norms Policy Brief*, March 2020.

Roguski, Przemysław. "The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States." *Just Security*, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

Rolle, Rashad. "Lawyers to Act in NSA Spy Row." *The Tribune*, 5 June 2014, http://www.tribune242.com/news/2014/jun/05/lawyers-act-ns-spy-row/.

Smith, Jeffrey H. "Symposium: State Intelligence Gathering and International Law: Keynote Address." *Michigan Journal of International Law* 28, no. 3 (2007): 543-52.

Schmitt, Michael N. "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law." *Virginia Journal of International Law* 54 (2014): 698-732.

Schmitt, Michael N. "Grey Zones in the International Law of Cyberspace." *Yale Journal of International Law Online* 42, no. 2 (2017): 1-21.

Schmitt, Michael. "In Defense of Sovereignty in Cyberspace." *Just Security*, 8 May 2018, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/.

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

Schmitt, Michael N., and Liis Vihul. "Respect for Sovereignty in Cyberspace." Texas Law Review 95 (2017): 1639-70.

Schmitt, Michael N., and Liis Vihul. "Sovereignty in Cyberspace: Lex Lata Vel Non?" *AJIL Unbound* 111, no. 1 (2017): 213-18.

Schöndorf, Roy. "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." *International Law Studies* 97, 2021: 395-406.

Switzerland, Federal Department of Foreign Affairs. "Position Paper on the Application of International Law in Cyberspace." *Federal Department of Foreign Affairs (FDFA)*, Annex UN GGE 2019/2021 (2021): 1-11, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

The Irish Times. "Italy Tells US to Respect Sovereignty after Kidnap." *The Irish Times*, 1 July 2005, https://www.irishtimes.com/news/italy-tells-us-to-respect-sovereignty-after-kidnap-1.1179451.

The Netherlands, Ministry of Foreign Affairs. "Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace — Appendix: International Law in Cyberspace." *Government of the Netherlands*, 5 July 2019, https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

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

Theussen, Amelie. "Why Did Denmark Help the US Spy on Its European Allies?" *The Conversation*. 8 June 2021, https://theconversation.com/why-did-denmark-help-the-us-spy-on-its-european-allies-161959.

United Kingdom. "Application of International Law to States' Conduct in Cyberspace." *Government of United Kingdom*, 3 June 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

United Nations. "United Nations Convention on the Law of the Sea." *United Nations*, 1833 UNTS 397, 10 December 1982.

United Nations Human Rights. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts." *United Nations Human Rights* Art. 43(2), 1125, 8 June 1977.

United Nations, Office for Disarmament Affairs. "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." *UNODA*, Final Report A/AC.290/2021/CRP.2, 10 March 2021.

United Nations, Office for Disarmament Affairs. "Report of the Group of Governmental Experts on Advancing State Behaviour in the Context of International Security." *UNODA*, advance copy, 28 May 2021.

United Nations, Office on Drugs and Crime. "United Nations Convention against Transnational Organized Crime." *General Assembly resolution*, Res. 55/25, Annex, Art.4, 15 November 2000.

United Nations Security Council. "Security Council Resolution 138 (Question relating to the case of Adolf Eichmann)." *United Nations Digital Library*, S/RES/4349, 30 June 1960.

United Nations Specialized Agency, "Convention on International Civil Aviation," *ICAO*, 61 Stat. 1180, 15 UNTS 295, 7 December 1944.

U.S. Department of Defense. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," *U.S. Department of Defense* (2 March 2020): 3-25, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

U.S. Department of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations*, 2nd ed., November 1999.

U.S. President "International Strategy for Cyberspace." *Obama White House*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

von Heinegg, Wolff Heintschel. "Legal Implications of Territorial Sovereignty in Cyberspace." In *4th International Conference on Cyber Conflict*, edited by Christian Czosseck et al. NATO CCD COE Publications, 2012.

Watts, Sean. "Low-Intensity Cyber Operations and the Principle of Non-Intervention." *Baltic Yearbook of International Law* 14, 2017.

Watts, Sean, and Theodor Richard. "Baseline Territorial Sovereignty in Cyberspace." *Lewis & Clark Law Review* 22, no. 3 (2018): 771-840.

Wivel, Anders, and Matthew Crandall. "Punching above Their Weight, but Why? Explaining Denmark and Estonia in the Transatlantic Relationship." *Journal of Transatlantic Studies* 17 (2019): 392-419.

Wrange, Pål. "Intervention in National and Private Cyberspace and International Law." In *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, edited by Jonas Ebbesson et al., 307-26. Brill/Nijhoff, 2014.

Ziolkowsk, Katharina. "Peacetime Cyber Espionage: New Tendencies in International Law." In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, 425-64. NATO CCD COE Publications, 2013.

ABOUT THE AUTHOR

Kevin Jon Heller is Professor of International Law and Security at the Centre for Military Studies, University of Copenhagen, and Professor of Law at the Australian National University. He currently serves as Special Adviser on International Criminal Law Discourse to the Prosecutor of the International Criminal Court.