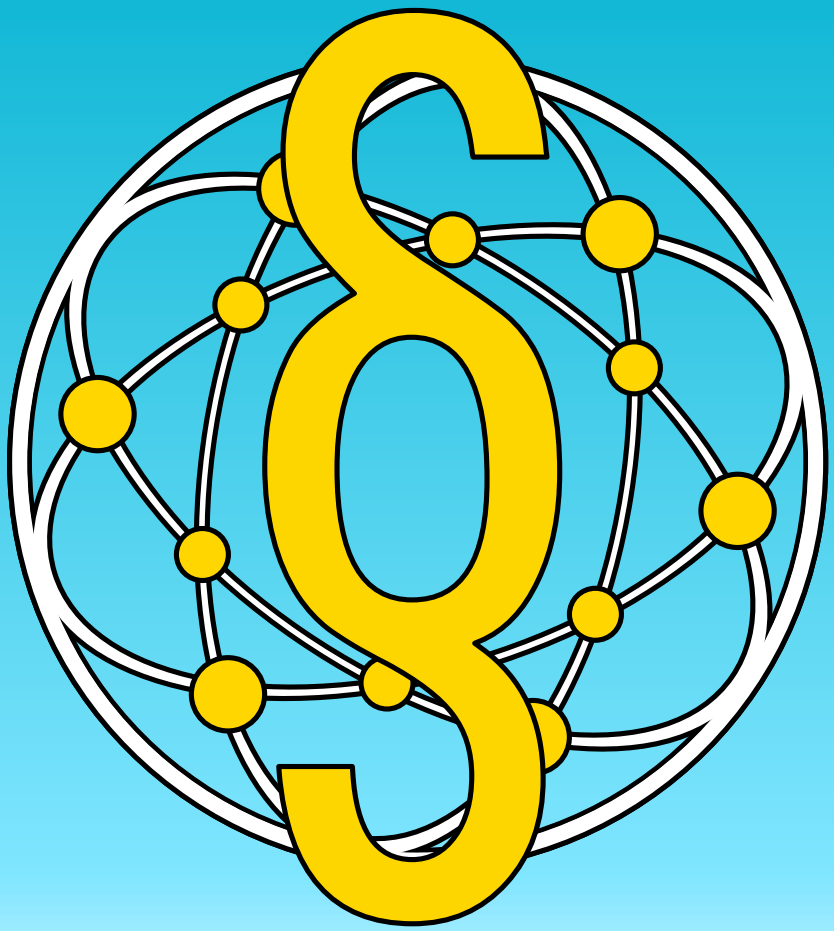

Sovereignty in Cyberspace

Is an International Cyber-Order Achievable?

Chloe Young

Chloe is a Juris Doctor student at the University of Washington School of Law. She graduated summa cum laude with degrees in Politics and Chinese from Whitman College. In 2024, she graduated with Distinction from the University of Glasgow (LLM in International Law), the Institut Barcelona d'Estudis Internacionals (MA in International Security), and the University of Tartu (MA in International Law and Human Rights). Chloe interned at the cyber diplomacy unit at the Estonian Ministry of Foreign Affairs.

1. Introduction

Every day, states, non-state actors, and individuals are exploiting vulnerabilities in cyberspace for political, ideological, or economic gain. For example, in 2007 the Estonian government witnessed thousands of distributed denial-of-service attacks which disabled the websites of government agencies, political parties, newspapers, and banks (Traynor, 2007). In 2014, the Pentagon repelled over thirty million cyberattacks directed towards government networks (Winnefeld et al., 2016). In 2022, the Costa Rican government declared a state of emergency after a widespread ransomware attack caused over $155 million worth of losses (Rosch, 2022). As the number of cyberattacks increases with widespread Internet accessibility and low costs of cyber operations, this heightens the importance of asking whether international consensus can be reached on how sovereignty applies in cyberspace (Franzese, 2009, 7).

Cyberspace:
Cyberspace comprises a physical, logical, and virtual environment whereby data and information are transported, accessed, and stored for communication purposes.

This legal problem must be addressed because state sovereignty "largely defines the current international order" and will likely lay the foundation for an international cyber-order (Liaropoulos, 2013, 21). Given this article's limited scope, other international legal principles like non-intervention and self-defence are not discussed. Although the definition of sovereignty varies among scholars, this article defines it as "the right of states to exercise exclusive authority over their territory" (Osula & Rõigas, 2016, 69). This article aims to understand disagreements between states over sovereignty's applicability to cyberspace. To achieve this goal, the article addresses the following three legal issues. Firstly, how does the borderless nature of cyberspace compare to other domains like the high seas, airspace, and outer space? Secondly, what should constitute a breach of sovereignty in cyberspace? Thirdly, how does anonymity in cyberspace complicate state attribution? This article contends that (1) the virtual side of cyberspace complicates traditional applications of territorial sovereignty but does not preclude states from exercising control over physical cyberspace infrastructure and activity within their borders, (2) violations of sovereignty should be determined individually based on the context of the violation and the severity of its effect, and (3) anonymity in cyberspace complicates state attribution but should not dissuade states from addressing violations in other ways.

To answer these questions, the article analyses national laws, international draft conventions and working group reports submitted to the United Nations (UN), and scholarly works like the Tallinn Manual. The article proceeds in four sections. Section one discusses three general challenges to cyberspace regulation. Section two outlines sovereignty's traditional role in the UN Charter and Tallinn Manual. Next, section three addresses three legal issues surrounding sovereignty in cyberspace. Finally, section four concludes by imploring states to unite and create a common understanding of how sovereignty applies in cyberspace to successfully address hostile cyber operations worldwide. Overall, this article argues sovereignty disagreements between states will make achieving consensus on an international cyber-order a daunting task.

2. Can Cyberspace be Regulated?

According to former Google CEO Eric Schmidt, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever seen" (Singer & Friedman, 2014, 40). Since its humble beginnings as a U.S. government agency project, roughly fifteen billion devices worldwide are now connected to the Internet (Vailshery, 2023). By 2030, the number of connected

devices is expected to double as online banking, shopping, and working become more common (Vailshery, 2023). As the Internet steadily grows in popularity, this heightens the importance of asking whether cyberspace can be regulated. Each connected device contributes to an ever-expanding cyber domain susceptible to fraud, denial of service, scam, sniffing, brand spoofing, and other attacks. This article defines cyberspace as comprising a physical, logical, and virtual environment whereby data and information are transported, accessed, and stored for communication purposes. Cyberspace regulation is possible but difficult to achieve due to several challenges like the private sector controlling most of the Internet's physical infrastructure, anonymity in the dark web, and the quick speed at which events unfold in the virtual world. After briefly outlining the history of cyberspace regulation from an international perspective since the late 1800s, this section of the article briefly analyses these three main challenges to effective cyberspace regulation.

This introductory section concludes by arguing in favour of cyberspace regulation to protect users, maintain global commerce, and uphold human rights. To effectively analyse the challenges of cyberspace regulation, it is important to outline the history of cyberspace regulation from an international perspective. In 1865, the international community convened to set common standards for telegraph communication. This meeting culminated in the establishment of the International Telegraph Union, which later became the International Telecommunications Union (ITU) tasked with developing technical standards for international Internet connectivity. In addition to the ITU, other international organisations like the Internet Engineering Taskforce (which regulates standards for the Transmission Control Protocol and Internet Protocol) and the Internet Corporation for Assigned Names and Numbers (which manages IP address space allocation and the domain name system) regulate the technical side of cyberspace. However, recent scholarly projects and international treaties have addressed the legal side of cyberspace. For example, the Tallinn Manual is a scholarly project that explains how jus ad bellum (i.e., the laws governing the use of armed force and the conditions under which states may resort to war) and jus contra bellum (i.e., international humanitarian law) apply to cyberwarfare. Additionally, the Budapest Convention (2004) was the first international treaty regulating cyberspace by imploring member states to pass domestic legislation addressing hacking, the damage and breach of data, fraud, child pornography, copyright and more. Although cyberspace regulation has become a recurring discussion topic at international organisations like the UN, North Atlantic Treaty Organization (NATO) and European Union (EU), it still sparks strong debate among states. On the one hand, strong cyberspace regulations make it easier for some regimes to limit freedom of speech (as evidenced by China's Great Firewall, whereby the Chinese government monitors, controls, and filters the availability of certain websites from within its territorial boundaries.) On the other hand, cyberspace regulations are crucial for global commerce, communication, and national security. Recognizing the importance of balancing law enforcement efforts with human rights, this article supports cyberspace regulation but lists three of its main challenges. First, cyberspace is difficult to regulate because the private sector controls most of the Internet's physical infrastructure. Before diving into this ownership problem, it is important to define the Internet's relationship to the World Wide Web (WWW). The Internet refers to the physical infrastructure of computers, fiber-optic cables, routers, antennas, internet exchange points, and data storage centers worldwide which create a network of networks for connectivity. The WWW refers to the logical realm of cyberspace that provides a collection of information accessible via the Internet. In simpler terms, surfing the web refers to jumping from page to page using Hypertext Markup Language (HTML).

At the international level, organisations like the ITU, ICANN, and the World Trade Organization

provide technical standards and telecommunication regulations for online users. However, the private sector (at least in the U.S.) owns and controls roughly ninety percent of the Internet's physical infrastructure (Singer & Friedman, 2014, 40). Therefore, the government cannot regulate cyberspace on its own and prevent cybercrime without cooperating with private companies. This co-dependency illustrates how traditional conceptions of the government as the legitimate monopoly provider of security does not translate from the physical world to cyberspace. Additionally, the plurality of state, non-state, and private actors in cyberspace challenges international law's conception of the state as the most essential subject of international law. For these reasons, governments must work with the private sector to effectively regulate cyberspace.

Secondly, cyberspace is difficult to regulate because anonymity in the dark web complicates state attribution and accountability. It is important to note that the WWW's structure resembles an iceberg with three layers of depth: the clear, deep, and dark web. The clear web is the smallest part of the WWW where search engines like Google and Bing can roam freely. The second largest part of the WWW is the deep web, which search engines cannot find because passwords are needed for access. Schools, businesses, and companies generally take advantage of the deep web to ensure random users cannot access sensitive, internal information.

Finally, the largest part of the WWW is the dark web whereby people use the Tor browser to clear their browsing history and make themselves harder to track (Santi, 2023). Anonymity in the dark web complicates both law enforcement efforts and international law's ability to regulate cyberspace activity. According to Article 8 of the Articles of States Responsibility for Internationally Wrongful Acts (ARSIWA), "the conduct of a person or group of persons shall be considered an act of a State under international law if…[they] are in fact acting on the instructions

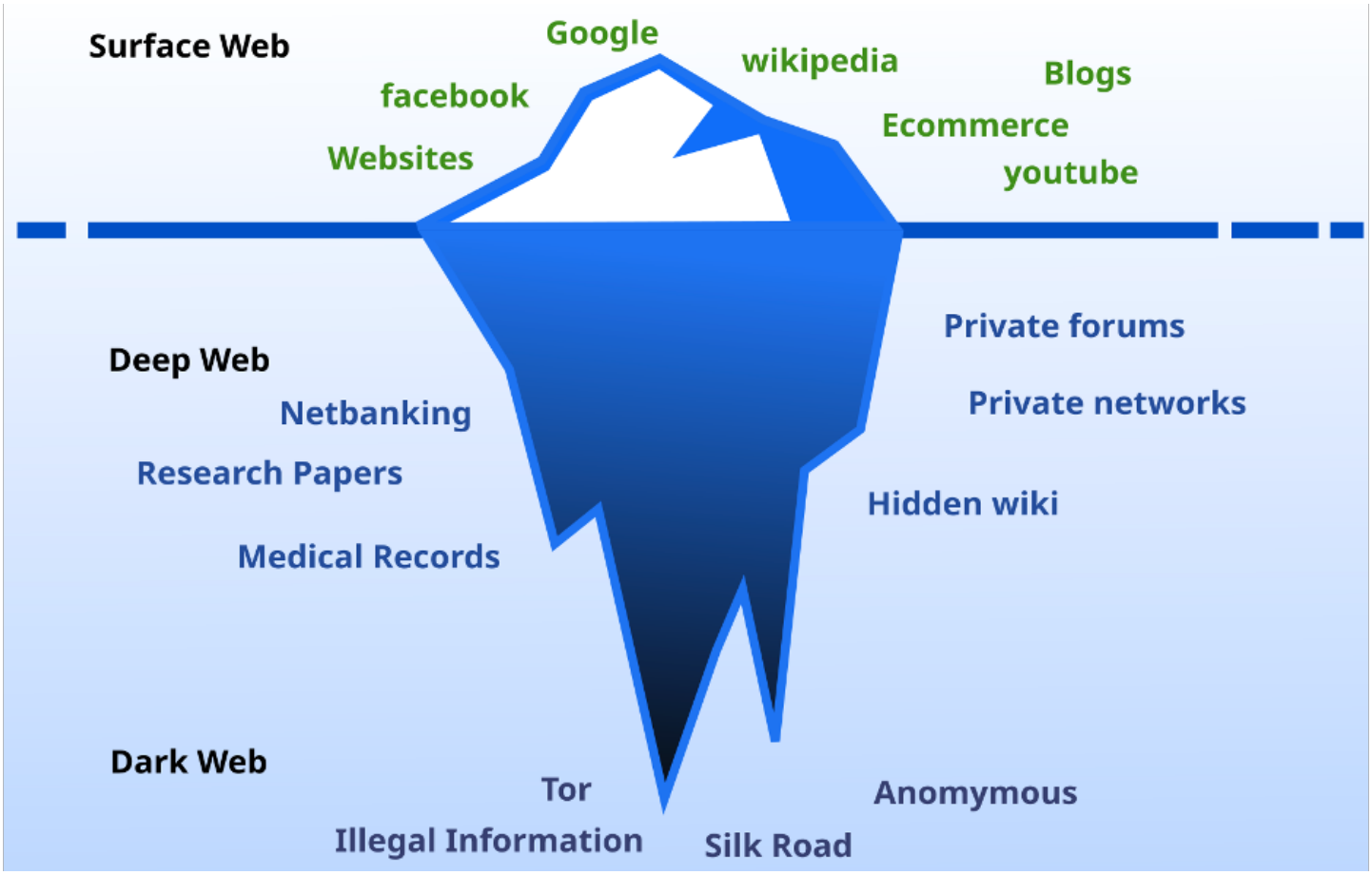

Figure 1:Graphical representation of surface web, deep web, and dark web (Ranjithsiji, 2018)

of, or under the direction or control of, that State in carrying out the conduct" (Draft Articles on Responsibility, art. 8). This effective control standard is nearly impossible to meet in cyberspace because people's identity and motives are oftentimes obscured. Even if law enforcement successfully tracked down a cybercriminal's IP address, the device's geolocation may not be authentic if it were re-routed from the cybercriminal's true location. Another complicating factor is whether the cybercriminal is controlling someone else's computer. Overall, challenges surrounding jurisdiction, state attribution, accountability, and "international law's traditional reliance on territorial borders" complicate efforts to effectively regulate cyberspace (Johnson and Post, 1996, 1367).

Thirdly, cyberspace is challenging to regulate because of the quick speed at which events unfold in the virtual world. As new devices hit the market, their lines of code contain hundreds of human error vulnerabilities ready for exploitation by cybercriminals.

Every second of every day, cybercriminals are tirelessly attempting to find coding vulnerabilities to make a profit, send political messages, and conduct cybercrime.

Given this fast-paced virtual environment, governments cannot keep up with cyberspace regulations due to limited budgets, staff, and expertise. For example, widespread ransomware attacks on the Costa Rican government (2022) forced the ministry to work with pen and paper for months until finding a solution.

Likewise in the United States, the SolarWinds IT management company suffered massive data breaches in 2019 when hackers slipped malicious code into a software update. The preliminary stages of this cyberattack went undetected for roughly two years (Zetter, 2023). These examples illustrate the difficulties of predicting and responding to cyber-attacks. Additionally, legislative solutions often require proposal, drafting, negotiation, implementation, and enforcement stages that span years. As cyberspace activity continues unfolding at the speed of light, the governments' ambition to craft quick legal solutions will remain unfeasible. In the meantime, governments should invest time and effort into strengthening their national resilience and implementing security defences in cyberspace to impede cybercriminals. Given these three challenges to effective cyberspace regulation, it is worth asking whether cyberspace should be regulated at all. For some, cyberspace should not be regulated because this paves the way for limiting freedom of speech and assembly. For example, John Barlow argued against government involvement by declaring "the global social space we are building [must] be naturally independent from the tyrannies [governments] seek to impose on us" (Barlow, 2018). However, to Barlow's dismay, the UN General Assembly (UNGA) accepted conclusions by the UN Group of Governmental Experts (GGE) in 2013 that international law and the principle of sovereignty applied to cyberspace (Moynihan, 2019). This consensus set the stage for states to develop national cyber security strategies to strengthen their cyberspace defence capabilities and resilience. In agreement with subsequent UNGA resolutions 70/237 and 73/27, this article supports cyberspace regulation to protect online users, maintain global commerce, and uphold human rights. Challenges surrounding anonymity and temporality in cyberspace heighten the importance of implementing cybersecurity measures and promoting social norms to regulate online behaviour to help prevent, deter, and respond to cyberattacks (Lessig, 2010, 124). Although avoiding all cyberattacks is unrealistic, passing security measures is an essential step towards making sure the Internet does not remain the largest experiment in anarchy that humanity has ever seen.

3. Sovereignty's Traditional Role in International Law

Before analysing several legal issues surrounding sovereignty in cyberspace, it is important to outline sovereignty's traditional role in international law. There are several types of sovereignty: domestic sovereignty (internal), interdependence sovereignty, international legal sovereignty (external), and Westphalia sovereignty (Liaropoulos, 2013, 22). The UN Charter enshrines external sovereignty and is "based on the principle of the sovereign equality [between] all its Members" (U.N. Charter art. 2, para. 1). The Charter also enshrines internal sovereignty by declaring "All members shall refrain in their international relations from the threat or use of force against the territorial or political independence of a state" (U.N. Charter art. 2, para. 4). Reinforcing the UN Charter's position, the International Court of Justice (ICJ) concluded "between independent states, respect for territorial sovereignty is an essential foundation of international relations" (Nicaragua v. United States of America, 1986).

Earlier on, the ICJ also addressed state sovereignty and argued British minesweeping in Albanian waters without the Albanian government's consent constituted a violation of sovereignty (United Kingdom of Great Britain and Northern Ireland v. Albania, 1949). Prior to the ICJ, the Permanent Court of International Justice (PCIJ) defined territorial sovereignty as a "situation recognized and delimited in space, either by so-called natural frontiers as recognized by international law or by outward signs of delimitation that are undisputed" (Netherlands v. USA, 1928). In this case, Arbitrator Huber implied territorial sovereignty confers rights and imposes obligations on states to respect each other's sovereignty (Netherlands v. USA, 1928, 858). Overall, sovereignty's traditional link to physical territoriality complicates matters in cyberspace because the virtual world is largely unconcerned with geographical boundaries. Although sovereignty is well-established in international law, cyberspace's "unprecedented novelty" sparks debate on its applicability (Osula & Rõigas, 2016, 49). In the early days of the Internet, an exceptionalist perspective emerged arguing cyberspace differed from previous domains regulated by international law (Osula & Rõigas, 2016, 49). For example, John Barlow argued "we must declare our virtual selves immune to [state] sovereignty" (Barlow, 2018).

Additionally, Kristen Eichensehr coined the phrase "cyberspace is sovereign" and argued cyberspace's opaque nature made it unconducive to state control (Eichensehr, 2014).

Over time, a competing sovereigntist viewpoint emerged which argued cyberspace remained fully under international law (Osula & Rõigas, 2016, 50). This article supports the sovereigntist viewpoint because if sovereignty is not applied to cyberspace, then states will continue acting in a wild west, lawless fashion with limited legal consequences. Although states may not want to tie their own hands with legal obligations, it is in their best interests to regulate cyberspace to ensure networks function properly, physical infrastructure remains protected, and relationships with the private sector are established. Supporting this position, the UN Group of Governmental Experts (GGE) in 2013 and 2015 concluded the UN Charter, international law, and the principle of sovereignty applied to cyberspace (Moynihan, 2019). Additionally, the Tallinn Manual stipulated "a state may exercise control over cyber infrastructure and activities within its sovereign territory" (Schmitt, 2017, 15). To better understand why sovereignty should apply to cyberspace, it is helpful to analyse how sovereignty applies to other domains and "global commons" (Franzese, 2009, 16).

4. How Does Cyberspace Compare to the High Seas, Airspace and Outer Space?

Given the globalised and free-flowing nature of information on the World Wide Web, cyberspace could be subject to similar

regulations applied to other international common spaces. According to Kish, the "law of international spaces" partially restricts state authority to ensure all states enjoy the peaceful use of a domain as sovereign equals (Kish, 1973; Weber, 2016, 19). For example, sovereignty was codified in the law of the sea which allows states to exercise sovereignty over twelve nautical miles from agreed-upon baselines (United Nations Convention on the Law of the Sea, art. 3). States can also exercise sovereignty over the airspace above their territory (United Nations Conference on the Law of the Sea, 1958). However, applying maritime or airspace delimitation to cyberspace does not work because physical baselines cannot be established in the virtual world. Additionally, could data packets be marked with national flags akin to ships and aircrafts? Could states be held responsible for or interfere with data packets passing through their territorial borders to reach their final destinations? Despite this uncertainty, sovereignty's eventual codification in the law of the sea and air is reassuring for the development of international law in cyberspace. A third international space worth discussing is outer space which "is not subject to national appropriation by claim of sovereignty" (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, art. 2). Although exceptionalists would support applying the anti-sovereignty perspective for outer space to cyberspace, it is ultimately unsuitable because cyberspace comprises physical, logical, and virtual realms. The physical realm includes fiber-optic cables, routers, antennas, internet exchange points, and data storage centers located on state territory which is subject to state sovereignty. Considering regulations in the high seas, airspace, and outer space do not perfectly suit cyberspace, this has sparked debate over whether international law should be re-invented for this new domain. In this debate, the U.S., China, and Russia hold opposing views on whether pre-existing or new international law should apply in cyberspace. Given this article's limited scope, the U.S., China, and Russia were selected for analysis based on their vocal and divergent views in the United Nations Open-Ended Working Group on Information and Communication Technologies Meetings. According to the U.S. International Strategy for Cyberspace, state conduct in cyberspace "does not require a reinvention of customary international law...[and] long-standing international norms guiding state behaviour...apply in cyberspace" (Von Heinegg, 2012, 10). In 2023, the U.S. government went one step further by declaring itself "ready to expose and contest behaviour inconsistent with [globally agreed upon cyberspace] norms and international law" (U.S. Department of Defence Cyber Strategy, 2023, 12). This article agrees that re-inventing international law for cyberspace is not needed because this new negotiation process would likely not result in international consensus, thus allowing some states to continue acting lawlessly in the cyber world. Having the U.S. contest state behaviour in cyberspace also raises questions on who should regulate and enforce compliance with international law in cyberspace. With no international regime governing cyberspace besides the Budapest Convention (2001), future state practice will likely determine what constitutes a violation of sovereignty and how states should respond. Unlike the U.S., China and Russia argue new international rules are needed for cyberspace (Franzese, 2009, 37). Both countries submitted a joint proposal to the UN General Assembly calling for strengthened individual state control over cyber networks (UNGA A/66/359, 2011). The proposal's preamble reaffirmed "policy authority for Internet-related public issues is the sovereign right of states" (UNGA A/66/359, 2011). Gaining inspiration from China's Great Firewall, Russia passed national legislation requiring all internet traffic be routed and stored inside the country (Sherman, 2018). This illustrates how states seek control over cyberspace to enforce law and order via censorship. Whereas states like China and Russia argue nationalising the Internet makes it easier to protect people's data, more democratic regimes

critique these actions for undermining human rights like freedom of expression and privacy (Tavenner, 2022). Overall, sovereignty in international law must acknowledge state authority but prioritise human rights.

affect the "integrity or functionality" of the state's cyber infrastructure (Von Heinegg, 2012, 11)?

Does the cyber operation need to have a direct, material effect in another state like injury or death? Would indirect effects in a third state violate that states' sovereignty?

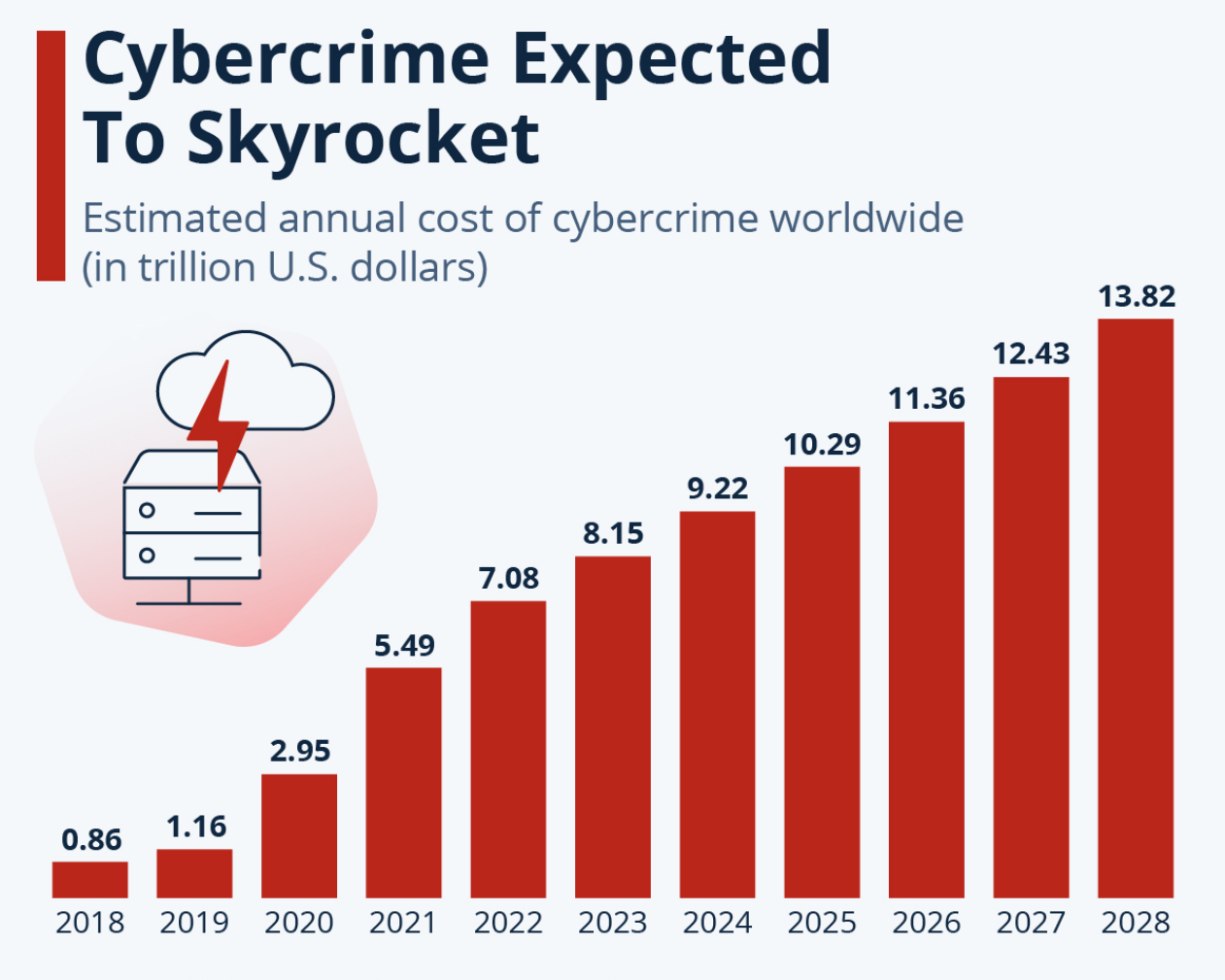

Figure 2: Estimated annual costs of cybercrime worldwide (Fleck, 2024)

5. What Should Constitute a Breach of Sovereignty in Cyberspace?

Another disagreement between states concerns which cyber operations qualify as a breach of sovereignty. According to the Tallinn Manual, "a cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage" (Tallinn Manual 2.0, 2019, 16). This phrasing suggests cyber operations must cause damage to qualify as a violation but does not specify the type or severity of damage. Does the damage need to negatively

Would the insertion of malware that causes no physical damage constitute a breach of sovereignty? It remains unsettled whether "minor material damage" to cyber infrastructure would be a violation of sovereignty (Von Heinegg, 2012, 11). For the U.S., hostile cyber operations can trigger the right to self-defence and the "use of all necessary measures" to maintain peace and stability (The White House, 2021, 14).

This wide scope suggests the country does not want to limit itself when responding to cyber operations at home.

The U.K. takes a more extreme approach by arguing sovereignty is a guiding principle rather

than a binding rule of international law (Roguski, 2020). In disagreement, France, Germany, Austria, Czech Republic, and the Netherlands argue sovereignty is an international rule and its violation constitutes an internationally wrongful act (Roguski, 2020). This article argues sovereignty should be considered an international rule because this creates more response opportunities for victim states (including the right to self-defence if the cyber operation constitutes an armed attack or countermeasures if the cyber operation constitutes an internationally wrongful act). Overall, offensive cyber operations should be evaluated on a case-by-case basis to determine whether the strategic context, direct effect, and severity violate state sovereignty.

To better understand what should constitute a breach of sovereignty in cyberspace, it is important to analyse existing state practice. No state or international organisation has "ever publicly and unequivocally qualified a cyber operation as a use of force [or an] armed attack" (Delerue, 2020). The threshold for armed attack is higher than the thresholds for use of force and sovereignty. However, states have responded to cyber operations in ways that suggest their sovereignty was breached. For example, in 2014 the U.S. responded to the Sony Pictures Entertainment cyberattack with sanctions on North Korea (Roberts, 2015). The attack caused physical damage by destroying Sony computers and hard drives, prompting the U.S. government to label the incident a "destructive cyberattack" linked to the North Korean government (U.S. Department of Justice, 2018). In 2016, Russian hackers accessed the U.S. Democratic National Committee's servers and published private emails during the presidential election. This time, the U.S. labelled the cyberattack a "violation of established international norms of behaviour" rather than a violation of sovereignty and imposed sanctions on Russian entities (Obama, 2016). In 2017, the U.K. condemned Russia's NotPetya ransomware attack on Ukraine as a "continued disregard for Ukrainian sovereignty" (Lord Ahmad of Wimbledon, 2018). The U.K. also criticised the Russian attack for disrupting "organisations across Europe [and] costing hundreds of millions of pounds" (Lord Ahmad of Wimbledon, 2018). The U.K.'s reaction suggests the indirect effect of cyber operations on third parties may breach state sovereignty. Overall, future state practice will help clarify what constitutes a breach of sovereignty in cyberspace.

6. How Does Anonymity Complicate State Attribution in Cyberspace?

After experiencing an offensive cyber operation that breaches sovereignty, states must attribute the action to another state to invoke state responsibility beyond due diligence obligations. Due diligence obligations require states "take measures to ensure their territories are not used for the detriment of other states" (Schmitt, 2015). To make state attribution easier, traditional domains generally require ships and aircrafts to register with a state (Franzese, 2009, 30). However, cyberspace's opaque nature makes state attribution more difficult. Even if a state determines where the cyberattack originated in terms of IP address, it rarely claims the country of origin violated state sovereignty (Franzese, 2009, 30). This reluctance likely stems from difficulties establishing state responsibility with non-state actors and hacktivists operating in cyberspace. The effective control test in Article 8 of the Articles of States Responsibility for Internationally Wrongful Acts (ARSIWA) stems from the ICJ's judgement that the United States' role in "financing, organising, training, supplying, and equipping the contras... [along with] planning [the whole] operation" was insufficient for state attribution (Nicaragua v. United States of America, 1986). This high threshold makes it nearly impossible for victim states to attribute the cyber operations of non-state groups or hacktivists to another state. For instance, Estonian Prime Minister Andrus Ansip accused the Russian government of involvement in the 2007 cyberattacks (Ashmore, 2009). However, the establishment of sufficient

government involvement to meet the effective control threshold was hindered because the attacks were linked to "spontaneously acting individuals" (NATO, 2007). Another Russian linked non-state actor group called 'Conti' likely implemented the widespread ransomware attack on the Costa Rican government, but the Russia government was not directly blamed for carrying out the attacks (Nast, 2022). Overall, the effective control test makes it difficult for states to attribute sovereignty violations to other states.

Given the difficulties of state attribution in cyberspace, this article argues states should address offensive cyber operations in other ways. According to the Tallinn Manual, state responsibility traditionally required actions be undertaken by or attributable to another state (Tallinn Manual 2.0, 2017). However, the manual also acknowledges an "embryonic view…that cyber operations conducted by non-State actors may violate a State's sovereignty" (Tallinn Manual 2.0, 2017, 18). Although victim states cannot impose countermeasures without state attribution, they can take other legal measures. For example, states can employ retorsion, which are "unfriendly diplomatic actions permissible under international law" (Schmitt, 2017, 258). Retorsion includes recalling diplomats, issuing public statements of condemnation, imposing economic sanctions, and more. Whereas states can only employ countermeasures against other states that breach their legal obligations, retorsion does not have this requirement (Schmitt, 2017, 242). In addition to retorsion, victim states can invoke the plea of necessity. This option can be used if an offensive cyber operation creates a "grave and imminent peril to an essential interest of the state concerned" (Schmitt, 2017, 251).

Similar to retorsion, the plea of necessity can be used even if the cyber operation is not deemed an internationally wrongful act. Overall, retorsion and the plea of necessity illustrate how anonymity in cyberspace should not dissuade states from addressing sovereignty violations.

7. Conclusion

In conclusion, this article analysed whether international consensus could be achieved on how sovereignty applies to cyberspace. After comparing cyberspace to the high seas, airspace, and outer space, the article established how virtual aspects of cyberspace complicate traditional notions of territorial sovereignty. Thus, states disagree over whether international law should be re-invented for cyberspace. This article argued against re-inventing international law in cyberspace and supported applying sovereignty in a way that acknowledges state authority but ultimately prioritises human rights like freedom of expression and privacy. Next, the article found states disagree over whether sovereignty constitutes a guiding principle or a binding rule of international law in cyberspace. This article supported conceptualising sovereignty as a binding rule of international law and evaluating offensive cyber operations on a case-by-case basis to determine whether they breach sovereignty. Finally, this article argued anonymity complicates state attribution in cyberspace and proposed responding to offensive cyber operations through retorsion and the plea of necessity to sidestep state attribution requirements. Overall, sovereignty disagreements between states will make achieving consensus on an international cyber-order a daunting task. In 2018, the UN General Assembly First Committee approved two proposals for separate working groups (one backed by Russia and the other by the U.S.) aimed at developing international cyber norms. These working groups illustrated widespread state commitment to developing international cyber norms, but they also risked splitting the UN's attention and potentially forcing member states to pick a side between the U.S. and Russia (The NATO Cooperative Cyber Defence Centre, 2023). Moving forward, states must unite to create a common understanding of how sovereignty applies in cyberspace to successfully address the rising number of harmful cyberattacks worldwide.

References

Treaties and UN Documents

United Nations Charter, June 26, 1945, https://www.un.org/en/about-us/un-charter.

United Nations Convention on the Law of the Sea, November 16, 1994, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations Conference on the Law of the Sea, February 24-April 27 1958, https://legal.un.org/diplomaticconferences/1958_los/docs/english/vol_1/a_conf13_4.pdf

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, December 19, 1966, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

United Nations General Assembly, "Letter dated 12 September 2011 from the Permanent Representatives," A/66/359, https://digitallibrary.un.org/record/710973?ln=en

International Law Commission Documents

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, A/56/10, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Court Judgements

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) I.C.J. Reports 1949, p. 244.

Island of Palmas Case (Netherlands v. USA). P.C.I.J. 1928, p. 831.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgement. I.C.J. Reports 1986, p. 14.

National Government Sources

Lord Ahmad of Wimbledon. (2018, February 15). Foreign office minister condemns Russia for Notpetya attacks. National Cyber Security Centre . https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

Obama, B. (2016). Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment. The White House, Office of the Press Secretary. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity#:~:text=All%20Americans%20should%20be%20alarmed,levels%20of%20the%20Russian%20government

The White House. (2021, May). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

U.S. Department of Defense. (2023). 2023 Cyber Strategy of Department of Defense. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

U.S. Department of Justice. (2018, September 6). North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber-attacks and intrusions. U.S. Office of Legal Affairs. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Books

Delerue, F. (2020). The Threshold of Cyber Warfare: From Use of Cyber Force to Cyber Armed Attack. In Cyber Operations and International Law (Cambridge Studies in International and Comparative Law, pp. 273-342). Cambridge: Cambridge University Press. doi:10.1017/9781108780605.009

Kish, J. (1973). The law of international spaces. Sijthoff.

Lessig, L. (2010). Code: Version 2.0. SoHo Books.

Osula, A.-M., & Rõigas, H. (2016). International Cyber Norms: Legal, policy and Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

Schmitt, M. (2017). Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. Cambridge University Press. https://doi.org/10.1017/9781316822524

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What everyone needs to know. Oxford University Press.

Von Heinegg,W.H. (2012). 'Legal implications of territorial sovereignty in cyberspace,' in C Czosseck, R. Ottis & K. Ziolkowshki (Eds.), Proceedings of the 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications.

Weber, R. H. (2016). Realizing a new Global Cyberspace Framework Normative Foundations and guiding principles. Springer Berlin.

Scholarly Articles

Ashmore, W. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review, 11.

Barlow, J. P. (2018, April 8). A declaration of the independence of Cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Eichensehr, K. (2014). The Cyber-Law of Nations (SSRN Scholarly Paper 2447683). https://papers.ssrn.com/abstract=2447683

Franzese, P. (2009). Sovereignty in Cyberspace: Can it Exist? The Air Force Law Review, 64, 1–42.

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review, 48(5), 1367–1402. https://doi.org/10.2307/1229390

Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? Journal of Information Warfare, 12(2), 19–26.

Moynihan, H. (2019). The application of international law to State cyberattacks. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/6-processes-reaching-agreement-application

NATO. (2007). 2007 Cyber Attacks on Estonia. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

Schmitt, M. (2015). In Defense of Due Diligence in Cyberspace. Yale Law Journal Forum, 125.

Schmitt, M. N. (2017). Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. 8.

Tavenner, E. (2022, February 1). Russian Cyber Sovereignty: Global Implications of an Authoritarian RuNet. American University. https://www.american.edu/sis/centers/security-technology/russian-cyber-sovereignty.cfm

The NATO Cooperative Cyber Defence Centre of Excellence. (2023). A surprising turn of events: UN creates two working groups on cyberspace. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/

Winnefeld, J., Kirchoff, C., & Upton, D. (2016, September 9). Cybersecurity's human factor: Lessons from the Pentagon. Cyber Security and Digital Privacy. https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

Online Sources

Nast, C. (2022). Conti's Attack Against Costa Rica Sparks a New Ransomware Era. Wired UK. https://www.wired.co.uk/article/costa-rica-ransomware-conti

Ranjithsiji. (2018, April 17). File:Deepweb graphical representation.svg - Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Deepweb_graphical_representation.svg

Roberts, D. (2015, January 2). Obama imposes new sanctions against North Korea in response to Sony hack. The Guardian. https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview

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

Rosch, C. (2022, June 1). A massive cyberattack in Costa Rica leaves Citizens Hurting. Latin American Politics. https://restofworld.org/2022/cyberattack-costa-rica-citizens-hurting/

Santi, M. (2023, March 16). Dark web statistics and trends for 2023. Prey Project. https://preyproject.com/blog/dark-web-statistics-trends

Sherman, J. (2018, December 24). Russia's Tightening Control of Cyberspace Within its Borders. Just Security. https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. The Guardian. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Vailshery, L. S. (2023, July 27). IOT connected devices worldwide 2019-2030. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

Zetter, K. (2023, May 2). The untold story of the boldest supply-chain hack ever. Wired. https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/#:~:text=Once%20they%20had%20the%20source,went%20dark%20for%20six%20months