Access*: Interdisciplinary Journal of Student Research and Scholarship

Volume 3 | Issue 1 Article 4

2019

The Next Frontier: Cyberspace in Current International Law

Adán Espino Jr.
University of Washington Tacoma, espinoa5@uw.edu

Follow this and additional works at: https://digitalcommons.tacoma.uw.edu/access

Recommended Citation
Espino, Adán Jr. (2019) "The Next Frontier: Cyberspace in Current International Law," *Access*: Interdisciplinary Journal of Student Research and Scholarship*: Vol. 3 : Iss. 1 , Article 4.
Available at: https://digitalcommons.tacoma.uw.edu/access/vol3/iss1/4

This Undergraduate Research Paper is brought to you for free and open access by the Teaching and Learning Center at UW Tacoma Digital Commons. It has been accepted for inclusion in Access*: Interdisciplinary Journal of Student Research and Scholarship by an authorized editor of UW Tacoma Digital Commons.

The Next Frontier: Cyberspace in Current International Law

Cover Page Footnote
This paper was submitted because of the inspiration my law professor from UW Tacoma, Elizabeth Bruch, gave me during that class. I not only enjoyed the class, but was moved from your encouragement during the writing process to submit the paper for publication. Thank you. Thank you, Adán E. Jr.

This undergraduate research paper is available in Access*: Interdisciplinary Journal of Student Research and Scholarship:
https://digitalcommons.tacoma.uw.edu/access/vol3/iss1/4

Abstract

As a general overview of cyberspace's current state within international law, *The Next Frontier* introduces readers to an evolving landscape of both international law and diplomacy. Cyberspace and cyberwarfare are ever more paramount to how states conduct relations and seek to advance their interests. Such a domain cannot be ignored as technology advances and its uses become increasingly widespread. As such, the current void of comprehensive law or regulations around such pose a strong disadvantage for states, especially in instances of cyberwarfare. Current international law can be interpreted to provide a foundation for more specific consensus to be built on, but little exists outside of that and especially in regard to non-hostile acts. This paper condenses the loose pieces of international law that exists into a general overview for readers. It is hoped this general overview will inspire more minds to develop the increasingly important field of cyber law and build upon the law that currently exists.

Keywords: cyberspace, international law, cyberwarfare, cyber law

Published by UW Tacoma Digital Commons, 2019

The Next Frontier: Cyberspace in Current International Law

The opening of video game series, *Fallout*, begins with the proverbial phrase, “War. War never changes." While the philosophical interpretation for this phrase may be true, the literal interpretation is less so. Especially in today’s information age, this phrase cannot be said to be accurate. Notably, the rise of the internet has made way for a new frontier of both war and international diplomacy. Cyberspace, defined in this paper as the space operated by computational devices where data may populate or transfer through, has emerged as a new realm that is continually more relevant to the rule of international law, given its growing importance and integration into everyday operations of modern society.

As such, the use of cyberspace as a domain for states to act within presents an array of questions, challenges, and conflicts that will have to be resolved in the future if the international community wishes to avoid the problems that an undefined section of international law may present. What are those supposed conflicts? They can range from questions of international humanitarian law (IHL) applications via cyberwarfare, questions of jurisdiction via cybercrimes, and questions of trade regulation via internet commerce. Wherever cyberspace may exist and however it may be used, those novel uses must be subject to the rule of international law to settle disputes and regulate behavior. If vagueness or a gray area exists, then one can be sure it will be exploited, whether for better or worse.

One could argue that customary international law will erase this initial vagueness, by citing norms or behavior states currently engage in within cyberspace. By itself,

though, customary law cannot be the only basis on which international law is initially applied to cyberspace. Especially in regard to cyberwarfare, it is important to establish clear and written conventions for this emerging realm of international relations. Some questions that may arise are: Does a cyberattack constitute a "use of force" and is Article 2(4)[1] of the UN Charter prohibiting the use of force applicable to it? Can a cyberattack be considered an act of aggression, allowing the UN Security Council to react to said attack? Cyberspace and cyberwarfare as a concept have not existed long enough to have established much customary law around these questions. Maybe one could attempt to apply customary law to cyberwarfare in the same way it pertains to traditional warfare. While this would be a useful step, we are still left with a range of concepts that do not exist in non-cyber activities yet still need to be defined (such as whether a virus should be considered a weapon or a program).

Therefore, the international community must interpret current international law within the context of cyberspace and attempt to resolve gaps that international law may not cover. This paper seeks to help in that matter. However, given the scope of identifying where current international law is applicable to cyberspace and where it is not, and where new laws must be created, this paper will narrow its focus to providing a general overview of the current literature's understanding of how international law applies to cyberwarfare and speculate, where possible, how that framework may translate to cyberspace more generally.

[1] In the UN Charter, under Chapter I, Article 2, paragraph 4 states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Link: http://legal.un.org/repertory/art2.shtml

Cyberwarfare in International Law

The literature has largely focused on how international law applies to cyberwarfare, and rightly so, given the potential catastrophes and harm unregulated cyberwarfare may lend itself to. In addition to the large interest in regulating armed conflict and the strict prohibition of the use of force according to Article 2(4) of the UN Charter, thinking about where and how cyberwarfare is applicable under current international law is easier than thinking of the jurisdiction international law has on virtual documents, for example. This is because, under international law, war has been discussed, debated, and regulated for centuries, which therefore has resulted in more clearly defined sections of international law compared to intellectual property law, trade law, jurisdiction, etc. More specifically, the fundamentals of the international law of war are well understood. And given that cyberwarfare is an emerging form of conflict, the initial step to understanding the fundamental concept of cyberwarfare is largely complete. The biggest hurdles are the definition and application of these fundamental understandings, which can then allow for inference in other areas. This is not to say it will be easy, however, as the nature of cyberwarfare lends itself to an array of complexities.

Cyberwarfare is unique compared to more understood forms of warfare in that it largely takes place within an apparently metaphysical area. More specifically, cyberspace, the domain where cyberwarfare largely operates, is less tangible than ground or naval warfare where targets and weapons are physical. Unlike ground, water, or even air, the domain of cyberspace passes through all nations and cyberwarfare

cannot be stopped without interfering in the other uses of cyberspace. Nils Melzer, of the University of Zürich, states in *Cyberwarfare and International Law* that “Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads are deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum” (Melzer, 2011, p. 5). To access cyberspace, one must be connected to the “electromagnetic spectrum” as all operations in cyberspace are inherently linked to it. Therefore, disrupting passage through cyberspace means disrupting all operations in cyberspace.

Harold Hongju Koh of Yale Law School, in a 2012 speech at the USCYBERCOM Inter-Agency Legal Conference discussing the roles of cyberspace in national defense, concurs and adds that there should be a larger priority for state sovereignty in cyberspace given that cyberspace itself is transnational but the means to access cyberspace are located in sovereign territory. Koh (2012) observes that “operations targeting networked information infrastructures in one country may create effects in another country. Whenever a state contemplates conducting activities in cyberspace, the sovereignty of other states needs to be considered” (p. 6), as cyberwarfare only becomes tangible through consequential action.

For example, if the mainframe of the network that controls the power grid of the city of Seattle is infected with malware and shuts off the power grid, the attack becomes tangible. Unlike an incoming missile aimed at the transformers in the power grid, which can be stopped via surface-to-air(SAM) missiles and is usually detected long before it reaches the target’s airspace, one cannot detect malware until it is either attempting passage or harbored in a device. The device housing the malware must then be

destroyed or undergo a complicated and time-consuming process of cleansing the software. Additionally, due to its instantaneous nature, it can be ambiguous as to when a cyberattack officially occurs (is it upon infection or upon consequence?) or, if defined, does it constitute an actual attack or an act of aggression under international law? In the case of the incoming missile, these questions would have clear answers: the launching of a missile towards its lawful target would clearly be when the attack occurs and would be generally regarded as an act of aggression.[2]

In an advisory opinion on the Legality of the Threat or Use of Nuclear Weapons in 1996, citing Articles 42 and 51 of the UN Charter (articles pertaining to allowing the Security Council to undertake lawful military enforcement and the right to self-defense if an armed attack occurs, respectively), the International Court of Justice (ICJ) stated "These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon" (ICJ, 1996, p. 244). This can be interpreted that there is no specific weapon that defines the use of force. As such, whatever is currently defined as a weapon falls into a "use of force" within the terms of the UN Charter. While the ICJ argued for the inclusion of nuclear weapons, the opinion also allows for the inclusion of cyber weapons.

Indeed, Melzer (2011) expresses that "it is relatively uncontroversial that cyber operations fall under the prohibition of article 2(4) of the UN Charter once their effects are comparable to those likely to result from kinetic, chemical, biological or nuclear weaponry" (p. 7). As it pertains to cyber weapons, the tangible, consequential results

[2] The Humanitarian Policy and Conflict Research program at Harvard published the *Manual on International Law Applicable to Air and Missile Warfare* for further reading.

from a cyberattack indicate a use of force, especially if the cyber weapon was “an offensive or defensive tool designed to cause death or injury to persons or the destruction of objects and infrastructure, irrespective of whether such destruction involves physical damage, functional harm, or a combination of both” (p. 7). Koh (2012) also expresses this view, saying, “Only a moment’s reflection makes you realize that this is common sense: if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force” (p. 4). However, one may ask if cyberattacks or operations that do not directly or indirectly result in death, injury, or destruction of property still fall under prohibition under Article 2(4).

So-called minor acts of force, or acts that would cause an international armed conflict that are carried out via cyber weapons or operations (but do not directly cause death, injury, or destruction of property), also fall under the UN Charter, as the ICJ ruled in the Nicaragua Case of 1986; such minor acts can be considered uses of force under the UN Charter. In its judgement, the ICJ states that it “does not believe that the concept of ‘armed attack’ includes only acts by armed bands, where such acts occur on a significant scale, but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States” (ICJ, 1986, p. 47). In layman's terms, simply assisting insurgents (regarding the US assistance of the Contras in Nicaragua), in addition to overtly fighting alongside them, may be regarded as a use of force.

Published by UW Tacoma Digital Commons, 2019

According to this ruling, the ICJ interprets that armed acts or “acts by armed bands” are not the sole characteristics of a use of force and unarmed actions or hostilities may also be regarded as such. Therefore, cyberattacks or operations not directly resulting in death, injury, or destruction of property can still be regarded as a use of force. Even though this ruling was applied within the context of assistance to insurgency groups, this principle can still be held outside of insurgent assistance based on the prohibition principle of the UN Charter. That is, even though the Charter’s prohibition of force was not explicitly extended to many nonviolent acts (for example, economic coercion or political pressure), the ICJ, in its 1996 advisory opinion, also stated that the UN Charter generally prohibits all uses of force and threats to use force that have not been exempted. Specifically, “The notions of ‘threat’ and ‘use’ of force under Article 2, paragraph 4 of the Charter stand together in the sense that if the use of force itself in a given case is – illegal—for whatever reason—the threat to use such force will likewise be illegal. In short, if it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter” (ICJ 1996, p. 246), which is the prohibition principle.

Additionally, Article 1 of the Charter expresses that the UN shall “maintain international peace and security, and . . . take effective collective measures for the prevention and removal of threats to the peace”. As such, any act that would breach said peace or lead to an international armed conflict falls under the scope of the UN’s purpose, and therefore the Charter, including cyberattacks and operations that would breach “international peace and security” (UN Charter 1(1)).

In concurrence, Melzer (2011) states that “As a matter of logic, the Charter cannot allow that the prohibition of interstate force be circumvented by the application of non-violent means and methods which, for all intents and purposes, are equivalent to a breach of the peace between the involved states,” citing examples of disabled power grids of major cities, disabled systems of industrial production, and disabled air defense systems (p. 8).

Thereby, we are given a basic framework for understanding the applicability of international law to cyber weapons, cyber operations, and cyberattacks—at least for that which results in consequences that breach the peace:

- All cyber operations or cyberattacks are an “act of aggression” or a “use of force” if such operations and attacks result in consequences similar to conventional operations and attacks that do constitute as an “act of aggression” or a “use of force” and are thus regulated under the Charter.
- Such operations or acts that may not constitute as an overt “act of aggression” or a “use of force,” but would seem to or do end up breaching international peace and security, as well as operations or acts that seem to or do start an international armed conflict, are still applicable under international law, specifically the UN Charter.
- Cyber weapons are regulated and treated similarly to their conventional counterparts.

At the risk of being redundant, an even simpler way to think about it is that cyberwarfare, cyber operations, and cyber weapons are to be treated no differently than similar acts or weapons lacking the word “cyber.” Concurrently, the principles of

responsibility are to be used when assigning attribution to an attack or action. Specifically, these principles and applications only apply to state actors or non-state actors acting as representation, on behalf of, or under the control of a state (according to the fundamental definition of what is a state).

Additionally, the law of neutrality, which establishes that states have a right to abstain from conflict and are thereby bound to uphold their abstention, is applicable to all cyber operations that may be conducted by belligerents. This can be tricky, however, as it is generally difficult to know where exactly a cyberattack or operation has been launched from. Given the transnational nature of cyberspace, it is also unlikely and largely unfeasible for neutral states to stop all belligerent cyber activities and the passage of belligerent cyber activities. Melzer (2011) reasons that neutral powers are exempt from regulating belligerent activity through their publicly available infrastructure because of the impossibility of controlling such publicly available infrastructure. Instead, the “rationale underlying the Hague Convention would suggest that neutral states can be expected to prevent belligerent states from conducting cyber hostilities from within their territory, but not the routing of belligerent cyber operations through their publicly accessible communications infrastructure” (p. 20).

While customary law is largely absent in regards to cyberwarfare, emerging practices are slowly creating a foundation for customary law to take shape. That is, with the relative ease of carrying out cyberattacks or hostile cyber operations, the frequency of such acts are far from uncommon. In addition, high profile cyberattacks or hostile cyber operations are becoming increasingly more common and more notable, such as Russia’s involvement with the US presidential elections and its spread of fake news

stories in places such as Germany's "Lisa" case, Sweden's anti-NATO propaganda, and France's email hacking of then-candidate Emmanuel Macron.[3]

While all these examples could probably be labeled as uses of force or acts of aggression, the language and identification as events such of these remains nearly non-existent. Rather, it seems that states are practicing a tit-for-tat method of dealing with such acts, as Western powers have used cyber operations to further their own foreign policy.[4] At least for now, these operations on all sides have been largely information-based and may be limiting customary law around cyberwarfare to this tit-for-tat method. However, this may be to avoid obvious and clearly unlawful actions that, despite possibly providing short-term benefit, may spur an international dilemma nobody wants to deal with yet.

Cyberspace in International Law

International law applicable to cyberspace that is not associated with *jus ad bellum* or *jus in bello* (international law before and during war, respectively) compromises a lesser portion of the literature in regard to cyberspace but is nonetheless just as important. Indeed, given that there seems to be a good deal of understanding of international law applicable to cyberwarfare, issues not pertaining to such are gaining more attention. For example, how does international law apply to cyber trade activities? How does international law apply to cyber documents? Can data be property regulated under international law? Could a state exercise jurisdiction in

[3] The Brookings Institute has an excellent report about Russia's cyber operations in this regard: https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf
[4] The Council on Foreign Relations has an article that can provide more insight into how states are shaping customary law in cyberspace for their interests: https://www.cfr.org/report/promoting-norms-cyberspace

cyberspace? Despite a gap in legal understanding for these questions, the principle understanding gained from the analysis of cyberwarfare law can help answer these questions.

The Equivalency Principle and Law Applicable to E-commerce and Cyber Documents

The equivalency principle is the most fundamental of the legal principles that form the basis for the above three bulleted points. Specifically, this principle bridges the gap between the seemingly abstract operations in cyberspace and traditional international law, as it states that cyberspace or cyber operations are functionally equivalent to their non-cyber counterparts. That is, laws governing said counterparts are applicable to their cyber equivalents.

An explicit mention of this principle appears in the United Nations Commission on International Trade Law's (UNCITRAL) 1996 measure, the Model Law on Electronic Commerce (MLEC). This law outlines the UNCITRAL's "functional-equivalent approach," which seeks to provide "an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques" (MLEC, 1996, p. 20). Additionally, in 2017, the UNCITRAL enacted its Model Law on Electronic Transferable Records (MLETR) "to enable the use of electronic transferable records on the basis of their functional equivalence" (MLETR, 2017, p. 17), thereby recognizing the use of transferable electronic records seemingly left out in the 1996 model law.

The two documents provide for a basis for both the use of the equivalency principle and the application of current international law to e-commerce and cyber

documents. Some notable applications come from article 5 of the MLEC and article 7 of the MLETR, which respectively state that “Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message” and that “An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form” (MLEC, 1996, p. 32; MLETR, 2017, p. 13). Additionally, both the MLEC and MLETR act together to indicate cyber documents that are functionally equivalent to paper-based documents or conventional processes are applicable under the same laws.

The summation of these model laws is the effective establishment of clearer legal understanding for contracts between parties within the cyber realm. As contracts and documentation are significant elements of commerce, establishing equivalency between cyber and conventional documentation and information covers a large piece of e-commerce in international law. However, both model laws fail to cover other aspects of e-commerce, such as sales of digital products. It is possible that these other aspects of e-commerce are better understood through other components of the law and are not as relevant under commercial law. How to enforce property rights over digital products is one example.

Data as Property

Though the equivalency principle bridges the gap between the cyber and the conventional, such a principle becomes useless in circumstances where it is not clear how the conventional and the cyber are equivalent. For instance, if data could be considered property, what is its equivalent? For media, connections and equivalents can be found as digital and film creations are not fundamentally different, at least not

legally. However, with the ease of transfer and creation—and therefore, re-creation—of digital content, it is possible that such a determination would complicate current legal understandings in property or copyright law.

The notion of data as property is an emerging one. So much so that there is very little literature discussing how data can be regarded as property. Despite property rights and ownership having a large role to play in trade, the UNCITRAL does not provide any basis for data (via cyber documents or processes in this case) to be regarded as such. In fact, the MLETR states that a "'person in control' of the electronic transferable record… does not imply that the person is also the rightful person in control of that record as this is for the substantive law to determine" (MLETR, 2017, p. 44).

Indeed, it seems that such a decision is mostly left to individual states to decide for themselves whether data could be considered as property and how. Yet, conflicts will abound eventually, as some states will differ on when and what kind of data is constituted as property, as well as how to resolve property disputes between parties in different states with differing data property laws.

This is already prevalent within emerging intellectual property law as states pass differing copyright institutions and enforcements. As it stands, data seems to be regarded as a form of intellectual property rather than physical property. Both in current laws and practice, data is treated as a medium of intellectual property, just as the paper used to print a book. This means that while data is not owned, access to data is, as seen through the distribution of digital products such as movies, video games, or literature. Users purchase product licensing in which the creator—assuming it has been copyrighted--retains intellectual property rights and merely allows someone else to

access the content.[5] In a similar vein, companies like Facebook and Twitter sell access to their users' data, rather than the data itself.[6] In both cases, a user agreement is made and holds the user accessing the data or content liable to respecting the copyrighted product by not illegally copying it.

Such agreements are not without their problems. Digital and online enforcement preventing illegal distribution of products proves difficult due to online pirating, as users are essentially given free rein to do what they please with their purchased copies. A user can allow another person to use the purchased copy without legal repercussions, as the user has legal right to use the product. However, users are not allowed to duplicate their purchased copies and distribute the duplicates, either free or at cost. This is why giving someone a purchased video game or reselling purchased video games is not illegal but selling or giving away pirated copies is. Yet, it is hard to police against the illegal distribution because to do so would mean having to watch what happens to every copy sold, which is impossible. As technology and IT knowhow develops, however, it should become possible to construct better policing techniques.[7]

Privacy concerns can arise from selling access to user data that is collected by companies like Facebook and Twitter, as seen with the infamous Cambridge Analytica-Facebook scandal, in which Cambridge Analytica bought access to Facebook's users'

[5] Here is a more detailed analysis of cyberspace and intellectual property law: Marilyn C. Maloney - Intellectual Property in Cyberspace https://www.jstor.org/stable/40687783?seq=1#page_scan_tab_contents

[6] CBS News - Facebook: Your personal info for sell https://www.cbsnews.com/news/facebook-your-personal-info-for-sale/

[7] PC Gamer - The State of Piracy in 2016 https://www.pcgamer.com/the-state-of-pc-piracy-in-2016/2/

data and devised methods to more or less trick users to giving them more access than Facebook had provided to Cambridge Analytica.[8]

Ownership and property claims are further complicated on streaming sites like YouTube or Twitch. The question becomes: who owns the content (or data) posted to YouTube or Twitch? Is it YouTube, or the user that posted it? Currently, this is largely left to the sites and companies involved, which largely allow the users to retain ownership over their content.[9] But how would this change if data is constituted as property? Additionally, these questions become more complex when applied on an international scale because websites can be accessed anywhere they are not blocked (China is a notable exception as it blocks many Western sites). Thus, their data can be accessed nearly anywhere in the world.

Despite the relative void in the literature about this subject, those that do seek to answer the question of whether data can be constituted as property provide significant insight and analysis as to how it could. Jeffrey Ritter and Anna Mayer of Duke Law School are two such individuals. In “Regulating Data as Property: A New Construct for Moving Forward,” they explain that current scientists agree that data is not merely an abstract concept, but a physical thing consisting of matter (Ritter & Mayer, 2018, pgs. 223 & 256). Many discussions about regulating data also omit regulating industrial data, including data produced through commerce but without personal information, such as data in financial services. They claim “the market confirms the wealth creation potential that can be extracted from industrial data . . . [which is] being realized without any

[8] Wikipedia - Facebook-Cambridge Analytica data scandal
https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
[9] TubularInsights - Who Owns Your YouTube Video?
https://tubularinsights.com/youtube-copyright-ownership/

substantive legal structure in place to define the information's ownership and attendants rights!" (Ritter & Mayer, 2018, p. 254).

To help provide a framework for the legal language to constitute data as property, Ritter & Mayer (2018) established that:

- Data becomes real the moment it is recorded by electronic or digital means (p.260).
- To exist, data must be capable of being computationally sensed and logged (p. 260).
- Ownership is attached at the point in time it is recorded, and an entity establishes control of the data and can reliably prove it recorded it (p. 267-269).

In short, Ritter and Mayer (2018) largely modified US and EU property law concepts for tangible items to be applicable to data and altered MELTR language to provide a detailed framework to constitute data as property. While Ritter and Mayer (2018) provided an insightful perspective on the question of data as property, the aforementioned challenges still present themselves. Some of these challenges could be resolved if data fell under current international property laws via the equivalency principle, but given the difficulty in preventing unlawful use of property that can so easily cross borders, this leaves said laws nearly moot.

Amidst these challenges, there does exist international law for intellectual property and patents, in which anything granted such distinctions or privileges in host states can be subject to current laws as per the equivalency principle. The Paris Convention for the Protection of Industrial Property of 1883, most recently amended on

1979, is an established standard for the protection of intellectual property (or industrial property as it was then called) and is used by the World Intellectual Property Organization (WIPO) as law, signed by many states since its promulgation, with Afghanistan as the most recent signee on May 14th, 2017.

The Paris Convention enshrined among its provisions that contracting states must grant the same protections to nationals from other contracting states as they do their own. Additionally, “the right of priority” allows applicants to apply for protection within a certain period of time in any of the other contracting states in addition to their home one. A more modern version of what was laid out in the Paris Convention can be found in the Patent Law Treaty of 2000, as it covers many of the same subjects. All other treaties or conventions established by or through the WIPO is applicable as well. For cyberspace law, this proves useful as once a convention has established how to define and regulate data or its access, data can fit into existing law, either formally or through customary practice.

Jurisdiction Claims over Data or Cyberspace

Almost certainly, the subject that holds the greatest interest is whether states could make jurisdictional claims over data or cyberspace. Jurisdictional claims are already complicated and contentious, but this is because of the high importance of the subject. More specifically, how jurisdictional claims can or cannot be made will dictate the long-term behavior of states in regard to cyberspace, as well as their role in international non-war activities.

While not representing expressed law, a group of international lawyers and experts from the NATO Cooperative Cyber Defence Centre of Excellence studied,

analyzed, and debated various applications international law has on cyberspace and operations to prepare a set of rules called The Tallinn Manual. The work contains extensive insight into how states may or may not exercise jurisdiction in cyberspace.

The Tallinn manual claims in Rule 8 that a state indeed may exercise both territorial and extraterritorial jurisdiction over cyber activities. The manual elaborates that “in principle, cyber activities and the individuals who engage in them are subject to the same jurisdictional prerogatives and limitations as any other form of activity” (Schmitt, 2017, p. 51), which refers to the equivalency principle. The manual states that because territorial jurisdiction is closely linked to sovereignty, states enjoy full control over people, objects, and activities located in their territory (p. 52). This allows Rule 9 to specify that a state may exercise territorial jurisdiction over “(a) Cyberinfrastructure and persons engaged in Cyber activities on its territory; (b) Cyber activities originating in, or completed on, its territory; or (c) Cyber activities having a substantial effect in its territory” (Schmitt, 2017, p. 55).

In practice, this could mean that states could exercise jurisdiction over cyber activities that are even minimally connected to their territory, as long as such connection has a substantial effect in their territory. While the manual states its experts agreed that activities similar to those mentioned in earlier sections of this paper or comparable are claimable, it is important to note that the manual also states the group was split on more minimally connected activities such as the passage of data through a state’s infrastructure (Schmitt, 2017, p. 55).

Rules 10-14 delve into extraterritorial claims and activities. The manual largely invokes the equivalency principle by expressing that cyber activities and operations

functionally similar to those already regulated are likewise subject to those existing regulations, such as: jurisdiction over the overseas conduct of a state's nationals, jurisdiction over foreign nationals seeking to undermine the host government, consent by a foreign government to the exercise of jurisdiction in its territory, and immunity of states or their representatives that enjoy immunity under international law. The manual does not explicitly mention anything about data itself, however. It can be inferred that territorial jurisdiction claims can be made regarding data itself if all other things cyber are also claimable; if they were not, there would be a serious loophole. For example, if a painting can be territorially claimed via intellectual property enforcement in both its physical and digital forms, but the physical data that compromises the digital form cannot be territorially claimed, then how do you enforce the claim? Not only is it needlessly complicated but it effectively eliminates state jurisdiction in cyberspace. Because of the equivalency principle this cannot be the case, hence, it can be inferred data itself can be claimed. Therefore, this principle is the fundamental bedrock of legal applicability in cyberspace.

A more complicated facet of data claims is the extraterritorial potential. Some aspects can be inferred, such as gaining express permission from a foreign government to exercise jurisdiction over data in its territory, but many aspects of extraterritoriality cannot be so easily inferred. For example, without express permission, can a state exercise jurisdiction over data generated overseas by one of its nationals?[10] As it stands now, the answer is speculative at best because, despite the principles laid out by the

[10] Lawfare has a primer on a specific example of an extraterritoriality controversy involving the US and Ireland:
https://www.lawfareblog.com/primer-microsoft-ireland-supreme-courts-extraterritorial-warrant-case

Tallinn Manual in regards to jurisdiction, such a question is subject to property law. Such law is not specifically covered by the Tallinn Manual, and data currently is not constituted as property. Another example is whether a state can claim jurisdiction over parts of the internet. Unlike cyberspace originating from infrastructure within a state's borders, the internet is transnationally connected by every computational device that can access it and only exists through that connection.[11] Therefore, if a state could claim jurisdiction over the internet, where would that jurisdiction end? It might be wise to conclude a state cannot claim jurisdiction over the internet for the same reasons that states cannot claim jurisdiction over the high seas or outer space.

Conclusion

Though cyberspace and the various activities that occur within it may seem complex, understanding how such activities can be regulated under international law is paramount to the sustainability of peaceful and orderly international relations for the future. There are still many questions that must be answered, but thankfully a basis for the many facets of cyberspace and cyber operations, the equivalency principle, allows current and future thinkers to continue working to answer those questions.

However, unlike other spheres regulated under international law, the domain of cyberspace is rapidly evolving, which means that corresponding law must rapidly adapt to change, despite significant unknowns. For example, in the most likely segment to expand—cyberwarfare—the world has yet to see true cyberwarfare waged. It would seem that a fully-fledged cyberwar would begin not with an open declaration or visible

[11] The Harvard Gazette has an article that, while focusing on net neutrality, provides more information on internet jurisdiction:
https://news.harvard.edu/gazette/story/2014/01/so-who-owns-the-internet/

attacks. Rather, it would take shape through subtlety and proxy, where part of the battle is simply figuring out who is carrying out the attack. Much like the way states wage proxy wars today, cyberwar will hide under the cover of more immediate or physical events. Rarely will these be obvious shutdowns of infrastructure or systems; they are more likely to be disruptions, big or small, that stack up over time or stoke fractures in a state. Political interference will be one front,[12] while economic issues will be another.[13] At the same time, the potential for spying will be clear.[14]

Jurisdictional and property issues will continually emerge with the introduction of new connective software and technologies. Determining how or when physical data can be interpreted as property may be best solved by linking said data to its intellectual source and relying on established and enforceable copyright law. What may remain truly impossible to solve are jurisdictional claims to data or to digital spaces. Maybe in the future there might exist technology that will allow cyberspace to manifest as a more tangible realm (possibly through virtual reality), which will make cyberspace easier to navigate. Maybe such speculation might be better left to a paper regarding technological advancements instead of law. Either way, the future for both fields awaits.

Hopefully, readers will find themselves excited about this future. The unknowns of future development and current uncertainty are intimidating, if not downright scary. But readers must remember their power to shape these unknowns and uncertainties.

[12] Russian interference in the 2016 US Election
https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election
[13] The Council of Economic Advisers, February 2018 - The Cost of Malicious Cyber Activity to the U.S. Economy
[14] Bloomberg - Vodafone Found Hidden Backdoor in Huawei Equipment
https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment

This paper's aim has been to provide an accessible overview of the laws that govern current systems and may guide future developments of new ones. Through this accessibility, it is hoped that readers may find themselves empowered to not merely continue expanding the literature, but use their knowledge to develop solutions. This paper has speculated on gaps in the literature at large, as well as how the space might develop, but there is so much more to cover.

We are always exploring the next frontier.

References

International Court of Justice. (1996). Legality of the threat or use of nuclear weapons, advisory opinion, p. 226. Retrieved from https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

International Court of Justice. (1986). Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, p. 14 Retrieved from https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Koh, H. H. (2012, December). International law in cyberspace [scholarly project]. In Yale Law School. Retrieved from http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

Melzer, N. (2011). Cyberwarfare and international law [Scholarly project]. In United Nations Institute for Disarmament Research. Retrieved from http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

Paris Convention for the Protection of Industrial Property. (20 March 20 1883). Retrieved from https://www.wipo.int/treaties/en/ip/paris/

Patent Law Treaty. (1 June 2000). Retrieved from https://wipolex.wipo.int/en/text/288996

Ritter, J., & Mayer, A. (2018). Regulating data as property: A new construct for moving forward [scholarly project]. In Duke Law School. Retrieved June 06, 2018, from https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1320&context=dltr&preview_mode=1&z=1521402986

Schmitt, M.N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber warfare. Cambridge: Cambridge University Press.

U.N. Charter art. 1, para. 1.

U.N. Charter art. 2, para. 4.

United Nations Commission on International Law. (1996). UNCITRAL Model Law on electronic commerce with guide to enactment. Vienna: United Nations. Retrieved from https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

United Nations Commission on International Law. (2017). UNCITRAL model law on electronic transferable record. Vienna: United Nations. Retrieved from http://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf