Violations of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach

Przemysław Roguski

Cite as: Roguski, Przemysław. 2020. "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, 65-84. London: Rowman & Littlefield International.

Chapter 4

Violations of Territorial Sovereignty in Cyberspace—an Intrusion-based Approach

Przemysław Roguski

Ever since the Treaty of Westphalia established the modern legal order, the sovereignty of states is one of the foundational principles of public international law. The principles of state sovereignty and sovereign equality have been reaffirmed in Art. 2(1) of the United Nations Charter and form the bedrock of the post–World War II international legal order. This legal order, conceived in a time when global computer networks carrying information across continents in seconds and making it available without regard for location and geographical distance were but a distant dream, must evolve to account for new technological developments such as the rise of information and communication technologies (ICTs), which link states and people closer together through cyberspace. Faced with a new medium with unique characteristics of ubiquity and aterritoriality of information, states as the principal actors of the international legal order had to decide whether this new medium—cyberspace—is a unique "space," requiring a different set of rules governing state rights and state behavior, or whether existing rules of international still apply.

Gradually, a consensus has begun to form around the proposition that rules and principles of international law, as enshrined in the UN Charter, apply in cyberspace. As the former legal adviser to the US Department of State, Harold Koh, put it: "cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint. (. . .) States conducting activities in cyberspace must take into account the sovereignty of other states" (Koh 2012, 3, 6). This consensus has been cemented through the work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which in 2013 and 2015 issued two reports detailing the rules and principles of international law applicable to state behavior

in cyberspace (United Nations General Assembly 2013, 2015). While the Group of Governmental Experts managed to clarify many fundamental aspects relating to state sovereignty in cyberspace, including the jurisdiction of states over cyber infrastructure located on their territory (United Nations General Assembly 2013, para. 20), the prohibition on the use of force and non-intervention in the internal affairs of other states (United Nations General Assembly 2015, para. 26), the interpretation of the principle of state sovereignty and its application to state conduct in cyberspace have not been addressed in great detail.

One of the questions left open by the GGE reports is whether cyber operations which do not constitute a use of force or intervention into internal affairs of another state are nevertheless prohibited by virtue of a duty to respect the sovereignty of states, or whether the absence of a specific prohibitive rule leaves states free to conduct cyber operations within and against cyber infrastructure located on the territory of other states (provided they do not rise to the level of force or intervene into internal affairs). It is, therefore, no surprise that the question whether international law recognizes a general rule of territorial sovereignty, operating below the threshold of use of force and intervention is currently one of the most contentious issues in international law, in light of the fact that such a rule may be violated through state-conducted or state-sponsored cyber operations. Moreover, it remains unclear if this rule is recognized, then how to precisely define its scope. Maybe the most prominent academic effort to comprehensively map and describe the rules applicable to state conduct in cyberspace is the *Tallinn Manual*. Now in its second edition, the *Manual* states in Rule 4 that "[a] State must not conduct cyber operations that violate the sovereignty of another State" (Schmitt and Vihul 2017c, 17). In ascertaining when such a violation of sovereignty may occur, the *Tallinn Manual 2.0* employs an effects-based test which focuses on two bases: the degree of infringement upon the state's territorial integrity and the interference with, or usurpation of, inherently governmental functions (Schmitt and Vihul 2017c, 20). Under this test, cyber operations which violate the integrity of ICT systems in another state by installing malware containing malicious payloads are not prohibited *per se*, unless they lead to the loss of functionality of the target system. In effect, a majority of the *Manual*'s authors does not regard the act of installing and sustaining malicious code in foreign ICT systems as a violation of international law.

This chapter critically examines the *Tallinn Manual*'s Rule 4 and argues that a purely effects-based approach to violations of territorial sovereignty is at odds with the traditional understanding of sovereignty as espoused by the Permanent Court of International Justice (PCIJ) and the International Court of Justice (ICJ). If we understand sovereignty as the exclusive right of states to regulate entry into their territory and the right to forbid any assertion of

jurisdiction or the performance of acts *de iure imperii* within their territory by another state without their consent, then any unauthorized presence and any act of foreign state power violates sovereignty, regardless of whether these actions cause physical harm or not. Therefore, the chapter argues for a different, intrusion-based approach to violations of territorial sovereignty in cyberspace. Under the proposed intrusion-based test, the violation of a state's territorial sovereignty is linked to the breach of the information security—especially the integrity—of the targeted ICT system. This allows for a more technical and precise determination of the boundary between permissible and impermissible acts in cyberspace and would help to reduce the legal uncertainties which currently exist in relation to low-intensity cyber operations.

This chapter proceeds in three steps. First, it discusses the traditional concept of sovereignty and addresses the question whether sovereignty is a principle of international law from which more concrete rules of state behavior—such as the prohibition on the use of force and the prohibition of intervention into internal affairs of other states—derive; or whether it is itself a rule of international law, prohibiting conduct which violates the territorial sovereignty of states. While this question has already been addressed in many publications (see, e.g., Eichensehr 2015; Heintschel von Heinegg 2012, 2013; Pirker 2013; Schmitt and Vihul 2017a, 2017b, 2017c), a recent speech by the United Kingdom attorney general, Jeremy Wright QC MP, in which he firmly spoke against the existence of such a rule of territorial sovereignty (Wright 2018), warrants a further look at this issue. Second, it addresses the *Tallinn Manual 2.0* Rule 4 and its interpretation of the rule of territorial sovereignty, with special regard to the tests proposed by the authors of the *Tallinn Manual* to ascertain when a violation of territorial sovereignty takes place. Last, it proposes a different, intrusion-based test of the violation of territorial sovereignty.

THE CONCEPT OF TERRITORIAL SOVEREIGNTY IN CYBERSPACE

Rule 4 of the *Tallinn Manual 2.0* states that "[a] State must not conduct cyber operations that violate the sovereignty of another State" (Schmitt and Vihul 2017c, 17). It is based on the assumption that the international legal order contains, apart from the prohibition on the use of force and the prohibition of intervention into the internal affairs of other states, a separate norm requiring respect for the (territorial) sovereignty of other states, which may be violated through the performance of certain cyber activities within other states' territories without their consent. However, the existence of such a rule has recently been put into question—at least with respect to activities in cyberspace. In his

Chatham House speech of May 23, 2018, the attorney general of the United Kingdom, Jeremy Wright QC MP, has stated that he is "not persuaded that we can currently extrapolate from [the] general principle [of sovereignty] 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" (Wright 2018). The United Kingdom has been the first state to officially articulate its doubts as to the existence of a rule of territorial sovereignty in such clear terms, but this position seems to reflect earlier arguments brought forth by (at least) some branches of the US government. The then legal adviser to the US Department of State, Brian Egan, noted that "cyber operations involving computers located on another State's territory do not constitute a violation of international law. (. . .) This is perhaps most clear where such activities in another State's territory have no effects or de minimis effects" (Egan 2016). Furthermore, as has been reported by some authors (Watts and Richard 2018, 859; Schmitt and Vihul 2017a, 1641), on January 19, 2017, the outgoing general counsel of the US Department of Defence has issued a memorandum on the "International Law Framework for Employing Cyber Capabilities in Military Operations." The memo—which is not publicly available and whose content the present author can therefore only assess through secondary sources—reportedly stated that sovereignty is not a rule but a "baseline principle" which undergirds other binding rules of international law such as the prohibition on the use of force and the prohibition of intervention (Schmitt and Vihul 2017a, 1642). The 2017 DoD memo's position seems to be shared by some American authors, including authors which at the time of writing are working for US Cyber Command (Corn and Taylor 2017; Corn and Jensen 2018).

Two Arguments Against Territorial Sovereignty in Cyberspace

The case against the existence of a rule of territorial sovereignty can be summarized as resting on two arguments. First, in what may be called the argument from lack of state practice, it is stated that there is not sufficient state practice and *opinio iuris* to conclude the existence of such a rule in customary international law (Wright 2018; Corn and Jensen 2018). Second, in what may be termed the argument from cyberspace design and practicality, it is held that while sovereignty has always been tightly tied to territory, the logical and social layers of cyberspace have "at most a tenuous connection to geography" (Corn and Jensen 2018) and thus territorial concepts are not readily transposable to an aterritorial medium by way of simple analogy. Moreover, the global reach and availability of cyber infrastructure makes it possible for malicious cyber operations to be mounted from a multitude of globally

dispersed locations (Corn and Jensen 2018). States wishing to protect their cyber infrastructure from such threats, therefore, need to be able to counter cyberattacks regardless of their starting location. The sovereignty-as-a-rule approach would create "unworkable hurdles to States conducting such limited but potentially important operations" (Corn 2017).

According to the lack-of-state-practice argument, sovereignty is a baseline principle of international law, from which other, more concrete prohibitive rules of international law flow. These rules, such as the prohibition on the use of force and the prohibition of intervention, exist as customary international law, because they are evidenced by a sufficiently uniform and universal practice and *opinio iuris* of states, and/or have been codified in the United Nations Charter. Below the threshold of these two rules, "international law does not obligate other states to refrain from all activities that might infringe upon or operate to the prejudice of the territorial state's internal sovereignty" (Corn and Taylor 2017, 209). Evidence of this is to be seen in the fact that states conduct espionage operations within the territory of other states, yet international law does not prohibit espionage as such (Corn and Taylor 2017, 209). Moreover, one cannot find evidence of one single universal rule of territorial sovereignty, as the content of rights in relation to a particular territory varies depending on which domain (land, sea, air, space) is affected. While access to airspace is severely restricted, and entry without consent is a serious violation of international law which may lead to grave consequences (as has most recently been evidenced by the shoot down of a Russian fighter jet by the Turkish army for violating Turkish airspace), international law allows the innocent passage of warships through the territorial sea of states and in the case of space, orbiting objects do not violate the airspace or territory states they overfly (Corn and Taylor 2017, 210). In consequence, given that no separate regime of restricted access to a state's cyberspace domain (below the thresholds of use of force and intervention) has yet developed, states are free to act as they wish by virtue of their sovereignty, as has been found by the PCIJ in the *Lotus* case (*S.S. Lotus* [*Fr. v. Turk.*], 1927 P.C.I.J. Rep. [ser. A] No. 10, at 18).

In the author's view, both arguments are to be rejected. They disregard long-standing jurisprudence of the PCIJ and ICJ, do not take account of more recent state practice, and are based on a false understanding of the so-called *Lotus* doctrine whereby states have unlimited freedom of action barring a prohibitive rule of international law.

International Jurisprudence Supports the Existence of a Rule of Territorial Sovereignty

The essence of state sovereignty is perhaps best captured in a passage from Judge Max Huber's arbitral decision in the *Island of Palmas* case. The

arbitrator stated that "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State" (*Island of Palmas* [*Neth. v. U.S.*], P.C.A. 1928, 2 R.I.A.A 829, 838). Traditionally, this independence is understood to contain an internal as well as an external aspect (Besson 2011; Tsagourias 2015, 17). While internal sovereignty means the supreme authority within the state to regulate political, social, and legal affairs and enforce rules, external sovereignty pertains to the rights and duties of states toward each other and denotes the competence of states to engage in activities outside of their territory, subject only to binding rules of international law (Crawford 2015, 118). From this internal sovereignty arises the authority to determine *inter alia* who may enter the territory. This is exclusive in the sense that "governmental authority carried out on the territory of another state is only lawful if performed with the latter's consent" (Crawford 2015, 121). The supreme authority of a state vis-à-vis other states within its territory thus gives rise to a fundamental "restriction imposed by international law upon a State (. . .) 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 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" (*S.S. Lotus* [*Fr. v. Turk.*], Judgement, 1927 P.C.I.J. Ser. A No. 10, p. 4, 18–19). This dictum of the PCIJ has been upheld after the entry into force of the UN Charter by the ICJ. In the *Corfu Channel* case, the Court had to decide whether a demining operation conducted by the United Kingdom in Albanian territorial waters violated Albanian sovereignty even if it was a necessary self-help measure. The court held that "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations. The Court recognizes that the Albanian Government's complete failure to carry out its duties after the explosions (. . .) are extenuating circumstances for the action of the United Kingdom Government. But to ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty" (*Corfu Channel* [*U.K. v. Alb.*], Judgment, 1949 I.C.J. Rep. 4, 35). Furthermore, in *Nicaragua*, the court clarified the relation between the requirement of respect for territorial sovereignty and the *lex specialis* prohibition on the use of force. It held that "[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 non-intervention. Thus the assistance to the contras (. . .) not only amount to an unlawful use of force, but also constitute infringements of the territorial sovereignty of Nicaragua, and incursions into its territorial and internal waters" (*Military and Paramilitary Activities in and Against Nicaragua*

[*Nicar. v. U.S.*], Judgment, 1986 I.C.J. Rep. 14, para. 251). What becomes clear from this brief overview is, therefore, that sovereignty is not only a principle, from which other more specific rules are derived, but that sovereignty demands respect for the supreme authority of a state within its territory and as such forms itself a prohibitive rule of international law. Territorial sovereignty is, therefore, a "baseline rule" derived from general international law (Watts and Richard 2018, 859), which reflects the structural framework of international law for the exercise of state sovereignty in order "to ensure the co-existence of independent communities and facilitate the achievement of common aims" (Hertogen 2015, 912). As Judge Shahabuddeen has noted in his dissent in the *Nuclear Weapons* advisory opinion: "It is difficult (. . .) to uphold a proposition that, absent a prohibition, a State has a right in law to act in ways which could deprive the sovereignty of all other States of meaning" (*Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, Dissenting Opinion of Judge Shahabuddeen, 1996 I.C.J. Rep. 226, 393–394).

State Practice Is Not Uniform

With regard to state practice, it is certainly true that so far only a small number of states have publicly presented their understanding of the application of sovereignty to cyberspace. Declarations such as the speech given by the UK attorney general help to identify and clarify the content of international norms applicable to cyberspace and may, in time, be of sufficient number and uniformity to restrict the application of a rule of territorial sovereignty to cyberspace along the lines advocated by Attorney General Wright and some American authors (Schmitt 2018, 18). However, in the author's view, the current state practice on this topic is not uniform and may even point to a majority position contrary to the attorney general's. For instance, in a speech held at Chatham House London on May 18, 2015, the then commissioner for International Cyber Policy of the German Foreign Office, Ambassador Norbert Riedel, stated that "There is consensus that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of activities related to information and communication technology, and to their jurisdiction over the required infrastructure within their territory." While cyberattacks which amount to a use of force or even an armed attack are prohibited by the UN Charter and customary international law, "[e]ven in cases where one cannot speak of a use of force, the use of cyber capabilities might constitute a violation of sovereignty, if the attack can be attributed to a state" (Riedel 2015). The argument that territorial sovereignty applies in cyberspace is even more forcefully put forward by France. The French "Strategic Review of Cyberdefence" (*Revue stratégique de cyberéfense*) of February 12, 2018 offers the view that cyber incidents of a significant,

but not extreme, impact fall below the threshold of armed attack, but may nevertheless constitute other internationally wrongful acts such as intervention, violation of sovereignty or use of force ("*les actions correspondant à ces niveaux pourraient néanmoins constituer d'autres faits internationaux illicites* [*intervention, violation de la souveraineté, usage de la force, etc.*])" (Secrétariat général de la défense et de la sécurité nationale 2018, 80). This view is elaborated upon in the declaration on "International Law Applicable to Operations in Cyberspace" (*Droit international appliqué aux opérations dans le cyberespace"*), published by the Ministry of Defence on 9 September 2019. The document argues that since France has sovereignty over ICT systems located within its territory, any cyberattack—defined as an operation which breaches the confidentiality, integrity, or availability of the targeted system—constitutes at minimum a violation of sovereignty, if attributable to another state. Such a violation occurs not only when effects are produced on French territory, but already when there is a penetration of French computer systems (Ministère des Armées 2019, 6–7).

Similarly, the GGE consensus reports clearly conclude that states have jurisdiction over ICT infrastructure located within their territory (United Nations General Assembly 2015, akap. 28[a]). States regularly assert jurisdiction, both civil and criminal, over activities within their cyber infrastructure. For example, on July 13, 2018, the US Special Counsel filed an indictment of twelve Russian intelligence officers alleged to have hacked the servers of the Democratic National Committee and thus to have committed computer-related offenses within the United States (*United States vs. Netyksho et al.*, US District Court for the District of Columbia, Case No. 1:18-cr-00215-ABJ, filed July 13, 2018). It is thus clear that states treat activities within their cyber infrastructure as falling into the territorial confines of their sovereignty (some states even speak of "national cyberspace," e.g., the Polish cybersecurity strategy "*Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej*" [Ministerstwo Administracji i Cyfryzacji 2013]), even though some states may deny the existence of a rule of territorial sovereignty. In the author's view, it follows from sovereignty over ICT devices that sovereign activities conducted within the cyber infrastructure located on the territory of other states violate their territorial sovereignty if they constitute an exercise of power without the consent of the affected state.

In summary, it may very well be that the rule of territorial sovereignty in cyberspace will have to adapt for the (perceived) aterritoriality of the logical and social layers of cyberspace, the loss of distance typical for geographical territory and the ease of access this structural characteristic of cyberspace presents to malicious cyber actors. The practical necessity of defending against threats originating from multiple locations and using cyber infrastructure located in various states, coupled with the currently slow process of

international legal assistance and the disinterest or inability of many states to actively counter malicious activity emanating from their cyber infrastructure, may require an adjustment of the international legal regime to allow for a greater degree of self-help (although, as the *Tallinn Manual* points out, legal remedies in the form of countermeasures and the doctrine of necessity are available [Schmitt and Vihul 2017c, 111–141]). But, as the law currently stands, the baseline rule of territorial sovereignty, as recognized by the ICJ in *Corfu Channel* and *Nicaragua*, still applies. States arguing for its nonexistence would have to demonstrate on the basis of universal state practice and *opinio iuris* the emergence of an exception to territorial sovereignty in cyberspace, not the other way around.

VIOLATIONS OF TERRITORIAL SOVEREIGNTY UNDER THE *TALLINN MANUAL 2.0* RULE 4

Assuming that territorial sovereignty exists as a rule of international law and further assuming that this rule is applicable to state conduct in cyberspace, the next question is to ascertain the precise content of this rule. So far, the most elaborate attempt to formulate a test for the violation of territorial sovereignty in cyberspace has been offered by the authors of the *Tallinn Manual 2.0* in Rule 4 (Schmitt and Vihul 2017c, 17). The *Tallinn Manual 2.0* stipulates that the lawfulness of remote cyber operations that manifest on a state's territory depend on the "degree of infringement upon the target State's territorial integrity" and/or on the "interference with or usurpation of inherently governmental functions" (Schmitt and Vihul 2017c, 20). With regard to the infringement upon territorial integrity, the *Manual's* authors stipulate that cyber operations, which result in physical damage, show a sufficient degree of infringement to constitute a violation of territorial sovereignty. Furthermore, the experts argue that a loss of functionality of the targeted system may constitute a violation of sovereignty, if it reaches a certain threshold. The precise threshold could not be established, but the experts agreed that cyber operations resulting in the requirement to replace and repair computer systems or their components are sufficiently akin to physical damage to constitute a violation of sovereignty (Schmitt and Vihul 2017c, 21). There was no consensus among the experts as to whether cyber operations falling below the threshold of loss of functionality violate territorial sovereignty; therefore, the *Tallinn Manual 2.0* does not take a position on this issue.

The *Tallinn Manual's* approach to territorial sovereignty is thus largely effects-based. The *Tallinn Manual* itself does not explain how the authors arrived at the abovementioned set of factors to determine the existence of a violation of sovereignty. It appears that these factors are derived from a

particular interpretation of the object and purpose of sovereignty: since the physical damage of targeted computer systems and the loss of functionality requiring repair and replacement lead to similar effects as unconsented physical presence, they, therefore, infringe sovereignty, which "clearly protects territorial integrity against physical violation" (Schmitt and Vihul 2017c, 20). Furthermore, the *Manual* takes into account the traditional aspect of sovereignty of regulating access to territory (*c.f. Vilvarajah and others v UK,* ECtHR, Ser. A, 215, October 30, 1991) and concludes that territorial sovereignty is violated if a state conducts cyber operations when its agents are physically present in the target state (Schmitt and Vihul 2017c, 19). Virtual presence through remote-access cyber operations, on the other hand, seems not to be sufficient to violate territorial sovereignty.

In the author's view, this approach overemphasizes physical effects on territory, while omitting a crucial aspect of sovereignty, namely the exercise of state power. Moreover, the emphasis on the physical effects of a cyber operation does not sufficiently take into account the technical side of most cyber operations, thus leading to difficulties in the precise determination when a violation of territorial sovereignty occurs or is ongoing.

Regarding the first point, the *Tallinn Manual 2.0* seems to consider the main object and purpose of sovereignty to be "the protection of territorial integrity against physical violation" (Schmitt and Vihul 2017c, 20). However, as discussed above, the regulation of access to territory is but one of the aspects of internal sovereignty. Furthermore, the main aim of this exclusive right of the state is not to protect its territory from physical effects—after all, unconsented overflights or transboundary abductions, which are regarded as violations of territorial sovereignty (Wilske 2012), do not usually cause damage or lasting physical effects on the territory of the affected state. Rather, the object and purpose of the rule of territorial sovereignty is to be seen in the protection of the exclusivity of state authority within its territory. As held by the PCIJ in the *S.S.Lotus*: "failing the existence of a permissive rule to the contrary [a State] may not exercise its power in any form in the territory of another State" (*S.S. Lotus* [*Fr. v. Turk.*], Judgement, 1927 P.C.I.J. Ser. A No. 10, pp. 4, 18–19). While in a globalized world, and especially in cyberspace, actions undertaken by one state may very well have a substantial effect on the (cyber) territory of other states, this effect has to be tolerated by virtue of the principle of sovereign equality only insofar as it is a consequence of the exercise of the acting state's internal sovereignty. Conversely, the exercise of state power within the territory of another state violates the target state's exclusive authority and thus its territorial sovereignty. Admittedly, one has to be careful with territorial analogies with regard to cyberspace, as the medium has different characteristics. Nevertheless, every action taken through cyberspace manifests itself on cyber infrastructure located within a specific

territory. As the UN GGE noted in its two reports, states have jurisdiction over the ICT infrastructure located within their territory (United Nations General Assembly 2015, akap. 28[a]) and they do assert their jurisdiction over actions performed by individuals as well as agents of other states. 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. Thereby they actively change the functioning of computer systems within the sphere of authority of another state and thus exercise a power which, by virtue of the principle of sovereignty, should remain exclusively with that state.

Secondly, if the violation of territorial integrity depended on the manifestation of physical effects, states would not have a legal remedy against cyber operations which are in their preparatory stages or ongoing. Looking at the technical side of cyber operations, one sees that conducting offensive cyber operations requires several preparatory steps: identifying a target, choosing the appropriate attack vector, bypassing the security of the attacked computer system and finally conducting the intended activity. There are many analytical models describing the various steps of a cyberoperation and its effects (Smeets 2017, 30; CCHS 2016, 5; Ducheine 2015, 230), but one of the most common models—the so-called Cyber Kill Chain, developed by employees of the Lockheed Martin Corporation—divides cyber operations into seven phases: Reconnnaisance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Action on objective (Hutchins, Cloppert and Amin 2011, 5). During the reconnaissance phase, the attacker identifies and selects potential targets. Information about the target can be collected from many sources: from open-source intelligence through secret intelligence sources, to the scanning of computer systems (for a detailed description see Maybaum 2013, 217–219). After identifying the proper target and its vulnerabilities, the attackers can gain access to the targeted system (delivery and exploitation phases). This can happen remotely (in so-called remote-access cyber operations, e.g., by sending an infected message to the victim's mailbox) or directly (in so-called close-access cyber operations, e.g., by installing malicious software directly on the target system by the agent, vendor) (Owens and ors. 2009, 87). Most often, malicious code installed after gaining access does not yet contain the proper harmful payload but is used for self-replication and "raising the drawbridge" through which the system will be accessed and further payloads will be installed. In many cases, the installed code is a so-called Remote Access Tool (RAT), which makes contact with the command and control server and waits for further commands from the attackers (Maybaum 2013, 122).

The activities described above are preparatory phases of a cyber operation. The further course depends on the intentions and decisions of the attacker. If the purpose of the operation is to obtain confidential information, the payload will contain code for searching information, tracking the user's computer communication, activating the camera and microphone, and so on. If the purpose is to destroy data or impact on machines and processes controlled by a given computer system, the payload will contain appropriate mechanisms. To this end, many RATs allow the installation of additional modules, depending on the operator's current needs. It should be noted that the nature of a cyber operation is not obvious at the time the information security of the infected system is first compromised. It is only the content of the payload that determines whether it is intended for espionage or for specific damage. In the case of most cyber operations, the determination of their character is possible only after technical analysis of the payload, which requires technical expertise, adequate resources and time (the technical analysis of *Stuxnet* took several months after its initial discovery [Falliere, Murchu, and Chien 2011]). Nevertheless, the initial illegal access to the targeted computer system, irrespective of the subsequent actions, already constitutes a criminal offense against the confidentiality, integrity, and availability of computer data and systems under the domestic law of many states, as required by Art. 2 of the 2001 Cybercrime Convention (Convention on Cybercrime, Budapest, 23.11.2001, E.T.S. No. 185).

The outline of a typical cyber operation above is obviously very simplified. However, three conclusions can be drawn: first, actors conducting cyber operations use previously identified vulnerabilities to gain access to computer systems without authorization, thus breaching the information security of the targeted systems. Second, the unauthorized intrusion into computer systems constitutes a breach of their information security and thereby a criminal offense. Third, the intended effect of a cyber operation is ascertainable either after the prior detection and technical analysis of the payload, or after the activation of the payload and the materialization of its effects. If the violation of territorial sovereignty were to depend exclusively on the physical effects of a cyber operation (either through physical damage or a significant loss of functionality), the intrusion into a computer system and the compromising of its information security would not yet constitute a violation of sovereignty (although in most cases it would already constitute a criminal offense under the domestic law of the targeted state). Under the so-called *Lotus* doctrine, which presumes a state's freedom of action unless a prohibitive norm has been created through state consent (Kwiecień 2012, 48), this freedom to act would in effect create a freedom to install malware on foreign computer systems. Although the targeted state would still be free to sanction violations of information security under its domestic law, it would be powerless to

prevent this under international law, as countermeasures and the obligation of cessation depend on the existence of an internationally wrongful act (United Nations International Law Commission 2001). In consequence, the international legal order would be put in a situation where, based on its external sovereignty, a state would be free to exercise its power through cyber operations, affecting the information security of computer infrastructure in other states, and to allow its agents to commit criminal offenses, while the targeted states would have no legal redress to enforce the exclusivity of their authority within their territory. To quote Judge Shahabuddeen again: "It is difficult (. . .) to uphold a proposition that, absent a prohibition, a State has a right in law to act in ways which could deprive the sovereignty of all other States of meaning" (*Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, Dissenting Opinion of Judge Shahabuddeen, 1996 I.C.J. Rep. 226, 393–394).

AN INTRUSION-BASED APPROACH TO VIOLATIONS OF TERRITORIAL SOVEREIGNTY

Given this unsatisfactory state of events, what could an alternative approach to violations of territorial sovereignty look like? The author proposes to start from what the rule of territorial sovereignty seeks to prohibit: the unauthorized exercise of state power in the territory of another state, as exemplified in the *Lotus* judgment (*S.S. Lotus* [*Fr. v. Turk.*], Judgement, 1927 P.C.I.J. Ser. A No. 10, pp. 4, 18–19). It is clear from this and other judgments such as *Corfu Channel*, as well as state practice, that the exercise of state power is not measured by the effects of one state's actions on the territory of another state, but rather by the nature of the action itself. Any activity of a sovereign (i.e., noncommercial) nature taken within or against another state's territory without that state's consent or a legal basis in international law constitutes an unauthorized exercise of state power and thus a violation of territorial sovereignty. This is why United Kingdom's demining operation in Albanian territorial waters (see *Corfu Channel* [*U.K. v. Alb.*], Judgment, 1949 I.C.J. Rep. 4, 35), the US training and financing of Contra rebels in Nicaragua (*Military and Paramilitary Activities in and Against Nicaragua* [*Nicar. v. U.S.*], Judgment, 1986 I.C.J. Rep. 14, para. 251) or the abduction of a person from the territory of a state by the agents of another state (Ghafur Hamid 2004, 79) constitute such violations.

It is furthermore clear that while cyberspace undoubtedly has other properties than physical space, it is by no means aterritorial, as has been claimed in the 1990s (Johnson and Post 1996). It is true that data mobility and interconnectedness pose a challenge to strictly territorial notions of jurisdiction

requiring a reconceptualization or a new approach (Daskal 2015; Roguski 2019), but this challenge does not invalidate the strict link between geography and sovereignty in cyberspace (but compare Corn and Jensen 2018). This is because actions taken against specific computers or networks, even if undertaken remotely, ultimately manifest themselves in the territory of the state where the physical infrastructure is located. For this reason, states continue to assert jurisdiction over the physical components of cyberspace (United Nations General Assembly 2015) and apply their national (criminal) law to actions taken against these components, irrespective of the location of the perpetrators (U.S. District Court, ND California, *U.S. v. Dmitry Dokuchaev, et al*., Case 3:17-cr-00103-VC).

Established notions of international law and current state practice, therefore, suggest that states can (and do) assert exclusive authority over computers and networks physically located within their territory and, in consequence, any exercise of power by other states in those networks, irrespective of its physical effects, would violate the territorial integrity of that state. What, then, should be the test for establishing the exercise of state power through cyberspace within the territory of another state? Rather than to focus on the physical effects of cyber operations, the present author proposes to focus instead on the technical aspects of a cyber operation. As has been shown above, the essence of every cyber operation is the act of "hacking," or—to use a definition well established in the technical (and legal) community, the breach of the information security of a computer system through an action compromising either the confidentiality, integrity, or availability of the information stored in the computer system (Kosseff 2018). This so-called CIA Triad, although not a legal definition, is well established in the realm of cybersecurity and is used by some states—Germany and Austria, for example—to define a cyberattack in their national cyber strategies (Bundeskanzleramt Österreich 2013, Bundesministerium des Inneren 2016). Moreover, under the Cybercrime Convention (Convention on Cybercrime, 23.11.2001, E.T.S. No. 185) states parties are obliged to penalize offenses against the confidentiality, integrity, and availability of computer data and systems (Convention on Cybercrime Articles 2–8). In particular, the Cybercrime Convention obliges states parties to criminalize illegal access to computer systems, data and system interference, computer-related fraud and so on. Most states parties have implemented these provisions into their national law or have similar provisions. The United States, for instance, have penalized computer crime, including computer intrusions, denial-of-service attacks, and viruses (Doyle 2014; US Department of Justice—Computer Crime and Intellectual Property Section 2010) through the Computer Fraud and Abuse Act (codified in 18 U.S. Code 1030).

Since computer crimes and state cyberattacks share the same technical characteristics and the forensic analysis of both types of attacks is the same—the difference lying only in the attribution of the action constituting a computer crime to a state actor, thus subjecting it to international rather than (only) national law—the present author proposes to use the criterion of computer intrusion or interference to assess the moment state power is exercised in the territory (cyber infrastructure) of another state. This means that whenever a foreign state damages, deletes, deteriorates, alters, or suppresses data stored on a computer system within the territory of another state (compare Art. 4 Cybercrime Convention), this action would be regarded as an exercise of state power and thus a violation of the territorial sovereignty of the targeted state.

The criterion of "intrusion," closely related to the integrity of data stored on a computer system, does not encompass every action of a state in foreign networks. For instance, intrusion does not mean the regular use of cyberspace infrastructure for their intended purposes, as no damage to or alteration of data is being done in this process. This is true even for actions undertaken with malicious intent, such as port scanning for the purposes of reconnaissance and preparation of a cyberattack in the future. Since the scanning of ports is possible without interference with data stored in a network due to the technical design and functioning of global networks such as the Internet and states allow the use of their ICT infrastructure for the purposes of information transfer, regular usage, even including the routing of cyber operations through foreign infrastructure, would therefore not violate territorial sovereignty. Similarly, even gaining access to a computer network without proper authorization (i.e., breaching the confidentiality of a computer system or network, for instance through phishing) would not constitute an intrusion under the proposed test as the integrity of data stored within the system would not be compromised. The present author submits that the focus on the integrity (rather than its confidentiality or availability) of a computer system or data stored therein is justified, as it is the interference with the functioning of a computer system in the territory of another state—for example, the deletion or alteration of data, the implantation of malware, remote access tools, the use of the computer system to cause effects on systems or processes controlled by that computer.—which bears the closest resemblance to the exercise of state power in the traditional sense.

The proposed intrusion-based approach would have several advantages over the no-sovereignty approach advocated by the UK attorney general (Wright 2018) or the effects-based approach proposed by the *Tallinn Manual 2.0* (Schmitt and Vihul 2017c). First, with respect to the sovereignty-as-a-principle view, it respects established international jurisprudence and international law, which is, in the view of the present author, unequivocal

in this point. Secondly, with respect to the *Tallinn Manual 2.0* approach, focusing on a technical, rather than an effects-based criterion, has the advantage of forensic clarity and predictability, thus enhancing legal certainty. Whereas a successful hacking operation may not produce any physical effects at all or these effects may not manifest for some time, under the intrusion-based approach it is the hacking itself which constitutes the violation of sovereignty. The affected state would thus not have to wait for physical effects to emerge—or to be severe enough—to be legally entitled to enact countermeasures. Thirdly, the close resemblance of the intrusion criterion to the legal framework regulating computer crimes would allow states to rely on technical expertise and procedures established by law enforcement. In other words—the terrain would be more familiar. And lastly, treating computer intrusions as violations of sovereignty would truly establish territorial sovereignty as the "baseline" norm (Watts and Richard 2018) in cyberspace, thus creating a predictable framework of primary norms and norms-imposing consequences for their breach (such as countermeasures) and could therefore enhance the stability of cyberspace through clear legal principles.

The approach proposed in this chapter has recently gained prominent support in the form of the French declaration on "International Law Applicable to Operations in Cyberspace," which has been published after the submission date of this article and thus can only be briefly referred to. In this document, France argues that a violation of sovereignty may already exist when there is a penetration of computer systems under the sovereignty of France (Ministère des Armées 2019, 6–7). Given that a penetration occurs when there is a breach of the information security, that is, the confidentiality, integrity, or availability, of the targeted system, it is similar to the criterion of intrusion proposed in this article.

CONCLUSION

This chapter argued that territorial sovereignty, which as a primary norm of international law is also applicable to state conduct in cyberspace, requires a clear and operable criterion in order to provide a clear and predictable framework for states to operate in. Rather than concentrating on the physical effects of cyber operations, it is proposed that an intrusion-based approach, which concentrates on the technical side of cyber operations, would provide a familiar, less ambiguous and more viable tool for assessing violations of sovereignty in cyberspace. The criterion of intrusion conforms to the essence of territorial sovereignty, which is the regulation of access to territory and the preservation of exclusivity of state power within its territory. It

is independent of the intent of the attacking state and the consequences of its actions and relies on a verifiable technical criterion to ascertain whether a violation of territorial sovereignty has taken place. Furthermore, if the internationally wrongful act of violating the territorial sovereignty of a state in cyberspace were to depend on the intrusion into the targeted computer system, rather than on the effects of that intrusion, the targeted state would have legal redress in the form of a right to demand cessation and to institute countermeasures before the harmful effects of the cyber operation materialize, rather than after. In conclusion, an intrusion-based approach to territorial sovereignty would more clearly reflect the object and purpose of sovereignty, allow states to counter malicious activities before their effects are manifested and would more clearly correspond to the technical side of cyber operations. Although the interpretation of international law in cyberspace has solidified with respect to many norms, for example, the use of force, only a fraction of states has thus far set out their views on the application of territorial sovereignty in cyberspace. New ideas can—and should—be explored and discussed. The new Group of Governmental Experts as well as the Open-Ended Working Group, which have been established in 2019 to further explore the interpretation and application of international law in cyberspace, would be good fora for such discussions.

BIBLIOGRAPHY

Besson, Samantha. 2011. "Sovereignty." In *Max Planck Encyclopaedia of Public International Law*, edited by Rüdiger Wolfrum. Oxford, NY: Oxford University Press.

Bundeskanzleramt Österreich. 2013. "Österreichische Strategie für Cyber-Sicherheit." http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50748.

Bundesministerium des Inneren. 2016. "Cyber-Sicherheitsstrategie für Deutschland." https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

CCHS. 2016. "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats." *Center for Cyber & Homeland Security*, 86. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Corn, Gary P. 2017. "Tallinn Manual 2.0—Advancing the Conversation." *Just Security*. https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

Corn, Gary P., and Eric Jensen. 2018. "The Technicolor Zone of Cyberspace—Part II." *Just Security*. https://www.justsecurity.org/57545/technicolor-zone-cyberspace-part-2/.

Corn, Gary P., and Robert Taylor. 2017. "Sovereignty in the Age of Cyber." *AJIL Unbound* 111: 207–212. https://doi.org/10.1017/aju.2017.57.

Crawford, James. 2015. "Sovereignty as a Legal Value." In *The Cambridge Companion to International Law*, edited by James Crawford i Martti Koskenniemi, 117–133. Cambridge: Cambridge University Press. https://doi.org/10.1017/CCO9781139035651.009.

Daskal, Jennifer. 2015. "The Un-Territoriality of Data." *Yale Law Journal* 125 (2): 326–398.

Doyle, Charles. 2014. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Washington, DC: Congressional Research Service.

Ducheine, Paul. 2015. "The Notion of Cyber Operations." In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan, 211–232. Cheltenham: Edward Elgar Publishing.

Egan, Brian. 2016. "Remarks on International Law and Stability in Cyberspace." https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

Eichensehr, Kristen E. 2015. "The Cyber-Law of Nations." *Georgetown Law Journal* 103 (2): 317–380. https://doi.org/10.1525/sp.2007.54.1.23.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32.Stuxnet Dossier." *Symantec-Security Response*. https://doi.org/20 September 2015.

Ghafur Hamid, Abdul. 2004. "Jurisdiction Over a Person Abducted from a Foreign Country: Alvarez Machain Case Revisited." *Journal of Malaysian and Comparative Law* 31: 69–86.

Heintschel von Heinegg, Wolff. 2012. "Legal Implications of Territorial Sovereignty in Cyberspace." In *4th International Conference on Cyber Conflict*, edited by Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 7–19. Tallinn: NATO CCD COE Publications.

Heintschel von Heinegg, Wolff. 2013. "Territorial Sovereignty and Neutrality in Cyberspace." *U.S. Naval War College International Law Studies* 89: 123–156.

Hertogen, An. 2015. "Letting Lotus Bloom." *European Journal of International Law* 26 (4): 901–926.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. 2011. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." In *6th Annual International Conference on Information Warfare and Security*, 1–14. http://papers.rohanamin.com/wp-content/uploads/papers.rohanamin.com/2011/08/iciw2011.pdf%5Cnhttp://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

Johnson, David R., and David Post. 1996. "Law and Borders—The Rise of Law in Cyberspace." *Stanford Law Review* 48 (5): 1367–1402.

Koh, Harold Hongju. 2012. "International Law in Cyberspace." *Harvard International Law Journal* 54: 1–9.

Kosseff, Jeff. 2018. "Defining Cybersecurity Law." *Iowa Law Review* 103: 985–1031.

Kwiecień, Roman. 2012. "Does the State Still Matter? Sovereignty, Legitimacy and International Law." *Polish Yearbook of International Law* XXXII: 45–74.

Maybaum, Markus. 2013. "Technical Methods, Techniques, Tools and Effects of Cyber Operations." In *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, 103–134. Tallinn: NATO CCD COE Publications.

Ministère des Armées. 2019. "Droit International appliqué aux opérations dans le cyberespace." https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf.

Owens, William A., Kenneth W. Dam, Herbert S. Lin, and National Research Council. 2009. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. The National Academies Press.

Pirker, Benedikt. 2013. "Territorial Sovereignty and Integrity and the Challenges of Cyberspace." In *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, 189–216. Tallinn: NATO CCD COE Publications.

Riedel, Norbert. 2015. "'Cyber Security as a Dimension of Security Policy.' Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London." London. https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

Roguski, Przemysław. 2019. "Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment." In *11th International Conference on Cyber Conflict: Silent Battle*, edited by Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky, 1–13. Tallinn: NATO CCD COE Publications. https://doi.org/10.23919/cycon.2019.8756900.

Schmitt, Michael N. 2018. "International Cyber Norms: Reflections on the Path Ahead." *Militair Rechtelijk Tijdschrift* 111 (3 Cyber Special): 12–20.

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

Schmitt, Michael N., and Liis Vihul. 2017a. "Respect for Sovereignty in Cyberspace." *Texas Law Review* 95: 1639–1670.

Schmitt, Michael N., and Liis Vihul. 2017b. "Sovereignty in Cyberspace: Lex Lata Vel Non?" *AJIL Unbound* 111: 213–218.

Secrétariat général de la défense et de la sécurité nationale. 2018. "Revue stratégique de cyberdéfense." http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

Smeets, Max. 2017. "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks." In *9th International Conference on Cyber Conflict: Defending the Core*, edited by Henry Roigas, R. Jakschis, L. Lindström, i T. Minárik, 25–42. Tallinn.

Tsagourias, Nicholas. 2015. "The Legal Status of Cyberspace." In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias i Russell Buchan, 13–29. Cheltenham: Edward Elgar Publishing.

U.S. Department of Justice—Computer Crime and Intellectual Property Section. 2010. "Prosecuting Computer Crimes Manual." Washington, DC. https://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

United Nations General Assembly. 2013. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Doc. A/68/98.

United Nations General Assembly. 2015. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Doc. A/70/174.

Watts, Sean, and Theodore Richard. 2018. "Baseline Territorial Sovereignty and Cyberspace." *Lewis & Clark Law Review* 22 (3): 803–872.

Wilske, Stephan. 2012. "Abduction, Transboundary." In *Max Planck Encyclopaedia of Public International Law*, edited by Rüdiger Wolfrum. Oxford, NY: Oxford University Press.

Wright, Jeremy. 2018. "Cyber and International Law in the 21st Century." London. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.