

American University Washington College of Law

Digital Commons @ American University Washington College of Law

Articles in Law Reviews & Other Academic Journals

Scholarship & Research

2018

Sovereignty in the Age of Cyber

Gary Corn

Follow this and additional works at: https://digitalcommons.wcl.american.edu/facsch_lawrev



Part of the [International Law Commons](#), [National Security Law Commons](#), and the [Science and Technology Law Commons](#)

SYMPOSIUM ON SOVEREIGNTY, CYBERSPACE, AND TALLINN MANUAL 2.0

SOVEREIGNTY IN THE AGE OF CYBER

Gary P. Corn* and Robert Taylor†

Introduction

International law is a foundational pillar of the modern international order, and its applicability to both state and nonstate cyber activities is, by now, beyond question. However, owing to the unique and rapidly evolving nature of cyberspace, its ubiquitous interconnectivity, its lack of segregation between the private and public sectors, and its incompatibility with traditional concepts of geography, there are difficult and unresolved questions about exactly how international law applies to this domain. Chief among these is the question of the exact role that the principle of sovereignty plays in regulating states' cyber activities.

The technological structure and global interconnectedness of cyberspace offers both state and nonstate actors a medium through which to operate against a broad array of targets, free from the physical constraints of geography and territorial boundaries. At an increasing rate, states are not just utilizing, but also aggressively exploiting, cyberspace as a novel means for engaging in traditional statecraft, including activities that advance national security such as espionage and low-cost, asymmetric offensive operations. Likewise, nonstate actors routinely use cyberspace to conduct harmful activities that threaten individuals and business interests, as well as nations. For example, ISIS uses the internet to command and control its operations, spread its toxic propaganda, recruit new members, and incite violence globally. And while ISIS may not yet possess the cyber sophistication or capabilities of certain nation-states, it has demonstrated the ability and willingness to engage in offensive cyber operations.¹ The vulnerabilities inherent in the cyber domain threaten states' basic governmental functions, territorial security, political independence, and economic well-being, as well as the individual security and well-being of their citizens.

Through both custom and treaty, international law establishes clear proscriptions against unlawful uses of force and prohibits certain interventions among states. And while questions remain as to the specific scope and scale of cyber-generated effects that would violate these binding norms, the rules provide a reasonably clear framework for assessing the legality of state activities in cyberspace above these thresholds, including available response options

* *Staff Judge Advocate, United States Cyber Command.*

† *Visiting Scholar, Harvard Law School Spring Term 2017, Former Principal Deputy General Counsel, Department of Defense. The views expressed are those of the authors and do not necessarily reflect the views of the United States Cyber Command, the Department of Defense, or the U.S. Government. Authors are listed in alphabetical order.*

¹ See U.S. Cong. Sen. Armed Services Committee, Hearing to Receive Testimony on United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2017 and the Future Years Defense Program, Apr. 5, 2016, 114th Cong. 1st sess. Washington: GPO, 2016 (testimony of Admiral Michael Rogers). See also, Joseph Marks, *ISIL Aims to Launch Cyberattacks on the US*, POLITICO (Dec. 29, 2015, 05:28 AM); Joseph Pagliery, *ISIS is Attacking the US Energy Grid (and Failing)*, CNN MONEY (Oct. 16, 2015, 12:28 PM).

for states. Below these thresholds, there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace. The process of adapting the existing legal framework to cyberspace must reflect the unique aspects of the domain in order to ensure the law continues to serve the goal of maintaining peace and stability while enabling states to thwart existing threats and prevent new threats from emerging.

Jus Ad Bellum and Nonintervention

International law provides a framework for cooperation that is foundational to the successful preservation of international peace and security, and includes variations across different domains that account for the particularities of each domain. Both the *jus ad bellum*, as reflected in Article 2(4) of the UN Charter and customary international law (CIL), as well as the CIL rule of nonintervention, are well-recognized binding norms applicable to interstate relations. There is general consensus that the *jus ad bellum* applies fully to cyber activities that rise to the level of a use of force. There has been a great deal of discussion as to what cyber actions would actually amount to a use of force, and many commentators have speculated on that issue. Despite the lack of complete clarity, it is generally accepted that at a minimum, cyber activities that proximately result in death, injury, or significant destruction, or that represent an imminent threat thereof, constitute a use of force.

There is also general consensus that cyber actions that amount to a prohibited intervention also violate international law. This category would include actions that are coercive or dictatorial and bear on matters of sovereignty such as the choice of a political, economic, social, and cultural system, as well as the formulation of foreign policy.² The quintessential example of a violation of the principle of nonintervention is one state coercively interfering in the internal political process of another state, such as by altering the votes recorded and thereby affecting the results of an election.³ Although the nonintervention rule is firmly ensconced in CIL, there is a dearth of state practice, let alone *opinio juris*, regarding the contours of its applicability to cyber activities. Further development of how the nonintervention rule applies to cyber activities is critical to informing policymakers on available response options such as the correlative doctrine of countermeasures.

Activities Below the Level of Prohibited Intervention

The *jus ad bellum* and the principle of nonintervention provide limited guidance in the realm of cyber because the vast majority of cyber operations are something less than a use of force, and do not fit squarely within the traditionally recognized elements of the nonintervention rule. Whether extant international law regulates this less-intrusive class of cyber activities is therefore a critical question. Some argue that limitations imposed by the concept of sovereignty fill this normative space—that sovereignty is itself a binding rule of international law that precludes virtually any action by one state in the territory of another that violates the domestic law of that other state, absent consent. However, law and state practice instead indicate that sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law. While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect

² *Military and Paramilitary Activities in and against Nicaragua* (Nicar. v. U.S.), Merits, 1986 ICJ REP 14, para. 205 (June 27); OPPENHEIM'S INTERNATIONAL LAW 432 (Robert Jennings & Arthur Watts eds., 9th ed. 2008).

³ CHATHAM HOUSE, THE PRINCIPLE OF NON-INTERVENTION IN CONTEMPORARY INTERNATIONAL LAW: NON-INTERFERENCE IN A STATE'S INTERNAL AFFAIRS USED TO BE A RULE OF INTERNATIONAL LAW: IS IT STILL? (Feb. 28, 2007).

cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention.

Sovereignty is a fundamental principle of international law and is considered a “basic constitutional doctrine of the law of nations.”⁴ Since at least the Treaty of Westphalia and the creation of the modern nation-state, sovereignty has been understood to encompass two distinct but related aspects—internal and external sovereignty. As a general concept, it refers to “the collection of rights held by a state, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people.”⁵ It is understood as encompassing “the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relation with other states.”⁶ With respect to internal sovereignty, it signifies the independent right, in regard to a portion of the globe, “to exercise therein, to the exclusion of any other state, the functions of a state.”⁷ This well recognized, near-exclusive right over the *domaine réservé* of the state—those matters of governance and jurisdiction committed to the sole responsibility of the state and its official actors—is at the heart of, and specifically protected by, the principle of nonintervention.⁸ In addition, internal sovereignty allows a state to prohibit acts within or affecting its territory as an exercise of governmental authority. However, 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.

A perhaps more foundational aspect of sovereignty is the equality of states in the international order.⁹ Sometimes referred to as external sovereignty, this corollary principle to the exclusive authority of the state to exercise jurisdiction and governance within its territory refers to the recognition in the international order of the absolute equality and independence of all states. External sovereignty forms the unifying principle of international law—that only states, *qua* states, have the legal personality necessary to create and be bound by international law.¹⁰ The principle of sovereign equality underlies the well-recognized premise in international law that “[r]estrictions on the independence of states cannot . . . be presumed.”¹¹ This premise, known as the *Lotus* rule, has long been understood to stand for the proposition that states are free to act on the international plane except to the extent that their actions are proscribed by treaty or customary international law.

Since the rise of the modern nation-state, countries have applied the doctrine of sovereignty in different ways, at times developing specific international law regimes tailored to the particular circumstances. For example, it is widely recognized that states have unquestioned authority to prohibit espionage within their territory under their domestic laws, but it is also widely recognized that international law does not prohibit espionage. States have long engaged in espionage operations that involve undisclosed entry and activities within the territory of other states, subject only to the risk of diplomatic consequences or the exercise of domestic jurisdiction over intelligence operatives if discovered and caught. Within this framework, it is understood that espionage may violate international law only when the modalities employed otherwise constitute a violation of a specific provision of

⁴ JAMES CRAWFORD, BROWNIE’S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 447 (8th ed. 2012).

⁵ *Id.* at 448.

⁶ Corfu Channel (U.K. v. Alb.), Merits, 1949 ICJ RER 4, 43 (Apr. 9) (individual opinion by Alvarez J.).

⁷ Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928). See also Samantha Besson, *Sovereignty*, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 119 (2011) (noting that sovereignty is generally characterized as the “powers and privileges resting on customary law which are independent of the particular consent of another state”).

⁸ CHATHAM HOUSE, *supra* note 3.

⁹ UN Charter art. 2(1) (“The Organization is based on the principle of the sovereign equality of all its Members.”).

¹⁰ Under limited circumstances, international organizations may create international law, but only to the extent states have conferred on them the authority to do so.

¹¹ The S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

international law, such as an unlawful intervention or a prohibited use of force. Thus states conduct intelligence activities in and through cyberspace, and generally, “to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities . . . such cyber operations would likely be treated similarly under international law.”¹² This framework applies equally to cyber operations directed at terrorist cyber infrastructure located within the territory of another state.

Further, the differences in how sovereignty is reflected in international law with respect to the domains of space, air, and the seas further support the view that sovereignty is a principle, subject to adjustment depending on the domain and the practical imperatives of states rather than a hard and fast rule. For instance, in the case of the space domain, objects in orbit are beyond the territorial claims of any nation, and outer space—including outer space above another state’s territory—is available for exploitation by all. In the case of the air domain, the regime is highly restrictive, such that any unconsented entry into the airspace of another state is regarded as a serious violation of international law subject to such exceptions as self-defense, Security Council authorization, or force majeure. In the case of the seas, many entries into and transits through the territorial waters of another state are permissible without the consent of that state, but there are conditions under which such entry would be a violation of international law—it depends on the particular facts and circumstances. The fact that states have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace. The principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and/or the development of treaty rules.

A contrary view asserts that sovereignty is more than a foundational principle of international law, upon which rules such as the prohibitions against the use of force and unlawful intervention are based. In this view, sovereignty is itself a rule of international law that can be violated.¹³ This view is frequently stated in terms of violations of or interferences with a state’s territorial sovereignty.¹⁴ However, this confuses the concept of territorial sovereignty, inherent in the notion of internal sovereignty discussed above, with the more precise concepts of territorial integrity and the inviolability of borders protected through Article 2(4), the Charter more broadly, and CIL. The prescriptions against violating territorial integrity or borders involve a threshold of harm much higher than the mere conduct of cyber operations limited to affecting, for example, cyber facilities owned or operated by terrorists, criminals, or by third states, located inside another state’s borders.¹⁵ Ultimately, whether and precisely when nonconsensual cyber operations below the threshold of a prohibited intervention violate international law is a question

¹² U.S. DEP’T OF DEFENSE, LAW OF WAR MANUAL sec. 16.3.2 (2015) (revised Dec. 2016).

¹³ Michael Schmitt, US Transparency Regarding International Law in Cyberspace, JUST SECURITY (Nov. 15, 2016, 9:11 AM).

¹⁴ Some point to cases such as *Costa Rica v. Nicaragua* (Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and *Construction of a Road in Costa Rica along the San Juan River* (Costa Rica v. Nicar.) (Dec. 16, 2015)), *Corfu Channel* (Corfu Channel, *supra* note 6)), and *Armed Activities on the Territory of the Congo* (Armed Activities on the Territory of the Congo (New Application 2002 (Dem. Rep. Congo v. Uganda), 2006 ICJ REP. 6 (Feb. 3)) as support for this position. While it is true that the ICJ has referred to violations in those cases, in each instance the facts ruled on involved substantial military presence, de facto control of territory, and in some instances, violent operations, all of which implicate higher thresholds than the sovereignty-as-a-rule proponents assert. For example, in *Armed Activities on the Territory of the Congo*, the ICJ found that Uganda’s “unlawful military intervention” inside the territory of the Democratic Republic of the Congo (DRC) constituted a use of force in violation of Article 2(4) and a prohibited intervention, as well as military occupation of some DRC territory, and as such, constituted a violation of the DRC’s sovereignty and territorial integrity in the broader sense.

¹⁵ See, e.g., The Final Act of the Conference on Security and Cooperation in Europe, Aug. 1, 1975, 14 I.L.M. 1292 (Helsinki Declaration).

that must be resolved through the practice and *opinio juris* of states, developed over time and in response to the need of states effectively to defend themselves and provide security for their citizens.¹⁶

The ramifications of the growing debate as to whether and how international law regulates state actions in cyberspace below the nonintervention threshold are easily observed in the case of the use of cyber capabilities in the fight against widely recognized terrorist organizations such as ISIS. In these cases, owing to the distributed nature of cyberspace, operations may involve cyber effects directed against terrorist-controlled infrastructure on networks or systems located in states outside areas of hostilities, and not subject to any preexisting authority to use force. While these “subintervention” cyber activities should consider the sovereignty of the states in whose territory these terrorist infrastructures reside, this does not answer the key question of whether or how sovereignty proscribes such cyber activities. While the principle of sovereignty should factor into the conduct of any cyber operation, it does not itself establish a bar against individual or collective state cyber operations against all cyber infrastructure within another state, particularly those controlled by widely-recognized terrorists and used for terrorist activity. In short, sovereignty is a principle, not a rule, and its legal consequences are not fully formed in this area.

Applying this Approach to Terrorist Operations

ISIS, like other transnational organizations, has a vast social media presence and uses the internet to communicate with its members and supporters, to recruit individuals to its cause, and to promote its views and activities. Its media operations are decentralized and originate from servers in numerous states throughout the world, encouraging crowdsourcing and volunteerism by individuals not directly associated with the terrorist organization. Additionally, ISIS adherents have formed the Cyber Caliphate and have taken active malicious cyber actions over the internet.¹⁷ This means that ISIS followers and adherents both inside and outside ISIS-controlled territory operate on servers and infrastructure scattered across the globe, taking advantage of the transparency and permeability of borders that characterize the internet. These states may have limited or no knowledge that ISIS is utilizing servers or cyber infrastructure under their sovereign authority. Further, these states may lack the capability to effectively counter or even discover ISIS’s cyber threat.

If the view were adopted that sovereignty is a rule violated by any action illegal under the domestic law of a state, states seeking to disrupt distributed terrorist cyber infrastructure would be under an obligation to either seek Security Council authorization or the consent of the state in whose territory the infrastructure resides. The nature of cyber operations and capabilities often require high degrees of operational security and the flexibility to act with speed and agility. Operating through a consent model could in important cases surrender operational initiative to the terrorist adversary or render response options unworkable. Further, these actions could involve cyber effects in, yet invisible to, the territorial state, but that only manifest operationally in the area of hostilities.

Because the doctrine of sovereignty does not prevent all actions by one state that affect another state or even “encroachment on other sovereign jurisdictions,”¹⁸ a state involved in operations against ISIS, such as the United States, is not precluded from taking action against ISIS’s cyber facilities in other states, even without the consent of the host state, unless doing so constitutes a prohibited intervention or use of force. Where the proposed cyber action is focused solely against the individual accounts or facilities of terrorists or terrorist organizations widely recognized as such, and when the cyber actions will generate only *de minimis* effects on nonterrorist infrastructure

¹⁶ Brian Egan (Legal Adviser, U.S. Dep’t of State), *International Law and Stability in Cyberspace* (November 10, 2016).

¹⁷ Faisal Irshaid, *How ISIS Is Spreading Its Message Online*, BBC News (Jan. 19, 2014); Paul Szoldra, *Inside the Hacker Underworld of ISIS*, BUSINESS INSIDER (June 16, 2016, 9:54 AM); Brendan I. Koerner, *Why ISIS Is Winning the Social Media War*, WIRED (Apr. 2016).

¹⁸ Egan, *supra* note 16.

within the host state, international law does not preclude those cyber actions. States may choose, as a matter of policy, to seek the host state's consent before taking such actions, but there is no customary law requirement to do so. The host state, exercising its sovereign domestic authorities, could proscribe such activities just as states proscribe espionage, but such proscription would be a matter of domestic law of the host state, rather than a matter of international law.

ISIS and other terrorist or criminal organizations, and indeed some states, are using and will continue to use the internet and cyber facilities to advance their malevolent ends. Effectively countering these activities is vital to national and international security. States must ensure that any response complies with international law and takes into account each state's sovereignty. Properly understood and applied, international law and the doctrine of sovereignty do not preclude per se individual and collective state cyber actions directed against terrorist-owned or -operated cyber facilities, or other malevolent infrastructure, located within other states.