DILEMMAS OF STATE SOVEREIGNTY, INTERNATIONAL LAWS AND CYBERSPACE

[**Issue Number 109 - July 2019**](https://www.lebarmy.gov.lb/en/content/109-d)

**Dilemmas of State Sovereignty, International laws and Cyberspace**  
Prepared By: Prof. Michel Nehme and Tania Nehme  
Professor at NDU , ABD global studies

**Introduction**

Westphalia treaties in 1648 considerably changed the landscape of international affairs. It illustrates among many aspects the start of one significant track and that is state sovereignty. The 1933 Montevideo Convention[[1]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn1" \o ") defined the state as territory with undisputable sovereignty. This notion was constructed into the first chapter of the United Nations’ charter which says that “the Organization’s foundation depends on the equal sovereignty of all its members”. De-facto, state sovereignty became an important pillar in all global affairs.

Sovereignty involves the allegation that there is no absolute authority above and beyond the sovereign state. States must be regarded as independent in all matters of internal politics and should in principle be free to determine their own fate within this framework. External sovereignty is a quality that political societies possess in the relationship to one another; it is associated with the desire of a community to control its own direction and politics without undue interference from other powers[[2]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn2" \o ").

Sovereign states system became entrenched in a complex of rules that evolved, from the seventeenth century, to secure the concept of an order of states[[3]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn3" \o ") as an international society of sovereign states. The emergence of a “society” of states, ﬁrst in Europe and later across the globe, went hand in hand with a new conception of international law.

After World War II a new model of international regulation fully crystallized, the regime of liberal international sovereignty which can be traced by attempts to extend the processes of delimiting public power to the international sphere and by attempts thereafter to transform the meaning of legitimate political authority from effective control to the maintenance of basic values that no political agent, whether a representative of a government or state, should, in principle, be able to abrogate. Effective power is challenged by the principles of self-determination, democracy, and human rights as the proper basis of sovereignty. In highlighting some of the legal transformations that have taken place in the domains of military confrontations, war crimes, human rights, democratic participation, as well as the environment which underlie this shift. These transformations have been ushered in with the approval and consent of states, but the delegation and changes in sovereignty have acquired a status and momentum of their own.

**The individual and war crimes**

The process of the gradual delimitation of state power can be illustrated further by another strand in international legal thinking that has overturned the primacy of the state in international law and buttressed the role of the individual in relation to and with responsibility for systematic violence against others. In the ﬁrst instance, by recognizing the legal status of conscientious objection, many states have acknowledged there are clear occasions when an individual has a moral obligation beyond that of his or her obligation as a citizen of a state[[4]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn4" \o "). The refusal to serve in national armies triggers a claim to a “higher moral court” of rights and duties.

Such claims are exempliﬁed as well in the changing legal position of those who are willing to go to war. The recognition in international law of the offenses of war crimes, genocide, and crimes against humanity makes clear that acquiescence to the commands of national leaders will not be considered sufﬁcient grounds for absolving individual guilt in these cases.

The Rule of Law, which indicates that the state is also subject to its own laws, is one factor limiting the sovereignty. With the Rule of Law we limit the internal sovereignty of the state to give the population more rights and to make them sovereign. This limitation of sovereignty is actually a measure to protect the democratic regime. It puts the constitution above the state and prevents the existence of a dictatorship in society. Additionally, liberal scholars argue that this rule is not a limitation, but it is a restoration of the rights of people by making them sovereign.

All of the international law also represents a loss of sovereignty to one degree or another. For example, the law of diplomatic immunity means that the police cannot arrest a diplomat for a common crime. There are many other examples of government actions being constrained by international law, especially in the areas of human rights, environmental law and economic law. Most of these international laws form actually the basis of a democratic society. However, nowadays the practical effects of international law have changed. In the past, the international law attempted more to strengthen the sovereignty of states rather than to restrain them[[5]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn5" \o "). Today, it serves as a tool to reduce the national sovereignty. On the other hand, when we talk about the effects of international law on sovereignty, we must also consider the international institutions, which create these laws.

European Union is another international institution, which has significant effects on the concept of sovereignty. To look at these effects we must first examine state sovereignty for the past several hundred years by defining the principle of interstate relations and the foundation of world order. The concept lies at the heart of both customary international law and the United Nations Charter and both remain an essential component for the maintenance of international peace and security and an eligible defense of weak states against the strong. At the same time, the concept has never been as inviolable, either in law or in practice, as a formal legal definition might imply. According to former Secretary-General Boutros Boutros-Ghali, "The time of absolute sovereignty … has passed; its theory was never matched by reality[[6]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn6" \o ")".

Empirically, sovereignty of weak states has routinely been violated by the powerful states. In today’s globalizing world, it is generally recognized that cultural, environmental and economic influences neither respect borders nor require an entry visa. The concept of state sovereignty is well entrenched in legal and political discourse. At the same time, territorial boundaries have come under stress and have diminished in significance as a result of contemporary international relations. Not only have technology and communications made borders permeable, but the political dimensions of internal disorder and suffering have also often resulted in greater international disorder. Consequently, perspectives on the range and role of state sovereignty have, particularly over the past decade, evolved quickly and substantially.

Political science scholars have repeatedly asserted that few subjects in international law and international relations are as sensitive as the notion of sovereignty[[7]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn7" \o "). Steinberger refers to it in the Encyclopedia of Public International Law as "the most glittering and controversial notion in the history, doctrine and practice of international law". On the other hand Margaret Klemperer[[8]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn8" \o ") sees it as "the one and only organizing principle in respect of the dry surface of the globe, all that surface now … being divided among single entities of a sovereign or constitutionally independent kind". As noted by Falk[[9]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn9" \o "), "There is little neutral ground when it comes to sovereignty".

**Globalization and cyberspace**

Globalization and cyberspace brought about limitations and decline to state sovereignty in the contemporary world. Conventional studies of interstate relations alone are not enough anymore to characterize the reality of international relations. Citizens everywhere are developing and adding new effective political and economic impacts to the arena of global relations. Effective international laws and the fact that citizens can communicate and share information like never before through the use of cyberspace fuelled by ceaseless global media coverage that no one state could control.

Non-Governmental Organizations (NGOs) also are assuming over state responsibilities by imposing global decisions similar to the UN or the International Court of Justice. Notwithstanding, multinational corporations have grown their power through providing services states cannot afford to deliver such as capital flow, bank loans, pharmaceutical health services and cheaper commodities[[10]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn10" \o ").

The Globalization of markets gave opportunities to companies to move away from offering personalized goods and now instead are manufacturing globally standardized products that are advanced, functional, reliable and low priced. That mass production means that only global companies will achieve long-term success by concentrating on what consumers everywhere in the world are in need for. Multinational companies use high tech production as a mean to efficiently penetrate the different sectors of global markets. Global multinational companies’ marketing strategy can be applied to outreach communication giants such as Facebook, Google and the Silicon Valley and their way of penetrating the global markets[[11]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn11" \o ").

In every society, there are certain basic services that are needed for people’s wellbeing. If governments are not capable of meeting those needs, they are obligated to accept the help of external actors to insure state stability, growth and development. This new imposed reality on states challenges the concept of sovereignty as having the full right and power of a governing body over itself, without any interference from outside sources or bodies.

**Cyberspace and sovereignty**

The official discourse surrounding the Internet, the cyberspace and its governance is often state-centered. UN Resolution 68/167[[12]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn12" \o "), envision states as the primary responsible actors with regard to the respect, assurance and enforcement of fair cyber practices, while left behind inaudible on the roles and responsibilities of other institutions and organizations on the matter. International law is well known in issues similar to this, that is to say the place of individuals and non-state actors are not well defined in a realm which by definition concern the conduct of affairs between nation states. Since the last century, however, multi-national corporations, non-governmental organizations and individuals have been assessed as de-facto international legal entities, notably in the realm of international human rights law and international criminal law[[13]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn13" \o ").

However, if in the case of international relations this became possible as a “top-down” development where states were in a position to “grant” rights in a judicial space created by themselves, the case of the cyber dimensions presents some thorny characteristics.

In the dimension of cyberspace, concepts such as coercive monopoly, territoriality, and order are irrelevant. While sovereignty of the state dates back to the Seventeen century, those of the cyberspace are rooted in the Cold War’s technological arm race between the two superpowers.

The whole current World Wide Web has witnessed its mainspring within the walls of the American Information Processing Technique Office. The idea of creating a series of linked computers which would allow people to access and share information was born for military objectives[[14]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn14" \o "). From this simple foundational principal, the basis of the new technology was developed. Universities adopted this principle to connect research communities, in what is known as host-to-host type of communication relying on protocol-based networking between two or more nodules. In this information exchange, the code, the commands, the algorithms containing the instructions about the transmission has a role of paramount importance.

**The U.S.A. as a case study**

The US Department of Justice on April 18, 2019, released a version of the report submitted by Special Counsel Robert Mueller about Russia’s interference in the 2016 US presidential elections[[15]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn15" \o "). The important part of this report presents the outcome of the investigation into Russia’s involvement in the election. The report exposes the inability of the American system to preserve its sovereignty in the nation’s organizational, legal, and technological preparedness to confront the digital space that is undermining internally and externally American sovereignty and the democratic process.

The Mueller Report provides a broad factual basis for analyzing the 2016 US presidential elections, thus adding to the data already made public through the three indictments handed down during the investigation naming Russian officers, citizens, and institutions; research institute publications; and books written by former senior members of the US intelligence and security establishment. Together, the data paint a stark picture: acting on direct orders from President Vladimir Putin, Russian intelligence agencies conducted an organized campaign to influence the presidential election.

To this end, the Russians adopted a multi-faced approach: organized, systematic activity by their intelligence agencies (led by the GRU), which included hacking computers belonging to individuals and institutions connected to the Democratic Party and the Clinton campaign; leaks of obtained information through websites and media financed by the Russian government, e.g., the Russia Today TV network and the Sputnik news agency; and dissemination of that information on social media using a massive army of trolls constructed by the Internet Research Agency over the course of several years and maintained via stolen profile pictures and fictitious biographies.

The Russians focused on spreading information about a series of scandals attributed to Clinton, including the “email affair,” the “Benghazi attack failure scandal,” the “Clinton Family Foundation contribution scandal,” and her “support for the Iraq war". The media generated material about the scandals and the trolls spread them on Facebook, Twitter, YouTube, and Instagram. The messages were uniform and matched those of Trump’s campaign: Hillary was corrupt, suffered from mental and physical ailments, and was connected to radical Islamic elements. At the same time, certain population segments were targeted for voter suppression.

The major problem is that currently, in cyberspace, there is no need to sign an agreement or enter a closed room and sit around the same table in order to sway public opinion[[16]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn16" \o "). This is the revolution that the current digital world has made possible: the ability to affect election results, mostly by means of social media. Such "virtual conspiracies" to affect elections can be made between two sides that never meet physically or even online (such as in chats or emails) and are not connected in the usual meaning of the word. Activities occurring in various locations and at various times can simply stem from shared interests and serve similar goals. It is enough that each side is aware of the other’s existence and their shared interests, and then echoes the messages coming from the other.

Such reverberations can be direct, by making message contents go viral via sharing to accounts with many followers or through networks of interconnected accounts, re-tweeting, and sharing to groups using private messaging programs (WhatsApp, Telegram Messenger). But it can also be indirect, such as one side using inflammatory information about the other for a scheme that “coincidentally” blows up on the same day embarrassing information is released on one’s partner so as to divert public attention away from the partner’s humiliation.

Joint influence by means of a “virtual conspiracy” can be realized both when a foreign campaign and a local campaign work toward the same goal, and when a partisan campaign and ancillary entities (NGOs or super PACs) do so. The ability to forge virtual conspiracies between various players, domestic and foreign, is thus a new and major feature of today’s world[[17]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn17" \o "). If the Mueller Report states that there was no criminal influence by Trump on the election, it is not that such influence wasn’t exerted, but because it cannot be labeled criminal by current legislation. The problem is that the lacuna in legislation reflects a much broader matter related to conceptual, organizational, and technological gaps.

The Russian campaign in the 2016 US presidential election came as a shock revelation to the U.S.A. sovereignty. The US intelligence community identified Russia’s involvement and apparently did not understand the essence of Russian’s activity, its goal, and its broader implications. The Americans did not grasp the idea of a campaign of influence in cyberspace, because the platforms used to spread the messages, i.e., social media, were all American, identified with the American ethos of freedom of expression and information. In their defense, senior figures in the US intelligence community say that the ban on gathering information about US citizens made it impossible to understand the overall picture of Russia’s actions and their ramifications. But the problem seems to have been more extensive: today, it is very clear that there was no one in the United States who saw himself as responsible for foiling the Russian campaign or had the organizational, conceptual, and technological qualifications to operate such an effort.

**“Code is Law”**

Lessig (2000) noted in his famous essay “Code is Law”[[18]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn18" \o "). Codes denote the very structural design of the cyberspace, as they contain the rules based on which interactions between servers and machines function. This way, codes function like the social norms and the laws which regulate relations between members of a society derived from the state structure. Thus, we can see protocols as all powerful “internet laws”, whose importance can command the type of interaction between not only computers, but also the actors behind them. Nevertheless, there is one important disparity we should make between the “normative/legal structural design” of the social and the cyber worlds and that is the feasibility to access knowledge.

Not with standing, how do we assess codes and protocols? The vast majority of internet users hardly know what codes and protocols are, let alone how they work and what is their content. Furthermore, this type of information can even be difficult to attain by closed-source software. Hence, expertise plays a pivotal role in the cyberspace, which speaks volumes about the challenges this place on state institutions and administration which often encounter complications with minor technological modification.

States might have represented the most adequate organizational structure to the capitalist mode of production, the management of natural resources, and the mobilization of intercommunal and global violence. However, they are now confronted by hackers, rootkits and viruses-writers, seemingly more knowledgeable and better-equipped to act in the cyber-environment.

The Internet world magnifies the importance of actors endowed with high expertise and quick adaptability as individuals or groups, at the expenses of complex governmental bureaucracies resisting change and technological development.

Still, another challenge emerges when we consider some technological developments which undermine altogether the important role of the state as the intermediary of social relations. This is the case of Block-chain technology[[19]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn19" \o "), and as an example to this is Bitcoins and Bit-nation. What makes Block-chain critical is the way through which it manages to evade political attempts to impose the norm of territoriality principles into the cyberspace. In simple terms, Block-chain can be described as a vast, shared database of information which is continuously updated, available and visible by and on each computer device with access to it (Bagley, 2016). None of these databases is a “copy” and none of them is the “original” to be preserved somewhere. On the contrary, millions of computers host the same content, a fact which surely guarantees for transparency and accessibility.

In this context it is important to elaborate on the landscape of data. Data is real information which is stored in physical servers in exact country and under a specific national legislation. Especially after Edward Snowden’s revelations on U.S.A. domestic and international surveillance, many states have pushed for a much stricter regulation of data localization, justifying it by reference to the need of their national security interest and the privacy of their citizens’ personal information[[20]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn20" \o ").

Data nationalization is particularly attractive for governments; it supports their idea of sovereignty by plausibly making foreign intervention and surveillance more difficult, while making it easier for them to scrutinize their own domestic flow of data. In the process of governmental protection of information from being violated by hackers and regimes, important implications would emerge with regard to central trans-factional institutions such as the state bureaucracy. This could be explained by using the Bitcoins phenomenon. Monetary systems are based on trust: trust on the value of a currency, trust on creditors to reimburse debts, trust on banks operating transactions on our behalf, trust on the stability of central banks.

The problem is what would ensue when the whole system is replaced by a stateless currency created by an algorithm?

What would occur if people start fluctuating between their trust for central bankers and an immense computer treasury? For a portion of the population, this feels like a daydream: freedom from government’s bureaucracy can finally be attained. For others, this development represents the ultimate madness of uncertainty. Definitely, governments are not enthusiastic to see their undisputed right to issue currency being eroded by a computer[[21]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn21" \o ").

**Political Science and technology**

By looking at International Technology as a source of disorder leading to instability and an obstacle to be dealt with, states and traditional scholars alike miss the fundamental differences between the cyberspace and the international arena.

Traditional political scientists at large perceive of technology and the cyberspace as developments threatening the established order. Cyberspace is a phenomenon that states feel the need to be disciplined or exploit it in their favor. In his famous “Abiding Sovereignty” Krasner[[22]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn22" \o ") mentions cyber only in relation to cybercrime and potential criminal activities; Hare[[23]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn23" \o ") defends borders as useful constructs in the field of cyber relations.  Jensen[[24]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn24" \o ") and Shen[[25]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn25" \o ") both understand cyber sovereignty as the need to impose national sovereignty on cyber actors.

The new dimension introduced by the Internet revolution is one where territoriality, nationality, laws, monopolies and war make little sense.

Agents in the cyberspace find themselves in a state-of-nature condition, in a cyber polity-in-the-making where reciprocal actions have still not evolved into mature cooperation. Cyberspace activists consider that states co-exist with a multiplicity of actors in a way which is far from our classical understandings of hierarchy and legitimacy, which instead are continuously questioned and overturned. Thus, interaction is not thoroughly institutionalized, coercion is not centralized, and laws, norms and “cyber consciousness” are barely present.

The idea of a “cyber social contract” is absent, and it is not expected to be imposed by governments. In fact, states are one among the many potential “citizens” of the cyberspace. The required initiative to sustain order is the realization of the disadvantages coming from the collective “abuse” of our natural freedoms and the willingness to partly renounce them for the sake of living in a functioning society. Thus, unless a Cyber Sovereign able to guarantee and uphold the rights of all its members is established, each actor is set to violate the freedoms of the others. This fact explains our difficulty in understanding the awkward positions of companies like Facebook and Microsoft vis-à-vis powerful nation state, and vice versa when it comes to data protection and surveillance.

Those that support cyberspace freedom assert that just like different organisms in nature function in different ways, the Cyber Sovereign would not need to function in the same way as modern nation states: regulated codes could perform the role of laws; institutionalized cooperation between the public, private and corporate sectors could represent a viable branch of “government”; decision-making processes could take advantage of the great opportunity the Internet offers with regard to direct democracy; and so on. “A new, revolutionary conception and practice of sovereignty will need to be combined by an agreeable style of governance which, indeed, will not emerge in the near future but will take time to be institutionalized and legitimized just as modern states did in the past[[26]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn26" \o ")".

There is no certainty when it comes to the future of the cyberspace and that of state sovereignty specifically when national borders are underscored in the ever-changing global system.

**Cyberspace and loopholes in law**

Two Tallinn Manual groups of experts explored applicability of state sovereignty to cyberspace operations between 2009 and 2017.  The first concluded in Rule 1 of the 2013 Tallinn Manual that “A State may exercise control over cyber infrastructure and activities within its sovereign territory".

An important part of what Tallinn manual explored is the right of state sovereignty and to legally assess this right within the existing international law[[27]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn27" \o "). As an example they elaborated on cases where a cyber operation by a State directed against cyber infrastructure located in another State may causes damage and thus violate the latter’s sovereignty. In other words, a cyber operation causing physical damage to either governmental or private cyber infrastructure violates the sovereignty of the state into which it is conducted and accordingly amounts to a breach of international law. As such, it opens the door to the taking of countermeasures in response.

The other group of experts who prepared Tallinn Manual 2.0 between 2013 and 2017 examined the mutual impact of cyberspace on sovereignty and visa-versa. They issued a statement: “A State must not conduct cyber operations that violate the sovereignty of another State". With respect to remotely conducted cyber operations, they concurred that whether sovereignty has been violated depends on: (a) The degree of infringement upon the target State’s territorial integrity; and (b) whether there has been an interference with or usurpation of inherently governmental functions. The first notion is based on the premise that a State controls access to its sovereign territory, and the second notion is based on the sovereign right of a state to exercise within its territory ‘to the exclusion of any other State, its legal right to function as a sovereign state’.

On the other hand there is still a gray area on whether a counter response is legally appropriate by the “injured” state that would be unlawful but for the fact that they are designed to put an end to the “responsible” state’s unlawful conduct, in this case a sovereignty violation.  The experts agreed that only cyber operations conducted by, or attributable to, states violate the prohibition, although they acknowledged that there is an “embryonic view” that non-state actors may do so as well.

Since sovereignty is a primary rule of international law, the initiator of violation damaging cyber operations, including those that interfere in a relatively permanent way with the functionality of the targeted cyber infrastructure, qualify as a crime violation, although agreement could not be reached on the precise scope of the concept of loss of functionality.

The Tallinn Manual groups’ experts who were willing to characterize as violations of sovereignty cyber operations falling below the threshold of loss of functionality extended a number of possibilities. These included, but were not limited to, a cyber operation causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation. (DDoS is short for Distributed Denial of Service). DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack).

Remarkably, all of the various interpretations of the sovereignty rule looked to the same justification, “the object and purpose of the principle of sovereignty that affords states the full control over access to and activities on their territory". This comes at a time when ambiguity still prevails with regard to the notion of "inherently governmental function". Some functions are obviously inherently governmental in nature, such as conducting elections, collecting taxes, and national defense.  But beyond these self-evident examples, the universe of inherently governmental functions becomes less clear.

However, sovereignty is both a principle of international law from which certain rules, such as the prohibition of intervention into the external or internal affairs of other states, derive, and a primary rule of international law susceptible to violation. That is why the challenge is to identify the sorts of cyber operations that cross the violation line. While there was agreement that cyber espionage, in light of extensive state practice to the contrary, does not, per se, violate sovereignty and that damaging cyber operations do, between these extremes the proposed law remains unsettled.

Moreover, coercion requires that the cyber operation in question be designed to compel the target state to take an action it would not normally take or to refrain from one in which it would otherwise engage. Merely malicious, disruptive or criminal cyber operations generally would not satisfy this criterion. Such operations therefore would have to rise to the level of a cyber use of force under Article 2(4) of the UN Charter (and customary law) to constitute an unlawful act. Unfortunately, the only consensus regarding the use of force threshold is that destructive operations qualify. This is problematic because, at least for the present, the uncertainty of law surrounding the notion of the use of force has been persistent with respect to cyber operations below its far-reaching edge.

There is now a general trend among states to see law and state practice as indicative that sovereignty serves as a principle of international law that guides state interactions. However, it is not by 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 a block against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention.

Political science scholars have repeatedly asserted that 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. But they argued that, as yet, rules of international law that address remotely conducted cyber intrusions have yet to emerge from the principle of sovereignty, as has happened, for instance, in the laws covering rights to open seas and air space domains.

**Conclusion**

National borders are losing their importance, so the redefinition and reconstruction of the concept of sovereignty becomes a necessity. Information in the cyberspace about the government enables the citizen to watch the state. The citizen can keep better track of government. On the other hand, with creation of cyberspace individuals may provide more information about their preferences to government through referenda and surveys. This function of cyberspace may serve to legitimize government action; because it can be based on citizen preferences. Therefore, this may increase the expression of individual preferences; thus an image of representative democracy.

In recent decades, and particularly since the end of the Cold War, four more radical challenges to the notion of state sovereignty have emerged: continuing demands for self-determination, a broadened conception of international peace and security, the undermining of state authority, and the increasing importance of popular sovereignty.

In many ways, a central contemporary difficulty arises from the softening of two norms that had been virtually unchallenged during the Cold War, the inviolability of borders and the illegitimacy of secession. For almost half a century, collective self-determination was limited to the initial process of decolonization. Existing borders were inviolable, and it was unthinkable that an area of a state would secede, even with the consent of the original state.

Sovereignty, still, is considered as a primary rule in international law as dictated by the charter of the United Nations. Thus sovereignty as a counter-normative fringe position designed to afford its proponents the legal basis for conducting various types of offensive cyber operations is not within legal toleration. It is a serious approach, proffered by first-rate lawyers and apparently championed by a number of government agencies that exercise significant power in cyber operational and policy circles. And, a rule of sovereignty, as distinct from a principle, has the potential for sometimes being an obstacle to achieving vital national security interests, such as defense against terrorism, stopping the spread of weapons of mass destruction, and ensuring adequate intelligence as to the capabilities and intentions of hostile states.

But what is cyber law[[28]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftn28" \o ")? Some see it as a process to legally regulate cyber activities to go along in responding to the sovereignty as principle. Scholars on this topic outlined contemporary assessments of sovereignty as applied to cyberspace. There is ample evidence that the prevailing view is that sovereignty is a primary rule of law and one applicable to cyber activities. This being so, it seemingly is not the only stance. The other stance take one of two alternative approaches in order to keep the rule of sovereignty from acting as an unacceptable barrier to cyber operations that might be necessary to safeguard a state’s national security interests.

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.

Not with standing, the differences in how sovereignty is reflected in international law with respect to the domains of space, air, and the seas further supports 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.

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 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.

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.

**References**

- Bagley, J. (2016, September 18). What is Blockchain Technology? A Step-by-Step Guide for Beginners. Retrieved October 28, 2017, from https://blockgeeks.com/guides/what-is-blockchain-technology/

- Biagio, S. (2017, October 20). Terrorismo, i big hi-tech al G7: così contrasteremo la cyberpropaganda. Il Sole 24 ORE. Retrieved from http://www.ilsole24ore.com/art/tecnologie/2017-10-20/terrorismo-big-hi-tech-g7-cosi-contrasteremo-cyberpropaganda-163932.shtml?uuid=AEFcJisC

- Bodoni, S., White, A., & Hodges, J. (2015, January 20). Microsoft Gave Data on Charlie Hebdo Probe to FBI in 45 Minutes. Bloomberg.Com. Retrieved from https://www.bloomberg.com/news/articles/2015-01-20/microsoft-fights-unregulated-snooping-amid-terrorist-threat

- Baldwin, T. (1992) The Territorial State. In H. Gross and T. R. Harrison (eds), Jurisprudence, Cambridge Essays, Oxford: Clarendon Press.

- Beitz, C. (1979) Political Theory and International Relations. Princeton: Princeton University Press.

- Beitz, C. (1994) Cosmopolitan Liberalism and the States System. In C. Brown (ed.), Political Restructuring in Europe: Ethical Perspectives, London: Routledge.

- Beitz, C. (1998) Philosophy of International Relations. In The Routledge Encyclopedia of Philosophy, London: Routledge.

- Bull, H. (1977) The Anarchical Society. London: Macmillan.

Byers, M. (1999) Custom, Power and the Power of Rules. Cambridge: Cambridge University Press.

- Cory, N. (2017). The Worst Innovation Mercantilist Policies of 2016. Information Technology and Innovation Foundation. Retrieved from https://itif.org/publications/2017/01/09/worst-innovation-mercantilist-policies-2016

- Cassese, A. (1986) International Law in a Divided World. Oxford: Clarendon Press.

- Cassese, A. (1988) Violence and Law in the Modern Age. Cambridge: Polity Press.

- Chinkin, C. (1998) International Law and Human Rights. In T. Evans (ed.), Human Rights Fifty Years On: A Reappraisal, Manchester: Manchester University Press.

- Crawford, J. (1995) Prospects for an International Criminal Court. In M. D. A. Freeman and R. Halson (eds), Current Legal Problems 1995, 48, pt 2, collected papers, Oxford: Oxford University Press.

- Crawford, J. and Marks, S. (1998) The Global Democracy Deﬁcit: An Essay on International Law and Its Limits. In D. Archibugi et al. (eds), Re-Imagining Political Community: Studies in Cosmopolitan Democracy, Cambridge: Polity Press.

- Dinstein, Y. (1993) Rules of War. In J. Krieger (ed.), The Oxford Companion to Politics of the World, Oxford: Oxford University Press.

- Donnelly, J. (1998) International Human Rights, 2nd edn. Boulder, CO: Westview Press.

- Dugard, J. (1997) Obstacles in the Way of an International Criminal Court. Cambridge Law Journal 56. The Changing Structure of International Law.

- Das, S. (2017, October 27). Bitcoin Banned as a Payment Method in Indonesia, Adopters Will Be “Dealt With". CryptoCoinsNews. Retrieved from https://www.cryptocoinsnews.com/bitcoin-banned-payment-method-adopters-will-dealt-indonesian-central-bank/

- Hare, F. (2009). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? 3, 88–105. https://doi.org/10.3233/978-1-60750-060-5-88

- Held, D. (1999) The Transformation of Political Community: Rethinking Democracy in the Context of Globalization. In I. Shapiro and C. Hacker-Cordón (eds), Democracy’s Edges, Cambridge:

Cambridge University Press.

- Higgins, S. (2017, September 28). Russia Likely to Ban Bitcoin Payments, Deputy Finance Minister Says. Coin Desk. Retrieved from https://www.coindesk.com/russia-likely-ban-bitcoin-payments-deputy-finance-minister-says/

- Hobbes, T., & Gaskin, J. C. A. (1998). Leviathan. Oxford: Oxford University Press.

- Jensen, E. (2014). Cyber Sovereignty: The Way Ahead. Texas International Law Journal 50, 275–304.

- Kleinrock, L. (2008). History of the Internet and its flexible future. IEEE Wireless Communications, 15(1), 8–18. https://doi.org/10.1109/MWC.2008.4454699

- Krasner, S. D. (2001). Abiding Sovereignty. International Political Science Review / Revue Internationale de Science Politique, 22(3), 229–251.

- Lessig, L. (2006). Code: Version 2.0. Basic Books. Retrieved from http://codev2.cc/download

- Mangoli, D. (2017, October 23). ICO Ban in Japan a “Definite Possibility". CryptoCoinsNews. Retrieved from https://www.cryptocoinsnews.com/japan-may-no-longer-be-a-safe-haven-for-icos/

- Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet. Presented at the 4th Workshop on Free and Open Communications on the Internet, San Diego (CA). Retrieved from https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben

- Pufong, M. G. (2001). State Obligation, Sovereignty, and Theories of International Law. Politics & Policy, 29(3), 478–519. https://doi.org/10.1111/j.1747-1346.2001.tb00600.x

- Senese, A., Mossé, M., Kent, G., & Sacquet, M. (2017, October 9). The Internet, private actors and security challenges. Sciences Po, Paris, France.

- Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. Chinese Political Science Review, 1(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

- S.S. Lotus – France v. Turkey (P.C.I.J. September 7, 1927). Retrieved from http://www.worldcourts.com/pcij/eng/decisions/1927.09.07\_lotus.htm

- Walker, S. (2016, November 17). Russia blocks access to Linkedin over foreign-held data. The Guardian. Retrieved from http://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data

- Weber, M. (1965). Politics as a Vocation. Fortress Press Philadelphia, PA.

[[1]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref1" \o ")- The Montevideo Convention on the Rights and Duties of States is a treaty signed at Montevideo, Uruguay, on December 26, 1933, during the Seventh International Conference of American States. The Convention codifies the declarative theory of statehood as accepted as part of customary international law.

[[2]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref2" \o ")- Professor Hinsley's book, first published in 1966, offers a general survey of the history of the theory of sovereignty, which seeks to illuminate the theory's character and function by stressing the changing social, political and economic frameworks within and between the political societies in which it has developed.

[[3]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref3" \o ")- Bull, H. (1977) The Anarchical Society: A Study of Order in World Politics, London: Macmillan.

[[4]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref4" \o ")- Andrew Vincent; Citizenship, poverty and the real will, University of Wales College of Cardiff.

First published: November 1992.

[[5]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref5" \o ")- Krasner, S. D. (2001). Abiding Sovereignty. International Political Science Review / Revue Internationale de Science Politique, 22(3), 229–251.

[[6]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref6" \o ")- Taken from: Hobbes, T., & Gaskin, J. C. A. (1998). Leviathan. Oxford: Oxford University Press.

[[7]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref7" \o ")- Encyclopedia of public international law : vol. IV.

[[8]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref8" \o ")- Klemperer, Margaret (2002). "Preserving a lost culture". The Natal Witness, 7 March 2002, p. 11

[[9]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref9" \o ")- Falk, R. (1969) The Interplay of Westphalian and Charter Conceptions of the International Legal Order. In R. Falk and C. Black (eds), The Future of the International Legal Order, vol. 1, Princeton, NJ: Princeton University Press.

[[10]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref10" \o ")- Held, D. and McGrew, A., Goldblatt, D., and Perraton, J. (1999) Global Transformations: Politics, Economics and Culture. Cambridge: Polity Press.

[[11]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref11" \o ")-  Thompson, G. (2000) Economic Globalization? In D. Held (ed.), A Globalizing World? Culture, Economics and Politics, London: Routledge.

[[12]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref12" \o ")-  In December 2013, the United Nations General Assembly adopted resolution 68/167, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication.

[[13]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref13" \o ")- Senese, A., Mossé, M., Kent, G., & Sacquet, M. (2017, October 9). The Internet, private actors and security challenges. Sciences Po, Paris, France.

[[14]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref14" \o ")- Kleinrock, L. (2008). History of the Internet and its flexible future. IEEE Wireless Communications, 15(1), 8–18. https://doi.org/10.1109/MWC.2008.4454699

[[15]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref15" \o ")- Itai Brun, Tehilla Shwartz Althsuler; The Mueller Report: What it Includes, What it Omits, and What it Teaches Publication Series: INSS Insight.

[[16]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref16" \o ")- Cory, N. (2017). The Worst Innovation Mercantilist Policies of 2016. Information Technology and Innovation Foundation. Retrieved from https://itif.org/publications/2017/01/09/worst-innovation-mercantilist-policies-2016

[[17]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref17" \o ")- Hare, F. (2009). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? 3, 88–105. https://doi.org/10.3233/978-1-60750-060-5-88

[[18]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref18" \o ")- Lessig, L. (2006). Code: Version 2.0. Basic Books. Retrieved from http://codev2.cc/download

[[19]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref19" \o ")- Walker, S. (2016, November 17). Russia blocks access to Linkedin over foreign-held data. The Guardian. Retrieved from http://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data

[[20]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref20" \o ")- Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet. Presented at the 4th Workshop on Free and Open Communications on the Internet, San Diego (CA). Retrieved from https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben

[[21]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref21" \o ")- Higgins, S. (2017, September 28). Russia Likely to Ban Bitcoin Payments, Deputy Finance Minister Says. Coin Desk. Retrieved from https://www.coindesk.com/russia-likely-ban-bitcoin-payments-deputy-finance-minister-says/

Mangoli, D. (2017, October 23). ICO Ban in Japan a “Definite Possibility". CryptoCoinsNews. Retrieved from https://www.cryptocoinsnews.com/japan-may-no-longer-be-a-safe-haven-for-icos/

Das, S. (2017, October 27). Bitcoin Banned as a Payment Method in Indonesia, Adopters Will Be “Dealt With". CryptoCoinsNews. Retrieved from https://www.cryptocoinsnews.com/bitcoin-banned-payment-method-adopters-will-dealt-indonesian-central-bank/

[[22]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref22" \o ")- Krasner, S. D. (2001). Abiding Sovereignty. International Political Science Review / Revue Internationale de Science Politique, 22(3), 229–251.

[[23]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref23" \o ")-  Hare, F. (2009). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? 3, 88–105. https://doi.org/10.3233/978-1-60750-060-5-88

[[24]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref24" \o ")- Jensen, E. (2014). Cyber Sovereignty: The Way Ahead. Texas International Law Journal 50, 275–304.

[[25]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref25" \o ")- Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. Chinese Political Science Review, 1(1), 81–93.

[[26]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref26" \o ")- Ibid

[[27]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref27" \o ")- On this topic see below references;

1. "The Tallinn Manual". Ccdcoe.org. Archived from the original on 2013-04-24. Retrieved 2013-04-20.

2. Boyle, Ashley (2012-09-24). "International law takes on cyber: significant challenges ahead". Thehill.com. Retrieved 2013-04-20.

3. "Security Think Tank Analyzes How International Law Applies to Cyber War". SecurityWeek.Com. 2012-09-04. Retrieved 2013-04-20.

4. "Politics". Mother Jones. Retrieved 2013-04-20.

5. Nakashima, Ellen (2013-03-10). "In cyberwarfare, rules of engagement still hard to define". Articles.washingtonpost.com. Retrieved 2013-04-20.

[[28]](https://www.lebarmy.gov.lb/en/content/dilemmas-state-sovereignty-international-laws-and-cyberspace" \l "_ftnref28" \o ")- Michael N. Schmitt and Liis Vihul; But what is cyber law? Texas Law Review Volume 95 - Issue 7.

**معضلات سيادة الدولة والقوانين الدولية والفضاء الإلكتروني**

مع تقدّم التكنولوجيا، تفقد الحدود الوطنية أهميتها. وبالتالي، يصبح من الضروري إعادة تحديد مفهوم السيادة وبنائها. فالمعلومات في الفضاء الإلكتروني بما يتعلّق بالحكومة، تمكّن المواطن من مراقبة الدولة وتتبّعها بشكلٍ أفضل. من ناحية أخرى، ومع إنشاء الفضاء الإلكتروني، قد يقدّم الأفراد المزيد من المعلومات حول خياراتهم للحكومة من خلال الاستفتاءات والدراسات الاستقصائية. وقد تساعد وظيفة الفضاء الإلكتروني هذه على إضفاء الشرعية على العمل الحكومي؛ لأنّه يمكن أن يستند إلى أفضليات المواطن. لهذا السبب، قد يزيد ذلك، التعبير عن التفضيلات الفردية؛ وبالتالي صورة الديمقراطية التمثيلية.

في العقود الأخيرة، وخاصة منذ نهاية الحرب الباردة، ظهرت أربعة تحديات جذرية أخرى أمام مفهوم سيادة الدولة وهي المطالب المستمرة لتقرير المصير، ومفهوم أوسع للسلام والأمن الدوليَيْن، وتقويض سلطة الدولة، والأهمية المتزايدة للسيادة الشعبية.

من نواح كثيرة، تنبع صعوبة معاصرة مركزية من تخفيف حدّة معيارَيْن لم يواجها فعليًا التحدي خلال الحرب الباردة، وهما حرمة الحدود وعدم شرعية الانفصال. طوال نصف قرن تقريبًا، كان تقرير المصير الجماعي مقتصرًا على العملية الأولية لإنهاء الاستعمار. وكانت الحدود القائمة مصونة، ولم يكن من الوارد أن تنشقّ منطقة عن الدولة، حتى لو كان ذلك بموافقة الدولة الأصلية.

لا تزال السيادة تُعدّ قاعدة أساسية في القانون الدولي حسبما يُمليها ميثاق الأمم المتحدة. وبالتالي، فإنّ السيادة بصفتها موقفًا هامشيًا معاكسًا للمعايير، مصمَّمًا لتوفير الأساس القانوني لمؤيديها بهدف إجراء أنواع مختلفة من العمليات السيبرانية الهجومية، لا تدخل في نطاق التسامح القانوني. إنّه نهج جاد، يعرضه محامون من الدرجة الأولى، وتُدافع عنه على ما يبدو عدد من الوكالات الحكومية، التي تمارس قوة كبيرة في الأوساط الإلكترونية التنفيذية والسياساتية.