STATE SOVEREIGNTY AND CYBER WARFARE IN INTERNATIONAL LAW

Dr. Jyotsna Singh, Assistant Professor, Amity Law School, Amity University Uttar Pradesh, Lucknow Campus

1. Introduction

The concept of state sovereignty, crystallized in the 1648 Peace of Westphalia, remains the primary constitutive principle of the international legal order. It denotes the competence of a state to exercise exclusive jurisdiction over its territory and its population to the exclusion of all other states. Historically, sovereignty was tied to physical borders—land, sea, and air. However, the emergence of the "fifth domain"—cyberspace—has disrupted this traditional geography.

Cyber warfare, characterized by the use of digital attacks to disrupt, damage, or destroy information systems, poses a systemic challenge to the UN Charter's framework. The central problem is that while the effects of a cyberattack may be felt within a physical territory, the "act" itself is often intangible, transborder, and difficult to attribute. This paper explores the shifting thresholds of sovereignty and whether the current international legal regime, largely designed for kinetic conflict, can effectively regulate the "grey zone" of state-sponsored cyber operations.

2. The Ontological Debate: Sovereignty as a Rule or a Principle?

In the discourse of international cyber law, a fundamental schism exists regarding the legal status of sovereignty. This is not merely an academic exercise; it determines whether a low-level "hack" that causes no physical damage is actually a breach of international law.

The debate over whether sovereignty is a "rule" or a "principle" is perhaps the most significant schism in modern international legal theory. The majority of the International Group of Experts (IGE) who drafted the **Tallinn Manual 2.0** contend that sovereignty is a primary rule of international law, the violation of which constitutes an internationally wrongful act. This position is rooted in the "Lotus Principle," which suggests that a State's jurisdiction is territorial and cannot be exercised outside its territory except by virtue of a permissive rule derived from

international custom or a convention.

Under the Tallinn Manual's **Rule 4**, a State's sovereignty extends to the "cyber infrastructure" located within its territory. This includes physical hardware—servers, routers, and fiber-optic cables—as well as the data residing on them. The legal logic here is a direct translation of traditional land-use laws: just as a foreign soldier cannot step an inch across a physical border without permission, a foreign state-sponsored packet of data cannot "enter" a domestic server to perform unauthorized functions without breaching the host State's territorial integrity.

This interpretation establishes a **strict liability threshold**. It posits that the mere unauthorized presence of a foreign state actor within another state's digital architecture is a violation. Unlike the "Use of Force" (Article 2(4)) or "Prohibited Intervention," which require a specific level of damage or coercion, a violation of sovereignty under Rule 4 requires only an **unauthorized intrusion**.

2.1. The "Low-Threshold" Implications

The "Sovereignty as a Rule" approach, as codified in the Tallinn Manual 2.0, posits that a state's digital infrastructure is not merely a tool but a sovereign asset. By establishing sovereignty as a standalone rule, international law creates a "protective shield" over the **domaine réservé**—the areas of state activity where a state exercises exclusive, independent authority. When this shield is pierced by an unauthorized state-sponsored cyber operation, the violation occurs the moment the digital "border" is crossed, regardless of the attacker's intent or the physical outcome. In traditional international law, peacetime espionage has occupied a "legal twilight zone." While states often criminalize spying within their domestic statutes, international law has historically remained silent, neither explicitly prohibiting nor permitting it. However, the "Rule-based" cyber doctrine challenges this status quo.

If a state-sponsored actor infiltrates a foreign ministry's network to silently monitor communications, the "Sovereignty as a Rule" approach classifies this as a per se violation of international law. The legal rationale is twofold:

- **The Infringement of Exclusive Control:** Sovereignty implies the exclusive right of a state to control access to its territory. Because servers and data are physically located within a state's borders, any unauthorized remote access is an exercise of authority by

a foreign power within that state's jurisdiction.

- **The Breach of Confidentiality:** Under this doctrine, the sanctity of government communications is a sovereign right. Passive monitoring is not "harmless"; it undermines the victim state's ability to conduct its internal and external affairs (its *domaine réservé*) without outside interference. Therefore, even if no file is altered and no system is crashed, the mere "presence" of the intruder constitutes a legal injury to the state's dignity and territorial supremacy.

A more complex application of this rule involves **Data Exfiltration**. In the physical world, if a foreign agent steals a paper document, the violation is clear because the state has lost a physical asset. In the cyber realm, data is often copied while the original remains perfectly intact. The system's functionality remains undisturbed, and the victim state may not even realize the data has been duplicated for months.

The "Rule-based" approach argues that this is nonetheless a breach of sovereignty for several critical reasons:

- **Usurpation of Sovereign Authority:** A state has the sole right to decide who may possess, view, or distribute its sensitive data. When another state copies that data without consent, it is usurping the victim state's sovereign authority over its intellectual and administrative property.

- **The "Intangible Property" Argument:** Modern legal theory increasingly treats state-owned data as a "sovereign asset." Just as a state has sovereignty over its natural resources (oil, minerals), it has sovereignty over its "informational resources." Exfiltrating this data is seen as a digital form of resource extraction conducted without the "permanent sovereignty over natural resources" consent required by international law.

- **Interference with Functional Integrity:** While the system still "works," its *functional integrity* has been compromised. The state can no longer rely on the confidentiality of its data to perform sovereign functions—such as national security planning or economic forecasting. This "informational insecurity" is, in itself, a violation of the sovereign state's right to operate securely within its own borders.

2.2. The Threshold of "De Minimis"

The debate over a *de minimis* threshold—derived from the legal maxim *de minimis non curat lex* (the law does not concern itself with trifles)—is the primary battlefield for scholars within the "Rule-based" camp. While there is a consensus among Tallinn adherents that sovereignty is a rule, there is a fierce disagreement over whether every "digital touch" constitutes an internationally wrongful act.

A significant faction of legal experts argues that for a violation of sovereignty to occur, the intrusion must rise above a certain level of intensity or duration. This "threshold" view is driven by the sheer technical reality of the internet. In any given second, state-owned servers are subjected to thousands of automated "pings," "port scans," and "sniffing" attempts.

Scholars in this camp argue that if every unauthorized state-sponsored "ping" were a violation of international law, the international legal system would be overwhelmed by trivial claims. They propose that an intrusion should only be considered a breach of sovereignty if it:

- **Occupies Capacity:** It consumes significant bandwidth or storage.
- **Persists:** It is not a "momentary" or "transient" contact.
- **Demonstrates Intent to Bypass:** It goes beyond mere observation and actively attempts to circumvent security protocols for a sustained period.

From this perspective, a brief scan of a government website’s public-facing vulnerabilities might be "unfriendly" or "unauthorized," but it lacks the requisite "gravity" to be labeled an illegal violation of territorial integrity.

Opposing the threshold view are the "absolutists," including many of the primary authors of the Tallinn Manual 2.0. Their argument is rooted in the fundamental nature of sovereignty as a **right of exclusion**.

In the physical world, if a foreign soldier steps one foot over a border, it is a violation of sovereignty, regardless of whether the soldier stayed for one second or one hour, or whether he caused damage. The absolutist view applies this "physicalist" logic to cyberspace. They argue that:

- **The Slippery Slope Risk:** If the international community agrees that a "little bit" of unauthorized access is legal, where is the line drawn? Does it include 1 megabyte of data? 5 minutes of access? Creating a threshold invites states to "test the fence," leading to an incremental erosion of sovereign control.

- **Injuria Sine Damno:** Under the principle of *injuria sine damno*, the legal "injury" is the violation of the right itself, not the resulting damage. The victim state's right to exclusive control over its cyber infrastructure is harmed the moment an unauthorized packet enters its system.

- **The Sanctity of the *Domaine Réservé*:** For a state to truly be sovereign, its "digital sanctuary"—the private servers and internal databases that house its national secrets—must be off-limits. Allowing *de minimis* intrusions would effectively legalize "digital trespassing," fundamentally altering the meaning of Westphalian sovereignty.

This debate often hinges on whether the breach is **territorial** or **functional**. A "territorial" breach occurs upon entry (the absolute view). A "functional" breach (the threshold view) requires that the intrusion actually interferes with the state's ability to exercise its sovereign functions.

For a research paper, this distinction is crucial. The threshold debate highlights the tension between **legal idealism** (protecting the absolute rights of states) and **diplomatic pragmatism** (recognizing that state-on-state digital interaction is constant and often harmless). If the international community moves toward an absolute rule, it raises the stakes for attribution and countermeasures; if it moves toward a *de minimis* threshold, it risks legitimizing a new era of state-sponsored "low-level" cyber interference.

2.3. Theoretical Justification: The "Usus" and "Jurisdictio"

The debate between sovereignty as a "rule" versus a "principle" is not merely semantic; it defines the existence of a **legal lacuna** (a gap in the law) in the digital age. Proponents of the "Rule-based" approach, such as the Tallinn Manual experts, argue that demoting sovereignty to a mere principle—as favored by the United Kingdom's 2018 Chatham House declaration—strips the international community of its primary tool for state accountability.

At the heart of this justification are two pillars of sovereign authority: *Usus* and *Jurisdictio*.

- **Usus (Right of Use):** This refers to a state's exclusive right to use and enjoy its territory and infrastructure. In the cyber context, it implies that a state has the sole authority to determine how its digital networks and data are utilized. Any unauthorized entry by a foreign power is a violation of this right of use.

- **Jurisdictio (Right of Administration/Authority):** This represents the state's legal authority to regulate conduct within its territory. When a foreign state conducts a cyber operation—such as modifying a database or observing private communications—it is exercising a form of "jurisdiction" over that infrastructure. Since two states cannot simultaneously hold exclusive jurisdiction over the same physical server, the foreign state's action is an unlawful usurpation of the victim state's *jurisdictio*.

By framing sovereignty as a rule, the law protects both the physical asset (*usus*) and the legal authority (*jurisdictio*) attached to it.

The primary criticism of the "Principle-only" view (the restrictive approach) is that it creates a sanctuary for "low-level" cyber aggression. If sovereignty is not a rule, then a cyber operation that does not reach the high threshold of a "Use of Force" (causing physical death or destruction) or a "Prohibited Intervention" (coercive interference in elections) is technically not "illegal" under international law.

This leaves states vulnerable to a wide array of harmful but "sub-threshold" activities, including:

- The theft of massive amounts of intellectual property.

- The disruption of social order through the manipulation of public service data.

- Economic espionage that destabilizes national markets.

Under the "Rule-based" approach, these actions are violations of international law from the first packet of data. By defining them as illegal, the international community ensures that there is no "grey zone" where states can act with impunity.

The most critical practical consequence of defining sovereignty as a rule is the activation of the **Law of State Responsibility**. Under international law, a state can only take

"countermeasures"—actions that would otherwise be illegal, such as a retaliatory hack—in response to a "prior internationally wrongful act" by another state.

- **The Deterrent Framework:** If sovereignty is a rule, State B can legally respond to State A's intrusion with its own proportionate cyber operations to force State A to stop.

- **The Principle-only Problem:** If sovereignty is only a principle, State A's intrusion is not "wrongful" in a legal sense. Therefore, State B has no legal right to take countermeasures. Its only options are "retortions" (unfriendly but legal acts like sanctions or expelling diplomats), which are often insufficient to stop a sophisticated cyber campaign.

Ultimately, the Tallinn proponents argue that the "Rule-based" approach is essential for the **predictability and stability** of the international system. Without a rule of sovereignty, cyberspace becomes a "lawless frontier" where the only limits on state behavior are technical capacity and the fear of kinetic escalation. By anchoring cyber operations in the rule of sovereignty, international law provides a structured, legalistic pathway for dispute resolution and state behavior.

2.4. The Functionalist Critique: Beyond "Physicalist" Orthodoxy

While the "Sovereignty as a Rule" approach offers a clear-cut legal boundary, a significant body of critics—including prominent legal advisors from the United Kingdom, the United States, and several academic circles—argues that this framework suffers from a profound **"architectural mismatch."** By attempting to impose 17th-century Westphalian border logic on a decentralized, 21st-century network, the territorial approach fails to account for the unique ontology of cyberspace.

Critics argue that the Tallinn Manual "over-physicalizes" the digital world by treating data as if it were a physical object or a tangible trespasser. In reality, data is "weightless," non-rivalrous, and infinitely replicable. Unlike a physical border crossing, where a person's location is binary (either inside or outside a territory), digital data is often fragmented. In the era of **cloud computing**, a single government file may be broken into "shards" stored across servers in Ireland, Singapore, and the United States.

From a functionalist perspective, applying strict territorial rules to such a fluid environment is

not only impractical but legally incoherent. If data fragments are stored globally, whose territorial sovereignty is violated when that data is accessed? Critics suggest that a "territorial-only" rule leads to an absurdity where international law depends more on the physical location of a server rack than on the nature of the act itself.

The most potent argument from this camp is that a violation of sovereignty should require a **functional impact** rather than mere unauthorized entry. This view shifts the focus from *where* the act happened to *what* the act did.

According to this standard, an intrusion only rises to the level of a sovereign violation if it prevents the State from exercising its essential functions. Examples of such functions include:

- Maintaining the integrity of the electoral process.
- Safeguarding the national power grid or water supply.
- Protecting the stability of the central banking system.

Under the functionalist view, a "passive" hack—such as a foreign state-sponsored actor gaining access to a government database but taking no action to disrupt it—would not necessarily be a violation of sovereignty. Instead, it would be treated as **espionage**, which international law has historically tolerated as a routine part of statecraft. By requiring a functional disruption, this approach prevents the "over-legalization" of cyberspace and maintains a higher threshold for what constitutes an internationally wrongful act.

Critics also point to actual state practice to support their view. Many of the world's leading cyber powers conduct "low-level" operations daily. If every unauthorized entry were a violation of sovereignty, then almost every major state would be in a perpetual state of international illegality.

The functionalist approach acknowledges this "grey zone" as a necessary safety valve. It allows for the collection of intelligence—a vital component of national security—without triggering the heavy legal machinery of countermeasures and state responsibility. This "Restrictive Approach" argues that by keeping the threshold high, we prevent minor digital skirmishes from escalating into full-blown international crises.

Finally, functionalists argue that the principle of **non-intervention** (prohibited intervention) already provides sufficient protection. If a cyber operation is coercive and targets a state's *domaine réservé* (like its elections), it is already illegal. Therefore, creating a separate, lower-threshold "sovereignty rule" is redundant and risks stifling the flexibility needed for states to navigate the complex realities of modern intelligence gathering and digital diplomacy.

III. The Threshold of "Prohibited Intervention"

When a cyber operation does not cause physical destruction (thus not being a "use of force"), it is analyzed under the principle of **non-intervention**. For a cyber act to be a prohibited intervention, it must satisfy two criteria:

1. **Domaine Réservé:** The act must interfere with matters in which each state is permitted, by the principle of state sovereignty, to decide freely (e.g., elections, tax policy, or national security).

2. **Coercion:** The act must be coercive.

In the digital age, "coercion" is being redefined. For example, if a state uses cyber means to manipulate an election's vote tally, it is coercing the sovereign will of the victim state. However, simple "propaganda" or "misinformation" disseminated via social media often falls below this threshold because it targets the *minds* of the populace rather than the *mechanics* of the state, making it a "grey zone" activity that currently lacks clear legal prohibition.

IV. Cyber Operations as a "Use of Force" (Article 2(4))

Article 2(4) of the UN Charter prohibits the "threat or use of force against the territorial integrity or political independence of any state." The challenge lies in the fact that the Charter was written with kinetic weapons (bombs, bullets) in mind.

To bridge this gap, international law utilizes the **"Scale and Effects" test** established by the International Court of Justice (ICJ) in the *Nicaragua* case. If the scale and effects of a cyber operation are comparable to those of a kinetic attack, it is classified as a "use of force."

- **Physical Damage:** If a hack causes a dam to open and flood a village, or causes a power grid to explode, it is a use of force.

- **The Economic Gap:** Currently, there is no consensus on whether a cyberattack that causes massive *economic* collapse (e.g., wiping out a nation's banking records) without physical death or destruction constitutes a "use of force." Most Western states argue it does not, though this is a point of significant legal tension.

V. The Attribution Crisis and State Responsibility

Even if a cyberattack clearly violates sovereignty, the victim state must prove *who* did it. In international law, the **Articles on State Responsibility (ASR)** dictate that a state is responsible for the acts of its organs (e.g., its military) or those acting under its "effective control."

Cyberspace allows for "plausible deniability." States often use "hacktivists" or private contractors to carry out attacks. The ICJ's "Effective Control" test (from the *Nicaragua* case) is incredibly high; it requires proving that the state issued the specific instructions for the illegal act. This creates a legal vacuum where states can launch devastating cyber operations through proxies and remain technically immune from legal "responsibility" because the evidentiary link is too weak for a court of law.

REFERENCES

I. Primary Legal Authorities (Treaties and Judgments)

- **UN Charter**, art. 2, para. 4 (Prohibition of the use of force).
- **UN Charter**, art. 51 (The right to individual or collective self-defense).
- **Military and Paramilitary Activities in and against Nicaragua** (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, p. 14. *(The foundation for the "scale and effects" and "effective control" tests).*
- **Corfu Channel Case** (United Kingdom v. Albania), Assessment of Amount of Compensation, ICJ Reports 1949, p. 244. *(The foundational case for the "Due Diligence" principle).*
- **Island of Palmas Case** (Netherlands v. USA), Reports of International Arbitral Awards, Vol II, 1928. *(Defining sovereignty as independence and the right to exclude).*

II. The "Tallinn Manual" Framework (Rule-Based Approach)

- **Schmitt, Michael N. (Ed.).** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

  Focus on Rule 4 (Violation of Sovereignty), Rule 6 (Attribution), and Rule 71 (Due Diligence).

- **Schmitt, Michael N., and Liivoja, Rain.** "The Tallinn Manual and the States." *Exeter Centre for International Law*, Working Paper Series, 2018.

III. The Functionalist & Restrictive Critique (UK/US Views)

- **Wright, Jeremy.** "Cyber and International Law in the 21st Century." *Speech at Chatham House*, May 23, 2018.

  This is the primary source for the argument that sovereignty is a "principle" rather than a standalone "rule."

- **Egan, Brian J.** "International Law and Stability in Cyberspace." *Berkeley Journal of International Law*, Vol. 35, No. 1, 2017. *(Reflecting the U.S. State Department's legal position).*

- **Koh, Harold Hongju.** "International Law in Cyberspace." *US Department of State Archive*, 2012.

IV. Scholarly Journals & Monographs (Theoretical Justification)

- **Buchan, Russell.** *Cyber Espionage and International Law*. Oxford: Hart Publishing, 2018. *(Crucial for the "Passive Espionage" section).*

- **Delerue, François.** *Cyber Operations and International Law*. Cambridge University Press, 2020. *(Analyzes the "Usus" and "Jurisdictio" concepts in cyber contexts).*

- **Tsagourias, Nicholas.** "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012.

- **Watts, Sean.** "Low-Intensity Cyber Operations and the Principle of Non-Intervention." *International Law Studies*, Vol. 90, 2014. *(Focuses on the "Grey Zone" and coercive intent).*

- **Ziolkowski, Katharina.** "General Principles of International Law as Applicable in Cyberspace." *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2013.

V. Reports & Institutional Documents

- **UN GGE Report.** *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (2015).

- **International Law Commission (ILC).** *Draft Articles on Responsibility of States for Internationally Wrongful Acts (ASR)*, 2001. *(Essential for the section on Attribution and Article 8).*