"Cyber-espionage in International Law": Confusion versus Prohibition

In *Cyber-espionage in International Law*, Thibault Moulin offers a clear perspective of the practice of cyber-espionage, its challenges, and its legal status. While there has been an explosion of research on cybersecurity and associated acts, such as espionage and intelligence, this small volume offers important guidance for scholarship on cyber-espionage and for legal scholars interested in the topic specifically.

Moulin describes cyber-espionage as comprising three characteristics: collection of data, collection without permission, and collection through computer networks. This is distinct from cyber-sabotage, which seeks to damage or disrupt. Cyber-espionage is neither prohibited in most cases nor condoned by both domestic and international entities (outside of a few specifics)—with normative silence dominating.

This volume should speak to both legal practitioners of cyber-espionage and, more importantly, theorists and students of cybersecurity. Moulin offers an important word of caution for the idea that cybersecurity practice is part of the intelligence cycle.[1] As the book demonstrates, there is a core difference between cyber-intelligence and cyber-espionage. For Moulin, intelligence refers to the aggregation/contextualization of data to guide decision-making. As Moulin notes, citing US Department of Defense guidance, “The intelligence cycle consists of five phases.... The fourth phase is ‘analysis’: the information is put in context and the ‘finished intelligence’ is produced” (p. 16). This connection between a finished product and data is often missed by theorists of cyber-intelligence. Intelligence suggests that there is intake and processing of data collected, but this is mostly not true in cyberspace. Petabytes of data go without examination. Countries collect massive amounts of data with no ability to analyze the data collected. There is the hope that one day artificial intelligence might sort out the challenge, but the fantas-
ies appear more in the world of James Bond than in reality.[2]

Since the practice of cyber-espionage focuses more on hoovering up data than on producing actionable intelligence data and does not facilitate analysis, it is difficult to note a change in strategy enabled by cyber-espionage. Despite most cyber incidents being cyber-espionage (when compared to cyber disruption and degradation), there is little evidence of any intelligence in this practice.[3] Instead, cyber-espionage mostly includes breaking into closed systems, surveilling communications, and observing criminal enterprises. Thus, scholars must recalibrate their views on cyber-espionage to properly understand how the practice affects international relations. There are few concrete functions of espionage banned specifically by international law with Moulin citing the prohibition on targeting data in transit from diplomatic missions from the Vienna Convention on Diplomatic Relations. Beyond this, the international record is lacking in firm prohibitions.

Returning to the focus of international law, is cyber-espionage illegal? Not automatically, since that depends on the conditions, the view of territorial sovereignty, and whether a “wrongful act” was committed. For Moulin, “cyber-space cannot be described as a territory, i.e. this ‘portion of terrestrial space, delineated by borders, and where [state] authority and jurisdiction do apply’” (p. 27). This makes the connection to sovereignty tenuous, but it is an open legal question that is constantly evolving, including in the forthcoming revised Budapest convention.[4]

The other key issue for Moulin is coercion. Does the event allow for coercion (forceful change of behavior) to be applied to the target? Moulin notes that state sovereignty can be violated if methods of coercion are applied and if the act has a bearing on a state’s domain reserve (i.e., does it apply to an area where a state is free from international obligations?). This issue addresses when and if force is leveraged, and what sort of implications this might have for something like cyber insurance or the activation of international treaties (such as Article 5 of the North Atlantic Treaty Organization [NATO]).

The overall guidance Moulin offers is that “normative silence here can neither be described as the tacit endorsement of cyber-espionage, nor as a prohibition” (p. 57). This lack of clarity is disappointing but realistic for a body of law that mostly involves domestic application of criminal law to international events and tricky considerations of sovereignty. If the cyber-espionage incident involved the use of force, or coercion, the practice might be prohibited under both domestic and international law, but this is a rare and unsettled legal landscape.

The Tallinn Manual clearly states that international law does apply to cyberspace. The challenge is to specify when and how.[5] The other challenges are that there is not a lot of case law and that there are no examples to guide practice since cyber conflict is relatively new. In fact, as Moulin notes, neither the UN Group of Government Experts or the Open-Ended Working Group mention cyber-espionage, but they do reaffirm that territorial sovereignty does apply. As future examples are analyzed and cyber events occur, the law governing cyber-espionage may change and evolve, but there are few examples that guide what might be common law for cyber-espionage at this moment. This is what makes cybersecurity such an interesting field; it evolves as we all engage and study the practice.

Methods of coercion are not permitted under international law because they can serve as an intervention, but is cyber-espionage a method of coercion? This is a pressing issue in the academic literature. My own past work notes that cyber coercion through espionage is possible but unlikely.[6] As Moulin asserts, “if states felt that cyber espionage was a breach of international law, it is arguable that they would have resorted to countermeasures” (p. 102). More work needs to be done to
uncover just how coercion through digital espionage might work and its escalatory (or retaliatory) processes. Regardless, no state, besides maybe France, according to Moulin, considers a cyber operation a use of force without physical destruction or harm.

Moulin’s *Cyber-espionage in International Law* is an important piece of work. Certainly, more research needs to be done in the field, but scholars of cyber conflict must understand the complexities of international law before theorizing about the impact and legality of cyber-espionage, making this volume a valuable resource. This book is firm in its conclusion: “cyber-espionage is a dematerialised and deterritorialised activity, and it cannot be considered analogous to physical incursion onto the territory of another State—even if infrastructures are indeed based there” (p. 65). But there are specific conditions under which cyber-espionage is unlawful. This means that it is the responsibility of individual states to construct laws to outlaw cyber-espionage under domestic law. It also means that states might avoid binding laws and resolutions since this will tie their hands in the future.

There is no cyber revolution but rather evolution. Computational power is actively altering the natural practice of intelligence and security, but this is neither new nor transformative. Without an associated revolution in data analysis and metrics, there is little evidence that we can even witness these changes, let alone assess their impact on international practice.

Notes


[3]. In the latest version of the Dyadic Cyber Incidents dataset, just over 60 percent of cyber incidents between 2001 and 2020 are espionage in nature. See Ryan C. Maness, Brandon Valeriano, Kathryn Hedgecock, Jose M. Macias, and Benjamin Jensen, “Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID),” *Cyber Defense Review* 8, no. 2 (2023): 65-90.


If there is additional discussion of this review, you may access it through the network, at https://networks.h-net.org/h-diplo


URL: https://www.h-net.org/reviews/showrev.php?id=59831

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.