State-sponsored cyber operations and international law: book review of Henning Lahmann, Unilateral Remedies to Cyber Operations (Cambridge University Press, 2020) and François Delerue, Cyber Operations and International Law (Cambridge University Press, 2020)

Mika Hayashi, William Letrône

State-sponsored cyber operations and international law: book review of Henning Lahmann, Unilateral Remedies to Cyber Operations (Cambridge University Press, 2020)…

Hayashi, Mika

Letrône, William

(Citation)
International Cybersecurity Law Review,2:195-200

(Issue Date)
2021-04-26

(Resource Type)
journal article

(Version)
Accepted Manuscript

(URL)
https://hdl.handle.net/20.500.14094/0100476686

State-Sponsored Cyber Operations and International Law: Book review of Henning Lahmann, *Unilateral Remedies to Cyber Operations* (Cambridge University Press, 2020) and François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020)

1. Introduction

There are increasing numbers of cybersecurity incidents for which foreign governments, and not private hackers, are named as perpetrators. In presence of these cybersecurity incidents, how to develop programs to defend the targets against such operations and ensure the resilience of cyber assets is the immediate concern for computer programmers. For a targeted state, an immediate concern at a time of such cybersecurity incident is how to react, in order to stop the operations and minimize the damage. For lawyers that look at these cases through the lens of public international law, one of the immediate questions to answer is what kind of reactions can be taken by a targeted state without breaking law. *Unilateral Remedies to Cyber Operations* by Henning Lahmann [1], in its entirety, and *Cyber Operations and International Law* by François Delerue [2], partially, explore answers, and provide insights, into this question.

The type of cybersecurity incidents described in the previous paragraph possesses two important characteristics. First, these incidents are orchestrated by foreign governments, definitely or allegedly. To use a short term, these are *state-sponsored* cyber operations. This delimitation is important in the legal discussion concerning reactions by targeted states, because what measures a targeted state can lawfully take against another state is inevitably different from measures it can lawfully take against private hackers. The former measures, available to a targeted state in its inter-state relations, and the corresponding part of public

international law, are set as a central issue in both books reviewed [1, p. 20] [2, p. 37]. Of course, the legal attribution of a cyber operation to a foreign government is difficult in concrete cases.[1] That is, whether any cybersecurity incident was conducted or sponsored by a foreign government is almost impossible to learn for certain, unless the responsible state makes a confession. Nevertheless, such state-sponsored cyber operations remain quite conceivable and believed to be in existence. A focus on the state-sponsored cyber operations in a legal discussion is thus justified. Second, the cybersecurity incidents discussed in this review are low-intensity operations that do not manifest the destructive force of an "armed attack." This delimitation is also important, because cyber operations of high intensity comparable to an armed attack must be evaluated in light of the branch of law pertaining to use of force,[2] which involves Article 2(4), and eventually Article 51, of the Charter of the United Nations. However, cases reported or observed rarely have such high intensity, as confirmed by an article from the previous volume of this Review [3, p.116].[3]

2. Assessment tools for the state-sponsored low-intensity cyber operations

[1] The question of attribution is combed through by Delerue as a factual question [2, pp. 55-85], then as a legal question [2, pp. 87-108]. Lahmann addresses this question in his proposal of a new legal framework for cyberspace [1, pp. 277-279].

[2] According to this distinction, the high-intensity cyber operations by foreign governments are addressed by Lahmann and Delerue in separate sections in their books [1, pp. 47-112] [2, pp. 273-342, 460-487].

[3] Lahmann [1, p. 31] and Delerue [2, p. 41] hold the same view. Authors focusing on high-intensity operations also concur with this observation, e.g., [4, p. 104].

Extracting information and data from the servers located in a foreign state, without causing any immediate and identifiable damage or injury, is a typical low-intensity cyber operation. In the same vein, mass online disinformation operations launched by a state to influence a foreign electorate do not cross the threshold of use of force, either. Still, against such an operation, a targeted state might wish to "hack-back" actively [1, pp. 126-128], or it might wish to implement a sanction in a non-cyber context [2, p. 433]. In assessing the lawfulness of these responses, it is important to determine whether the cyber operations that prompted such responses in the first place are unlawful. The two books reviewed in this article have very different approaches to this question of the legality of the low-intensity cyber operations sponsored by foreign governments. Accordingly, they have very different suggestions about the possible responses available to targeted states.

The clear and exclusive focus of the first book is on the principle of non-intervention. Lahmann does not propose to change or adapt the traditional principle of non-intervention; he keeps the traditional threshold for determining the illegality of a state-sponsored malicious cyber operation. Hence, for an action to be considered an illegal intervention, the action in question must be of coercive character.[4] Thus, for example, a 2014 case of the hacking of Sony Pictures Entertainment, an American private company, does not qualify as a violation of this principle; there was no coercive effect on the U.S. government in the case [1, p. 36]. An extraction of data located in a targeted state for the purpose of election interference leads to a similar

[4] Coercion as a necessary factor in order for an act to constitute an illegal intervention is firmly established, e.g., [5, I-76].

assessment; such a cyber operation alone, the data extraction, is unlikely to coerce the targeted state to change its behaviour in any way. A related but separate question arises for a case where "the extracted emails *were employed to distort* the public's perception of one candidate [1, p. 40]."[5] The essence of this question is whether some forms of cyber operations "should be regarded as unlawful violations of the sovereignty of the targeted state, *without the further need to establish coercion* [1, p. 38]."[6] The analysis is short, and the conclusion is cautious: Only by extending the discussion to self-determination in a human rights treaty, there might be a room to argue an election interference that manipulates the decision-making process in a targeted state is a violation of the sovereignty of that state [1, p. 41]. This exclusion of sovereignty as an assessment tool for cyber operations by a foreign government seems to be a reaction to the recent controversy over the operational value of sovereignty in the cyber context [1, p. 37].[7]

The second book cast a much wider net to assess state-sponsored cyber operations, and also discusses election interferences extensively. To begin with, this analysis employs "territorial sovereignty" as an independent tool of assessment, in addition to the principle of non-intervention. Thus, the first contrast it produces with the analysis of the first book is that "a mere penetration into a computer system located on the territory of a foreign State constitutes a violation of the territorial sovereignty" of the targeted state [2, p. 272]. Viewing sovereignty as an independent rule which can be breached in the cyber context is in line with France's broad interpretation of this rule for cyber operations [7]. In fact, the scepticism observed in a

[5] Emphasis added.

[6] Emphasis added.

[7] See a speech by the British Attorney General at Chatham House in 2018 [6].

contentious statement of the British Attorney General about its operational value in the cyber context [6] is dismissed by the author as "relatively isolated [2, p. 221]." According to this analysis that employs the territorial sovereignty as an assessment tool, whether there was an intention to coerce the targeted state to act in a certain way does not matter. As a result, all ten listed cases of State-sponsored cyber operations from the period 2009-2017 are characterized as cases of violations of territorial sovereignty [2, pp. 500-501]. One of them is the hacking of Sony Pictures Entertainment followed by the public release of stolen document.

Next, Delerue also casts a wider net to capture state-sponsored cyber operations by using a different criterion for determining coercion in the principle of non-intervention. In the first book, when examining the Sony Picture Entertainment case, Lahmann appears to consider the perception of the targeted state and the resulting change in its behaviour as requirements for coercion. He writes: "Had the US Government felt compelled to ban the movie [a comedy about the leader of North Korea that Sony Picture Entertainment was making] in order to prevent further harm," the case would have been a case of coercion and the violation of the principle of non-intervention [1, p. 36]. By way of contrast, the only criterion used to evaluate a coercive character of a cyber operation in the second book is the intention of the sponsoring state. Thus, if a cyber operation is conducted as "an attempt to coerce the targeted State by directly or indirectly interfering" in the targeted state, it constitutes coercion and can be considered as a violation of the principle of non-intervention [2, p. 235]. The analysis of the two cases of election interferences, the cyber operations against the US presidential elections in 2016 and the cyber operations against the French presidential elections in 2017, are illustrative. The extraction of data by the cyber operations in both cases is seen as violations of the territorial sovereignty, of the United States and of France, respectively [2, p. 250, p. 254].

The public release of the stolen data with an objective of changing the course of electoral process in both cases is then separately assessed; they are instances of violations of the principle of non-intervention [2, p. 250, p. 254].

3. Assessment tools for the reactions of a targeted state

Given this striking difference in the presentation of basic legal frameworks in the two books, the analyses that follow regarding the reactions of targeted states are also structured very differently. In the second book, as long as there is some type of meddling with data located in a targeted state, there is a high possibility that that cyber operation is illegal. This means a vast majority of cyber operations launched against a targeted state and sponsored by a foreign government are indeed illegal [2, p. 272]. In terminologies of the law of state responsibility, the targeted state becomes an "injured" state [8]. Therefore, what an injured state is entitled to do and claim in this branch of law is what must be examined in detail [2, pp. 381-421] in discussing the range of measures that can be taken by a targeted state. The question whether a targeted state is permitted to make a reaction where this reaction itself is also a violation of international rules is answered from the same perspective. The answer is positive, in that the targeted state is entitled to take countermeasures. These are measures that are unlawful themselves, of which wrongfulness is nevertheless precluded because of the preceding violation against the targeted – now injured – state [8]. These legal tools should offer a sufficient framework to evaluate reactions by a targeted state. Consistent with this view, Delerue makes an extensive analysis of the concept of countermeasures and their conditions, as applied to the reactions of targeted states in the context of low-intensity cyber operations by foreign governments [2, pp. 433-460]. In accordance with the assessment that this alone can

deal with a majority of cases where low-intensity cyber operations prompt reactions, other types of "circumstances precluding the wrongfulness" are given a marginal treatment, subject to a much more cursory examination [2, pp. 343-351].

In contrast, the first book cannot follow the same path, because only a tiny fraction of cybersecurity incidents can qualify as violations of the principle of non-intervention in that analysis. Unlike the second book, the territorial sovereignty in the first could not be relied upon to label a low-intensity cyber operation as illegal [1, p. 262]. Against this background, countermeasures cannot be the most useful tool to justify the reactions to "pure access operations" when the reactions themselves constitute unlawful measures [1, p. 124]. As a result, while countermeasures are explored at some length [1, pp. 113-200], another legal tool is given a special attention: necessity defence in the law of state responsibility [1, pp. 201-257]. The advantage of this tool, in comparison to countermeasures, is also clear when one is reminded of the attribution problem. In case of a countermeasure, the targeted state has to know the foreign government responsible for the cyber operation. In a necessity defence, there is no need for that knowledge. The response is directed against the immediate source of the incident, which does not have to be a state. Nevertheless, Lahmann seems very much aware that the necessity defence is supposed to deal with truly exceptional cases. He therefore admits that it does not sit well with foreseeable, frequent operations such as cyber operations of the kind in question [1, pp. 265-266]. Accordingly, the last two chapters before the concluding chapter in the book explore proposals of new legal frameworks that may capture more readily both the low-intensity cyber operations and the reactions to them [1, pp. 267-281].

4. Concluding remarks

One could of course raise questions on each of these books. Is it appropriate to brush aside the sovereignty in the debate, as the first book does?[8] Is it appropriate to focus, as the second book does, on the intention of the foreign government in the assessment of the coercion on a targeted state, in order to determine whether the cyber operations constituted a prohibited intervention? That there must be an intention to coerce is undisputed. However, the view does not touch upon a few other aspects of coercion that are regularly debated for the principle of non-intervention. Indeed, provided that the coercion must be intended, how, exactly, that intention is formulated and expressed,[9] or what the actual result of that intended coercion is[10] can be important in the assessment.

Beyond these technical questions, the combined reading of the two books confirms us something essential for lawyers to work on. States agree that international law applies to cyber operations in principle [14] [15] [16]. International lawyers also agree that it does [1, p. 21] [2, pp. 1-27] [17]. Yet, when it comes to concrete cases, there is no shared understanding to make the law operational. Currently, if targeted by cyber operations, states still need to seek measures

[8] In discussing the election interferences, Gaeta P et al [9] explicitly cautions that there are other fundamental principles to be examined, "even in those cases where the non-intervention principle is not breached [9, p. 56]."

[9] It is taken into account in, e.g., [10, p. 160].

[10] It is taken into account in, e.g., [11, para. 25]; [12, p. 268]. In the cyber context, [13, pp. 52-53].

of self-help in the sea of uncertainty. For this reason, among many others, the reviewed books are welcome contributions to the debate.

References

1. Lahmann H (2020) Unilateral remedies to cyber operations. Cambridge University Press, Cambridge
2. Delerue F (2020) Cyber operations and international law. Cambridge University Press, Cambridge
3. Assaf A, Moshnikov D et al (2020) Contesting sovereignty in cyberspace. International Cybersecurity Law Review 1:115-124. https://doi.org/10.1365/s43439-020-00004-5
4. Roscini M (2014) Cyber operations and the use of force in international law. Oxford University Press, Oxford
5. Vitzthum W, Proelß A eds (2019) Völkerrecht, 8th edn. De Gruyter, Berlin
6. Wright J (2018) Cyber and international law in the 21st century. Available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. Accessed 25 March 2021
7. Ministère des armées français (2019) International law applied to operations in cyberspace (10 April 2019). Available at https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international. Accessed 25 March 2021
8. International Law Commission (2001) Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Accessed 25 March 2021

9. Gaeta P et al (2020) Cassese's international law, 3rd edn. Oxford University Press, Oxford.
10. Corten O, Dubuisson F et al (2017) A critical introduction to international law. Editions de l'Université de Bruxelles, Brussels
11. Kunig P (2018) Intervention, prohibition of. In: Max Planck encyclopedias of international law. Available at https://opil.ouplaw.com/home/MPIL. Accessed 23 March 2021
12. Combacau J, Sur S (2016) Droit international public, 12e édn. LGDJ, Paris
13. Tsagourias N (2020) Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace. In: Broeders D and van den Berg B (eds) Governing cyberspace: behavior, power and diplomacy. Rowman & Littlefield, Lanham, pp. 45-63
14. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (2013). https://undocs.org/A/68/98. Accessed 27 March 2021
15. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174 (2015). https://undocs.org/A/70/174. Accessed 27 March 2021
16. UN Doc A/RES/70/237 (2015). https://undocs.org/A/RES/70/237. Accessed 27 March 2021
17. Schmitt M (2017) Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, Cambridge