PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 2 Number 4 December 2023

Comments on Speech by the Attorney General of UK on International Law in Cyberspace

Jiarong Fu[1]

[1] School of Cyber Science and Engineering, Wuhan University, Wuhan, China
Correspondence: Jiarong Fu, School of Cyber Science and Engineering, Wuhan University, Wuhan, China.

doi:10.56397/SLJ.2023.12.06

Abstract

In a significant address delivered at the Chatham House, the Attorney General, the Rt Hon Suella Braverman QC MP outlined the United Kingdom's position on international law's application in cyberspace. This speech marks a pivotal statement on a crucial topic, following a similar speech by her predecessor in 2018.

The speech comprises six sections, with a focus on the core non-intervention principle, its application to key sectors, and avenues for response. Braverman's stance on this principle is heavily intertwined with the UK's denial of sovereignty's obligatory nature in cyberspace, which distinguishes it from the majority of countries advocating for sovereignty-based obligations.

While emphasizing the importance of the non-intervention principle, the UK offers a broader interpretation of the "coercion" element, which may inadvertently complicate the distinction between sovereignty and non-intervention principles. Braverman provides illustrative examples of potential non-intervention principle violations in critical sectors, facilitating discussions for more specific guidance.

Notably, the speech suggests a leaning toward collective countermeasures without explicitly endorsing their legality, further adding to the international discourse's complexity. Collective countermeasures remain a contentious topic, with various nations holding contrasting positions.

In conclusion, the UK's proactive approach to shaping international norms in cyberspace offers valuable insights for other nations. While the UK's stance warrants careful consideration, nations like China must actively engage in research, promote their positions, foster international cooperation, and navigate the evolving landscape of international law in cyberspace. This evolving discourse is crucial for establishing an equitable and secure global digital environment.

Keywords: Suella Braverman, the Attorney General, international law, cyberspace, non-intervention principle, sovereignty, coercion, cyber norms, response options, collective countermeasures, international norms, cyber hegemony, cybersecurity, sovereignty

1. Introduction

On May 19, the Attorney General, the Rt Hon Suella Braverman QC MP delivered a speech at

the Chatham House in the United Kingdom, titled "International Law in Future Frontiers." In her address, she elaborated on the UK's stance regarding the application of international law in cyberspace, with a particular focus on the non-intervention principle, its application to key sectors, and avenues for response. This speech follows a similarly important position statement on the same theme made by her predecessor, Jeremy Wright, in May 2018 at Chatham House.

The speech is divided into six sections, with the "Shaping the International Order" section emphasizing how the UK considers the application of international law in cyberspace during peacetime, particularly focusing on the non-intervention principle, its application to key sectors, and avenues for response.

In the "The rule on non-intervention" section, Braverman stated that the UK's position is as follows: the non-intervention principle provides a clear international legal basis for assessing the legitimacy of a state's conduct in cyberspace during peacetime. It serves as a benchmark for evaluating legitimacy, assigning responsibility, and calibrating response measures. Braverman explained two specific reasons for the crucial significance of the non-intervention principle in cyberspace and reaffirmed the UK's stance in denying the obligatory nature of sovereignty in cyberspace.

In the "Threshold for a prohibited intervention" section, Braverman explains that, like some other countries, the United Kingdom agrees that the core element of the non-intervention principle is coercion. She argues that coercion can extend beyond "one state compelling another state into a specific act or omission." Essentially, if intervention in another state's affairs is forceful, dictatorial, or otherwise coercive, depriving a state of control over matters allowed by the principle of state sovereignty, it is illegal.

In the "Illustrative Examples" section, Braverman provides non-exhaustive examples of conducts that would breach the rule on non-intervention in four of the most critical areas impacted by disruptive cyber conduct:

1.1 Energy and Medical Sectors

Foreign covert cyber actions that coercively restrict or obstruct the provision of essential medical services or essential energy supplies would contravene the non-intervention principle. This may encompass:

1) Interrupting systems that manage emergency medical transport, such as dispatch services.
2) Causing the function cessation of hospital computer systems.
3) Disrupting the supply chains for essential medicines and vaccines;
4) Preventing the supply of power to housing, healthcare, education, civil administration, and banking facilities, as well as essential medical infrastructure.
5) Damaging or obstructing pipelines, interchanges, and depots, resulting in the national-level cessation of the energy supply chain or hindering the operation of power generation infrastructure.

1.2 Economic Stability

Covert foreign cyber actions that coercively interfere with a nation's management of its domestic economy or impede the freedom to provide critical domestic financial services to the country's financial system would violate the non-intervention principle. Such cyber actions may include undermining the fundamental capabilities to control a nation's implementation of monetary policy or the collection and distribution of revenue (e.g., through taxation) and disrupting systems that support the overall economy, such as lending, savings, and insurance.

1.3 Democratic Processes

Covert foreign cyber actions that coercively interfere with the freedom and fairness of electoral processes would constitute prohibited intervention. Similarly, each activity needs to be evaluated based on its specific circumstances, but such activities may include:

1) Actions aimed at disrupting systems that oversee the counting of votes to change the election outcome.
2) Actions that completely undermine another country's ability to hold elections, for instance, by causing system failures that impede voter registration.

In the "Response Options" section, Braverman emphasizes that various effective response options are available, whether or not cyber activities constitute internationally unlawful acts. While countries can pursue remedies through the courts, including accepting the jurisdiction of international courts, Braverman highlights

that response measures do not need to match the nature of the threat (i.e., non-cyber measures can be used to counter unlawful conduct in the cyber domain). Faced with hostile and unlawful cyber intrusions, some countries may lack the capacity for effective independent responses, and it is open to States to consider how the international law framework accommodates, or could accommodate, calls by an injured State for assistance in responding collectively.

In the "Free, Open, Peaceful, and Secure Cyberspace" section, Braverman outlines additional efforts the UK is undertaking to promote a free, open, peaceful, and secure cyberspace, beyond applying international law frameworks. She underscores the importance of coordination and cooperation among nations.

Finally, Braverman underscores the importance of the application of international law and provides an outlook on the UK's future work in this field, expressing a desire to collaborate closely with states who share the same ambition to shape and strengthen the international order in future frontiers.

2. Analysis

Suella Braverman's speech is not a generic, superficial presentation of the UK's positions on various issues related to international law in cyberspace. Instead, it builds upon Jeremy Wright's 2018 speech, shifting the focus from the threat of "cyber warfare" to the regulation of peacetime cyber activities, with a particular emphasis on the non-intervention principle, its application to key sectors, and avenues for response. The choice of rules and principles to reaffirm or clarify in this speech evidently takes into account the backdrop of the Russia-Ukraine conflict, carrying a certain political response.

2.1 Regarding Sovereignty

Suella Braverman reaffirmed the UK government's position, expressed by her predecessor Jeremy Wright, in denying the obligatory nature of sovereignty in cyberspace. She refused to acknowledge that the principle of sovereignty can directly impose obligations or constrain a state's cyber behavior. In fact, the UK government has been the earliest and most explicit representative of the viewpoint that denies the obligatory nature of the cyber sovereignty principle. Denying the obligatory nature of sovereignty in cyberspace can provide greater operational freedom for technologically advanced states to undertake actions that infringe upon the sovereignty of other countries, essentially representing a form of cyber hegemony.

However, whether in general international law or in the context of cyberspace, the denial of the obligatory nature of the sovereignty principle lacks a basis both in practice and in theory. In several significant cases, such as the "Lotus Case," the International Court of Justice has affirmed the binding nature of the sovereignty principle, which can directly restrict a state's activities within another country's territory. One major reason for the UK's adherence to the denialist viewpoint is the absence of specific rules derived from the sovereignty principle in cyberspace. Nevertheless, on one hand, the effectiveness of specific rules derived from the sovereignty principle is still rooted in the sovereignty principle's efficacy. On the other hand, as noted by authoritative international legal scholar Oppenheim, it is impractical to enumerate all acts that violate another country's sovereignty. Nonetheless, each state has an obligation not to infringe upon the independent and territorial sovereignty of other states. Even if specific rules have not yet emerged from the sovereignty principle in cyberspace, this does not negate its applicability. Recognizing the obligatory nature of the cyber sovereignty principle is the stance of the majority of countries, including China, and is an essential requirement for fostering a stable cyberspace.

2.2 Regarding the Non-Intervention Principle

Braverman holds the non-intervention principle as the core of international law. Similar to most other countries, the UK considers the core element of the non-intervention principle as coercion. However, the UK provides a broader interpretation of what constitutes coercion.

The enthusiasm that Braverman displays for the non-intervention principle and the broader interpretation of the "coercion" element is closely related to the UK's denial of sovereignty's obligatory nature. For the UK, which advocates the viewpoint that denies the obligatory nature of the cyber sovereignty principle, the ability to engage in self-help is limited when malicious cyber activities do not meet the threshold of intervention or are subject to doubt. The UK's lowering of the threshold for constituting acts of interference is aimed at compensating for the shortcomings of the sovereignty principle's inability to be directly

applied. However, such a proposition may lead to confusion between the sovereignty principle and the non-interference principle.

The UK also provides a non-exhaustive list of conducts that may violate the non-intervention principle in what it considers the four most critical areas affected by destructive cyber activities. This is advantageous for protecting the UK's national interests, including the use of the non-intervention principle to hold responsible states accountable when state interests are harmed. It may also encourage more specific discussions regarding the non-intervention principle.

2.3 Regarding Response Methods

In the section on response options, it's worth noting that the UK, while not explicitly acknowledging the legality of collective countermeasures, shows a tendency towards accepting collective countermeasures.

Collective countermeasures refer to situations where the victim state, which has the right to take countermeasures, can request assistance from other states or have other states take countermeasures on its behalf. Existing international law only specifies that the purpose of taking countermeasures must be to induce the violating state to comply with its obligations, with other conditions for taking countermeasures remaining unclear. Collective countermeasures are a highly controversial issue related to countermeasures, and they have received widespread attention. Discussions on this topic have occurred in frameworks like the United Nations Group of Governmental Experts (UNGGE) and the United Nations Open-ended Working Group (OEWG). However, states have not reached a consensus on this issue, with France, for example, not supporting collective countermeasures in its official position, while Estonia takes an opposing stance.

3. Conclusion

Given the considerable controversy and uncertainty regarding how existing international law should be interpreted and applied in cyberspace, the United Kingdom's gradual and clear articulation of its positions and assertions through high-level speeches helps the UK assert influence and shape international norms in the field of international law in cyberspace. Faced with the UK's positions and assertions, there are two key considerations:

On one hand, its proactive approach and methods in shaping international rules for cyberspace are worthy of consideration and emulation by other countries. Other nations can also officially articulate their core stance on the development of international rules for cyberspace.

On the other hand, the assertive and somewhat hegemonic nature of its positions and assertions should be a source of caution for other countries. It is essential for other nations to encourage scholars to engage in research on international law in cyberspace and actively promote recognition and support for their own proposals through international cooperation, both within the United Nations and in regional forums.

References

Banks, W. (2021). Cyber Attribution and State Responsibility. International Law Studies Series. *US Naval War College, 97*, 1039-1072.

Corn, G. P., & Taylor, R. (2017-2018). Sovereignty in the Age of Cyber. *AJIL Unbound, 111*, 207-212.

Corn, G., & Jensen, E. (2018). The use of force and cyber countermeasures. *Temple International & Comparative Law Journal, 32*(2), 127-134.

Corthay, E. (2016). The asean doctrine of non-interference in light of the fundamental principle of non-intervention. *Asian-Pacific Law & Policy Journal, 17*(2), 1-41.

Jensen, E. (2015). Cyber sovereignty: the way ahead. *Texas International Law Journal, 50*(2-3), 275-304.

Jeremy Wright (2018). Cyber and International Law in the 21st Century <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 23 May 2018.

Khanna, P. (2018). State sovereignty and self-defence in cyberspace. *BRICS Law Journal, 5*(4), 139-154.

Kiessling, E. K. (2021). Gray zone tactics and the principle of non-intervention: can "one of the vaguest branches of international law" solve the gray zone problem?. *Harvard National Security Journal, 12*(1), 116-163.

Kilovaty, I. (2018). Doxfare: politically motivated leaks and the future of the norm on non-intervention in the era of weaponized information. *Harvard National Security*

Journal, 9(1), 146-179.

Mamychev, A., Zolochevskaya, E., Miroshnichenko, O., Yevtushenko, S., & Yuryevich, K. (2019). National sovereignty: socio-political transformation in context of modern cyber realities. *Journal of Politics and Law, 12*(3), 11-17.

O'Neill, P. (2018). Crossing the line: law of war and cyber engagement the U.S. position. *International Lawyer, 51*(3), 589-612.

Ossoff, W. (2021). Hacking the domaine reserve: the rule of non-intervention and political interference in cyberspace. *Harvard International Law Journal, 62*(1), 295-324.

Pattnaik, A., & Palo, S. (2018). Cyber Sovereignty: Dichotomy. *GNLU Law Review, 5*, 70-89.

Payne, C., & Finlay, L. (2017). Addressing obstacles to cyber-attribution: model based on state response to cyber-attack. *George Washington International Law Review, 49*(3), 535-568.

Schmitt, M. N. (2017). Peacetime cyber responses and wartime cyber operations under international law: an analytical vade mecum. *Harvard National Security Journal, 8*(2).

Schmitt, M. N., & Watts, S. (2021). Collective cyber countermeasures?. *Harvard National Security Journal, 12*(2), 373-411.

Stein, C. T. (2020). Hacking the electorate: non-intervention violation maybe, but not an act of war. *Arizona Journal of International and Comparative Law, 37*(1), 29-48.

Suella Braverman. (2022). International Law in Future Frontiers <https://www.gov.uk/government/speeches/international-law-in-future-frontiers> accessed 19 May 2022.

Tay, X. W. (2022). Reconstructing the principle of non-intervention and non-interference electoral disinformation, nicaragua, and the quilt-work approach. *Berkeley Journal of International Law, 40*(1), 39-94.

Wang, A. (2020). Cyber sovereignty at its boldest: chinese perspective. *Ohio State Technology Law Journal, 16*(2), 395-466.

Watts, S. (2014). Low-Intensity Cyber Operations and the Principle of Non-Intervention. *Baltic Yearbook of International Law, 14*, 137-162.

Wheatley, S. (2020). Foreign interference in elections under the non-intervention principle: we need to talk about "coercion". *Duke Journal of Comparative and International Law, 31*(1), 161-198.

Willmer, L. (2023). Does digitalization reshape the principle of non-intervention?. *German Law Journal, 24*(3), 508-521.

Zhao, W. (2020). Cyber disinformation operations (cdos) and new paradigm of non-intervention. *U.C. Davis Journal of International Law & Policy, 27*(1), 35-80.