The intelligence community as a normative actor under international law

Research Handbook on Intelligence and International Law (Russell Buchan & Iñaki Navarette eds., Edward Elgar Publishing, forthcoming, 2025).

The Intelligence Community as a Normative Actor under International Law

Sophie Duroy*

Abstract

Although the exact parameters remain debated, it is now undisputed that international law applies to intelligence activities. A more difficult—and still unanswered—question is how international law and the intelligence community influence one another. In this chapter, I demonstrate that the relationship between international law and the intelligence community is bidirectional and mutually constitutive. International law first constitutes a strong permissive tool for the intelligence community. The intelligence community invokes international law to explain, justify, and legitimate its activities, while international law itself provides legitimation to the intelligence community for many of its activities. At the same time, international law also constrains the intelligence community through the risk of accountability, which matches the increase in exposures. In turn, the intelligence community shapes international law when it uses it for political legitimation. Whereas, in the past, the intelligence community remained silent on its practices, at best uttering 'neither confirm nor deny', the situation has changed. Forced exposure has triggered a matching need to legitimise intelligence activities through law. The intelligence community is now openly engaging with and interpreting international law, putting forward interpretations that will legitimise its preferred outcomes and empower it to pursue its choices of policies. In doing so, the intelligence community changes the meaning ascribed to international norms. In addition, when the intelligence community refuses to abide by the rules of the legalism game by not providing a legal justification for its activities, it undermines the status of international legal norms, which may be perceived as less binding by the rest of the international community. For these reasons, the intelligence community has truly become a normative actor under international law and should be considered an occasional norm-shaper, if not yet a norm-setter.

Keywords: intelligence community; international law; legitimation; normative actor; accountability

* Essex Law School, University of Essex, United Kingdom.

1. INTRODUCTION

Although the exact parameters remain debated, it is now undisputed that international law applies to intelligence activities. A more difficult and still unanswered question is how international law and the intelligence community influence one another. In this chapter, I tackle this question from the two mirroring perspectives of international law and the intelligence community and demonstrate that this relationship is bidirectional and mutually constitutive. In other words, international law and the intelligence community influence and shape one another. For the purpose of this chapter, the 'intelligence community' is understood broadly. Domestically, it is constituted of all actors, agencies, and oversight bodies taking part in any way in the intelligence cycle.[1] Transnationally, it is understood as a community of practice bringing together these domestic communities or parts thereof. A final definitional remark concerns public statements purporting to justify intelligence activities in the rhetoric of international law. While these are often given by a public figure of the executive branch rather than by a direct member of the intelligence community, in this chapter, I consider these statements to be part of the justificatory discourse of the intelligence community.

In section 2, I start by conceiving of international law as a permissive tool for the intelligence community. Drawing on international relations scholarship on legitimation, I analyse why and how the intelligence community uses international law to explain, justify, and legitimate its activities. In this context, legitimacy refers to an audience's subjective belief about the rightfulness of an institution's conduct[2]—in this case, activities of the intelligence community. A legitimation process relies on justifications by the institution regarding how its conduct aligns with important normative principles.[3] The term 'justification' is used here in its non-legal meaning. It refers to statements attempting to legitimise behaviour through both legal and extra-legal (e.g., moral or political) arguments. For present purposes, what matters is the intelligence community's discourse concerning the alignment of its activities with international law. The intelligence community sometimes needs to deploy complex justifications to present its conduct as falling within the scope of a permissive rule (or outside that of a constraining one). Other times, however, its legitimation efforts are facilitated by arguments provided by a legitimate authority (e.g., courts or international organisations). In the second part of this section, I thus look at the means through which international law itself provides legitimation to intelligence communities: treaty law, case law, and United Nations Security Council (UNSC) resolutions.[4] In all these instances, international law constitutes a permissive tool, enabling the intelligence community to pursue its activities because it can present them as lawful.

---

[1] See *X (Chapter X of this Handbook).*

[2] Ian Hurd, 'Legitimacy and authority in international politics' (1999) 53 *International Organization* 379-408 at 381.

[3] Fernando G. Nuñez-Mietz, 'Legalization and the legitimation of the use of force: revisiting Kosovo' (2018) 72 *International Organization* 725-57 at 729.

[4] I do not discuss customary international law in this section as it is rarely used by itself for legitimation purposes. As explained by Rapp, in practice, 'decision-makers will especially prefer to reference codified international agreements over customary international law, seeing a particular value to referencing a written text even if it is not as directly connected to the issue at hand'. Kyle Rapp, 'Justifying force: international law, foreign policy decision-making, and the use of force' (2022) 28 *European Journal of International Relations* 337-60 at 337.

In section 3, I turn to the constraining power of international law over the intelligence community. Rather than being an abstract force, international law is becoming increasingly relevant for the intelligence community because of the growing difficulty of maintaining complete secrecy over intelligence activities. Until recently, many States did not even acknowledge the existence of their intelligence communities, and all of them enforced both secrecy and silence over these communities' activities. However, most intelligence communities now have legal status in their domestic legal orders, and an increasing stream of (involuntary and voluntary) disclosures regarding intelligence activities has breached the cloak of secrecy surrounding them. Exposure renders intelligence communities and their States vulnerable to processes of accountability for internationally wrongful acts stemming from intelligence activities. In turn, self-interest and reputational concerns require that intelligence communities account for the risk of accountability in their decision-making. Accountability thus acts both as a deterrent against extra-legal measures and an incentive for States and their intelligence communities to comply with international law. I conclude this section by assessing whether the influence of international law on the intelligence community constitutes a hindrance to effective national security protection. I argue that it instead constitutes a protective factor and a path toward true national security.

In section 4, finally, I reverse the focus and look at the normative role of the intelligence community, i.e., the influence that the intelligence community has on international law. Through its statements attempting to legitimate its activities in the language of international law, the intelligence community might indeed shape the content of this law. Interestingly, the absence of justification, or a justification using extra-legal arguments, might also affect international law. I distinguish three situations: (1) where intelligence activities remain secret and unacknowledged; (2) where intelligence activities are exposed but remain unacknowledged; and (3) where intelligence activities are both exposed and justified in the rhetoric of international law. In these three situations, the influence of the intelligence community in shaping international law differs in both form and degree. Still, it remains constant that the content of the law changes through its use by the intelligence community. I conclude that the intelligence community can be considered an occasional norm-shaper, if not yet a norm-setter.

2. INTERNATIONAL LAW AS A PERMISSIVE TOOL: JUSTIFICATION AND LEGITIMATION

Although it might initially seem counter-intuitive, international law constitutes a strong permissive, sometimes even enabling, tool for intelligence communities. Politicians generally turn to covert means when they cannot offer adequate legitimation to domestic and/or international audiences.[5] Intelligence communities, by contrast, often prefer to act covertly as a matter of course. If all intelligence activities could be kept completely secret forever, intelligence communities would only ever need to justify them to the authorising authority, usually the executive, and law would play a very limited role in this justification. However,

[5] Michael Poznansky, 'Feigning compliance: covert action and international law' (2019) 63 *International Studies Quarterly* 72-84.

given the multiplication of leaks and disclosures, even policies that are to remain secret must be capable of (ex-post) legitimation to a wider public. In this context, international law can be a powerful legitimating tool. Intelligence communities thus use international law—or the *language* of international law—to justify and legitimate (some of) their activities.[6]

A key driver of the need for legitimation is an audience's insistence that officials explain themselves.[7] In this regard, intelligence communities might have to justify their activities to three different audiences: the domestic public, foreign States, and other intelligence communities. These audiences might be more sensitive to different types of legitimation. Put simply, a domestic audience might be particularly receptive to narratives and arguments of national interest and security;[8] foreign States will grant more weight to justifications resting on international law;[9] and partner intelligence communities may prefer either international law justifications or effectiveness ones.[10] This 'three-level game', which builds on Putnam's two-level game[11] to include partner intelligence communities, acknowledges that the official attempting to justify intelligence activities must be concerned simultaneously with political, diplomatic, and corporatist pressures. Trying to satisfy all audiences using different rhetoric is theoretically possible, but consistency and the possibility of reverberation between different audiences must be accounted for,[12] particularly in the internet age. In this regard, international law often constitutes an official's safest route, especially insofar as international law can be moulded and invoked differently to fit different audiences.

2.1 Using International Law as Legitimation

The hegemony of international law as a form of legitimation on the international scene is visible in its invocation by political leaders, even when disingenuous or politically motivated.[13] Justifications using international law reflect the place of legalism, i.e., the 'practice of using law and legal arguments to explain, justify, or contest acts and policies'[14] in international relations. With the increased exposure of intelligence activities, legalism in the intelligence community is also becoming expected.[15] Scholarly work on the use of international law as

[6] Historically, justifications based on morality, religion, or ideology (e.g., the fight against communism) were often sufficient to legitimate the activity to a domestic audience and foreign allies. In modern times, however, intelligence communities are expected to abide by international law and appeals to other normative values will rarely suffice to legitimate their activities if these are perceived as unlawful.
[7] Stacie E. Goddard and Ronald R. Krebs, 'Rhetoric, legitimation, and grand strategy' (2015) 24 *Security Studies* 5-36 at 18.
[8] Goddard and Krebs, 'Rhetoric'.
[9] Ibid., 10-11; Rapp, 'Justifying force'.
[10] As I explain in section 3, compliance with international law increases effectiveness, meaning that these types of justification should theoretically be identical. In practice, however, effectiveness is often confused with toughness.
[11] Robert D. Putnam, 'Diplomacy and domestic politics: the logic of two-level games' (1988) 42 *International Organization* 427-60. The two-level game is a metaphor purporting to explain how, in international negotiation processes, central decision-makers within the State face both domestic pressures and international ones and must seek to satisfy and address both audiences at the same time.
[12] Putnam, 'Diplomacy and domestic politics', 435.
[13] Ian Hurd, *How to Do Things with International Law* (Princeton: Princeton University Press, 2017), p. 134.
[14] Ian Hurd, 'The empire of international legalism' (2018) 32 *Ethics & International Affairs* 265-78 at 266.
[15] Margo Schlanger, 'Intelligence legalism and the National Security Agency's civil liberties gap' (2015) 6 *Harvard National Security Journal* 112-205.

legitimation for covert actions, whether conducted by intelligence communities or the military, confirms this assessment.[16] States might assess the plausibility of legal justifications in deciding whether to carry out an operation,[17] or they might scramble for a legal justification during the operation or when exposure has become unavoidable. The latter situations correspond to what Robbie Sabel recounts concerning his role as a deputy legal advisor asked to devise a legal justification for Israel's operation Entebbe while it was happening.[18] The rationale behind the need for a legal justification is that, in a deeply legalised international system, if an action is exposed, State actors will feel compelled to portray their behaviour as lawful.[19] They will do so foremost to avoid the costs of being perceived as hypocritical and untrustworthy,[20] but also to shape the interpretation of the legal norm at stake.[21]

The fact that intelligence communities (or any other member of the executive doing so on their behalf) might have to justify and legitimate their activities retrospectively forces them to evaluate options and strategies from a legitimacy perspective, necessarily taking some options off the table because they are not publicly defendable. While this appears constraining, there remains a permissive effect of international law in this context. Intelligence communities can shape their justifications and construct threats in the process. There is productive power in the invocation of international law.[22] Even behaviour that is prima facie restrained by law can be legitimated by legal claims.[23] Political justifications invoking international law thus 'transform a prohibited behaviour into something lawful' in the eyes of the audience.[24] If this audience is an international one, the justification can effectively shape international law and empower the intelligence community to pursue its interests.

By framing intelligence activities in international law terms, intelligence communities attempt to legitimate them and shape how the law is interpreted. For instance, when revelations about the functions and widespread use of the Pegasus software came out in July 2021,[25] most suspected governments first denied buying the software.[26] When confronted with mounting evidence, several then admitted to having bought it but denied having *used* it.[27] Finally, in an

[16] Poznansky, 'Feigning compliance'; Alexandra H. Perina, 'Black holes and open secrets: the impact of covert action on international law' (2014) 53 Colum. J. Transnat'l L. 507-83.
[17] See, for instance, the case studies discussed in Rapp, 'Justifying force'.
[18] Robbie Sabel, 'Is international law relevant to the Arab-Israeli conflict?' (2019) 49 Isr. Y. B. Hum. Rts. 221-36 at 222. Operation Entebbe, also known as the Entebbe Raid or Operation Thunderbolt, was a counter-terrorist hostage-rescue mission carried out by commandos of the Israel Defense Forces at Entebbe Airport in Uganda on 4 July 1976.
[19] Rapp, 'Justifying force', 337.
[20] Poznansky, 'Feigning compliance'.
[21] Perina, 'Black holes'. See section 4 below.
[22] Hurd, *How to Do Things with International Law*, p. 8.
[23] Rapp, 'Justifying force', 340.
[24] Ibid.
[25] David Pegg and Sam Cutler, 'What is Pegasus spyware and how does it hack phones?', *The Guardian*, 18 July 2021, www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones accessed 15 March 2022.
[26] Anon., 'Response from NSO and governments', *The Guardian*, 20 July 2021, www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments accessed 16 March 2022.
[27] Stephanie Kirchgaessner, 'FBI confirms it obtained NSO's Pegasus spyware', *The Guardian*, 2 February 2022, www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware accessed 17 March

ultimate attempt to save face, the Hungarian government, later followed by others, admitted to using Pegasus but stated that they did so *in compliance with the law*.[28] What this means—aligning with the way Pegasus is promoted by the Israeli company NSO—is that the software was allegedly used solely to fight terrorism and criminal activities (a legitimate aim) and was the only/most effective way to do so (necessary/non-arbitrary). Consequently, it allegedly constituted a proportionate and lawful restriction on the right to privacy of targeted persons.[29] By presenting their use of this extremely intrusive software as *lawful*, these governments are not only attempting to shape the factual narrative ('we only spied on suspected criminals') but also the legal narrative ('this type of interference is authorised and even legitimate under international law').

Surveillance notoriously infringes on individuals' right to privacy. Justifications for surveillance practices construct a phenomenon (e.g., terrorism, organised crime) as a threat to a legitimate interest, such as national security or public order. This threat's existence necessitates a response to prevent it from materialising: surveillance. In this way, the justification constructs the threat as triggering a legitimate exemption from the rule (the right to privacy) and presents the response (surveillance) not as a violation of the rule but as a necessary and proportionate interference with it. The result is that bulk data collection/mass surveillance, or spyware like Pegasus, is presented as lawful.[30] Because the exemption from the rule is (allegedly) provided by the legal framework itself,[31] international law offers a strong legitimating force: intelligence communities only need to put forward an interpretation of the legal norm that suits their needs. The point of claiming such a legal exemption is to persuade observers that the action conforms to international law and is, consequently, legitimate.[32] In this way, legal rhetoric carries a utilitarian and strategic value in its permissiveness.[33] In most cases,

---

2022; Vincent Manancourt, 'Brussels, EU governments on collision course over Pegasus spyware', *POLITICO*, 15 February 2022, www.politico.eu/article/brussels-eu-government-collision-course-pegasus-spyware/ accessed 16 March 2022.

[28] Anon., 'German police secretly bought NSO Pegasus spyware', *Deutsche Welle*, 9 July 2021, www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197 accessed 16 March 2022; Anon., 'Top Hungarian official admits government bought Pegasus spyware', *Radio Free Europe/Radio Liberty*, 11 April 2021, www.rferl.org/a/hungary-admits-pegasus-spyware/31546293.html accessed 16 March 2022. In both cases, the 'law' referred to presumably encompasses both domestic law and international human rights law.

[29] While the justification broadly follows the line of assessment conducted by human rights courts and bodies, it is unlikely to pass their four-part proportionality test as this test notably requires a sound legal basis for surveillance. Generally, interference with the right to privacy is considered arbitrary and therefore impermissible if it is not prescribed by law, legitimate, necessary, and proportionate. See UN General Assembly, 'Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (28 May 2019) UN Doc. A/HRC/41/35, para. 24; UN General Assembly, 'The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc. A/HRC/27/37, paras. 21-30.

[30] Note that the 'prescribed by law' prong of the proportionality assessment (fn 29) is almost always left out of such justifications.

[31] See Art. 8(2) of the European Convention on Human Rights, Rome, 4 November 1950, in force 3 September 1953, 213 UNTS 222 (ECHR); Art. 17(1) of the International Covenant on Civil and Political Rights, New York, 16 December 1966, in force 23 March 1976, 999 UNTS 171 (ICCPR); and Art. 11(2) of the American Convention on Human Rights, San José, 22 November 1969, in force 18 July 1978, 1133 UNTS 143 (ACHR) (in these two conventions, only 'arbitrary or unlawful interference' is prohibited, meaning that non-arbitrary or lawful interference is permitted). The African Charter on Human and Peoples' Rights, Nairobi, 27 June 1981, in force 21 October 1986, 1520 UNTS 217 (ACHPR) does not explicitly protect the right to privacy.

[32] Poznansky, 'Feigning compliance', 74.

[33] Rapp, 'Justifying force', 340-1.

the privileged position of the State—particularly of powerful States—in shaping international law will allow this interpretation to prevail against that of non-governmental organisations and other non-state actors. Only if (international) courts get involved can the rhetorical use of international law forming the justification be legally challenged.

In contrast, the lack of legal justification for the National Security Agency (NSA) Prism programme—revealed by Edward Snowden in 2013 and for which the American intelligence community likely did not think they would ever need public justification[34]—triggered and legitimated international disapproval.[35] Henceforth, it became clear that governments must account for the possibility that a practice or policy might be brought to public knowledge. Preparing a legal justification in case of exposure is thus pragmatically sound, even if it means renouncing activities that cannot be publicly legitimated. Without justification, States and their intelligence communities forfeit their privileged position to legitimate their activities and shape the law.[36] Other sources, including third States and non-state actors, are then free to shape the factual and legal narrative as suits them. Further, should courts get involved, the void created by a silent State or a State incapable of justifying its activities in the accepted rhetoric of international law legitimates these alternative sources.[37]

Domestic audiences' demand for legitimation increases with the visibility of intelligence activities. Although domestic audiences might care less about international law than international audiences, justifications to domestic audiences allow lawyers to manipulate international law more than on the international scene. Due to their monopoly on the interpretation of international law in the domestic legal order, intelligence and government lawyers are comparatively freer in their interpretations of international legal norms and these norms' status in the domestic legal order. Before a domestic audience, it is thus easier for the intelligence community to proclaim that their activities comply with international law—as they interpret it—than before international audiences, who might put forth competing interpretations. In this sense, gross misinterpretations, for instance, of the prohibition on torture in the infamous Bybee-Yoo memoranda drafted as a legal justification for the CIA-led rendition, detention, and interrogation programme,[38] show both the hegemony of international law as a source of legitimation[39] and the extent to which a State might be willing to distort it to

[34] G. Alex Sinha, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy* (New York: Human Rights Watch, 2014), pp. 67-8.
[35] Janille Smith-Colin and Nabil Kleinhenz, 'Analyzing public and state reactions to global surveillance disclosures: using ethical frameworks to gain understanding', in Margaret E. Kosal (ed.), *Technology and the Intelligence Community* (Cham: Springer, 2018).
[36] Perina, 'Black holes', 549.
[37] Ibid., 551.
[38] Jay S. Bybee, 'Memorandum for John A. Rizzo. Re: Interrogation of al Qaeda operative', *US Department of Justice*, 1 August 2022, www.justice.gov/media/852831/dl?inline accessed 17 August 2023; Jay S. Bybee, 'Memorandum for Alberto R. Gonzalez. Re: Standards of conduct for interrogation under 18 U.S.C. §§ 2340-2340A', *US Department of Justice*, 1 August 2002, www.justice.gov/media/852816/dl?inline accessed 17 August 2023. The memoranda were authored by John Yoo and signed by Jay Bybee. They are also known as the 'Torture Memos'.
[39] On the political power of international law in this specific instance, see Hurd, *How to Do Things with International Law*, ch. 6.

defend its intelligence activities before a domestic audience.[40] In contrast, the justifications given to partner intelligence communities invoked effectiveness,[41] and despite multiple (quasi-)judicial proceedings,[42] there was no attempt to justify the programme on the international scene.

I have thus far alluded to intelligence communities' interested use of legal justifications to legitimate their activities. However, international law sometimes provides justifications without intelligence communities needing to (disingenuously) contort it, demonstrating a permissive effect. In other words, the intelligence community can sometimes readily appropriate and use arguments provided by a legitimate authority in the text of a treaty, case law, or UNSC resolutions. Using these arguments, the intelligence community can then legitimate its activities, regardless of whether these activities are identical to those envisioned by the legitimate authority.

2.2 Legitimation through Treaty

Treaty law sometimes provides authorisation and/or legitimation for specific intelligence activities by regulating their effects, means or limits, or by using 'legal euphemisms'.[43] Hence, while intelligence activities are never explicitly declared lawful, some must nevertheless be considered legally permissible. In such cases, the specific treaty regime authorising the activity functions between the parties as *lex specialis* to more general principles of international law and, consequently, may constitute a permissive tool. Activities fitting this description include specific forms of reconnaissance and wartime espionage.[44]

---

[40] The public justification by then-US President George W. Bush described the programme as 'safe and lawful and necessary' and insisted on its effectiveness, showing the interplay of legal and non-legal justifications at stake before domestic audiences. George W. Bush, 'President Bush's speech on terrorism', *The New York Times*, 6 September 2006, www.nytimes.com/2006/09/06/washington/06bush_transcript.html accessed 28 March 2022.

[41] The Central Intelligence Agency (CIA) provided misleading information about the operation of the programme and its effectiveness to multiple audiences, even leaking some false information to the press. These audiences also included foreign intelligence agencies and governments. See US Senate Select Committee on Intelligence, *Torture Report: Committee Study of Central Intelligence Agency's Detention and Interrogation Program: Executive Summary* (Washington, DC: US Government Printing Office, 2014), pp. 406-7 and Findings 2, 5, 6, 9 and 10; UK Intelligence and Security Committee of Parliament, *Detainee Mistreatment and Rendition: 2001-2010* (London: Dandy Booksellers, 2018); Nicky Woolf, 'CIA gave faulty information to media in order to mislead public on torture', *The Guardian*, 9 December 2014, www.theguardian.com/us-news/2014/dec/09/cia-false-information-journalists-mislead-public-senate-report accessed 3 March 2023.

[42] The CIA programme triggered proceedings before domestic courts in many countries, including in the USA, before several regional human rights courts and bodies, and before UN treaty bodies. The USA never took part in these proceedings and used a variety of legal, political, and coercive strategies to try and ensure that they would not reveal new information about the programme. For an analysis of these proceedings and US engagement with them, see Sophie Duroy, *The Regulation of Intelligence Activities under International Law* (Cheltenham: Edward Elgar, 2023), ch. 6.

[43] Iñaki Navarrete and Russell Buchan, 'Out of the legal wilderness: peacetime espionage, international law and the existence of customary exceptions' (2019) 51 Cornell Int'l L. J. 897-953 at 928.

[44] Although one might consider Art. 3(1)(d) of the Vienna Convention on Diplomatic Relations, Vienna, 18 April 1961, in force 24 April 1964, 500 UNTS 96 to permit a certain level of intelligence collection, States have made no attempt to use it as a legitimating tool for their diplomatic intelligence collection. Further, the International Court of Justice (ICJ) clearly stated that acts of 'espionage' by diplomatic (and presumably consular) officials constitute 'abuses of their functions' and cannot be regarded as a lawful means through which information may be collected. This authoritative statement prevents the text from being used as a legitimating tool. *United States*

Through various treaty provisions, reconnaissance has first been 'authorised' from international spaces, namely outer space, the high seas, and international airspace. The Outer Space Treaty of 1967 provides that:

> States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.[45]

The treaty further clarifies that '[t]he moon and other celestial bodies shall be used by all State Parties to the Treaty exclusively for peaceful purposes'.[46] Although the language was purposefully left ambiguous, and the 'peaceful purposes' provision should theoretically only concern the moon and other celestial bodies, it has been interpreted as authorising the use of reconnaissance satellites from outer space.[47] In very similar language, the United Nations Convention on the Law of the Sea (UNCLOS) proclaims in Article 87 the freedom of the high seas and clarifies in Article 88 that '[t]he high seas shall be reserved for peaceful purposes'.[48] Finally, parallel to the freedom of the high seas exists a freedom of international airspace,[49] including airspace over the high seas and the more recently created exclusive economic zone (EEZ) of States.[50]

It is now rather generally accepted, in the form of State practice and matching *opinio juris*, that surveillance and reconnaissance activities conducted from outer space, the high seas, and international airspace are lawful in that they do not infringe on the sovereignty of any State and do not violate any rule of international law.[51] However, this results from a permissive interpretation of an otherwise ambiguous norm in all three situations, whereby the rule's ambiguity has been exploited to provide substantive authorisation to act. By agreeing to this expansive interpretation of a norm purposefully silent about reconnaissance,[52] State practice and *opinio juris* have consolidated the permissive power of international law in these situations.

Diplomatic and Consular Staff in Tehran (United States of America v. *Iran)* (Judgment) [1980] ICJ Rep. 3 at para. 84.

[45] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Washington, Moscow, London, 27 January 1967, in force 10 October 1967, 610 UNTS 205, Art. III.

[46] Ibid., Art. IV.

[47] Jinyuan Su, 'Use of outer space for peaceful purposes: non-militarization, non-aggression and prevention of weaponization' (2010) 36 J. Space L. 253-72 at 258. See also, with regard to the monitoring of telecommunications effectuated via satellites and the use of data thereby collected, *Weber and Saravia* v. *Germany*, App. No. 54934/00 (ECtHR, 29 June 2006) ECHR 2006-XI at para. 88.

[48] United Nations Convention on the Law of the Sea, Montego Bay, 10 December 1982, in force 16 November 1994, 1833 UNTS 397 (UNCLOS).

[49] Convention on International Civil Aviation, Chicago, 7 December 1944, in force 4 April 1947, 15 UNTS 295 (Chicago Convention), Art. 12.

[50] Chicago Convention, Arts. 1 and 2. Reconnaissance from *within* the EEZ is a more contested matter, as I explain below.

[51] [Reference to other chapters in the handbook]

[52] Navarrete and Buchan, 'Out of the legal wilderness', 929-31.

In all likelihood, due to the legitimation provided by law, actions undertaken following this authorisation have been bolder and more overt than they would have been without it.

As regards the EEZ, reconnaissance from the international airspace *over* the EEZ should be distinguished from reconnaissance from *within* the EEZ itself (i.e., in the EEZ waters). Indeed, EEZ waters and the airspace over the EEZ are not subject to the same legal regime. International air law recognises each State's full and absolute sovereignty over the airspace above its territory and territorial waters, including the right to impose its jurisdiction over such airspace.[53] Airspace above the EEZ is thus excluded from the scope of State sovereignty[54] and justifiably so since coastal States do not enjoy territorial sovereignty in their EEZ but only sovereign rights over economic resources within it.[55] Hence, it would be difficult to justify why the coastal State should enjoy any kind of sovereignty or regulatory power regarding the airspace over the EEZ. UNCLOS instead preserves third States' full overflight freedoms, including for military uses.[56] Consequently, if it does not interfere with the coastal State's economic rights, reconnaissance from the airspace over the EEZ cannot be considered unlawful under UNCLOS.

However, some confusion in literature and State practice has muddied the distinction. As a result of the conflation of reconnaissance from within and over the EEZ, this type of reconnaissance is less unanimously considered lawful than from the high seas and/or international airspace over the high seas. Lubin, himself blending the EEZ with the airspace over it in his analysis, highlights the opposing approaches that States have adopted towards the issue of EEZ reconnaissance.[57] Of interest for present purposes is the permissive side, led by the United States (USA) and including the majority of States.[58] The permissive side relies on the language of Article 58(1) of UNCLOS[59] to argue that, as in the high seas with its 'peaceful purposes' provision,[60] EEZ reconnaissance must be considered part of 'internationally lawful uses of the sea'.[61] In this sense, and despite the subject being actively avoided during treaty

[53] Chicago Convention, Arts. 1 and 2.
[54] Raul Pedrozo, 'Military activities in the exclusive economic zone: East Asia focus' (2014) 90 *International Law Studies* 514-43 at 519-20; Joshua Cornthwaite, 'Can we shoot down that drone? An examination of international law issues associated with the use of territorially intrusive aerial and maritime surveillance drones in peacetime' (2019) 52 Cornell Int'l L. J. 475-543 at 506.
[55] UNCLOS, Art. 56; Kay Hailbronner, 'Freedom of the air and the Convention on the Law of the Sea' (1983) 77 AJIL 490-520 at 506; Efthymios Papastavridis, 'Intelligence gathering in the exclusive economic zone' (2017) 93 *International Law Studies* 446-75 at 453-4.
[56] UNCLOS, Art. 58(1). Hailbronner, 'Freedom of the air', 506.
[57] Asaf Lubin, 'The Dragon-Kings' restraint: proposing a compromise for the EEZ surveillance conundrum' (2018) 57 Washburn L. J. 17-75.
[58] The prohibitive side, led by China, includes eighteen States claiming a security interest in EEZ, typically by purporting to restrict foreign-flagged military activities: Brazil, Uruguay, Kenya, Cape Verde, Iran, Pakistan, India, Bangladesh, Myanmar, Thailand, Cambodia, Malaysia, Vietnam, North Korea, Maldives, Mauritius, Indonesia, and China. James Kraska and Raul Pedrozo, *International Maritime Security Law* (Leiden: Martinus Nijhoff, 2013), p. 278.
[59] 'In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in Article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention.'
[60] UNCLOS, Arts. 87 and 88.
[61] For an exposé of their arguments, see Lubin, 'The Dragon-Kings' restraint', 25-38.

negotiations,[62] the rather vague formulation of the treaty provision is used to legitimate the practice of reconnaissance from *within* the EEZ, necessarily also justifying reconnaissance from *over* the EEZ.

Reconnaissance has also been authorised from the territorial airspace of States in more limited ways through arms control treaties. Chesterman identifies the verification regime of the Anti-Ballistic Missile Treaty and Strategic Arms Limitation Talks (SALT I) Agreement[63] as providing for a right to collect intelligence, protected by corresponding obligations of the territorial State.[64] This verification regime model, reproduced or extended in later arms control agreements between the USA and Union of Soviet Socialist Republics (USSR) and in multilateral settings,[65] effectively establishes a claim right[66] to reconnaissance from the territorial airspace of other parties with respect to assessing compliance with arms control obligations.[67] This represents a pragmatic solution to evident issues of trust between parties to arms reduction agreements. This narrowly regulated right to intelligence collection constitutes a well-defined exception to States' exclusive sovereignty over their territorial airspace, which does not spill over to create any such right outside specific treaty regimes. However, it provides a clear justification and legitimation for activities falling within its scope without any straining of the law being required.

Wartime espionage represents another example of expansive interpretation leading to legitimation. The laws of war only address the prisoner status of spies. They thus legitimate but do not explicitly declare the legality of spying, although the 1899 and 1907 Hague Regulations, unique in this respect, permit the employment of 'methods necessary for obtaining information about the enemy and the country'.[68] Various conventions regulate the treatment of enemy spies

[62] See discussion in Lubin, 'The Dragon-Kings' restraint', 35-6 and 45-6.

[63] Treaty on the Limitation of Anti-Ballistic Missile Systems, Moscow, 26 May 1972, in force 3 October 1972, 944 UNTS 13 (Anti-Ballistic Missile Systems (ABM) Treaty) (the United States announced its withdrawal on 13 December 2001), Art. XII; Strategic Arms Limitation Talks, Moscow, 26 May 1972, in force 3 October 1972, 945 UNTS 13, Art. V.

[64] Simon Chesterman, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford: Oxford University Press, 2011), p. 34 referencing the ABM Treaty, Art. XII paras. 2 and 3; and SALT I Agreement, Art. V, paras. 2 and 3.

[65] See Intermediate-Range Nuclear Forces (INF) Treaty, Washington, DC, 8 December 1987, in force 1 June 1988, 1657 UNTS 1, Art. XII; Strategic Arms Reduction Treaty (START I), Moscow, 31 July 1991, in force December 1994, Art. X; and Treaty on Open Skies, Helsinki, 24 March 1992, in force 1 January 2002, Arts. I(1), II(4), III–VI, and IX.

[66] Whereas other forms of permissible reconnaissance may be conceived of as liberty rights in the sense that such reconnaissance constitutes a privilege (i.e., States have no duty not to practice reconnaissance in the ways identified above), this specific form of reconnaissance is better understood as a claim right. Indeed, it imposes on the territorial State a corresponding duty to allow and enable reconnaissance from its territorial airspace by the other parties to the treaty. The terms 'liberty right' and 'claim right' originate in the work of Wesley Hohfeld: Wesley Newcomb Hohfeld, 'Fundamental legal conceptions as applied in judicial reasoning' (1917) 26 Yale L. J. 710-70.

[67] Chesterman, *One Nation Under Surveillance*, p. 34.

[68] Regulations Concerning the Laws and Customs of War on Land, annexed to Convention No. II with Respect to the Laws and Customs of War on Land, The Hague, 29 July 1899, in force 4 September 1900) 187 CTS 429, 32 Stat. 1803, 187 Consol. T.S. 429 (the 1899 Hague Regulations), Regulations: Art. 24. According to the UK, Ministry of Defence, *Joint Service Manual of the Law of Armed Conflict* (Shrivenham: Ministry of Defence, 2004), p.63, this can include 'the employment of informers or agents in enemy-held territory'. Although, as the USA, Department of Defense, *Law of War Manual* (Washington DC: Department of Defense, 2015), p.309, rightly states, 'Information gathering measures … may not violate specific law of war rules.' Further, IHL emphasises that

by belligerent States[69] and determine who can be considered a spy.[70] In this sense, while spies can be harshly punished by the injured party, they are not war criminals, and their actions do not engage the international responsibility of the sending State because wartime espionage is not an internationally wrongful act. Further, it can also be argued that to respect international humanitarian law (IHL), particularly the principle of distinction, IHL mandates intelligence collection, at least for the purpose of identifying targets as lawful or unlawful.[71] In sum, despite—or maybe thanks to—this superficial textual regulation, wartime (human) espionage is thus made legitimate.

Covert action and territorially intrusive means of intelligence collection during wartime are legitimated on a similar basis as human intelligence because they can be repressed by the territorial State, as when a State shoots a reconnaissance aircraft in its territorial airspace. In contrast, non-intrusive means of intelligence collection cannot result in the punishment of any 'spy' caught in the act by the injured party. However, as Wright explained, 'the legitimacy of espionage in time of war arises from the absence of any general obligation of belligerents to respect the territory or government of the enemy State, and from the lack of any specific convention against it'.[72] This justification covers all types of wartime intelligence activities. Hence, non-intrusive means of intelligence collection must also be considered permissible during wartime because the necessities of war lift the principle of sovereignty. In consequence, despite how very little treaty law has to say about them, all forms of wartime intelligence activities can be legitimated on this basis.

However, there is a caveat to this seemingly general authorisation. The prohibition of certain acts, or means and methods of espionage, also applies in wartime. Because IHL functions as a *lex specialis* to some of the international law applicable during peacetime, wartime espionage is lawful only insofar as it does not violate IHL[73] or any other rule of international law that is not displaced by the applicability of IHL. The latter includes norms of international human rights law and general international law that become or remain applicable during armed conflicts. In this sense, the justification must account for these limits to the general authorisation to spy during armed conflicts. Pragmatically, however, it might be easier for intelligence

---

neither prisoners of war nor protected persons under the Fourth Geneva Convention may be ill-treated in the search for intelligence (Art. 31 of the Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949, in force 21 October 1950, 75 UNTS 287).

[69] 1899 Hague Regulations, Art. 30: 'A spy taken in the act cannot be punished without previous trial.' and Art. 31: 'A spy who, after rejoining the army to which he belongs, is subsequently captured by the enemy, is treated as a prisoner of war, and incurs no responsibility for his previous acts of espionage.' See also Geneva Convention IV, Art. 5; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, Geneva, 8 June 1977, in force 7 December 1978, 1125 UNTS 3 (Additional Protocol I), Arts. 45(3) and 46(1); and Rule 107, ICRC Study on the Codification of International Humanitarian Law: Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, Vol. I: Rules and Vol. II: Practice (Cambridge: Cambridge University Press, 2005).

[70] 1899 Hague Regulations, Art. 29; 1977 Additional Protocol I, Art. 46(2).

[71] United Nations, International Criminal Tribunal for the former Yugoslavia, Final Report of the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (2 June 1999) para. 29.

[72] Quincy Wright, 'Espionage and the doctrine of non-intervention in internal affairs', in Roland J. Stanger (ed.), *Essays on Espionage and International Law* (Columbus: Ohio State University Press, 1962), p. 12.

[73] For instance, collecting intelligence by torturing prisoners of war would be unlawful.

communities to legitimate activities in breach of international law in wartime than peacetime due to the general authorisation and strong political legitimacy of these activities in armed conflicts. This point also underlines the importance of extra-legal forms of justification, such as national security and state survival, in reinforcing the political legitimation brought by international law.

In sum, States have purposively interpreted vague, ambiguous, or unrelated treaty provisions to legitimate wartime espionage and reconnaissance from international airspaces. The sole exception is the explicit right to reconnaissance stipulated within arms control treaties, which provides a clear justification and legitimation for reconnaissance activities falling within the treaties' scope.

2.3 Legitimation through Case Law

Another form of legitimation arises through international courts' decisions on intelligence activities. Such decisions have multiplied in the past two decades, notably due to the increasing targeting of individuals and the difficulty of keeping intelligence activities secret. A prominent example of legitimation through case law was brought by the European Court of Human Rights (ECtHR) in its Grand Chamber judgments in the *Big Brother Watch* (BBW) and *Centrum för Rättvisa* (CFR) cases.[74] Despite finding against the respondent States in both cases, these judgments effectively legitimated and made lawful the bulk interception and collection of foreign communications (also called mass surveillance), in a move harshly criticised by academic commentators.[75]

Starting in the aftermath of 9/11, the ECtHR gradually legitimated the practice of bulk interception of foreign communications, culminating in its 'normalisation' in BBW and CFR. As Watt underscores, in *Weber and Saravia* v. *Germany*[76] and *Liberty and Others* v. *UK*,[77] the ECtHR had already endorsed in principle the strategic surveillance of foreign communications as falling within States' wide margin of appreciation.[78] In BBW and CFR, the Grand Chamber

[74] *Big Brother Watch and Others* v. *The United Kingdom* [GC], App. Nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) (BBW); *Centrum för Rättvisa* v. *Sweden* [GC], App. No. 35252/08 (ECtHR, 25 May 2021) (CFR).

[75] Eliza Watt, 'Much ado about mass surveillance – the ECtHR Grand Chamber "opens the gates of an electronic 'Big Brother' in Europe" in *Big Brother Watch v UK*', *Strasbourg Observers*, 28 June 2021, https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/ accessed 30 June 2021; Marko Milanovic, 'The grand normalization of mass surveillance: ECtHR Grand Chamber judgments in *Big Brother Watch* and *Centrum för Rättvisa*', *EJIL:Talk!*, 26 May 2021, www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ accessed 16 March 2022; Massimo Frigo, '*Big Brother Watch v. UK*: a landmark judgment missing the mark', *Opinio Juris*, 4 June 2021, http://opiniojuris.org/2021/06/04/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/ accessed 7 June 2021; Mark Klamberg, 'Big Brother's little, more dangerous brother', *Verfassungsblog*, 1 June 2021, https://verfassungsblog.de/raettvisa/ accessed 1 June 2021; Monika Zalnieriute, 'Procedural fetishism and mass surveillance under the ECHR', *Verfassungsblog*, 2 June 2021, https://verfassungsblog.de/big-b-v-uk/ accessed 16 March 2022.

[76] *Weber and Saravia* v. *Germany*, App. No. 54934/00 (ECtHR, 29 June 2006) ECHR 2006-XI.

[77] *Liberty and Others* v. *UK*, App. No. 58243 (ECtHR, 1 July 2008).

[78] Watt, 'Much ado about mass surveillance'.

extended this endorsement to mass surveillance by considering that operating a bulk interception regime is not, in principle, unlawful and/or disproportionate. The Court thus found that the British and Swedish bulk interception regimes before it were 'valuable'[79] and of 'vital importance'[80] to the security of member States—notwithstanding the lack of evidence concerning their actual performance. On this basis, the Court confirmed that national authorities enjoy a 'wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security'.[81] Through these two judgments, the Grand Chamber affirmed the legitimacy of mass surveillance, succumbing to what Zalnieriute called the 'inevitability of the mass surveillance narrative'.[82]

The consequence of this finding, for the majority of the Grand Chamber, is that end-to-end safeguards are needed. The Court thus establishes a new eight-part test to assess the compatibility of bulk interception regimes with Article 8 of the ECHR.[83] As applied in both cases, the test focuses on the regulatory framework and procedural safeguards rather than actual practice. In other words, the test focuses exclusively on the 'in accordance with law' prong of the proportionality assessment and assumes satisfaction of the 'legitimate aim', 'necessary' and 'proportionality' prongs.[84] Indeed, both decisions exemplify the Court's blind trust in respondent States' assessments that interception, storage, and data and metadata analysis are necessary and proportionate to protect national security.[85] As Marko Milanovic concludes, the two judgments constitute a definitive normalisation of mass surveillance.[86]

The 'proceduralist' approach[87] to mass surveillance adopted by the ECtHR greatly facilitates States' legitimation of their bulk collection regimes. Provided States' regulatory frameworks respect the eight-part (procedural) test established by the Grand Chamber, they can legitimate any bulk regime by presenting it as necessary, proportionate, and lawful. Based on the two decisions, it seems that whether this regime is actually 'valuable' and whether practice complies with the regulatory framework are of virtually no importance for the outcome of a case. Nevertheless, in a more recent case concerning domestic surveillance, the Court underlined that procedural safeguards should not only exist on paper but also operate in practice.[88] Despite this welcome if belated reminder, through its case law, the ECtHR provides States with strong political and legal legitimation for their mass surveillance programmes.

2.4 Legitimation through the UN Security Council

UN Security Council resolutions can provide similar legitimation. The best example is probably the international framework for combating terrorism, drafted through a series of post-9/11

[79] BBW, para. 323; CFR, para. 237.
[80] BBW, para. 424; CFR, para. 365.
[81] BBW, para. 228; CFR, para. 252.
[82] Monika Zalnieriute, '*Big Brother Watch and Others v. the United Kingdom*' (2022) 116 AJIL 585-92 at 590.
[83] BBW, para. 361; CFR, para. 275.
[84] See fn. 29 above.
[85] Frigo, '*Big Brother Watch v. UK*'.
[86] Milanovic, 'The grand normalization'.
[87] Zalnieriute, 'Procedural fetishism'.
[88] *Ekimdzhiev and Others* v. *Bulgaria*, App. No. 70078/12 (ECtHR,11 February 2022) at para. 419.

UNSC Chapter VII resolutions. This framework effectively made intelligence cooperation to fight terrorism a legal obligation of States. It thereby provided an extremely powerful justification for increasingly intrusive intelligence practices that would otherwise have been considered unlawful under international human rights law (IHRL).

Before 9/11, it would have been unconscionable for Chapter VII resolutions to require States to introduce specified counterterrorism legislation in their domestic legal orders.[89] Yet, the post-9/11 Security Council adopted a 'dominant super-legislative role',[90] using binding resolutions to regulate States' responses to terrorism. Resolution 1373,[91] adopted in the immediate aftermath of 9/11, thus required all States to change their domestic laws to create a separate crime of terrorism and made international intelligence cooperation a legal obligation.[92] The template established in Resolution 1373 was followed and elaborated upon in a series of further Chapter VII resolutions aiming to combat terrorism.[93]

In these Chapter VII resolutions—which are both binding and take precedence over other State obligations[94]—all States were addressed, and all were required to prepare themselves to combat terrorism in the manner outlined in the resolutions. States were not only permitted but often 'required to respond to the threat of international terrorism by expanding the scope of executive power, loosening restraints on surveillance, deploying the military in unconventional ways, engaging in deepening transnational cooperation among security services, and more'.[95] Despite the sensitive area (national security) and the extremely demanding changes required of States,

[89] Fionnuala Ní Aoláin, 'The ever-expanding legislative supremacy of the Security Council in counterterrorism', in Arianna Vedaschi and Kim Lane Scheppele (eds.), *9/11 and the Rise of Global Anti-Terrorism Law: How the UN Security Council Rules the World* (Cambridge: Cambridge University Press, 2021), p. 34.
[90] Ibid., p. 36.
[91] UNSC Res. 1373 (28 September 2001) UN Doc. S/RES/1373(2001).
[92] The Resolution indeed decided that 'States shall … Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information'. It further called upon States to 'Find ways of intensifying and accelerating the exchange of operational information …; Exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts; Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts; …' UNSC Res. 1373, paras. 2(b) and 3(a), (b), and (c).
[93] See, especially, UNSC Res. 1611 (7 July 2005) UN Doc. S/RES/1611(2005); UNSC Res. 1618 (4 August 2005) UN Doc. S/RES/1618(2005); UNSC Res. 2133 (27 January 2014) UN Doc. S/RES/2133(2014); UNSC Res. 2170 (15 August 2014) UN Doc. S/RES/2170(2014). For an analysis of the architecture and impacts of the transnational counter-terrorism order established as a result, see Fiona de Londras, *The Practice and Problems of Transnational Counter-Terrorism* (Cambridge: Cambridge University Press, 2022).
[94] The ICJ held that Art. 103 of the Charter of the United Nations, San Francisco, 26 June 1945, in force 24 October 1945, 59 Stat. 1031, TS 993, 3 Bevans 1153, requires that UN Charter obligations of member States prevail over any other international treaty, and that member States' obligations under Ch. VII Security Council resolutions are the same as under the Charter itself. See *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America)* (Jurisdiction and Admissibility, Judgment) [1986] ICJ Rep. 392 at para. 107; *Questions of Interpretation and Application of the 1971 Montreal Convention Arising from the Aerial Incident at Lockerbie* (*Libyan Arab Jamahiriya* v. *United Kingdom*) (Provisional Measures, Order) 1992 ICJ Rep. 3 at para. 42, and *Questions of Interpretation and Application of the 1971 Montreal Convention Arising from the Aerial Incident at Lockerbie* (*Libyan Arab Jamahiriya* v. *United States of America*) (Provisional Measures, Order) 1992 ICJ Rep. 114 at para. 39.
[95] Kim Lane Scheppele and Arianna Vedaschi, 'Conclusion: The afterlife of 9/11', in Arianna Vedaschi and Kim Lane Scheppele (eds.), *9/11 and the Rise of Global Anti-Terrorism Law: How the UN Security Council Rules the World* (Cambridge: Cambridge University Press, 2021), p. 247.

compliance was swift and quasi-universal.[96] While governments' self-interest in implementing resolutions increasing the executive power should not be discounted to explain compliance, it bears noting that the UNSC mandated these domestic changes. In other words, they were made *in order* to comply with international law, hence providing them with the strongest form of legitimacy before all audiences and facilitating their implementation.[97]

Still, the tools established in the UNSC's global counterterrorism framework lacked meaningful safeguards. This regulatory framework thus allowed States, including authoritarian ones, to address their own domestic 'threats' through the language of counterterrorism. It thereby legitimated a crackdown on human rights and the rule of law in the name of preventing and fighting terrorism—now a legal obligation of States.[98] The Security Council's far-reaching global legislative measures have displaced and rendered many constitutional and international human rights protections almost meaningless.[99] Instead of acting as a gatekeeper for international law, the UNSC undermined the very principles of international law. It provided states with a justification and a legal obligation to enact legislation and act in violation of previously non-derogable obligations. Intelligence communities worldwide thus saw some of their most controversial practices amenable to legitimation as long as the fight against terrorism—a term that the UNSC did not bother to define—could be invoked. The rule of law became a secondary concern, if at all, in intelligence cooperation, while the role of intelligence communities became virtually unlimited in countering terrorism. The justification for this new state of affairs was compelling: not only could these changes and activities be presented as lawful, but they were also necessary to *comply* with international law.

3. INTERNATIONAL LAW AS A CONSTRAINING FORCE: ACCOUNTABILITY AND DETERRENCE

Parallel to its permissive and enabling potential, international law also constrains the intelligence community. Intelligence activities are increasingly being exposed, resulting in States being held accountable for their intelligence community's acts in breach of international law. In this sense, international law possesses a deterrent effect.

[96] UN Secretary-General Kofi Annan even stated in January 2002 that 'the cooperation it has received from Member States [has] been unprecedented and exemplary'. United Nations, Secretary-General, Addressing Council Meeting on Counter-Terrorism, Says United Nations 'Stands Four-Square' against Scourge. Press Release SG/SM/8105; SC/7277, 18 January 2002: https://press.un.org/en/2002/sgsm8105.doc.htm, accessed 25 August 2023.

[97] Scheppele and Vedaschi, 'Conclusion', pp. 247-8.

[98] See, on the framework developed to address 'foreign terrorist fighters', Kim Lane Scheppele, 'Common template, diverse agendas: the futility (and danger) of legislating for the world', in Arianna Vedaschi and Kim Lane Scheppele (eds.), *9/11 and the Rise of Global Anti-Terrorism Law: How the UN Security Council Rules the World* (Cambridge: Cambridge University Press, 2021).

[99] Martin Scheinin, 'Impact of post-9/11 counter-terrorism measures on all human rights', in Manfred Nowak and Anne Charbord (eds.), *Using Human Rights to Counter Terrorism* (Cheltenham: Edward Elgar, 2018).

When an act attributable to the State constitutes an internationally wrongful act, the State's responsibility is engaged.[100] Hence, State responsibility might be engaged for intelligence activities in breach of the right to private and family life;[101] the prohibition of torture and complicity thereof;[102] the rights to access to information, to a fair trial, equal protection, and judicial protection;[103] the right to life;[104] the right to security and liberty of the person;[105] the prohibition of enforced disappearance;[106] the principle of territorial sovereignty;[107] or the principle of non-intervention.[108] This list and the examples provided are self-evidently non-exhaustive and only serve an illustrative purpose.

I refer to the process to enforce State responsibility as 'international legal accountability'. I define it as 'the process by which a state legally justifies its performance vis-à-vis other international actors, in which an assessment or judgement of that performance against international legal standards is rendered, and through which consequences can be imposed if the state fails to live up to applicable international legal standards'.[109] Accountability can take place between States, as envisioned by the International Law Commission's Articles on the Responsibility of States (ARSIWA),[110] and is then interstate. Accountability can also take place between a non-state actor, for instance, an individual, and the State. It is then mediated, because individuals have no standing in international law and need to use another international actor (a court, treaty body, or similar quasi-judicial mechanism) to hold the State to account.

Interstate forms of accountability are usually implausible when intelligence is at stake because holding one another to account would damage trust and possibilities of cooperation, might risk an escalation in exposure,[111] or encourage the wrongdoer to 'double down' on the wrongful

[100] ILC, 'Draft articles on responsibility of states for internationally wrongful acts', in *Yearbook of the International Law Commission. 2001, Volume II, Part Two: Report of the Commission to the General Assembly on the Work of its Fifty-Third Session* (New York: UN, 2008) (ARSIWA), pp. 76-143, Art. 1.
[101] E.g., *Szabo and Vissy* v. *Hungary*, App. No. 37138/14 (ECtHR, 12 January 2016).
[102] *Al-Nashiri* v. *Poland* (Judgment) App. No. 28761/11 (ECtHR, 24 July 2014) at para. 516; *Husayn (Abu Zubaydah)* v. *Poland* (Judgment) App. No. 7511/13 (ECtHR, 24 July 2014) at para 511.
[103] E.g., *Active Memory Civil Association* v. *Argentina* (Admissibility and Merits), Case No. 12.204, Report No. 187/20 (IACtHR, 14 July 2020). These violations occurred as a result of investigatory failures that were covered up by intelligence services. The case has been referred to the IACtHR and a hearing on the merits took place in late 2022.
[104] E.g., Human Rights Council, 'Use of armed drones for targeted killings. Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions' (15 August 2020) UN Doc. A/HRC/44/38, Annex, para. 82.
[105] E.g., *El-Masri* v. *The Former Yugoslav Republic of Macedonia*, App. No. 39639/09 (ECtHR, 13 December 2012).
[106] E.g., *Goiburú et al.* v. *Paraguay* (Merits, Reparations and Costs), Series C No. 153 (IACtHR, 22 September 2006).
[107] E.g., UNSC Res. 138 (23 June 1960) UN Doc. S/RES/138(1960), the 'Question relating to the case of Adolf Eichmann'.
[108] E.g., *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America)* (Merits, Judgment) [1986] ICJ Rep. 14.
[109] Sophie Duroy, 'Remedying violations of human dignity and security: state accountability for counterterrorism intelligence cooperation', in Christophe Paulussen and Martin Scheinin (eds.), *Human Dignity and Human Security in Times of Terrorism* (The Hague: TMC Asser Press, 2020), p. 135.
[110] ARSIWA, Part III.
[111] On States exposing one another, see Ofek Riemer, 'Politics is not everything: new perspectives on the public disclosure of intelligence by states' (2021) 42 *Contemporary Security Policy* 554-83.

act.[112] However, mediated forms of accountability, commonly triggered by individual complaints before human rights courts and bodies and by States' reporting obligations, have increased exponentially following revelations about the CIA-led and NSA-led programmes. In the past 20 years, intelligence activities have become the subject of sustained international litigation, and their legality has been thoroughly assessed.[113]

During the same period, intelligence communities witnessed a series of interlocking changes that heightened the importance of international law for their legitimacy. The evolving nature of intelligence activities after the Cold War, now targeting individuals more directly, and the parallel 'humanisation' of international law, led individuals to have legitimate expectations that their rights would be respected.[114] Further, due to technological developments and an expanding 'intelligence bureaucracy'[115] providing more people with access to classified material, intelligence activities are increasingly difficult to keep secret. The increase in intelligence leaks and scandals triggered a renewed interest in intelligence activities and negatively affected intelligence communities' legitimacy. These changes increased demands for, and possibilities of, accountability. We are thus observing a new pervading legalism in intelligence communities, resulting from these communities' renewed understanding that compliance with international law is increasingly necessary to be perceived as legitimate and benefit from citizens' and foreign services' cooperation.[116]

In recent years, therefore, there has been an increase in the likelihood that the intelligence community will be held to account by partner intelligence communities and citizens.[117] This has been matched by a parallel increase in the likelihood that States will be held legally accountable for the acts of their intelligence community, both before human rights courts and bodies and before the international legal order as a whole. Such an increase necessarily affects what States perceive to be their interest in national security matters. If exposure and accountability are increasingly likely, then this changes the costs and payoffs of pursuing a policy that would otherwise have remained secret. The result is that the likelihood of effective accountability, a legal factor, now represents the most important variable to explain and

[112] Jacob Otto and William Spaniel, 'Doubling down: the danger of disclosing secret action' (2021) 65 *International Studies Quarterly* 500-11.
[113] E.g., Case C-511/18 *La Quadrature du Net and Others* v. *Premier Ministre and Others* ECLI:EU:C:2020:791 (Grand Chamber Judgment, 6 October 2020); Case C-311/18 *Data Protection Commissioner* v. *Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559 (Grand Chamber Judgment, 16 July 2020) (*Schrems II*); BBW; *Al-Nashiri* v. *Poland*; *Husayn (Abu Zubaydah)* v. *Poland*; *El-Masri* v. *Macedonia*; *Agiza* v. *Sweden*, CAT/C/34/D/233/2003 (25 May 2005); *Alzery* v. *Sweden*, Communication No. 1416/2005, CCPR/C/88/D/1416/2005 (10 November 2006); *Khaled El-Masri* v. *United States* (Report on Admissibility), Report 21/16, Petition 419-08, OEA/Ser.L/V/II.157, Doc. 25 (IACHR, 15 April 2016).
[114] Ashley S. Deeks, 'Confronting and adapting: intelligence agencies and international law' (2016) 102 Va. L. Rev. 599-685 at 621-30.
[115] Jack Goldsmith, *Power and Constraint: The Accountable Presidency After 9/11* (New York: WW Norton, 2012) p. 37.
[116] Deeks, 'Confronting and adapting', 600-29.
[117] While this naturally applies more visibly to intelligence communities operating in democratic States, the possibility of those operating in non-democratic States being held to account by foreign intelligence communities that they cooperate with should not be completely excluded.

determine whether a State will comply with international law in its intelligence activities.[118] I explain why in the following paragraphs.[119]

The intelligence community's role is to protect national security, and in national security matters, States are self-interested. From this perspective, international law should not matter much for the intelligence community's choice of action: decision-making should be guided solely by the national interest. Yet, depending on how States value their reputation, actions by other actors of the international legal order may affect what States perceive to be their interest. States' willingness to cultivate a good reputation induces them to consider the impact of their actions on their reputation, even when there might be benefits in acting otherwise.[120] States can have a reputation for various things, for instance, complying with international law; respecting human rights; being a dependable treaty partner; siding with allies; but also being tough or ensuring complete secrecy. Their reputation is mainly a matter of how other States perceive them, whether they ascribe a particular behaviour to the actor or the situation, and how they evaluate the behaviour. Assessing the impact of reputation on State compliance can prove challenging,[121] especially since many biases and heuristics impact how others perceive a State.[122] Nevertheless, reputation remains an important factor in explaining compliance with international law,[123] not least because the international legal order relies on conditional cooperation to function and being perceived as compliant enhances trust and brings political legitimation.[124]

For reputation to be affected, however, other actors must attribute the State's behaviour to dispositional rather than situational factors.[125] Dispositional attribution assigns the cause of behaviour to the actor's internal characteristics, whereas situational attribution assigns it to an event outside the actor's control.[126] International courts and bodies produce information about States' non-compliant behaviour. They publicly expose such behaviour and shape the saliency, credibility, and framing of information for other actors of the international legal order.[127] Said otherwise, judicial decisions produce information facilitating effective reputational deterrence. They also indicate the type of behaviour that would have constituted a lawful response to the factual situation faced by the State. State accountability thus sets a normative benchmark. The judgment or decision authoritatively declares that, when facing situation *x*, States may not respond with *y*. If, in future instances, States still decide to face situations similar to *x* with

[118] Sophie Duroy, 'State compliance with international law in intelligence matters: a behavioural approach' (2022) 13 JIDS 233-63.
[119] These paragraphs summarise an argument I made in a previous publication: Duroy, 'State compliance'.
[120] Andrew T. Guzman, *How International Law Works: A Rational Choice Theory* (Oxford: Oxford University Press, 2008) p. 34.
[121] See Rachel Brewster, 'Unpacking the state's reputation' (2009) 50 Harv. Int'l L. J. 231-69.
[122] Anne van Aaken, 'Behavioral international law and economics' (2014) 55 Harv. Int'l L. J. 421-81 at 479.
[123] Guzman, *How International Law Works*.
[124] Hurd, *How to Do Things with International Law*.
[125] Van Aaken, 'Behavioral international law', 477.
[126] Edward E. Jones and Keith E. Davis, 'From acts to dispositions: the attribution process in person perception', in Leonard Berkowitz (ed.), *Advances in Experimental Social Psychology*, vol. 2 (New York: Academic Press, 1965).
[127] Roy Shapira, *Law and Reputation: How the Legal System Shapes Behavior by Producing Information* (Cambridge: Cambridge University Press, 2020), p. 35.

response *y*, then other States are more likely to attribute this behaviour to dispositional rather than situational factors since *y*'s unlawfulness and the existence of alternative courses of action were indicated before. State accountability thus has a dual role. It is first an informational device for States, allowing them to adjust their perception of other States by relying on the normative benchmark set by the court. Second, accountability constitutes a tool directly affecting the State's reputation through the persuasive quality of the judgments and decisions.

This dual role of State accountability means that the sanctions imposed through accountability processes, whether of a direct, reputational, or indirect nature, can increase the (direct, reputational, and indirect) costs of violations. When costs increase, it becomes less interesting for States to resort to extra-legal measures to respond to national security threats. The reputational threat induced by State accountability thus functions as a deterring factor. According to theories of deterrence, actors will generally be deterred from breaching the law when the legal penalty they would receive for a breach, multiplied by the likelihood of swift detection and conviction, outweighs the gain.[128] The *perception* of the risk of accountability, more than the actual risk, deters actors from breaching the law.[129] Hence, how a State perceives the costs of accountability will determine the success of a deterrence strategy. In intelligence matters, this is also a function of the value that the State's intelligence community bestows upon relevant aspects of its reputation and (continued) cooperation with other States' intelligence communities.[130]

Accountability further constrains intelligence cooperation through the 'trickle down' effects of the normative benchmarks. Deeks conceptualised this as 'mechanisms of peer constraints' between intelligence communities.[131] This means that international legal constraints on one State's intelligence community can also constrain peer intelligence communities because of the willingness or necessity of continued cooperation. For instance, a State facing a decision that its surveillance legislation breaches a human rights treaty will (ideally) change its domestic legal framework. Then, to avoid being held to account for the acts of partner intelligence communities, the State's own intelligence community should require that information received from partner intelligence communities adhere to similar legal standards. It should further demand that any information shared be treated in compliance with the caveats imposed by its domestic legal framework.[132] Therefore, the standards imposed by the accountability forum will 'trickle down' to the State's intelligence partners due to their reliance on information sharing and cooperation. In addition, States subject to the jurisdiction of the same human rights body may preventively apply equivalent standards to their domestic surveillance regulation, thereby triggering a similar trickle-down effect with their own intelligence partners. The need for

[128] Christine Parker and Vibeke Nielsen, 'Compliance: 14 questions', in Peter Drahos (ed.), *Regulatory Theory: Foundations and Applications* (Acton: ANU Press, 2017), p. 227.
[129] Ibid., p. 228.
[130] Duroy, 'State compliance', 243.
[131] Ashley S. Deeks, 'Intelligence services, peer constraints, and the law', in Zachary K. Goldman, Samuel J. Rascoff and Jane Harman (eds.), *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (New York: Oxford University Press, 2016).
[132] *Schrems II*, para. 105. But see BBW, para. 362; and CFR, para. 276: 'This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer'.

cooperation, therefore, creates an accountability web whereby States are encouraged to comply with the standards imposed on their intelligence partners by accountability forums that they may not even be subject to. In turn, a single decision may constrain multiple intelligence communities and have much broader effects than the sole case forming the cause of action.

Intelligence communities are, therefore, constrained by international law in several ways. A remaining matter is that of the normative assessment. Would the intelligence community be more effective in protecting national security if it were not constrained by international law? To answer this question positively, one must consider that the intelligence community is a rational actor, always choosing the solution that best serves national security after a rational decision-making process. I have explained elsewhere why this is not the case, as the intelligence community is subject to many biases and heuristics.[133] These biases and heuristics are present at all stages of the intelligence cycle and in all decision-making processes therein. Furthermore, they are reinforced by the insular organisational culture and structural secrecy of intelligence agencies.

The role of international law, then, is to guard the intelligence community against its misperceptions. Law corrects some of the biases and heuristics of the intelligence community by obliging it to conform to a fixed (legal) framework. For instance, research has shown that groupthink behaviour may be moderated by emphasising specific procedural rules that regulate the decision-making process.[134] By imposing strict limits on what can be done, especially in acute crises, (international) law allows decision-makers to safeguard their own values and address the crisis lawfully and effectively. Not only is trespassing the confines of legality to respond to a crisis ineffective,[135] but it also undermines the legality of the institutions of the State. Law can be cumbersome and hinder swift action. However, it represents a safeguard for what national security really means: values, institutions, and the rule of law. From this perspective, one can argue that terrorism represents a national security threat more in the sense that we might undermine our democracy in response than for the real threat to the nation as an entity.[136] Further, the risk of a backlash triggered by non-compliance further increases a nation's security risk. It provokes an escalation in threats and conflict, on top of jeopardising intelligence cooperation.[137] Hence, as Baker underlined, international law reflects good national security policy along with good legal policy.[138]

---

[133] Duroy, 'State compliance', 235-41.
[134] Christoph Engel, 'The behaviour of corporate actors: how much can we learn from the experimental literature?' (2010) 6 *Journal of Institutional Economics* 445-75 at 453-5.
[135] Christian Bjørnskov and Stefan Voigt, 'When does terror induce a state of emergency? And what are the effects?' (2020) 64 J. Conflict Resol. 579-613; Oren Gross and Fionnuala Ní Aoláin, *Law in Times of Crisis: Emergency Powers in Theory and Practice* (Cambridge: Cambridge University Press, 2006).
[136] David M. Driesen, 'How courts can protect democracy from abuse of emergency powers', *Lawfare*, 22 February 2022, www.lawfareblog.com/how-courts-can-protect-democracy-abuse-emergency-powers accessed 23 February 2022.
[137] Sophie Duroy, 'The regulation of intelligence cooperation under international law: a compliance-based theorization', in Arianna Vedaschi and Kim Lane Scheppele (eds.), *9/11 and the Rise of Global Anti-Terrorism Law: How the UN Security Council Rules the World* (Cambridge: Cambridge University Press, 2021).
[138] James E. Baker, 'What's international law got to do with it? Transnational law and the intelligence mission' (2006) 28 Mich. J. Int'l L. 639-61 at 656.

4. THE INTELLIGENCE COMMUNITY AS A NORMATIVE ACTOR UNDER INTERNATIONAL LAW

Turning to the Chapter's second perspective: can the intelligence community be considered a normative actor under international law? Is it a norm-setter, or at least a norm-shaper? Whereas, in the past, the intelligence community remained silent on its practices, at best uttering 'neither confirm nor deny', the situation has changed. Forced exposure has triggered a matching need to legitimise intelligence activities through law. The intelligence community is now openly engaging with and interpreting international law. As its legal reasoning is necessarily instrumental and self-interested, it becomes crucial to evaluate whether and how the intelligence community's use of international law shapes the content of that law. In the following paragraphs, I distinguish three situations: (1) where intelligence activities remain secret and unacknowledged; (2) where intelligence activities are exposed but remain unacknowledged or unjustified in international law; and (3) where intelligence activities are both exposed and justified in the rhetoric of international law.

The starting point for assessing the normative role of the intelligence community is that secret practice is not State practice for the purpose of customary international law (CIL) development.[139] Hence, intelligence activities that remain secret and unacknowledged do not participate in shaping CIL and leave no overt trace on international law. However, they may have a more insidious effect on international law (regardless of its source) in two ways. First, secret practice may incrementally affect international law by developing an internal jurisprudence on interpreting the norm at stake.[140] One could here think of the Bybee-Yoo memoranda mentioned earlier and their effect on the USA's interpretation of the definition of torture under international law in contexts other than the CIA-led rendition, detention, and interrogation programme. Further, the memoranda's authors might have pursued their reasoning and arguments in their other professional positions, such as scholars or judges. In this way, even if the practice had remained secret and unacknowledged, the secret justification developed for it could still have influenced the State's interpretation of international law through domestic courts or scholarly literature. Secondly, secret, unacknowledged practice can increase the intelligence community's confidence that it can violate international law without incurring any costs.[141] This might trigger or reinforce an optimism bias,[142] emboldening the intelligence community to resort to similar practices more often or to use tougher means.

Rather differently, intelligence activities that are exposed but not explicitly acknowledged by the perpetrating State, i.e., that are not justified and legitimated in international law, can undermine international law and its compliance pull. The USA's strike on Ayman Al-Zawahiri, which killed him while standing on his balcony in the centre of Kabul, constitutes a recent example of an act for which the justification process did not involve any reference to

[139] Navarrete and Buchan, 'Out of the legal wilderness', 921.
[140] Perina, 'Black holes', 555-7.
[141] Ibid., 580.
[142] The optimism bias refers to individuals' tendency to overestimate their chances of positive experiences and underestimate their chances of negative experiences, causing overconfidence. Neil D. Weinstein, 'Unrealistic optimism about future life events' (1980) 39 *Journal of Personality and Social Psychology* 806-20.

international law.[143] A State's refusal to offer a legal justification for its intelligence community's activities can call into question whether the intelligence community feels bound by applicable legal norms, thus undermining the norms. A State's ambiguity about the legality of its intelligence community's activities may also facilitate political tolerance by the international community. Exposed but unacknowledged intelligence activities not condemned by the international community increase the risk that other actors will be incentivised to use similar practices, as the political costs of non-compliance are low.[144] Tolerance or ambiguity by the international community might thus even legitimate the practice. Only international legal accountability could then redress and rehabilitate the breached norm. In this sense, State accountability might mitigate the negative effect of unacknowledged or unjustified intelligence activities on international law.

At the same time, by refusing to offer a legal justification for an exposed intelligence activity, the State renounces its role in shaping international law. The State thus cedes this power to other States and non-state actors. The principle of sovereignty in cyberspace provides a contemporaneous example of a norm that is explicitly *not* shaped by States whose cyber operations are exposed. States are usually wary of framing their claims regarding specific incidents in cyberspace in international law terms. No State has ever claimed credit, openly or privately, for a cyber-espionage operation, and other States also tend to refer to (voluntary) 'norms of responsible behaviour in cyberspace' to complain about foreign States' malicious cyber operations.[145] However, States sometimes make an explicit claim that the principle of sovereignty has been breached in this context.[146] In addition to expansive scholarship on the topic,[147] States have also started to issue more general statements about the applicability of international law in cyberspace—thus providing a framework against which to issue statements

[143] The White House, 'Remarks by President Biden on a successful counterterrorism operation in Afghanistan', 1 August 2022, www.whitehouse.gov/briefing-room/speeches-remarks/2022/08/01/remarks-by-president-biden-on-a-successful-counterterrorism-operation-in-afghanistan accessed 21 August 2023. For an analysis of the legitimation process of the strike through an appeal to morality and notions of public good and revenge, see Marie Robin, 'Cibler Ayman Al-Zawahiri : Élimination juste ou juste une élimination ?', *Le Rubicon*, 8 February 2023, https://lerubicon.org/cibler-ayman-al-zawahiri accessed 15 February 2023.

[144] Perina, 'Black holes', 579.

[145] See, e.g., NATO's statement in support of Albania following the cyberattack targeting it. NATO, 'Statement by the North Atlantic Council concerning the malicious cyber activities against Albania. Press Release (2022) 118', 8 September 2022, www.nato.int/cps/en/natohq/official_texts_207156.htm accessed 21 August 2023. See, for various examples of unacknowledged cyber operations and an assessment of their international legality, François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020), ch. 5.

[146] This is particularly the case of states victims of cyber operations. For instance, after the Snowden revelations, Brazil called the wiretapping of President Dilma Rousseff's phone 'an attack on our country's sovereignty'. Patricia Rey Mallen, '"An attack on sovereignty": Brazil and Mexico react to NSA espionage', *International Business Times*, 3 September 2013, www.ibtimes.com/brazil-reacts-fury-nsa-spying-mexico-orders-probe-1402437 accessed 3 March 2023. Likewise, after the large-scale cyberattack targeting the country on 28 October 2019, Georgia stated that the attack 'infringed [its] sovereignty'. The Czech Republic also stated (on Twitter) that 'Attacks like the one on Georgia are a clear violation of state sovereignty'. Czech Ministry of Foreign Affairs, *Twitter*, 20 February 2020, https://twitter.com/CzechMFA/status/1230488370528346113 accessed 21 August 2023. See statements and discussion in Przemysław Roguski, 'Russian cyber attacks against Georgia, public attributions and sovereignty in cyberspace', *Just Security*, 6 March 2020, www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/ accessed 21 August 2023.

[147] See, e.g., Delerue, *Cyber Operations*; Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart, 2018); Antonio Coco, Talita Dias and Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under international law' (2022) 33 EJIL 1275-86.

about specific incidents.[148] Altogether, this process is slowly clarifying and/or changing the scope and content of the principle of sovereignty, but without the participation as such of the States whose cyber operations have been exposed. Non-acknowledgement by these States estops them from relying on that conduct as evidence that defines or shapes the law. It also precludes other States from using the practice as a legitimate precedent. Alexandra Perina thus concludes that, in this respect, a covert event 'may be less destructive than an overt, acknowledged violation' for international law.[149]

Thirdly, intelligence activities that are exposed *and* justified in the rhetoric of international law effectively shape the law. When States develop, assert, and persuade others of their interpretations of a rule, its meaning and/or scope can change.[150] This change usually occurs through an ongoing process of claims and counterclaims regarding the international legality of specific conduct. This has been most visible regarding the right to privacy following Edward Snowden's revelations about bulk data collection.[151] As Yuval Shany notes, this right's continued relevance in the digital age was helped by the theoretical shift from a dominant conception of privacy as a right to be left alone to notions of privacy involving the right to exercise control over personal data and its derivative uses, including control over inter-personal communication flows.[152] Yet, States' claims and counter-claims about how exactly the right to privacy constrained their bulk collection activities have also led the scope and content of this right to be seriously debated and, one could argue, restricted.[153] Starting immediately after the Snowden revelations exposed widespread practices of bulk data collection, States have made claims concerning the compatibility (or lack thereof) of the practice with the right to privacy in the UN General Assembly,[154] through diplomatic channels,[155] but also before human rights courts and tribunals.[156]

---

[148] A compilation of published national positions is available at NATO Cooperative Cyber Defence Centre of Excellence, 'National positions', edited 26 July 2023, https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions accessed 21 August 2023.

[149] Perina, 'Black holes', 574. See also Ashley S. Deeks, 'Intelligence communities and international law', in Anthea Roberts *et al.* (eds.), *Comparative International Law* (Oxford: Oxford University Press, 2018), p. 268 arguing that the US's lack of justification 'preserves the integrity of the "ordinary rules" of international law but at the expense of suggesting that certain areas of action remain unregulated by that law'.

[150] Hurd, *How to Do Things with International Law*.

[151] For a catalogue of the various revelations by Edward Snowden regarding the United States' surveillance activities, see Lawfare, 'Snowden Revelations', https://www.lawfaremedia.org/article/catalog-snowden-revelations, accessed 25 August 2023.

[152] Yuval Shany, 'Digital rights and the outer limits of international human rights law' (2023) 24 *German Law Journal* 461-72.

[153] For an analysis, see Sophie Duroy and Liliya Khasanova, 'Cyberespionage and human rights: a disappointing balance', in Antonio Segura Serrano (ed.), *The Challenge of Global Cybersecurity* (London: Routledge, 2024).

[154] For instance, when, in the immediate aftermath of the Snowden revelations, Germany and Brazil introduced a draft resolution in the UN General Assembly that envisaged the extra-territorial applicability of the right to privacy in surveillance activities, the USA objected to such extra-territoriality. See UN General Assembly, 'Brazil and Germany: Draft resolution. The right to privacy in the digital age' (1 November 2013) UN Doc. A/C.3/68/L.45; Colum Lynch, 'Exclusive: Inside America's plan to kill online privacy rights everywhere', *Foreign Policy*, 20 November 2013, https://foreignpolicy.com/2013/11/20/exclusive-inside-americas-plan-to-kill-online-privacy-rights-everywhere/ accessed 21 August 2023.

[155] See, for a summary and analysis, Smith-Colin and Kleinhenz, 'Analyzing public and state reactions'.

[156] See, e.g., the pleadings and participation of the governments of France, Norway and the Netherlands in the BBW case.

With regard to bulk data collection, the intelligence community could even be considered somewhat of a norm-setter in the legal sense. Ilina Georgieva thus argues that intelligence communities have generated norms for the rest of the international community through their bulk collection practices.[157] She identifies a bottom-up process of norm entrepreneurship, which can be summarised as follows. First, intelligence communities began secretly collecting data in bulk by tapping into optic fibre cables. Then, the Snowden revelations exposed this practice. Rather than fully submitting to the global outcry, the intelligence community defended its practice and managed to gain States' support, resulting in domestic legislation regulating the practice. The normalisation and legitimation of bulk data collection slowly ensued internationally, confirmed even by human rights courts and bodies.[158] Georgieva thus concludes that the intelligence community's 'capacity to [push the norm on bulk data collection] reflects their normative power—something assigned so far to rather state-like structures only'.[159]

When intelligence activities are exposed and acknowledged, claims by the intelligence community might be accepted, decisively rejected, or contested only partially or by certain actors. Accepted claims will change the content or scope of the rule being invoked as justification, while rejected claims will usually not directly affect this rule's content. In contrast, claims not decisively rejected or defeated in this initial contestation process will not instantaneously change the rule's content. However, they may create a precedent, providing a justification for future action and producing their effects on international law at this later stage.[160] This change may be normatively positive as a rule can adapt to ensure its relevance to evolving contexts. It may also be considered a regrettable change when States distort the law so much that it loses its meaning or boundaries. Article 51 of the UN Charter on the right to self-defence is an unfortunate example of such an effect.[161] Yet, regardless of how one assesses these changes, by justifying and legitimating its activities in the language of international law, the intelligence community shapes how the law evolves.[162] Intentionally or not, the intelligence community and its parent State reshape legal standards to fit their preferences for the case at issue, but with effects beyond intelligence activities.[163] If their justifications are uncontested or even accepted as valid by the international community, the legal standards and their interpretation will be strengthened.[164] Conversely, if the justification is contested or rejected, both the interpreting State's credibility and international law might end up undermined or

[157] Ilina Georgieva, 'The power of norms meets normative power', in Denis Broeders and Bibi van den Berg (eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Lanham: Rowman & Littlefield, 2020). Georgieva also makes the argument regarding the NSA's network infiltration technique Territorial Dispute (TeDi), but only a social norm, rather than legal, can be considered to have emerged in this context: Ilina Georgieva, 'The unexpected norm-setters: intelligence agencies in cyberspace' (2020) 41 *Contemporary Security Policy* 33-54.
[158] See section 2.3.
[159] Georgieva, 'The power of norms', p. 238.
[160] Kyle Rapp, *By Word, Not Deed: Advancing a Theory of Rhetorical Compliance in International Law* (PhD thesis, University of Southern California, 2022), p. 172.
[161] See Hurd, *How to Do Things with International Law*, ch. 4.
[162] Rapp, 'Justifying force', 338.
[163] Deeks, 'Intelligence communities', p. 262.
[164] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (Jurisdiction and Admissibility, Judgment), para. 186; Rapp, 'Justifying force', 356.

challenged. The legal norm might lose its relevance or compliance pull, and legal certainty will be affected.[165]

5. CONCLUSION

Whether or not one agrees that the intelligence community can ever be deemed a norm-setter, it is becoming harder to argue that the relationship between international law and the intelligence community is either superficial or one-sided. Rather, this relationship is better qualified as bidirectional and mutually constitutive. International law both constrains and enables the intelligence community. In turn, the intelligence community shapes international law. The intelligence community uses international law by putting forward interpretations that will legitimise its preferred outcomes and empower it to pursue its choices of policies. In doing so, the intelligence community changes the meaning ascribed to international norms. In addition, when the intelligence community refuses to abide by the rules of the legalism game by not providing a legal justification for its activities, it undermines the status of international legal norms, which may be perceived as less binding by the rest of the international community. For these reasons, the intelligence community has truly become a normative actor under international law.

[165] Ibid.