Chapter 2. Intelligence Activities and International Law

2.1 Introduction

For as long as intelligence activities and international law have coexisted, it has been written and believed that there was 'something almost oxymoronic about addressing the legality of espionage under international law'.[1] According to this view, both would have developed side by side without ever (meaningfully) interacting. This 'realpolitik' vision of international law has prevailed in scholarly writings and international practice up until the end of the Cold War. Until then, scholars and policy-makers alike considered that national security objectives trumped legal and ethical concerns or, to put it simply, that the end justified the means. This view was reinforced by the strikingly underdeveloped domestic legal status of intelligence communities and the almost complete absence of arrangements for overseeing intelligence activities.

Yet, although peacetime espionage is never explicitly addressed by international law, since the birth of international law itself,[2] a small but constant stream of scholarly articles has examined the international legality of espionage. The focus on intelligence activities more generally is rather recent. It can be considered a consequence of the appearance of new threats, new responses, and overall a new legal paradigm for the work of intelligence communities. For simplicity purposes, one could date the beginning of this new 'intelligence era' to 9/11, but most of its components can be traced back to the end of the Cold War. Indeed, the collapse of the USSR marked the downfall of the equilibrium established between the West and East blocks, according to which the principle of reciprocity was the crucial means of regulation of intelligence activities.

As defined in the Introduction, intelligence is secret, state activity to understand or influence foreign and domestic entities.[3] A review of the existing international law literature clearly evidences the lack of a framework that comprehensively addresses all intelligence activities and makes sense of the various interactions identified between intelligence activities and international law. The present Chapter seeks to fill this gap by providing a comprehensive account and analysis of these interactions. I start by reviewing the main scholarly positions on the status of intelligence activities in international law (section 2.2), a review necessary to understand the (legal) paradigm shift witnessed in the past decades (section 2.3). I then build upon these foundations to sketch the international legal framework governing intelligence activities today (section 2.4). Finally, I highlight how this legal framework, together with the automatic engagement of state responsibility for its violation, represents the first layer of the regulation of intelligence activities under international law (section 2.5).

---

[1] Daniel B. Silver, Intelligence and Counterintelligence, in National Security Law 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005) (updated and revised by Frederick P. Hitz & J.E. Shreve Ariail).
[2] Grotius 'On the Law of War and Peace', Book III, Ch. IV xviii 655 (1695: F. Kelsey translation, Oxford, 1925).
[3] Chapter 1, section 1.2.1.

2.2 The Scholarly Divide: Realpolitik vs Formalism

Scholars writing about the relationship between international law and intelligence often endorse one of either side of an unresolved debate: the realist view or the formalist view. The realist view sustains that intelligence protects the very existence of states, so that states have not and will not allow any international legal constraint on it. In contrast, formalists consider that international law naturally applies to the intelligence community as organs of the state, and thus intelligence activities are subject to the same international legal constraints as other state activities.

An important part of the academic literature focuses on the age-old question of the legality of peacetime espionage — it indeed seems to be universally accepted that spying is legally permissible during armed conflicts.[4] A few authors go further and attempt to list and analyse the various ways in which international law and intelligence activities interact. From their work emerges a set of disparate rules that indirectly constrain the conduct of intelligence communities worldwide. What also becomes evident when reviewing this literature, however, is that scholars are lacking a common framework through which to assess the status of intelligence activities under international law. This lacuna is apparent in the differing approaches taken by the authors, as well as in the various models they use to present the results of their analyses.

2.2.1 The Formalist Account

Cold War-era intelligence regulation was almost exclusively state-centric and reliant on the principle of reciprocity. Focusing on Cold War-era espionage, Simon Chesterman thus identifies three corpuses of international rules restricting the freedom of the intelligence community in peacetime.[5] First, the principle of non-intervention, as formulated by the PCIJ in the *Lotus* case,[6] prohibits unauthorised entry into a foreign state's territory as well as unauthorised use of such territory. Second, treaty law governing diplomatic and consular relations implicitly tolerates limited intelligence gathering as forming a necessary part of diplomacy. However, it also grants states an absolute discretion to terminate consular or diplomatic relationships, or the presence of any such personnel.[7] The final area of interaction concerns arms control treaties. Chesterman regards the various agreements on strategic arms limitations between the US and the USSR (and later in multilateral settings) concluded in the 1960s and 1970s as explicitly providing for a right to collect intelligence in order to assess compliance with the treaties' obligations.[8] The treaties protect this right by providing for a corresponding duty of the state under surveillance not to interfere with the collection of information.

---

[4] See below section 2.4.2.2 for a more nuanced analysis of this issue.
[5] Simon Chesterman, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford University Press 2011) Chapter 1 'The Spy Who Came From the Cold War'.
[6] S.S. Lotus (France v. Turkey), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7), para 18: 'The first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary— it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.'
[7] Chesterman (n 5) 32.
[8] Chesterman (n 5) 33–34.

Hinting at a paradigm shift, Chesterman highlights that the end of the Cold War destabilised the existing equilibrium,[9] whereas 9/11 put an end to reciprocity as the rationale for limiting intelligence activities. Indeed, the post-9/11 terrorist threat was not counterbalanced by fears of state-imposed consequences for violating the law.[10] Although the remainder of Chesterman's book focuses on surveillance, other authors have attempted to list the current sources of regulation for intelligence activities generally in the twenty-first century security landscape.

Dieter Fleck, adopting a different approach, starts by questioning the generally accepted premise that all intelligence activities would inherently be tolerated by international law.[11] According to this premise, when examined in isolation from the means used to achieve their objectives, intelligence activities do not constitute an internationally wrongful act. Hence, the reasoning goes, intelligence objectives themselves are permissible, if not lawful, and only the underlying conduct can be questioned.[12] Yet, looking at covert action in particular, Fleck observes that international law contains a corpus of rules prohibiting subversive action in peacetime, as reflected in the UN General Assembly 'Friendly Relations Declaration'.[13] The principles of sovereignty and of non-intervention, as defined in the Declaration, thus prohibit intervention in the political independence of another state; unauthorised entry into a foreign state's airspace or territory; illegal exercise of jurisdiction on foreign territory; and attempts to destabilise the government of another state.[14] Hence, covert action, which aim usually conflicts with at least one of these principles, would be prohibited due its objective and not (only) the underlying conduct.[15]

For this reason, Fleck emphasises that intelligence activities in breach of these principles can never be justified under customary international law.[16] In addition, he argues, the fact that states commit these acts clandestinely shows the absence of opinio juris in favour of recognising the legality of covert action.[17] This argument, whether it applies to covert action only or to intelligence activities more generally, has been highly debated in the literature. Realist authors have attempted to rebuke it by arguing that 'several states' now claim responsibility for their intelligence acts.[18] Consequently, because espionage is admitted by states and 'a majority of

---

[9] Chesterman (n 5) 36–37.
[10] Chesterman (n 5) 38.
[11] Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering Symposium: State Intelligence Gathering and International Law' (2006) 28 Michigan Journal of International Law 687, 688–694.
[12] This is the position defended by the most nuanced realist scholars and the majority of the formalist side.
[13] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, adopted by UN General Assembly Resolution 2625 (XXV), 24 October 1970.
[14] Fleck (n 11) 692–693.
[15] Fleck nevertheless mentions that the underlying conduct, if it constitutes 'a crime', can also be the cause of illegality. Fleck (n 11) 693.
[16] Fleck (n 11) 693.
[17] Fleck (n 11) 693.
[18] As far as the present author is aware, only the US has ever formally acknowledged its involvement in espionage over foreign states, and only on three occasions: the U-2 incident in 1960; the 1982 incident involving US reconnaissance flights over Nicaragua; and the Snowden revelations in 2014. See, respectively: Secretary Herter, 'United States Plane Downed in Soviet Union: Statement by Secretary Herter', 42 DEP'T ST. BULL. 816, 816 (1960); US Ambassador to the UN, Jean Kirkpatrick, 'Declaration before the UN Security Council', U.N. SCOR, 37th Sess., 2335th meeting, para 132, U.N. Doc. S/PV.2335 (25 March 1982); and Barack Obama, 'Remarks by the President on Review of Signal Intelligence' (17 January 2014), para 139.

scholarly literature', states practicing it would demonstrate the required opinio juris of believing they are acting lawfully.[19] Yet, in order to agree with these authors,[20] one would have to consider that (mostly secret and patchy) state practice makes the law. Such a position cannot be sustained without discarding the well-established process of formation of customary international law (CIL), which necessarily comprises public, general, and uniform state practice, together with opinio juris.[21]

Responding to this scholarly claim that the illegality of some intelligence activities would be nullified by CIL developments, Iñaki Navarrete and Russell Buchan thoroughly debunk the 'mainstream view' by providing a comprehensive analysis of the formation of customary exceptions in matters of peacetime espionage.[22] Regarding state practice, they first explain that physical acts of espionage committed in secret on the ground do not qualify as state practice for the purpose of CIL formation.[23] In addition, they note that the sole form of available public state practice, coming through domestic legislation providing a legal basis for the functions of intelligence agencies and delineating the extent of their powers, merely represents a trend that can be found in a few Western liberal democracies. It is therefore neither general nor representative.[24]

Then, regarding opinio juris, Navarrete and Buchan carefully examine states' statements on peacetime espionage. They are forced to conclude with the absence of any opinio juris in favour of customary exceptions to international law for any form of espionage.[25] Indeed, while states have not shied away from supporting the permissibility of espionage from international spaces, they have been extremely careful never to express themselves about the existence of a customary rule authorising other forms of espionage. States have thus either used legal euphemisms[26] to ensure that conventional developments did not spill over into CIL, or adopted a plausible deniability attitude preventing any development of a legal norm.[27] In conclusion, despite frequent practice, the different forms of peacetime espionage used by states have never given rise to any customary exception because the practice is accompanied by a 'sense of wrong'.[28] Strikingly, no claim as to the existence of a customary exception to international law has ever been made by a state.

---

[19] For an express rebuttal of Fleck's argument, see Fabien Lafouasse, *L'espionnage Dans Le Droit International* (Nouveau monde 2012) 26–27. Quotes translated from French.

[20] See Iñaki Navarrete and Russell Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 897 footnote 12 for an extended list of scholars supporting this view and arguing for customary exceptions to international law regarding peacetime espionage.

[21] See ILC, 'Draft conclusions on identification of customary international law', Adopted by the International Law Commission at its seventieth session, in 2018, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/73/10, para 65).

[22] Navarrete and Buchan (n 20).

[23] Navarrete and Buchan (n 20) 920.

[24] Navarrete and Buchan (n 20) 923–926.

[25] Navarrete and Buchan (n 20) 927–934.

[26] Navarrete and Buchan (n 20) 928 on the 'Policy of Silence'.

[27] Navarrete and Buchan (n 20) 934–941. See also Alexandra H Perina, 'Black Holes and Open Secrets: The Impact of Covert Action on International Law' (2014) 53 Colum. J. Transnat'l L. 507.

[28] Navarrete and Buchan (n 20) quoting; Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in Roland J Stanger, Richard A Falk and Quincy Wright (eds), *Essays on espionage and International law* (Ohio State University Press 1962) writing that peacetime espionage 'appears to be a case in which frequent practice has not established a rule of law because the practice is accompanied not by a sense of right but by a sense of wrong'.

Dieter Fleck further looks at the corpuses of law that intelligence activities, whether inherently lawful or not, might be breaching when operationalised. Breaking with the interstate focus adopted by the rest of the literature, Fleck highlights that most modern intelligence activities may be in breach of international human rights law due to the methods used.[29] He also stresses that intelligence objectives do not justify derogating from human rights regimes, a welcome clarification in the midst of talks about trade-offs between liberty and security. Then, as was also argued by Chesterman, Fleck notes that special treaty regimes may contain specific restrictions to intelligence gathering methods. He concludes, expectedly, that international law prohibits intelligence gathering if and when coupled with additional elements of illegality. Yet, he is the first one to consider objectives, and not only conduct, as susceptible of constituting an element of illegality.[30]

2.2.3 Formalism and Pragmatism

Taking account of the post-9/11 paradigm shift in the interactions between international law and intelligence communities, Ashley Deeks adopts yet a different approach to the issue.[31] Starting from the premise that we are facing a necessary momentum towards a more formalist view of the relationship between intelligence and international law, Deeks advocates moving from a state-centric paradigm of intelligence regulation to one that takes into account and protects individual rights. Accordingly, she identifies three sources of law governing peacetime intelligence activities: customary international law related to sovereignty, non-intervention, and territorial integrity; treaties governing diplomatic and consular relations; and IHRL. Deeks adopts a pragmatic middle ground in the realism/formalism debate, proposing a framework that would 'strike a sustainable balance between the national security equities of states and core rights-related values'.[32] Such framework would achieve this aim thanks to a sliding-scale interpretive approach to the international law/intelligence relationship. Hence, when the target of an activity is an individual, states should interpret their international obligations strictly in order to minimise the risk of harm. In contrast, when states undertake more traditional intelligence activities that primarily implicate the equities of other states, they should be permitted greater flexibility in interpreting relevant international law. Deeks justifies this approach primarily on the basis that states have tacitly consented to it. However, by so doing, she invokes one of the customary exceptions later debunked by Navarrete and Buchan.[33]

In his response to Deeks, Craig Forcese presents an original three-tier analysis of the interactions between intelligence activities and international law.[34] He first distinguishes intelligence collection, which he argues is not regulated per se by international law, from covert action. He deems the latter regulated by international law 'to the extent that it amounts to coercive interference into the affairs of another state or the non-consensual exercise of state

[29] Fleck (n 11) 693.
[30] See also Craig Forcese, 'Pragmatism and Principle: Intelligence Agencies and International Law' (2016) 102 19, 80.
[31] Ashley Deeks, 'Confronting and Adapting: Intelligence Agencies and International Law' (2016) 102 Virginia Law Review 599.
[32] Deeks (n 31) 606.
[33] Deeks (n 31) 605.
[34] Forcese (n 30).

powers on the territory of another state'.[35] Forcese then nuances this duality with a third layer. He thus points out that both intelligence collection and covert action are regulated by more specific international rules or regimes (such as IHRL) governing the underlying conduct of the activity at stake.[36]

Forcese then moves on to assessing Deeks' sliding-scale model. While recognising virtue to the pragmatism of the approach, which incorporates international law into the decision-making process of intelligence agencies,[37] he warns against the resulting weakening of international legal norms that would inevitably follow the adoption of this realist policy as representing the *content* of the law.[38] Concluding, Forcese underlines that 'it is better to protect law, and accept that questions of expediency may deprioritize legality in the calculus conducted by states, than to "collapse … any distinction between law and politics, between breach and compliance".'[39]

A similar attempt at pragmatism can be observed in Asaf Lubin's endeavour to theorise a 'liberty right to spy' on the model of just war theories.[40] Lubin starts from the assumption that intelligence collection is necessary in all domains of international relations, but also that it actually advances international peace and security. This flawed realist premise leads to an attempt to justify, using a kind of backward inductive reasoning,[41] a right to spy belonging to states. Yet, this is done without sufficient legal grounding or justification. On the contrary, this conflation of international politics, state practice, and the law demonstrates a misunderstanding of the function and workings of international law. Further, damaging the integrity of the law through a pragmatic attempt to align it with state practice has the perverse consequence of granting states a legal right to advance their national security, no matter how they define it, through whatever means they deem fit. Lubin's approach also confuses issues of legality and compliance: non-compliance should be addressed by appropriate support activities and enforcement interventions, not by changing the law to make the problem disappear.[42] As Lauterpacht emphasised in a different context, the failure of existing enforcement strategies is 'a failure of political will, not of legal right'.[43]

The realist belief in military force and unfettered intelligence activities forming the premise of Lubin's argument has failed to create the national (or indeed international) security

---

[35] Forcese (n 30) 80.
[36] Forcese (n 30) 68; 80.
[37] Forcese (n 30) 82.
[38] Forcese (n 30) 83–85.
[39] Forcese (n 30) 84 quoting Nigel D. White, Advanced Introduction to International Conflict and Security Law (Edward Elgar Publishing 2014) 70.
[40] Asaf Lubin, 'The Liberty to Spy' (2020) 61 Harv. Int'l LJ 185.
[41] In game theory, backward induction is the process of reasoning backwards in time, from the end of a problem or situation, to determine a sequence of optimal actions. Here, the solution to the problem (non-compliance) would however be found by creating a right removing (rather than solving) the problem: states' right to spy.
[42] The danger of such an approach was highlighted by the US Supreme Court in a case concerning Native American land, in which the Court stated that: 'Unlawful acts, performed long enough and with sufficient rigor, are never enough to amend the law. To hold otherwise would be to elevate the most brazen and longstanding injustices over the law, both rewarding wrong and failing those in the right'. *McGirt* v. *Oklahoma*, 591 U.S. 18-9526, 9 July 2020, 42.
[43] Records of the International Military Tribunal, Volume 19, 461 (26 July 1946), Statement by British prosecutor Shawcross, partially authored by Hecht Lauterpacht.

it promised. Rather, it aggravated the security dilemma.[44] It has also been repeatedly disproved by empirical evidence[45] and one could easily argue that realist theories have made the world manifestly less secure. Yet, these theories constitute the sole rationale justifying why international law should apply differently to intelligence activities compared with other state activities in peace and security matters. Damaging the integrity and normative strength of general norms of international law on the basis of such realist assumptions should, therefore, not appear wise nor promising to anyone concerned about improving security. This conclusion stands even if one assumes, as Lubin does, that 'the law on espionage is filled with a myriad of legal gaps'[46] and 'blind spots'.[47]

2.2.4 Stuck in Another Era? The Realist Account

Other scholars, on the contrary, stick to the realpolitik view and refuse to acknowledge that international law could possibly, let alone meaningfully, regulate intelligence activities.[48] John Radsan thus advises the academic community that, 'accepting that espionage is beyond the law, we should move on to other projects — with grace'.[49] Others also consider that regulation would be detrimental to peace and security.[50] Yet, because of their strictly interstate perspective and their focus on establishing either the legality of intelligence activities per se or their lack of regulation by international law (and thus their non-illegality), the positions embraced by realist authors are necessarily incomplete and outdated.

First, by failing to account for the increasing importance of human targets in modern intelligence activities (bulk data collection, surveillance, counterterrorism, rendition, lethal drone strikes, etc.), realist authors negate the relevance of IHRL in assessing the legality of such activities. The abstract object of 'espionage' thus conceived by realist authors is a fiction, separated from its objectives and underlying conducts. And there seems to be very little value in asserting that espionage is unregulated if one cannot operationalise it lawfully. As a result, the realist assessment is necessarily incomplete, if not artificial.

In addition, because realist authors simultaneously misunderstand the formation of customary international law,[51] their argument on customary exceptions would result in an

---

[44] The security dilemma is a situation whereby 'the means by which a state tries to increase its security decrease the security of others'. Robert Jervis, 'Cooperation under the Security Dilemma' (1978) 30 World Politics 167, 169.

[45] For an analysis of damages inflicted to international peace and security by political espionage justified on the basis of realist theory, with multiple historical and recent examples, see Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing 2019) Chapter 2.

[46] Lubin (n 40) 231.

[47] Lubin (n 40) 242.

[48] See e.g., Matteo Tondini, 'Espionage and International Law in the Age of Permanent Competition' (2018) 57 Military Law and Law of War Review 17; Catherine Lotrionte, 'Countering State-Sponsored Cyber Economic Espionage under International Law' (2015) 40 North Carolina Journal of International Law 443; Lafouasse (n 19); Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2007) 28 Mich. J. Int'l L. 625; Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 AFL Rev. 217; Geoffrey B Demarest, 'Espionage in International Law' (1995) 24 Denv. J. Int'l L. & Pol'y 321. To a lesser extent, see A Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 Michigan Journal of International Law 595 arguing not that espionage is lawful but that it simply is 'beyond the law' (597) and that 'international law does not change the reality of espionage' (623).

[49] Radsan (n 48) 597.

[50] Sulmasy and Yoo (n 48).

[51] See Navarrete and Buchan (n 20).

absurd conclusion if we applied it to modern intelligence activities. The fact that all states are violating IHRL through their intelligence activities and consider it 'right' to do so for national security reasons would make it lawful for states to violate IHRL and demonstrate the required opinio juris at the same time. The realpolitik argument therefore appears fallacious. It is also outdated, belonging more to the Cold War era than to the post-9/11 context, and it increasingly moves away from the practice of intelligence communities themselves, which dedicate growing resources to ensuring the international legality of their actions.[52] Paradoxically, therefore, realists appear disconnected from the very reality of today's intelligence activities.

Further, the focus of many of these authors on showing the legality of intelligence activities in abstracto is redundant: the legality of intelligence activities cannot be dissociated from the legality of the underlying conduct and from the legality of their objectives. Hence, and without purporting to solve the age-old debate over legality,[53] it appears from the literature review conducted in this section that the inherent legality (or non-prohibition) of certain or all intelligence activities is a moot question. What matters is whether the means and objectives of the intelligence activity under scrutiny are of such a nature as to constitute an internationally wrongful act. Intelligence activities triggering the application of international law either involve an unlawful underlying conduct and/or objective, and they constitute an internationally wrongful act; or the underlying conduct *and* objective do not breach any principle or rule of international law, and the activity is permissible.

2.3 The Paradigm Shift

Intelligence historian Christopher Andrew thoroughly documented the difficulties that Western intelligence communities experienced in adapting to the changes resulting from the end of the Cold War.[54] The breakdown of the equilibrium induced by the opposition of the West and East blocks meant that intelligence agencies could no longer accurately predict threats.[55] However, Andrew also highlights that both the West and the East had experienced important intelligence failures already before the 1990s.[56] Such failures, he explains, can be attributed to intelligence services' lack of attention to the Middle East and their insufficient knowledge about theology and non-Western cultures.[57] Surprisingly, however, the end of the Cold War did not result in a redirection of resources to those so-called 'emerging' threats. Quite the opposite, until 9/11, most intelligence communities in the West were blind to the threat posed by al Qaeda. Exacerbating this blissful ignorance were institutional blockages and an embedded short-term

---

[52] E.g., the number of legal officers within the CIA grew from ten in the mid-1970s to approximately 150 in 2010. See Jack Goldsmith, *Power and Constraint: The Accountable Presidency After 9/11* (W W Norton & Company 2012) 87. Reasons for this pervading legalism are explained in the next section.

[53] Over which the ICJ declined to pronounce itself, despite several opportunities to do so. *United States Diplomatic and Consular Staff in Tehran (United States v Iran)* [1980] ICJ Reports 1980 3 (ICJ) [40]; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)* [1986] ICJ Reports 1986 14 (ICJ) [123, 136–140].

[54] Christopher Andrew, *The Secret World: A History of Intelligence* (1st Edition, Allen Lane 2018).

[55] Andrew (n 54) 701–730 Chapter 30 'Holy Terror'.

[56] To cite only one, the Iranian Revolution caught the US completely unprepared and unaware. Andrew (n 54) 701–703.

[57] Andrew quotes Sir Mark Allen, the 'leading Arabist in SIS', who concluded after 9/11: 'We were just looking the wrong way . . . the failure to appreciate the significance of radical Islam since the Second World War was largely a consequence of our mindset that Arab nationalism was the key issue.' Andrew (n 54) 737.

historical perspective,[58] both of which made it 'impossible to understand adequately the threat from Islamist terrorism'.[59] As Dick Heuer famously explained, 'major intelligence failures are usually caused by failures of analysis, not failures of collection. Relevant information is discounted, misinterpreted, ignored, rejected, or overlooked because it fails to fit a prevailing mental model or mind-set'.[60] The dramatic intelligence failures of 9/11 and Operation Iraqi Freedom are evidence that the transition to a post-Cold War world was arduous.

The end of the equilibrium made necessary by the Cold War also brought down the principle of reciprocity as the leading legal principle regulating intelligence activities. Instead, intelligence communities now faced non-state actors. With different agendas to Cold War-superpowers' intelligence agencies, these non-state actors could not be expected to abide by the same rules nor use the same means and methods. As old threats became less significant and new challenges arose, intelligence communities started reacting to their repeated failures in sometimes extreme ways.[61] They thus experimented with 'new' types of responses or, more accurately, reverted to extra-legal means and methods where deemed 'necessary'. This was particularly visible in the US-led response to 9/11, the 'global war on terror', aptly labelled as both 'a moral failure and a lamentable fiasco'.[62] Alongside, the development and increasing use of modern technologies by intelligence communities started to pose new legal issues. Human targets became the norm, triggering questions as to the applicability of IHRL, and intelligence leaks and scandals multiplied. It became untenable to continue to pretend that intelligence activities remained unregulated by international law and obeyed only to a realist reciprocity principle between superpowers. In other words, it could no longer be argued that international law authorised states to respond to security threats in any way and manner they deemed necessary.

The literature review conducted in the previous section evidenced a real paradigm shift between the regulation of intelligence activities during the Cold War era, and the modern post-9/11 regulation. While a more realist vision of the issue, in which the principle of reciprocity governed intelligence activities in a purely interstate paradigm, prevailed during the Cold War, we have now moved to a more formalist vision of the interactions between intelligence activities and international law. This is due to a number of factors, some of which were identified in preceding paragraphs.

Ashley Deeks justifies the necessary shift towards a formalist vision of the interactions between intelligence activities and international law by reference to four interlocking domains of change,[63] providing a sensible framework to apprehend the rationale underlying the modern paradigm. First, she explains, the general public has acquired a new breadth of knowledge about, and is increasingly attentive to intelligence activities undertaken by states. This is both

---

[58] Andrew (n 54) 720–723; 728; 737.
[59] Andrew (n 54) 730.
[60] Richards J Heuer, *Psychology of Intelligence Analysis* (Center for the Study of Intelligence, Central Intelligence Agency 1999) 65.
[61] This has been referred to as 'accountability ping-pong', i.e., reactive measures that overcorrect the last politicised and sensationalised intelligence failure, thus paving the way for flipside errors. Philip E Tetlock and Barbara A Mellers, 'Intelligent Management of Intelligence Agencies: Beyond Accountability Ping-Pong' (2011) 66 American Psychologist 542.
[62] Hugues Moutouh and Jérôme Poirot, *Dictionnaire du renseignement* (PERRIN 2018) 193. Translated from French.
[63] Deeks (n 31) 600–629.

due to and reinforced by the stream of intelligence leaks (facilitated by electronic means), but also by somewhat voluntary efforts of transparency from intelligence communities,[64] as well as by the increased physical detectability of some intelligence activities (e.g., rendition flights, targeted killings, cyber malware, etc.). The consequence of this 'near-real time' provision of information is that the public reacts to the information and can exert pressure on its government (which may in turn exert pressure on a foreign government) through its reactions.

Second, in the wake of what was perceived as a massive failure in intelligence gathering (9/11) and following claims for increased executive powers to face the 'new' transnational and globalised terrorist threat, intelligence agencies worldwide have gained, de facto or de jure, more powers and missions than ever before in democracies (e.g., law enforcement, interrogation, detention, use of force, and virtually unlimited surveillance powers). As Deeks highlights, 'these new missions implicate non-state actors as never before'[65] and trigger interactions with individuals who are not associated with any foreign government. This renders moot any reliance on the principle of reciprocity to govern such interactions.

Third, Deeks emphasises the increasingly legalised culture of intelligence communities. This phenomenon, termed 'intelligence legalism',[66] began when states gave legal status to their intelligence agencies. It was exacerbated in recent decades due to increasing domestic regulations[67] (which include international rules and standards) and an increased understanding by agencies of the relevance of legal compliance for their perceived legitimacy and the necessities of cooperation.[68] In other words, because the public is more aware of their activities, intelligence agencies are increasingly governed by law. This leads them to pay increasing attention to the law and to include it as a relevant factor in their decision-making processes.[69] In addition, intelligence activities are increasingly the subject of litigation, causing intelligence communities to adapt as decisions on their legal compliance are made. Deeks predicts that, as disclosures about intelligence activities become more frequent, litigation will increase exponentially and plaintiffs' chances of being successful will follow suit.[70]

Finally, as a link to the three preceding changes, Deeks highlights the 'humanisation' of international law, or the move away from a pure Westphalian vision of international law. Indeed, the protection of individuals by international law can be observed in diverse areas beyond human rights law, including investment, intellectual property, the conduct of hostilities, and the environment. This goes on par with individuals' increased access to international forums. Hence, the argument could be summarised as follows: because individuals are subject to legal protection, have more information about intelligence activities and avenues to obtain redress if their rights are breached, intelligence communities must take the law into account in

[64] On public disclosures and their motives, see Ofek Riemer, 'Politics Is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States' (2021) 42 Contemporary Security Policy 554.
[65] Deeks (n 31) 622.
[66] Margo Schlanger, 'Intelligence Legalism and the National Security Agency's Civil Liberties Gap' (2015) 6 Harv. Nat'l Sec. J. 112.
[67] Deeks (n 31) 624.
[68] Deeks (n 31) 628.
[69] See Chapter 7 for the modelling of these decision-making processes.
[70] Deeks (n 31) 625–628.

their activities. In consequence, placing human rights at the centre of security intelligence is right not only in principle but also at the pragmatic level.[71]

Furthermore, both the nature of modern security threats, emanating as much from non-state actors as from states themselves, and the development of new technologies and methods of intelligence collection have shifted the focus from the principle of reciprocity to a wider corpus of rules. As I explained earlier in this section, this shift has rendered moot the carefully attained interstate equilibrium of the Cold War.[72] While the rules developed during the Cold War era remain applicable to interstate relations, new intelligence activities have triggered the applicability of a number of 'new' rules. These rules of international law have a territorial and extraterritorial reach, they apply to activities targeting both states and individuals and, as demonstrated in the next section, they apply to *all* intelligence activities. There is no 'legal limbo' or ambiguity about the applicability of international law to intelligence activities in the post-9/11 paradigm. With this new paradigm has come an era of increased state accountability for intelligence activities constituting internationally wrongful acts. Accountability processes have clarified the principles and legal framework governing intelligence activities, and affirmed their applicability to intelligence activities. As a result, a legal framework can now be unambiguously identified.

2.4 International Law and Intelligence Activities: The Legal Framework

Having established that addressing the international legality of intelligence activities is not as oxymoronic as it may seem from a Cold War era mind-set, I now move to sketching the international legal framework governing intelligence activities. It is common practice to consider that the interaction of disparate rules of international law with intelligence matters simply 'constrain' intelligence communities' range of action. However, this section shows that it is no less correct to claim that international law actually *governs* intelligence activities.

The areas of interaction between international law and intelligence activities are usually presented according to different models: wartime/peacetime; geographical; conduct-based; rule-based; etc. I propose to abandon these distinctions, focusing instead on examining intelligence activities and categories of constituent acts according to whether they inherently constitute an internationally wrongful act; are explicitly allowed by international law; or are regulated through their underlying conduct only.

2.4.1 Intelligence Activities Inherently Prohibited by International Law

The permissibility of many wartime intelligence activities can be justified on the basis that the obligation to respect the territory or government of enemy belligerents is lifted by the necessities of war.[73] Outside armed conflicts, however, the principles of sovereignty, non-intervention, territorial integrity, self-determination, and the prohibition of the use of force form the foundations of the post-World War II international legal order. Affirmed in Article 2 of the UN Charter,[74] the precise content of these principles has been developed first in UNGA

[71] Peter Gill and Mark Phythian, *Intelligence in an Insecure World* (Polity Press 2018) 213.
[72] Chesterman (n 5) 38.
[73] See below section 2.4.2.2.
[74] United Nations Charter, Article 2: 'The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.
(1) The Organization is based on the principle of the sovereign equality of all its Members.

Resolution 2625 (XXV) ('Friendly Relations Declarations'),[75] widely considered to represent customary international law.[76] The Friendly Relations Declaration defined non-intervention and listed conducts in breach of state sovereignty. A decade later, UNGA Resolution 36/103 – which status as representing positive law is more contested due to having been adopted through a vote[77] – further specified the content of states' rights and obligations with regard to Articles 2(1) and 2(4).[78] Two types of intelligence activities are identified as inherently contravening the principles of non-intervention and territorial sovereignty as defined in those instruments: covert action and territorially intrusive acts. They are examined and analysed separately in the following subsections.

2.4.1.1 Covert Action

Covert action is the US term of choice to refer to what other states might call 'special operations', 'special political action', 'disruptive operations', 'active measures', 'event-shaping', and many other things. I use the term 'covert action' to refer to these types of active measures generally, without prejudice to the state conducting them. The literature generally adopts the definition provided by the US National Security Act Sec. 503 (e). It defines covert action as an 'activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly'.[79] While we should also account for the existence of covert action on a state's own territory (for instance by the British intelligence community in Northern Ireland), a generalised (non-US specific) version of this definition constitutes a good starting point. However, it should be clear that covert action is not exclusive of intelligence collection. Covert action not relying on previous and concomitant intelligence collection and analysis would likely be doomed and, in practice, composite operations involving both collection and action are legion.

The core of any covert action is its objective, namely to 'influence political, economic, or military conditions abroad' through all means deemed necessary. Secrecy and/or plausible deniability are the two other constitutive elements. The various official and unofficial definitions focus on the objective (influencing foreign states' internal affairs) and the nature of the action (secret), but do not mention the means used to do so. The term 'covert action' and its non-US synonyms thus cover a broad spectrum of activities. They include in particular propaganda, clandestine diplomacy, political and economic action, paramilitary operations, and lethal action. Cyber operations aiming at secretly influencing political, economic, or military conditions abroad would also be covered by existing definitions.[80]

…
(4) All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.'

[75] Friendly Relations Declaration (n 13).

[76] See *Nicaragua v. US* (n 53) paras 99–111.

[77] 120 in favour, 22 against, 6 abstentions, with most Western states voting against.

[78] UN General Assembly, Resolution 36/103, 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States', U.N. Doc A/36/761 (1981).

[79] National Security Act of 1947 (50 U.S.C. 3093), Section 503 (e).

[80] See Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre*

Covert action, which implies secretly influencing foreign political, economic or military situations, inherently contravenes core principles of international law. Indeed, both the prohibition on the use of force, either amounting to an armed attack[81] or constituting 'less grave' forms of the use of force,[82] and the principle of non-intervention, which involves 'the right of every sovereign state to conduct its affairs without outside interference',[83] form part of customary international law[84] and constitute 'an essential foundation of international relations'[85] as expressed by Articles 2(1) and (4) of the UN Charter.

Regarding coercive (covert) action under the principles of non-use of force and of non-intervention, the ICJ explained in *Nicaragua* v. *US* that

> The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State. As noted above (paragraph 191), General Assembly resolution 2625 (XXV) equates assistance of this kind with the use of force by the assisting State when the acts committed in another State "involve a threat or use of force". These forms of action are therefore wrongful in the light of both the principle of non-use of force, and that of non-intervention.[86]

Covert action falling short of the use of force would still be in breach of the principle of non-intervention provided it includes an element of coercion. In practice, the means and techniques used by a state to coerce another state in relation to the exercise of the latter's state powers can be varied and nuanced. The Friendly Relations Declaration defines the principle of non-intervention as including the following prohibition: 'No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and *all other forms of interference* or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law' (emphasis added). Resolution 36/103, though of a more contested status,[87] added the phrase 'in any form or for any reason whatsoever' to that statement, and further defined which rights of states were covered by the principle of non-intervention:

> (a) Sovereignty, political independence, territorial integrity, national unity and security of all States, as well as national identity and cultural heritage of their peoples;
>
> (b) The sovereign and inalienable right of a State freely to determine its own political, economic, cultural and social system, to develop its international relations and to exercise permanent sovereignty over its natural resources, in accordance with the will of its people, without outside intervention, interference, subversion, coercion or threat in any form whatsoever;
>
> (c) The right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information

---

of Excellence (2nd edn, Cambridge University Press 2017) (hereinafter: 'Tallinn Manual 2.0') rule 66: 'A State may not intervene, including by cyber means, in the internal or external affairs of another State'.

[81] UN Charter, Article 2(4).

[82] Friendly Relations Declaration (n 13) and *Nicaragua v. US* (n 53) para 191.

[83] *Nicaragua v. US* (n 53) para 202.

[84] *Nicaragua v. US* (n 53) para 191.

[85] *Corfu Channel Case (United Kingdom v Albania) (Merits)* [1949] ICJ Reports 1949 35 (ICJ).

[86] *Nicaragua v. US* (n 53) para 205.

[87] See footnote 77.

> media in order to promote their political, social, economic and cultural interests and aspirations, based, inter alia, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order.[88]

Hence, covert action aimed at coercively influencing in any way, in any form and for any reason whatsoever, the internal (political, economic, cultural, social) affairs of another state by definition violates the principle of non-intervention because such action interferes with a sovereign state's right to control its own internal affairs and to function effectively.[89] It is therefore difficult to envisage a way in which covert action, the very purpose of which is to intervene in the domestic affairs of another state, could ever be internationally lawful.[90] In fact, research shows that states resort to covert action when they lack a legal exemption from the non-intervention principle.[91] This leads to the unavoidable conclusion that covert action targeting a foreign state is inherently prohibited by international law.

Cyber covert action deserves specific attention. Indeed, while cyber espionage does not, as a matter of positive law and by itself, trigger a breach of the principle of non-intervention,[92] other cyber activities can constitute covert action. Thus, cyberattacks and operations coming short of the prohibition on the use of force will come under the principle of non-intervention, as will composite acts involving cyber espionage followed by a coercive use, by the same state, of the information thus collected.[93]

In addition, and as noted by Dieter Fleck, covert action can also be prohibited due to the methods used to achieve the stated interventionist objective.[94] However, this is simply an additional ground of illegality, as the activity itself is already inherently unlawful. Thus, regulation on the basis of the underlying conduct is secondary to regulation of the objectives, or ends, of this specific type of intelligence activity. Yet, it is worth mentioning — if only because it opens additional avenues to seek redress — that, as individuals are increasingly the direct targets of covert action (e.g., extraordinary rendition or lethal drone strikes), IHRL is applicable. IHRL thus governs the underlying conduct when individuals are implicated, directly or indirectly, by state action abroad and end up under the extraterritorial jurisdiction of the directing state.

2.4.1.2 Territorially Intrusive Acts

Territorially intrusive acts form a category of intelligence activities comprising any non-consensual or unauthorised intrusion into a foreign state's territory. They include covert action but also various forms of intelligence collection, and thus deserve to be analysed separately from covert action. The legality of territorially intrusive acts should be assessed with regard to

---

[88] UN General Assembly, Resolution 36/103 (n 78). The Declaration was adopted by a vote and, due to the number of oppositions to it, is less representative of customary law than the Friendly Relations Declarations. Nevertheless, it provides additional precisions regarding the content of the principles.
[89] *Nicaragua v. US* (n 53) para 202.
[90] Covert action on the state's own territory, for instance targeting non-state domestic entities, would be subjected to a different corpus of rules. International human rights law and, in the case of a non-international armed conflict, international humanitarian law would constitute the applicable legal framework to assess its legality.
[91] Michael Poznansky, 'Feigning Compliance: Covert Action and International Law' (2019) 63 International Studies Quarterly 72.
[92] Buchan (n 45) 65.
[93] François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 241–257.
[94] Fleck (n 11) 693.

the principles of non-intervention and territorial sovereignty, which form the foundation of the sovereignty of states. While the principle of non-intervention will be triggered by coercive action on the part of a foreign state, likely leading to the characterisation of the activity as a covert action, the principle of territorial sovereignty follows a doctrine closer to that of strict liability. Indeed, central to territorial sovereignty is every state's right to determine entry and egress from its own territory, which includes its land area, internal waters,[95] territorial sea,[96] national airspace,[97] and cyber infrastructure physically located within its borders,[98] as well as the right to perform governmental functions, to the exclusion of any other state, within its territory.[99]

Territorially intrusive acts therefore violate international law notably because they are inherently in breach of the principle of territorial sovereignty. The principle requires respect for the territorial integrity of other states and prohibits the exercise of sovereign power over the territory of another state. While simultaneously a regulation of the nature of the underlying conduct (territorially intrusive), the principle of territorial sovereignty excludes from lawfulness whole categories of intelligence activities regardless of how the territorial intrusion is performed, and therefore irrespective of whether the underlying conduct is also prohibited by international law under a specific rule or treaty regime. In that sense, the principle of territorial sovereignty relates to the nature of territorially intrusive acts and only leaves few, precisely defined, intelligence activities in the realm of intrinsic non-illegality or permissibility based on the lawfulness of their underlying conduct.

Hence, notwithstanding the permissibility of specific forms of territorially intrusive acts under lex specialis or through consent,[100] the following taxonomy can be drafted:

1) Intelligence activities involving a physical intrusion on the target state's territory, apart from those by diplomatic and consular staff,[101] violate the target state's territorial sovereignty. These encompass undercover agents without diplomatic or consular status, and thus what is commonly referred to as 'spying' or human intelligence.

---

[95] UN General Assembly, Convention on the Law of the Sea (UNCLOS) 1982, Article 8.
[96] UN General Assembly, Convention on the Law of the Sea (UNCLOS), Article 3.
[97] International Civil Aviation Organization, Convention on Civil Aviation (Chicago Convention) 1944 (15 UNTS 295) Article 1.
[98] Tallinn Manual 2.0 (n 80) Rule 2: 'A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.'
[99] See Judge Max Huber's statement in *Island of Palmas*, 2 RIAA (Perm Ct Arb 1928) 829, 838: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State'.
[100] The International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10 ('ASR'), Article 20 provides that: 'Valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act in relation to the former State to the extent that the act remains within the limits of the consent'. There are several crucial elements in that provision. First, the consent must be valid, i.e., it may not be presumed but it can be implicit; it must be given by a person authorised to consent on behalf of the state; and it may not conflict with a peremptory norm. Second, the act only becomes lawful in relation to the state that gave consent, and may therefore remain wrongful in relation to other states. This also means that the primary obligation remains in force between all parties: it is only dispensed with for that specific act. Third, the act only becomes lawful insofar as it remains within the limits of the consent: consent to a given act only precludes the wrongfulness of that very act, for the duration and within the conditions attached to the consent. Unforeseeable consequences will thus not be covered by consent to the act from which they derive. Fourth, consent must be given in advance or at the time of commission of the act.
[101] For these, see below Section 2.4.3.1.

2) Intelligence activities involving an intrusion into the target state's national airspace, except when authorised or consensual, violate the target state's territorial sovereignty[102] as well as the Chicago Convention (Article 3bis).[103]
3) Intelligence activities involving an intrusion into the target state's territorial waters (internal waters or territorial sea), except when authorised or consensual, violate the target state's territorial sovereignty as well as the UNCLOS (Article 19(2)(c)).[104]
4) Intelligence activities involving an electronic intrusion into cyber infrastructure physically located within the target state's borders violate its territorial sovereignty. This is the case irrespective of whether targeted computer networks and systems are operated by state organs or private actors, and of whether they produce damage to the infrastructure or involve an interference or usurpation of inherently governmental functions.[105] Such factors are only relevant to the proportionality of the response by the injured state, and not to the breach itself, which is characterised as soon as there is intrusion.[106]

Regarding remote access cyber espionage, Craig Forcese raises another potential ground of illegality. According to him, remote intrusion onto the territory of another state through cyber means constitutes an exercise of extraterritorial enforcement jurisdiction, or extraterritorial state power, which in most cases would be in breach of the principle of sovereignty.[107] Forcese justifies this claim on the basis that remote access cyber operations involve 'the transmission of electrical impulses in a manner that changes (and does not simply observe) the status quo in a foreign state'.[108] While the justification may appear stretched, it provides further support to the position that any intrusion, whether it produces effects or not, constitutes a violation of territorial sovereignty.

This is however not the position adopted by the International Group of Experts in charge of drafting the Tallinn Manual 2.0. According to them, remote access cyber intelligence activities breach the principle of territorial sovereignty only to the extent that they involve an intrusion into cyber infrastructure physically located within the target state's borders *and* that they produce physical damage and/or affect the functionality of the infrastructure or involve an interference with or usurpation of inherently governmental functions.[109] Territorially intrusive cyber activities coming short of these additional criteria would most likely involve intelligence

---

[102] *Nicaragua v. US* (n 53) para 205.
[103] International Civil Aviation Organization, Convention on Civil Aviation (Chicago Convention).
[104] UN General Assembly, Convention on the Law of the Sea (UNCLOS).
[105] UN General Assembly (2015), *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, para 27.
[106] Buchan (n 45) 54: 'My view is that states exercise territorial sovereignty over the cyber infrastructure that is physically located within their territory on the same basis and to the same extent that they exercise territorial sovereignty over their physical territory'. Menno Kamminga 'Extraterritoriality' (2012) *Max Planck Encyclopedia of Public International Law*, para 22: 'The legal regime applicable to extraterritorial enforcement is quite straightforward. Without the consent of the host State such conduct is absolutely unlawful because it violates that State's right to respect for its territorial integrity'. Forcese (n 30) 80: 'I am not aware of any authority demonstrating that the legality of enforcement jurisdiction depends on the scale of the physical presence'. States' reactions to the Snowden revelations also invoked the principle of sovereignty to condemn US cyber espionage. For a recent example and an argument in favour of recognising a breach of sovereignty in the absence of physical effects, see Talita Dias, Antonio Coco and Tsvetelina J van Benthem, 'Illegal: The SolarWinds Hack under International Law (Forthcoming EJIL 2022)' <https://papers.ssrn.com/abstract=4174397> accessed 2 August 2022.
[107] Forcese (n 30) 78–80.
[108] Forcese (n 30) 80.
[109] Tallinn Manual 2.0 (n 80) Rule 4.

collection (exfiltration of data) or observation[110] and be construed as 'cyber espionage'. They would be regulated under Rule 32, which provides that 'Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so'. In other words, the Tallinn Manual 2.0 proposes that they be regulated according to their underlying conduct only, and that their lawfulness 'depends on whether the way in which the operation is carried out violates any international law obligations that bind the State.'[111]

The discussion under Rule 66 further clarifies that

> Cyber espionage per se, as distinct from the underlying acts that enable the espionage . . . does not qualify as intervention because it lacks a coercive element. In the view of the International Group of Experts, this holds true even where intrusion into cyber infrastructure in order to conduct espionage requires the remote breaching of protective virtual barriers (e.g., the breaching of firewalls or the cracking of passwords).[112]

Hence, if a cyber operation does not breach sovereignty as defined by Rule 4 and does not constitute a prohibited intervention under Rule 66, its legality could only be assessed based upon the lawfulness of the method employed. This would be so irrespective of the severity of the damages, such as the exfiltration of data (including, e.g., nuclear codes), inflicted on the receiving state by such an intrusive but non-destructive cyber operation.

Yet, it bears noting that the Experts did not provide any legal justification for their position that the principle of sovereignty provides less protection to a state's cyber infrastructure than to a state's physical territory.[113] Hence, it appears preferable to follow the well-established standards of customary international law on the principle of territorial sovereignty[114] to analyse the legality of cyber activities involving an intrusion into the cyber infrastructure of a state.

Activities in breach of the principle of territorial sovereignty may also be unlawful on the ground that they violate the prohibition on the use of force, constitute a prohibited intervention or an armed attack. They may further be unlawful because their underlying conduct violates applicable treaty regimes or rules, such as the Chicago Convention; the UNCLOS; international telecommunications regulations; diplomatic and consular law; rules on immunities; IHRL; international humanitarian law (IHL); or other applicable bilateral and multilateral agreements.

2.4.2 Intelligence Activities Explicitly Allowed by International Law

In contrast, international law sometimes provides authorisation and legitimation for specific intelligence activities through the regulation of their effects, means or limits, or by using 'legal euphemisms'.[115] 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 (under a designation that never mentions 'intelligence' or 'espionage')

---

[110] To the extent that observation could be performed without exfiltrating data, which is doubtful in most cases.
[111] Tallinn Manual 2.0 (n 80) Rule 32, discussion para 6.
[112] Tallinn Manual 2.0 (n 80) Rule 66, para 33.
[113] See footnote 106 for critics of the Tallinn Manual's approach, and support for following the standards established by customary international law.
[114] The ASR (n 100), Article 37, commentary para 4 recalls that 'State practice also provides many instances of claims for satisfaction in circumstances where the internationally wrongful act of a State causes non-material injury to another State. Examples include ...violations of sovereignty or territorial integrity'.
[115] Navarrete and Buchan (n 20) 928.

functions as a lex specialis to more general principles of international law. Therefore, provided the activity at stake respects the limitations and conditions imposed by treaty, such activity must be considered lawful even if, in the absence of a treaty provision, it would violate the principle of non-intervention or of territorial sovereignty. Activities fitting this description include specific forms of reconnaissance and of wartime intelligence.

2.4.2.1 Reconnaissance

Reconnaissance has first been 'authorised' from international spaces, namely outer space, the high seas, and international airspace, through various treaty provisions. 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.[116]

The treaty further clarifies that 'The moon and other celestial bodies shall be used by all State Parties to the Treaty exclusively for peaceful purposes'.[117] 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.[118]

In very similar language, the UNCLOS proclaims in Article 87 the freedom of the high seas, and clarifies in Article 88 that 'The high seas shall be reserved for peaceful purposes'.[119] Comparable interpretation of the peaceful purpose provision has led to considering reconnaissance from the high seas as generally permissible.[120] Finally, parallel to the freedom of the high seas exists a freedom of international airspace,[121] which includes airspace over the high seas but also over the more recently created exclusive economic zone (EEZ) of states.[122] States' freedom of flight in international airspace, including for reconnaissance purposes, is commonly recognised.[123]

It is now 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

---

[116] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Article III.
[117] Article IV.
[118] Jinyuan Su, 'Use of Outer Space for Peaceful Purposes: Non-Militarization, Non-Aggression and Prevention of Weaponization' 36 21, 258. See also ECtHR, *Weber and Saravia* v. *Germany*, 29 June 2006, Application No. 54934/00, para 88.
[119] UN General Assembly, Convention on the Law of the Sea (UNCLOS).
[120] Oliver J Lissitzyn, 'Electronic Reconnaissance from the High Seas and International Law' (1980) 61 International Law Studies 563, 569.
[121] International Civil Aviation Organization, Convention on Civil Aviation (Chicago Convention) Article 12.
[122] Chicago Convention, Articles 1 and 2. Reconnaissance from *within* the EEZ is a more contested matter, as I explain below.
[123] Raul Pedrozo, 'Military Activities in the Exclusive Economic Zone: East Asia Focus' (2014) 90 International Law Studies 240: 'Long-standing state practice supports the position that surveillance and reconnaissance operations conducted in international airspace beyond the 12-nm territorial sea are lawful activities. Since the end of World War II, surveillance and reconnaissance operations in international airspace have become a matter of routine'.

do not violate any rule of international law.[124] This is the result of 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,[125] state practice and opinio juris have consolidated the permissive power of international law in these situations. 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 without it.

As regard the EEZ, reconnaissance from the international airspace *over* the EEZ should be distinguished from reconnaissance from *within* the EEZ itself. 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.[126] Airspace above the EEZ is thus excluded from the scope of state sovereignty[127] and justifiably so since the coastal state does not enjoy territorial sovereignty in its EEZ but only sovereign rights over economic resources within the EEZ.[128] Hence, it would be hard to justify why the coastal state should enjoy any kind of sovereignty or regulatory power regarding the airspace over the EEZ. The UNCLOS instead preserves third states' full freedoms of overflight, including for military uses.[129] Consequently, insofar as it does not interfere with the coastal state's economic rights, reconnaissance from the airspace over the EEZ cannot be considered unlawful under the UNCLOS. Some confusion in literature and state practice has however muddied the distinction,[130] and reconnaissance from within/over the EEZ is less unanimously considered lawful than from the high seas/international airspace.

Reconnaissance has also been authorised from the territorial airspace of states in more limited ways through arms control treaties. Simon Chesterman identifies the verification regime of the Anti-Ballistic Missile Treaty and SALT I Agreement[131] as providing for a right to collect intelligence, protected by corresponding obligations of the territorial state.[132] This verification regime model, reproduced or extended in later arms control agreements between the US and USSR and in multilateral settings,[133] effectively establishes a claim-right to reconnaissance from the territorial airspace of other parties with respect to assessing compliance with arms

---

[124] Navarrete and Buchan (n 20) 943–944.
[125] Navarrete and Buchan (n 20) 929–934.
[126] Chicago Convention, Articles 1 and 2.
[127] Pedrozo (n 123) 519–520; Joshua L Cornthwaite, 'Can We Shoot Down That Drone?' (2019) 52 Cornell International Law Journal 475, 506.
[128] UNCLOS, Article 56; Kay Hailbronner, 'Freedom of the Air and the Convention on the Law of the Sea' (1983) 77 The American Journal of International Law 490, 506; Efthymios Papastavridis, 'Intelligence Gathering in the Exclusive Economic Zone' (2017) 93 International Law Studies 31, 453–454.
[129] UNCLOS Article 58(1); Hailbronner (n 128) 506.
[130] Asaf Lubin, 'The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum' (2018) 57 Washburn Law Journal 17.
[131] Anti-Ballistic Missile Systems Treaty (ABM), done at Moscow, 26 May 1972, in force 3 October 1972 (United States announced its withdrawal on 13 December 2001), Article XII; SALT I Agreement, done at Moscow, 26 May 1972, in force 3 October 1972, Article V.
[132] Chesterman (n 5) 34 referencing ABM Treaty, Article XII paras 2 and 3; and SALT I Agreement Article V, paras 2 and 3.
[133] See: Intermediate-Range Nuclear Forces (INF) Treaty, done at Washington, DC, 8 December 1987, in force 1 June 1988, Article XII; Strategic Arms Reduction Treaty Text (START I), done at Moscow, 31 July 1991, in force December 1994, Article X; and Treaty on Open Skies, done at Helsinki, 24 March 1992, in force 1 January 2002, Articles I(1), II(4), III–VI, and IX.

control obligations.[134] 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.

2.4.2.2 Wartime Intelligence

Wartime intelligence represents another example of expansive interpretation leading to authorisation. Indeed, 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'.[135] Various conventions regulate the treatment of enemy spies by belligerent states[136] and determine who can be considered a spy.[137] In this sense, while a spy can be harshly punished by the injured party, they are not a war criminal and their actions do not engage the international responsibility of the sending state because wartime espionage is not an internationally wrongful act. Despite – or maybe thanks to – this superficial regulation, wartime human espionage is thus made legitimate and, in consequence, permissible.

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 Quincy 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'.[138] This justification covers all types of wartime intelligence activities. Hence, non-intrusive means of intelligence collection must also be considered legitimate and permissible during wartime because the principle of sovereignty is lifted by the necessities of war. In consequence, despite how very little treaty law has to say about them, all forms of wartime intelligence activities can be legitimated on its basis.

However, there is a caveat to this seemingly general authorisation. The prohibition of certain acts, or means and methods, also applies in wartime. Because international humanitarian law (IHL) functions as a lex specialis to some of the international law applicable during

---

[134] Chesterman (n 5) 34.

[135] Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899, Article 24. According to the United Kingdom's *Joint Service Manual of the Law of Armed Conflict*, this can include 'the employment of informers or agents in enemy-held territory'. Although, as the United States' *Law of War Manual* rightly states, 'Information gathering measures … may not violate specific law of war rules'. Further, IHL emphasises that neither prisoners of war nor protected persons under the Fourth Geneva Convention may be ill-treated in the search for intelligence (Article 31, Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949).

[136] 1899 Hague Regulations (n 135), Article 30: 'A spy taken in the act cannot be punished without previous trial.' and Article 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 (n 135), Article 5; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Articles 45(3) and 46(1); and Rule 107, ICRC Study on the Codification of International Humanitarian Law.

[137] 1899 Hague Regulations (n 135), Article 29; 1977 Additional Protocol I (n 136), Article 46(2).

[138] Wright (n 28) 12.

peacetime, wartime intelligence is lawful only insofar as it does not violate IHL, 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 (IHRL) and general international law that become or remain applicable during armed conflicts.[139] Therefore, as an agent of the sending state, the spy may engage the responsibility of the state for an internationally wrongful act if, during the course of their mission, they commit an act in violation of applicable rules of international law. In this sense, wartime espionage is also regulated according to the underlying conduct.

The status of cyber intelligence during armed conflict deserves special consideration, especially considering that IHL explicitly regulates only the prisoner status of spies.[140] The Tallinn Manual 2.0 emphasises that the rules governing the conduct of hostilities are directly applicable to cyberattacks and operations.[141] Thus, during armed conflicts, cyber operations may not be indiscriminate[142] (they must capable of being aimed and be aimed at a military objective, and their effects must be controllable) and they must be proportionate.[143] While dual use cyber targets (i.e., cyber infrastructure used for both military and civilian purposes) are military objectives, IHL requires that all feasible measures be taken to identify the targeted cyber infrastructure as a military objective.[144] Further, some property is especially protected from cyberattack and parties to the conflict have a duty to take 'passive precautions' to protect the civilian population against the dangers that might result from cyber operations.[145] In addition, data necessary for the delivery of protected services is protected pursuant to the principle of distinction.[146] This includes civil (governmental) data, banking data, and medical data, although the latter would be protected in any event. Indeed, irrespective of whether a cyber operation rises to the level of an attack under IHL, certain cyber infrastructure, such as medical systems, may not be made the object of a cyber operation.[147] Existing state practice and opinio juris overwhelmingly supports this interpretation of the law.[148] Hence, while some cyberattacks and operations may become lawful under IHL, limits remain as to what parties to the conflict may lawfully achieve through cyber means and methods during armed conflicts. Any cyber operation going beyond what is authorised by IHL would engage the responsibility of the state for a breach of the relevant IHL rule, as well as of any other applicable rule of international

---

[139] E.g., regarding the inviolability of diplomatic premises during armed conflict, Vienna Convention on Diplomatic Relations (VCDR) 1961 (500 UNTS 95) Article 45(1); Vienna Convention on Consular Relations (VCCR) 1963 (596 UNTS 261) Article 27(1)(a).

[140] Tallinn Manual 2.0 (n 80) Rule 89 reproduces for cyber espionage the IHL rule on the treatment of spies but, due to a geographical criterion, de facto excludes remote access cyber espionage.

[141] Tallinn Manual 2.0 (n 80) Rule 80. See also, for a summary of the applicability of IHL to cyber activities, J Horowitz, 'Cyber Operations under International Humanitarian Law: Perspectives from the ICRC' (2020) 24 ASIL Insights.

[142] Additional Protocol I, Article 51(4). See also Tallinn Manual 2.0 (n 80) Rules 105 and 111.

[143] Additional Protocol I, Articles 51(5)(b) and 57(2)(a). See also Tallinn Manual 2.0 (n 80) Rules 113 and 117.

[144] Additional Protocol I, Articles 48 and 52(2). See also Tallinn Manual 2.0 (n 80) Rules 99-102 and Rule 115.

[145] Additional Protocol I, Article 58(c). See also Tallinn Manual 2.0 (n 80) Rules 114 and 121.

[146] Additional Protocol I, Article 52(1), Article 12 and Geneva Convention I Article 19 and Geneva Convention IV Article 18 for medical units. See also Tallinn Manual 2.0 (n 80). Rues 93-97.

[147] Additional Protocol I, Article 57(1).

[148] See the Paris Call for Trust and Security in Cyberspace, 12 November 2018, supported by 78 states; and several public governmental views on the applicability of international law (including IHL) to cyber operations: <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions>. Note, however, the surprising British interpretation of the principle of territorial sovereignty, denying it the status of a 'rule' with regard to cyber activities.

law. In particular, cyber operations targeting civilians or civilian infrastructure do not become lawful during armed conflicts.

2.4.3 Intelligence Activities Regulated According to their Underlying Conduct

Intelligence activities that are not explicitly allowed by international law, nor inherently prohibited because they constitute covert action or territorially intrusive acts in violation of the principle of territorial sovereignty, are neither inherently lawful nor unlawful. Rather, their legality must be determined by examining the underlying conduct. The relevant question is whether the underlying conduct constitutes an internationally wrongful act. Activities falling into this category are as follows: diplomatic and consular intelligence collection; remote access non-intrusive cyber intelligence activities; and domestic intelligence.

2.4.3.1 Diplomatic and Consular Intelligence Collection

The practice of intelligence collection by diplomatic and consular staff posted abroad is implicitly acknowledged by the 1961 Vienna Convention on Diplomatic Relations (VCDR), which includes among the functions of a diplomatic mission that of 'ascertaining *by all lawful means* conditions and developments in the receiving State, and reporting thereon to the government of the sending State'.[149] This provision implies that intelligence collection (including through cyber means)[150] by members of the diplomatic mission is authorised insofar as the underlying conduct does not breach any applicable legal norm. The caveat refers to the obligation of diplomatic and consular staff to respect the rules and regulations of the receiving state,[151] in addition to applicable rules of international law regulating intelligence collection more generally. In that respect, the 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.[152]

This interpretation is reinforced by Article 41 of the VCDR, which provides that the premises of the mission shall not be used 'in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State'.[153] This provision makes it unlawful to, for instance, use diplomatic premises as cyber data collection centres or as a base to engage in cyber espionage against the receiving state or a third state.[154]

If the Convention implicitly admits some intelligence collection as part of the functions of diplomatic missions,[155] it also grants the receiving state powers to prevent, limit, and end it.

---

[149] VCDR Article 3(d) (emphasis added); see also VCCR Article 5(c). And see Tallinn Manual 2.0 (n 80) Rule 43 with regard to cyber activities.
[150] See Buchan (n 45) 70–94 for the applicability of the VCDR and VCCR to cyber espionage, and 89-94 for the use of diplomatic missions and consular posts for cyber espionage.
[151] But see Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 J. Nat'l Sec. L. & Pol'y 179, 200 arguing that if the receiving state were to expressly preclude such information collection by law, thereby rendering all such activities unlawful, the local law could not be reconciled with the Convention because it would preclude the very exercise of the diplomatic function.
[152] *Tehran Hostages* (n 53) para 84.
[153] For consular staff, see VCCR Article 55.
[154] Buchan (n 45) 92. See also Tallinn Manual 2.0 (n 80) Rules 41 and 43, paras 3 and 5.
[155] But see Delupis' interpretation of *what* can be collected: 'I believe that diplomats commit acts contrary to international law if they gather *secret* information. Their task may be to collect information from various sources in the host state, but they have a duty not to overstep a certain mark beyond which their activities become

Hence, the receiving state can limit a mission's size and composition, and its consent is required to install a wireless transmitter or establish regional offices. In addition, diplomats' freedom of movement may be restricted for reasons of national security.[156] The Convention also provides for receiving state approval of military attachés, presumably in order to ascertain their intelligence function.[157] More generally, diplomats have a duty to respect the laws and regulations of the receiving state and not to interfere in its internal affairs.[158] With regard to these last two provisions, state practice regards espionage as well as cyber espionage as constituting an unlawful interference and almost all domestic jurisdictions criminally prohibit espionage. In consequence, diplomatic or consular (cyber) espionage does not appear to ever be construed as lawful under the VCDR and VCCR.[159] In addition, acts of cyber espionage against the receiving state would constitute a violation of the principle of territorial sovereignty.[160]

As agents of the sending state, the breach of international rules by diplomatic staff engages the responsibility of the sending state. Yet, it would not be engaged for an unlawful act of intelligence collection (which is per se permitted by the Vienna Conventions, although with stringent limitations), but for the breach of rules violated by the underlying conduct: the use of unlawful means to collect intelligence. Because the procedural immunity granted to diplomatic staff is absolute,[161] it protects those engaged in intelligence collection through *unlawful means*. Therefore, the traditional remedy for overstepping the explicit and implicit boundaries of diplomacy is to declare a diplomat 'persona non grata', normally prompting a swift recall of the person to the sending state.[162] Strikingly, no state has ever explicitly invoked the responsibility of the sending state for acts of espionage. Rather, the formula often used to justify declaring a diplomat persona non grata or to break off diplomatic relations (in extreme cases) is that a diplomat has engaged in 'activities incompatible with his or her diplomatic status', without mention of state responsibility. Yet, this practice based on the principle of reciprocity does not erase the underlying legal issue: although no criminal pursuits against the diplomat can be instituted by the receiving state, their actions still engage the responsibility of the sending state if the means used to operationalise the collection of intelligence were in breach of international law. Applicable international rules governing the underlying conduct are numerous and include, in addition to diplomatic and consular law, the principle of non-intervention; IHRL; international telecommunications law; and the immunity of heads of states.

---

treacherous and hostile to the host state. Once they attempt to amass "secret" information i.e., information not commonly available or classified as secret by authorities in the host state, diplomats overstep the line of legality in international law'; Ingrid Delupis, 'Foreign Warships and Immunity for Espionage' (1984) 78 American Journal of International Law 53, 69.

[156] VCDR Articles 11, 27(1), 12, and 26; VCCR Articles 20, 35(1), 6, and 34.

[157] VCDR Article 7.

[158] VCDR Article 41(1); VCCR Article 55(1).

[159] Buchan (n 45) 90–91.

[160] Buchan (n 45) 92.

[161] Note however the more limited immunity granted to consular staff (VCCR, Art. 41) and that honorary consular officers do not enjoy immunity from criminal proceedings (VCCR, Art. 63). In particular, consular staff only enjoys immunity for acts performed in the exercise of their consular functions, which espionage is not. Thus, and despite a qualified procedural immunity (Art. 41(1)), since espionage constitutes a grave crime in most jurisdictions, consular staff can be arrested and tried for such acts under the VCCR.

[162] VCDR Article 9(1); VCCR Article 23(1).

2.4.3.2 Remote Access Non-Intrusive Cyber Intelligence Activities

Cyber activities involving an intrusion into cyber infrastructure located on the territory of another state constitute a violation of the territorial sovereignty of that state.[163] However, states may store their data on another state's territory, and some cyber operations may be non-intrusive. These remote access non-intrusive cyber intelligence activities are not governed, prima facie, by the principle of territorial sovereignty. They are not necessarily lawful either, but an analysis of the underlying conduct is necessary to determine their legality.

The first situation is that of cyber espionage targeting a state's data while it is located on foreign cyber infrastructure. This could be regarded, in certain circumstances, as an interference with that state's right to perform governmental functions. The Tallinn Manual 2.0 Experts concluded that a computer operation that changes or deletes data related to the delivery of a governmental function amounts to an unlawful interference.[164] While the Experts did not specifically address the example of cyber espionage in this paragraph, the implication is nevertheless clear: the Experts did not regard the observation and/or exfiltration (as opposed to the 'changing or deleting') of data as constituting an interference with the performance of governmental functions.[165] This view is not shared by all authors, but state practice and the current state of international law do not permit to depart from it as a matter of positive law.[166] Hence, to the extent that they do not change or delete data related to the performance of a governmental function, and thus do not constitute an unlawful exercise of jurisdictional power, remote access non-intrusive cyber intelligence activities are regulated according to their underlying conduct only.

A second situation concerns the production of effects on cyber infrastructure located on the territory of the target state without intrusion. Such situation is often the result of a remote operation involving a distributed denial of service (DDoS),[167] alone or in combination with another cyber or physical act. This kind of operation could be construed as a breach of sovereignty on the ground that it constitutes an interference with the target state's exercise of governmental functions. Such view is not widespread,[168] but it is grounded in customary international law. Indeed, the production of effects abroad,[169] such as when an upstream state pollutes a watercourse, producing effects in a downstream state, engages the responsibility of the state from which the effects are produced.[170] The same should normally hold true for all

---

[163] See section 2.4.1.2 above.
[164] Tallinn Manual 2.0 (n 80) Rule 4, discussion para 16.
[165] This is confirmed by Rule 32 of the Manual.
[166] See Buchan (n 45) 56–61 for a comprehensive discussion.
[167] According to Newton's Telecom Dictionary, a denial of service (DoS) attack 'prevents a website from being responsive by overwhelming it with thousands of requests (pings). Often these requests originate from a robotic network, more commonly referred to as a botnet. "Bots" are malware-infected computers belonging to unwitting individuals. The bots become part of a botnet—a grouping of bots—which is controlled by the unfriendly actor. Bots may be used to perform a variety of unsavory acts, such as sending spam and collecting data for identity theft. Botnets are usually composed of computers from many geographic locations, so the action is called a distributed DoS, or DDoS.'
[168] But see some support from the French and Japanese governmental views (n 148).
[169] See the 'no-harm' principle, best articulated in the ILC 2001 Draft Articles on the Prevention of Transboundary Harm. The principle requires states to exercise due diligence in preventing, stopping or redressing foreseeable and significant transboundary harm, including where it results from lawful activity carried out by non-state actors.
[170] In the *Trail Smelter* arbitration, the US made a claim for violation of its sovereignty in respect of the damage caused by a smelter located on Canadian territory. The Tribunal did not refer explicitly to sovereignty in its

state-sponsored cyber operations producing effects, irrespective of whether there has been any penetration or intrusion in cyber infrastructure located on the territory of the target state. However, it remains a reflection *de lege ferenda*. Notwithstanding, when such state-sponsored non-intrusive cyber operations result in the temporary loss of functioning of governmental services, as was the case in the DDoS operation conducted against Estonia in 2007, then it can reasonably be argued that, because it constitutes an interference with the state's performance of governmental functions, it constitutes a breach of that state's sovereignty.[171] Absent such a breach of sovereignty, other non-intrusive cyber operations will be regulated according to their underlying conduct only.

Few rules of international law are applicable to the underlying conduct of non-intrusive remote access cyber operations. Indeed, if the remote access activity does not violate either the principle of sovereignty or the principle of non-intervention, then the only constraints on the activity stem from a reduced number of rules, including diplomatic immunities, privacy protections[172] (to the extent that their applicability does not depend upon the jurisdiction of the state directing the operation),[173] and rules governing international spaces if the operation is conducted from these spaces.

2.4.3.3 Domestic Intelligence

Intelligence collection conducted by a state on its own territory is lawful insofar as the state does not breach any applicable rule of international law. Indeed, their sovereign status provides states with the freedom to collect intelligence over places, persons, and things situated under their jurisdiction. This freedom is only limited by the specific rules of international law the state has consented to, among which we find diplomatic immunities and international human rights law, though other rules can potentially become applicable depending on the underlying conduct.

First, a state cannot breach the inviolability of diplomatic and consular staff, premises, communications, and bags in order to collect intelligence.[174] As a consequence, states that intercept communications occurring in diplomatic missions or in the personal premises of diplomats violate international law. Likewise, a state that opens official diplomatic correspondence acts unlawfully, even when such correspondence is stored electronically on servers located abroad.[175] Further, all states are under an obligation of due diligence to protect the premises of diplomatic missions and consular posts. This obligation requires them, among

---

judgment but stated that, 'under the principles of international law… no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties of persons therein, when the case is of serious consequence and the injury established by clear and convincing evidence'. Trail Smelter Arbitration (*United States v. Canada*), Arbitral Trib., 3 U.N. Rep. Int'l Arb. Awards 1905 (1941).

[171] The very definition of state sovereignty includes the state's right to perform governmental functions, to the exclusion of any other state, within its territory. See above footnote 99.

[172] A violation of the right to privacy of a human person is an internationally wrongful act. However, obtaining 'information' as such is not if (hypothetically) nobody's privacy was violated.

[173] See Buchan (n 45) 95–122 for an assessment of the extra-territorial application of the ICCPR and the ECHR in cyber espionage; and Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 66, 111 suggesting a new ground of jurisdiction in surveillance cases: 'virtual control of data'.

[174] VCDR Articles 22, 24, 27, 29, 30, and 31; VCCR Articles 31, 33, 35, 41, and 43. With regard to cyber operations and cyber infrastructure located in a sending State's diplomatic or consular premises, see Buchan (n 45) 73–89.and Tallinn Manual 2.0 (n 80) Rules 39, 40 and 41.

[175] Buchan (n 45) 89.

other things, to protect cyber infrastructure and computer devices located on the premises against cyber threats, regardless of the source of the threat.[176] Taken together, the inviolability provisions of the VCDR and the VCCR provide an extensive legal protection to physical and electronic information related to the performance of the functions of diplomatic missions and consular posts against intelligence collection by the receiving state[177] and, to a lesser extent, by third states.[178]

In addition, following the ICJ order of 3 March 2014 in the case of Timor-Leste against Australia,[179] it can be argued that, when states are engaged in the peaceful settlement of a dispute with another state under Article 2(3) of the UN Charter, they are under an obligation to respect the confidentiality of the other state's communications with their judicial counsel. Such obligation applies even if the documents, data, or communications are stationed or take place on their territory. Hence, the prohibition of intervention in the domestic affairs of another state, deduced from the sovereign equality of states, extends to cover the communications between states and their counsel in international dispute settlement – irrespective of where they take place.[180] In that sense, it constitutes another limit on domestic intelligence collection.

Further, the means used to collect intelligence domestically may not be in breach of international human rights norms, such as the right to privacy and the prohibition of torture and cruel, inhuman and degrading treatment. The evolving case-law of regional and international human rights courts and bodies regarding the permissibility (and conditions thereof) of surveillance measures and interrogation methods constitutes the legal framework of reference. There are thus regional variations depending on the competent body's case-law. Generally, however, interference with the right to privacy is considered arbitrary and therefore impermissible if it is not prescribed by law, legitimate, necessary, and proportionate.[181] In addition, in cases where a state accesses the electronic data of an individual located within its territory, privacy guarantees apply even if the data collected resides on cyber infrastructure located outside its territory.[182] Regarding interrogation methods, it is commonly accepted that 'human intelligence cannot be extracted through abusive interrogation',[183] though the standards of what is considered abusive might differ slightly.

There also exists a 'duty to warn' in international law, read under IHRL provisions and applicable to both territorial and extraterritorial intelligence collection, but restricted to persons

---

[176] VCDR Article 22; VCCR Article 31; Buchan (n 45) 78–82.
[177] Buchan (n 45) 89.
[178] In addition to the duty of the receiving state to protect the premises, property and means of transportation of the mission (VCDR Art. 22, VCCR Art. 31), third states must respect the inviolability of official correspondence when in transit, which includes transit through their electronic servers (VCDR Art. 40(3) and VCCR Art. 54(3). Buchan (n 45) 89.
[179] *Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste* v. *Australia)*, Provisional Measures, Order of 3 March 2014, ICJ Reports 2014, 147.
[180] For further analysis of this 'new' right to non-interference with a state's communications with its counsel, see Iñaki Navarrete, 'L'espionnage en temps de paix en droit international public' (2016) 53 Canadian Yearbook of international Law/Annuaire canadien de droit international 1, 51–62.
[181] Surveillance and Human Rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/41/35, 28 May 2019, para. 24; The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/27/37, 30 June 2014, paras 21-30.
[182] Buchan (n 45) 97. Tallinn Manual 2.0 (n 80) Rule 34.
[183] Forcese (n 151) 196.

under the jurisdiction of the state. Hence, states have an obligation, arising from their duty to protect under human rights law, to 'warn individuals subject to their jurisdiction of any real and immediate risk to their life, bodily integrity, or liberty and security of person, posed by foreign intelligence services'.[184] Whereas domestic law may impose a duty to warn also in relation to persons not subject to the jurisdiction of the state,[185] in international law the duty is subject to a jurisdictional threshold[186] and is only triggered if a specific unlawful threat to the life of an individual was reasonably foreseeable to the state. It is an obligation of due diligence, meaning that the state can take a number of relevant considerations into account in deciding on how to fulfil it.[187]

Finally, domestic intelligence operations matching the definition of covert action 'at home' are also subject to IHRL. Relevant rights notably include the rights to life, to liberty and security of the person, to privacy, and the prohibitions of torture, cruel, inhumane and degrading treatments and of enforced disappearance. If hostilities between the government and non-state entities rise to the level of a non-international armed conflict,[188] relevant IHL provisions would also become applicable and govern the permissibility of intelligence operations within the conflict.

2.5 Conclusions: Legality as the First Layer of Regulation

The present Chapter demonstrated that intelligence activities and international law are not as foreign as parts of the literature portray them. Following the paradigm shift induced by the end of the Cold War equilibrium and confirmed by states' responses to the modern terrorist threat, the move away from the realpolitik view of the relationship between international law and intelligence activities became ineluctable. In consequence, I adopted a more formalist stance to make sense of the interactions between international law and intelligence activities in the twenty-first century security landscape. This approach is supported by an analysis of the scholarly literature and by modern intelligence activities and practices.

The most important purpose served by this Chapter was to establish that international law comprehensively addresses intelligence activities, so that there is no 'grey zone' or 'legal limbo' in which states would be free to act fully unconstrained. The Chapter also disproved claims that 'espionage' would be either internationally lawful or unlawful as constituting misunderstandings of public international law and of the formation of customary international

---

[184] Marko Milanovic, 'More on the Duty to Warn Persons Threatened by Foreign Intelligence Services' (*EJIL Talk!*, 10 June 2019). See also, with regard to the murder of Jamal Khashoggi, the report by the U.N. Special Rapporteur on extrajudicial, summary or arbitrary killings Agnes Callamard, A/HRC/41/CRP.1, stating in particular: 'If the United States (or any other party to the ICCPR) knew, or should have known, of a foreseeable threat to Khashoggi's life and failed to warn him, while he was in Turkey (or elsewhere), and under circumstances with respect to which it could be argued that he was under their functional jurisdiction, then the United States or any other State would have violated their obligations to protect Mr. Khashoggi's life.'

[185] E.g., US Intelligence Community Directive 191. For an account of recent US practice towards persons not under its jurisdictions, see Edwin Djabatey, 'Duty to Warn: Has the Trump Administration Learned from the Khashoggi failure?', *Just Security*, 6 November 2019.

[186] However, note the differing approaches to jurisdiction – the Human Rights Committee adopting a looser conception than regional human rights bodies. Milanovic emphasises that 'the key point here . . . is that a state lacking the capacity to fulfil the duty to warn will never be expected to have to do so'. Milanovic (n 184).

[187] Milanovic (n 184).

[188] ICTY, *Prosecutor* v. *Dusko Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para 70.

law. Rather than address this moot issue in detail, I looked instead at the international legality of the objectives and means of all types and categories of intelligence activities. This approach allowed for a comprehensive sketch of the international legal framework governing intelligence activities. Using a novel taxonomy, I divided intelligence activities between three categories: those inherently prohibited by international law; those explicitly allowed by international law; and intelligence activities that belong to neither of the first two categories and are therefore regulated according to their underlying conduct only. This three-tiered taxonomy is particularly valuable because it includes all intelligence activities and is flexible enough to incorporate new activities and technological developments as they emerge.

The issue of legality, dealt with in this Chapter, constitutes the key part of the first layer of regulation of intelligence activities under international law. This first layer also comprises the engagement of state responsibility as a direct and immediate consequence of the breach of legality.[189] Chapter 3 provides an illustration of this process, addressing complex issues of state responsibility and complicity in intelligence matters through a case-study on the CIA-led 'global war on terror'. Nevertheless, legality itself should not be confused with the separate issues of state responsibility and of states' choices and motives for complying with or ignoring international law in their intelligence decision-making. Indeed, this Chapter focused exclusively on clarifying the framework of primary norms applicable to intelligence activities. It is then left upon the law of state responsibility, subsequently and through a separate analysis involving the application of secondary norms, to determine whether a prima facie breach of an applicable primary norm constitutes an internationally wrongful act engaging the responsibility of the state, and what consequences should follow. This Chapter thus established the foundations necessary to pursue, in following chapters, an analysis of issues of responsibility and accountability for internationally wrongful acts resulting from intelligence activities.

[189] See generally International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001 (Supplement No 10 (A/56/10), chpIVE1) 76; James Crawford, *State Responsibility: The General Part* (Cambridge University Press 2013).