VIRGINIA LAW REVIEW

VOLUME 102 MAY 2016 NUMBER 3

ARTICLES

CONFRONTING AND ADAPTING: INTELLIGENCE AGENCIES AND INTERNATIONAL LAW

Ashley S. Deeks[*]

[*] Associate Professor, University of Virginia School of Law. Many thanks to Kate Andrias, Harlan Cohen, Jack Goldsmith, Molly Land, Marty Lederman, Alexandra Perina, Sai Prakash, Rich Schragger, Paul Stephan, and participants in workshops at the University of Virginia School of Law, the University of North Carolina School of Law, and William & Mary Law School for thoughtful comments and suggestions.

INTRODUCTION

CONVENTIONAL wisdom holds that international law should matter little to a state when it conducts intelligence activities.[1] That body of law notionally regulates and limits the actions one state may

[1] Although "intelligence activity" is notoriously hard to define, I intend to capture all intelligence-related activities (including both intelligence collection and covert activities) undertaken by intelligence services, except for uses of force that would implicate Article 2(4) of the U.N. Charter, such as targeted killings overseas. Because states have not overtly questioned whether international law constraints generally attach to state uses of force, even when undertaken by intelligence actors, I do not include those activities in the scope of the Article. See Lori Fisler Damrosch, Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs, 83 Am. J. Int'l L. 1, 5 (1989) ("[F]orcible and nonforcible forms of influence are sufficiently different to warrant separate legal treatment. Forcible activities, of course, must be judged against Article 2(4) of the United Nations Charter . . . ."). To the extent that some states do in fact interpret international law constraints as inapplicable to these activities, this Article is relevant to their analysis. Further, the analysis herein might fruitfully be applied to clandestine or covert cyber activities, whether conducted by militaries or intelligence agencies, because important questions exist about whether and how international law should apply to those activities.

take inside the territory of other states, but states have historically treated those constraints as inapplicable to intelligence operations.[2] Instead, states decide which forms and targets of intelligence collection or covert action are in their national security interests and conduct those activities without heeding international laws that, on their face, would constrain those acts. And until recently there was little reason to do otherwise; states rarely suffered consequences when they ignored the rules. This is the realpolitik view of the intelligence/international law relationship: Intelligence operations sustain the very existence of states, which have been and will remain impervious to pressures to constrain those operations.

In the face of new revelations about states' intelligence activities, a competing narrative has begun to garner adherents. The alternative approach finds its roots in classical international law. In this view, international law represents commitments assumed by a state; unless a treaty specifies otherwise, the state's commitments attach to all of its agents and representatives.[3] This formalist approach to international law insists that *of course* this law applies to intelligence officials and the acts they undertake. Intelligence services are no different from military, diplomatic, or economic officials; each set of state actors is bound by the same international obligations. History and practice to the contrary are not sufficient to alter that premise.

Each approach to the international law/intelligence relationship holds a certain appeal. The realpolitik view reflects the critical importance of intelligence activities to states and, in some variants, avers that espionage and certain covert forms of transnational influence may diminish military conflict and so should face few limits. The formalist view offers a straightforward interpretive approach consistent with longstanding principles of international law. Given the international rules that potentially regulate intelligence,[4] this approach further reflects an interest in

[2] This Article focuses on foreign intelligence activity—that is, intelligence activity directed against foreign, rather than domestic, threats. While the latter *can* implicate international law, as when domestic intelligence activity implicates rights contained in the International Covenant on Civil and Political Rights, the former is far more likely to do so.

[3] See Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 2, ¶ 5 *in* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc A/56/10, at 71 (2001).

[4] States often do not specify the areas of activity to which particular bodies of international law will apply. However, the longstanding ambiguity about the relationship between intelli-

preserving the integrity of states (by requiring states to respect rules that protect other states' sovereignty) while reducing harm to individuals who find themselves targets of intelligence activity (by requiring states to respect human rights and international humanitarian law ("IHL")).

One problem is that these diametrically opposed approaches fail to grapple with each other's strengths. The formalists ignore that there *is* something unique about intelligence activity, and that requiring intelligence services to play by precisely the same rules as law enforcement, diplomatic, and military actors is doomed to produce state noncompliance. Those in the realpolitik camp fail to recognize that, in the face of new intelligence missions, a widened public visibility into intelligence activities, and pressures to protect individuals affected by these new missions, it is no longer sustainable to claim that intelligence activity can remain unbounded by norms such as those that protect basic humanity.

Another problem is that both approaches also adopt a one-size-fits-all approach to the application or nonapplication of international law constraints, without taking into consideration that distinct intelligence activities target different subjects and implicate different actor and victim equities. Specifically, some intelligence activities (such as renditions[5] and bulk data collection) are often directed against individuals who are not associated with foreign governments, while other activities (such as the Stuxnet cyber operation against Iran's nuclear centrifuges and cell phone surveillance of German Chancellor Angela Merkel) directly affect state actors or the state itself. Further, intelligence activities produce different types of victim harms. Some harms are serious, physical, and tangible (as with renditions or cyber operations that damage corporate assets),

gence activity and international law means that states perpetuate this ambiguity when they fail to specify whether particular international rules apply to intelligence activities.

[5] It is unclear whether activities such as the rendition of an individual from within one state's territory to another state without the former's consent violate Article 2(4). See, e.g., Auth. of the FBI to Override Int'l Law in Extraterritorial Law Enf't, 13 Op. O.L.C. 163, 178 (1989); W. Michael Reisman & James E. Baker, Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law 71 (1992) (stating that, even for nonconsensual renditions, "contemporary state practice may suggest that 'forcible extradition,' while often protested vociferously on the bilateral level, is tolerated on the international level, provided a minimal or proportionate use of force is involved in the seizure and the norm that the seized person violated is deemed to be one of general concern"). For purposes of this Article, I assume that an intelligence service undertaking a rendition has obtained the consent of the state from which the service removes the person.

while others are nebulous, intangible, and difficult to quantify (as with the theft of foreign diplomatic secrets).

An alternative—and more desirable—way to approach the international law/intelligence relationship is to identify the intersections between arguably relevant international legal norms, potential intelligence targets, and potential harms to those targets. A nuanced examination reveals that some of the potentially applicable legal norms were crafted to protect states, while others were intended to protect individuals. Relatedly, state targets and individual non-state actor targets are differently situated in their abilities to deter or defend against foreign intelligence activity ex ante and react to that activity ex post.[6] States are far more empowered than individuals to protect against and respond to foreign intelligence activities. The harms to states often are less immediate and less certain. And states rightly fear a lack of reciprocity if they agree to limit their own intelligence activities targeting other states. This suggests an approach to international law that should be more invested in a generous interpretation of rules that protect individuals, and less concerned with the way states interpret the rules that protect other states. Such an approach produces the best balance between individual and state equities, while doing little damage to the integrity of the international system.

This Article has four goals. First, it seeks to illustrate why the dominant view of the (nonexistent) relationship between intelligence and international legal constraints is overstated, descriptively and predictively. Part I sets the stage by discussing the source of the longstanding perception that international law does not regulate intelligence activities. It also introduces the contrary position that existing international rules can and do regulate those activities. It then explains why international law has the potential to play an important role in this area, notwithstanding the fact that many states already use domestic law to constrain various foreign intelligence activities by their counterparts.

Part II advances the idea that the realpolitik view, even if largely accurate as an historical matter, cannot endure. This Part argues that four important changes have taken place in the wider intelligence landscape,

[6] President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) [hereinafter Obama NSA Speech], https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [https://perma.cc/4JQS-3W5H] (drawing distinction between gathering information on governments and ordinary citizens).

fostering a more receptive atmosphere for the application of international law constraints to intelligence and a wider group of actors who seek to change the way states conduct intelligence activities. First, intelligence services are undertaking activities such as renditions, bulk data collection, and other counterterrorism and counterproliferation-focused actions that reach beyond traditional state targets. Second, the general public has a new breadth of knowledge about the intelligence actions states are undertaking. These two developments are effecting a sea change in how the average person conceives of intelligence activities and are serving as a catalyst for new regulatory control over those activities.[7] Third, a new "legalism" pervades certain intelligence communities. This keen attention to law is endogenous to intelligence agencies themselves, making the shift away from the realpolitik view seem inexorable. Fourth, the broader trend to "humanize" international law has created expectations about protecting individuals across all areas of state activity.

Even if one concludes that the changes captured in Part II are producing momentum toward a more formalist approach to the international law/intelligence relationship, this does not dictate that states must interpret various international law doctrines in the same manner across the spectrum of intelligence actions. The second goal of this Article is to illustrate that, in this context, not all international law is created equal. One basket of rules, containing IHL and certain human rights laws, is relatively detailed and focuses on protecting individuals. The other basket, composed of rules such as respect for state sovereignty and territorial integrity, regulates state-to-state activity. These rules tend to be broad and their scope less well defined; states have contested their meaning and boundaries for decades. (Some international laws fall between those poles.) Part III explores the implications of the fact that intelligence activities now create two distinct sets of relationships, covered by distinct bodies of international laws. Various actors are pressing states to apply the rules in both baskets, but this Part argues that the pressures to ensure individual protections are more compelling than pressures to protect state equities.

The Article's third goal is to demonstrate that this hybrid approach to international law is not as novel as it seems. Part IV uses the practices of

[7] Cf. M. Ryan Calo, The Drone as Privacy Catalyst, 64 Stan. L. Rev. Online 29, 29 (2011) (stating that drone technology may create the "visceral jolt" needed to restore privacy regulations).

the United States and United Kingdom to argue that some states are currently interpreting, as a matter of law or policy, certain individually-focused rules as constraining their intelligence activities, while paying far less heed to international rules that implicate the equities of states. For example, the United Kingdom has applied human rights law to its bulk electronic surveillance activities, but surely does not view other states' territorial integrity as limiting its ability to recruit operatives inside those states to steal government secrets. This Part also challenges the conventional wisdom described in Part I by identifying pre-and post-September 11 cases in which intelligence actors were attuned to the rules of international law.

The final goal of the Article is to introduce a new framework within which to interpret international law for intelligence activities. The most detailed effort to date to resolve whether a particular covert action violates or is consistent with international law takes a highly consequentialist approach that is very difficult to apply consistently.[8] This Article draws from the most compelling parts of the realpolitik and formalist approaches to suggest a different set of criteria, focused primarily on the identity of, and nature of harm to, the individuals impacted by the intelligence activity in question. Part V argues that states should apply a sliding scale interpretive approach to the international law/intelligence relationship. When engaged in intelligence activities that target actors not associated with governments, states should interpret strictly (in favor of the target) international rules that clearly address themselves to the type of harm the intelligence service is contemplating inflicting and that function to minimize the risk that a state will erroneously undertake a particular harmful activity against an individual. In contrast, when states undertake more traditional intelligence activities that primarily implicate the equities of other states, states should be permitted greater flexibility in interpreting relevant international law. The Article justifies this approach primarily on the basis that states have tacitly consented to it, and on a theory of international law as a form of due process. Of course, even a strict interpretation of international law in this context does not necessarily mean that the law will forbid the action contemplated. But it

[8] Reisman & Baker, supra note 5, at 26–27; see also Craig Forcese, Spies Without Borders: International Law and Intelligence Collection, 5 J. Nat'l Sec. L. & Pol'y 179, 183–84 (2011) (describing the various geographic categories into which electronic surveillance may fit); id. at 198 (noting that extraterritorial spying may have gradations of legality).

can impose an important—and in some cases the only—check on that action.

This approach will require two sets of actors to adapt: intelligence services (many of which to date have taken a realpolitik approach) and the formalists, who advocate for international legal constraints to apply broadly and strictly to all intelligence activity. If the latter group hopes to gain traction among states with robust intelligence capacities, it must allow states to adapt their international law interpretations to the special circumstances engendered by secret state activities, accepting that states require greater flexibility in interpreting some bodies of international law. At the same time, states and their intelligence services should adapt by formally acknowledging that they will interpret more strictly in favor of the targets certain types of international law constraints on their operations. If states make clear that they interpret some international law constraints to apply in these circumstances—as certain states do today—it will increase the perceived legitimacy of the operations, advance core rights protections, and potentially improve cooperation with allied intelligence services. Nor would this approach necessarily require dramatic changes to the known practice of several Western states.[9] Importantly, it would rationalize the relationship between international law and intelligence and offer legal guideposts for intelligence communities as their activities evolve. The ultimate goal of the approach is to strike a sustainable balance between the national security equities of states and core rights-related values that have come under challenge in this new world of intelligence activity.

I. INTERNATIONAL LAW'S (NON)REGULATION OF INTELLIGENCE

Two narratives are competing for control of the international law/intelligence relationship. The first, traditional, approach takes a starkly realist view of intelligence and assesses that international law does not (and will never) constrain the conduct of the bulk of intelligence activities.[10] In this story, states are intensely motivated to collect

[9] This Article focuses heavily on intelligence practices of Western democracies. Not only is less known about intelligence practices by states such as China and Russia, but those states are also subject to fewer external pressures to subject their practices to international law constraints. What this implies for this Article's proposed approach is discussed infra Section V.D.

[10] Gary D. Brown & Andrew O. Metcalf, Easier Said than Done: Legal Reviews of Cyber Weapons, 7 J. Nat'l Sec. L. & Pol'y 115, 116–17 (2014) ("[T]here is a long-standing (and

intelligence about the decision-making processes and capacities of foreign governments, particularly those of rivals.[11] Those states that are able to spy do so, using their intelligence capabilities as a key tool to advance their national security and foreign policy goals. And states with the capacity to conduct actions covertly to influence the foreign, economic, or military policies of foreign states have strong incentives to do so. Because states have historically faced little pressure from each other or from the public to regulate their intelligence activities, they reasonably have concluded that the benefits from unconstrained intelligence activity are high and the corresponding costs are few.[12]

This story resonates, particularly when one considers why spying and certain activities often undertaken as covert actions have proven hard to regulate.[13] First, intelligence activities implicate a state's core national

cynically named) 'gentleman's agreement' between nations to ignore espionage in international law . . . ."); W. Hays Parks, The International Law of Intelligence Collection, *in* National Security Law 433, 433–34 (John Norton Moore et al. eds., 1990) ("No serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each."); Jeffrey H. Smith, Keynote Address at the University of Michigan Journal of International Law Symposium: State Intelligence Gathering and International Law (Feb. 9, 2007), *in* 28 Mich. J. Int'l L. 543, 544 (2007) ("[B]ecause espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law."); see also Peyton Cooke, Bringing the Spies in from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War, 44 U.S.F. L. Rev. 601, 618 (2010) (erroneously arguing that the CIA will not abide by laws of war).

[11] This Part draws from Ashley Deeks, Intelligence Communities and International Law: A Comparative Approach, *in* Comparative International Law (A. Roberts et al. eds., forthcoming 2016) [hereinafter Deeks, Intelligence Communities] and Ashley Deeks, An International Legal Framework for Surveillance, 55 Va. J. Int'l L. 291 (2015) [hereinafter Deeks, International Legal Framework].

[12] This is not to say that this group of scholars and states has asserted that intelligence activities never interact with international law. These actors might acknowledge, for instance, that international law operates in the background, such that a spy operating under diplomatic cover would be entitled to diplomatic immunities under the Vienna Convention on Diplomatic Relations and customary law. They also presumably would acknowledge that nothing in international law requires states to *privilege* spying; domestic laws that prohibit espionage transgress no international rules. This Article instead focuses on *constraints* contained in international law: The debate between the realpolitikers and formalists centers on how to interpret various legal rules that facially constrain all state actors, including intelligence actors.

[13] See Deeks, International Legal Framework, supra note 11, at 300–13. The term "covert action" appears to be a uniquely American term, one that lacks a fixed definition in international relations. Abram N. Shulsky, Silent Warfare: Understanding the World of Intelligence 75–76 (1991). In using the phrase, I intend to capture activities that intelligence agencies

security interests, which involve anticipating hostile actions by states and terrorist groups and countering strategic threats.[14] States therefore are loath to limit their ability to protect themselves by any means that are not obviously unlawful. Second, espionage and covert action (at least when done well) typically occur without detection. The secrecy that attaches to such acts would make it hard for a state to detect violations of an agreement that reciprocally limited those acts. As a result, a state is less likely to assume such a commitment in the first place. Third, states closely guard their spying capacities. It is difficult for states to seriously discuss ways to limit spying on other states without revealing certain information about their capabilities, which chills possible discussions. Fourth, states with high levels of expertise have incentives to resist excessive regulation. Finally, because historically spying was costly and the most significant threats came from other governments, states rarely focused on non-state actors. As a result, public pressure to regulate intelligence activity was minimal, because spying and covert action seldom directly affected the average citizen.[15]

In the face of these incentives not to regulate intelligence activities, states and scholars have generally agreed about international law's relation to espionage: International law either fails to regulate spying or affirmatively permits it. One group draws on the *S.S. Lotus* case in the Permanent Court of International Justice.[16] There, the Court stated that international law allows states "a wide measure of discretion which is only limited in certain cases by prohibitive rules" and that in the absence of such rules "every State remains free to adopt the principles which it regards as best and most suitable."[17] This group thus invokes the proposition that, absent a positive rule, states may act as they see fit.[18] For

commonly have undertaken to influence the policies of or conditions in foreign states, where the state does not intend its role in those actions to be revealed publicly. These activities include support for friendly governments, influencing foreign perceptions using propaganda or forgeries, and supporting opposition activities through financial or other nonforcible assistance. Id. at 76–88. For an extensive typology of activities that states have undertaken covertly, see Reisman & Baker, supra note 5, at 11–12.

[14] Loch K. Johnson, Spies, Foreign Pol'y, Sept.-Oct. 2000, at 18, 18.

[15] Deeks, International Legal Framework, supra note 11, at 313–15.

[16] S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

[17] Id. at 18–19.

[18] See, e.g., Gary D. Brown, The Fourteenth Annual Sommerfeld Lecture: The Wrong Questions About Cyberspace, *in* 217 Mil. L. Rev. 214, 223 (2013) ("[E]spionage is not considered to be prohibited by international law . . . ."); Nigel Inkster, The Snowden Revelations: Myths and Misapprehensions, Survival, Feb.-Mar. 2014, at 51, 53.

them, nothing in international law forbids states from spying on other states; states therefore may spy on each other—and each other's nationals—without restriction.[19]

Another group interprets the widespread state engagement in espionage as indicating that states affirmatively recognize a right to undertake that conduct under international law.[20] As a former U.K. intelligence official noted, "Finding out what other governments are thinking is what [intelligence] agencies do."[21] Indeed, several government officials have publicly asserted that spying is permissible. President Obama recently stated that "few doubt[] the legitimacy of spying on hostile states."[22] Though legitimacy and legality are not identical, this clearly implies that the United States spies, at least on non-allies. British Prime Minister David Cameron reportedly pointed out at a European Union summit that spying capabilities have prevented many terror attacks.[23] In addition,

[19] See, e.g., Office of Gen. Counsel, Dep't of Def., An Assessment of International Legal Issues in Information Operations 34 (1999), *reprinted in* 76 Int'l L. Stud. 459, 502 (2002) ("International communications law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime."); Geoffrey B. Demarest, Espionage in International Law, 24 Denv. J. Int'l L. & Pol'y 321, 321 (1996) ("International law regarding peacetime espionage is virtually unstated . . . ."); Reese Nguyen, Navigating *Jus Ad Bellum* in the Age of Cyber Warfare, 101 Calif. L. Rev. 1079, 1082 (2013) (arguing espionage "is neither condoned nor condemned under international law"); A. John Radsan, The Unresolved Equation of Espionage and International Law, 28 Mich. J. Int'l L. 595, 596 (2007) (same); Roger D. Scott, Territorially Intrusive Intelligence Collection and International Law, 46 A.F. L. Rev. 217, 217 (1999) (noting that international law does not specifically prohibit espionage); Daniel B. Silver, Intelligence and Counterintelligence, *in* National Security Law 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005) (chapter updated and revised by Frederick P. Hitz & J.E. Shreve Ariail) (noting the ambiguous state of espionage under international law); Thomas C. Wingfield, Legal Aspects of Offensive Information Operations in Space, 9 U.S.A.F. Acad. J. Leg. Stud. 121, 140 (1999) (same).

[20] See, e.g., Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, The Intelligence Function and World Public Order, 46 Temp. L.Q. 365, 394 (1973); Smith, supra note 10, at 544. For recent examples of states spying on each other, see David E. Sanger, In Spy Uproar, 'Everyone Does It' Just Won't Do, N.Y. Times (Oct. 25, 2013), http://www.nytimes.com/2013/10/26/world/europe/in-spy-uproar-everyone-does-it-just-wont-do.html [https://perma.cc/WV9H-2GEY].

[21] Keir Simmons & Michele Neubert, Everyone Spies: Intelligence Insiders Shrug amid Outrage over U.S. Snooping Allegations, NBC News (Oct. 29, 2013, 5:13 PM), http://www.nbcnews.com/news/other/everyone-spies-intelligence-insiders-shrug-amid-outrage-over-us-snooping-f8C11487245 [https://perma.cc/G8SG-TQF4].

[22] Obama NSA Speech, supra note 6.

[23] Jacob Appelbaum et al., The NSA's Secret Spy Hub in Berlin, Der Spiegel (Kristen Allen & Charly Wilder trans., Oct. 27, 2013, 7:02 PM), http://www.spiegel.de/internation

some scholars have suggested that spying is an integral part of a state's right to act in self-defense because it allows states to accurately anticipate and prepare for armed attacks before they occur.[24]

Much of the writing in this area has been about espionage, but espionage is not the only intelligence activity that may operate beyond the reach of international law constraints. Some argue that international law does not purport to regulate covert action either.[25] Professor Kenneth Anderson, for instance, takes a broad approach:

> The traditional, yet mostly unstated and informal, position of countries' intelligence agencies on covert operations [includes the idea that] covert actions are something like 'extralegal' as regards international law. . . . Covert action's extralegal status is either a bug or a feature, depending mostly on how secret you manage to keep operations.[26]

A more modest claim about covert action's relationship to intelligence would include many covert actions short of force but would treat covert

al/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html [https://perma.cc/U9VU-GE5R].

[24] See Forcese, supra note 8, at 198–99; see also Christopher D. Baker, Tolerance of International Espionage: A Functional Approach, 19 Am. U. Int'l L. Rev. 1091, 1092 (2004) (arguing that espionage is essential to guarantee international cooperation). Although this argument supports spying on hostile or enemy states, it does not justify spying on close allies.

[25] See Michael Jefferson Adams, *Jus Extra Bellum*: Reconstructing the Ordinary, Realistic Conditions of Peace, 5 Harv. Nat'l Sec. J. 377, 402–03 (2014) ("Of particular relevance . . . is international law's silence on countless low-visibility national security activities, including forms of intelligence collection, clandestine activities, covert action, and low visibility operations."); Robert D. Williams, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, 79 Geo. Wash. L. Rev. 1162, 1165, 1178 (2011) ("The status of covert actions under transnational legal regimes is a subject of some debate, but there are no treaties or customary norms that explicitly proscribe the practice. . . . The status of covert action under international law is at least as uncertain as the status of espionage."). But see Alexandra H. Perina, Black Holes and Open Secrets: The Impact of Covert Action on International Law, 53 Colum. J. Transnat'l L. 507, 535 (2015) (arguing that international law applies to covert actions).

[26] Kenneth Anderson, Law and Order, The Weekly Standard, June 6, 2011 at 23, 23; see also Reisman & Baker, supra note 5, at 9 ("Conceptions of the lawfulness of covert activities that are derived from doctrines prohibiting the use of force against the territorial integrity or political independence of states are essentially inapplicable to . . . covert operations [that are directed against nongovernmental entities that use military force]."); Robert Chesney, Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate, 5 J. Nat'l Sec. L. & Pol'y 539, 544 (2012) (describing "lingering uncertainty with respect to whether and when international law prohibits one state from conducting espionage, covert action, or other operations within another state's territory").

uses of force in this construct as being unambiguously regulated by the U.N. Charter.[27] Call this the "realpolitik" school.

There are at least two possible theories in support of the view that certain categories of covert action operate outside international law constraints. The first presumably tracks the argument that espionage operates outside international law constraints: States anticipated that they and their allies and enemies would frequently engage in these activities and did not intend or expect "normal" international law to serve a regulatory function. Indeed, covert action and intelligence collection often are intertwined; it would be strange to treat one as clearly constrained by international law and the other as not so constrained. Under this approach, international law effectively contains carve-outs for various activities that states often have taken covertly, such as bribing foreign officials, interfering with foreign elections, and physically intruding into foreign states in ways that do not implicate Article 2(4)'s prohibition on the use of force.[28] The second possible theory is that states may not have deliberately intended to exclude these acts from being considered international law violations, but states undertake them so often that it would undermine the integrity of international law to treat them as such. We might say that international law thus evidences a tolerance for these activities.[29]

[27] See, e.g., Chesney, supra note 26, at 622 ("[T]here is neither a textual basis for construing Article 2(4) to contain an exception for covert operations, nor a good case for construing Article 2(4) to have such an exception."); Smith, supra note 10, at 545 (arguing that many activities carried out covertly are legal, but that "it is difficult to argue, absent some extraordinary circumstances, that a covert paramilitary effort to overthrow another government is consistent with international law").

[28] See, e.g., Reisman & Baker, supra note 5, at 29 (stating that there is no international prohibition on engaging in covert economic coercion, such as bribery); id. at 68 (describing the diplomatic, economic, and ideological modalities of covert action as "little regulated and generally tolerated"); Damrosch, supra note 1, at 38 (arguing that "increasing acceptance of nonforcible political influence may have a constructive effect in mitigating the factors that all too often have led to transboundary uses of force"); id. at 49 (stating that covert efforts to influence elections would be permissible if they increased the opportunity for citizens to participate in governance); W. Michael Reisman, Remarks at the International Studies Association Annual Meeting Intelligence Section: Covert Action (Mar. 29, 1994), *in* 20 Yale J. Int'l L. 419, 419–20 (1995) ("[W]e found that the international legal process, while often condemning uses of covert instruments at the verbal level, frequently accepted or accommodated itself to such uses.").

[29] Reisman & Baker, supra note 5, at 27 ("[W]hat is arguably textually prohibited by the Charter may well be tolerated and even supported in practice in certain circumstances.").

A competing narrative has developed, however. Some actors today reject these permissive positions, arguing that international law prohibits espionage and other intrusive intelligence activities.[30] Members of this school make a straightforward formalist argument that a state's international obligations apply to all actors within that state, and contain no carve-outs for intelligence operations.[31] This school also notes that states tend not to overtly claim that spying is legal—though this presumably is due in large part to the fact that spying usually violates the spied-upon state's domestic laws, making it difficult to assert a legal "right to spy." This school has identified at least four bodies of international law that could be read to regulate and constrain intelligence activities: customary international law ("CIL") related to sovereignty, nonintervention, and territorial integrity; the Vienna Convention on Diplomatic Relations ("VCDR"); the International Covenant on Civil and Political Rights ("ICCPR") or, more generally, human rights-focused CIL principles; and IHL.[32] The arguments for applying these bodies of international law to intelligence activities are fleshed out in greater detail in Part III. Call this the "formalist" approach.

Like many competing narratives, each side of the story contains some truth. The strength of the realpolitik approach is its overall historical accuracy and alignment with state interests. States have treated many intelligence activities as if they were carved out from the rules governing "normal" international relations. At the core of the realpolitik approach is the belief that states place so much weight on the value of intelligence and of exercising covert influence on other states that they are unlikely to adopt constraints on intelligence activities. This is particularly so because states are skeptical that their counterparts will comply; thus,

[30] See, e.g., Shulsky, supra note 13, at 92 (stating that covert action may be contrary to norms of international law, such as nonintervention in the internal affairs of sovereign states); Dieter Fleck, Individual and State Responsibility for Intelligence Gathering, 28 Mich. J. Int'l L. 687, 693 (2007) (arguing that many covert acts implicate human rights).

[31] Martin Scheinin, Rep. of the Special Rapporteur on the Promotion and Prot. of Human Rights and Fundamental Freedoms While Countering Terrorism, ¶ 12, Hum. Rts. Council, U.N. Doc. A/HRC/14/46 (May 17, 2010) [hereinafter Scheinin Report]; Fleck, supra note 30, at 702 ("Under international law, no state can rely on an 'intelligence exception.'"); Perina, supra note 25, at 535.

[32] Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95; International Covenant on Civil and Political Rights, opened for signature Dec. 19, 1966, S. Exec. Doc. No. E, 95-2, 999 U.N.T.S. 171. This school presumably would also assert that the U.N. Charter, including its rules regulating the use of interstate force, regulates intelligence activities. See Perina, supra note 25, at 528.

agreeing to new rules would leave them at a disadvantage. Indeed, it seems correct that states will be loath to tie their own hands when doing so would give an advantage to their competitors. On the other hand, a formalist approach means that states—at least in theory—already face international law limits when undertaking intelligence activity. States that violate that law should face state responsibility for those violations, as well as political pressure and other transactional and legal costs. Strip away those legal obligations, furthermore, and intelligence services are free to operate in a legal black hole. That opens the door wide to increased interstate friction and serious human rights abuses.

Neither approach recognizes that the other may have a point. To date, there has been very limited discussion across the divide, or even conversation about the debate itself. Until recently, states have remained reticent about their positions, preferring to keep their intelligence activities (and legal analyses thereof) in the shadows. Sharpening the terms of the debate, however, helps identify whether there are more satisfying approaches to the international law/intelligence relationship. Fortunately, several recent changes to the geopolitical landscape are bringing discussions about intelligence activities onto the international stage and creating new opportunities for states and other actors to take public positions on the relationship between intelligence communities and international law.

Before turning to the next Part, which identifies and analyzes the changing background against which intelligence services now operate, it is important to consider what is at stake in the international law debate. After all, many states have enacted domestic laws that regulate acts that often occur during intelligence operations, such as renditions (which may constitute a type of kidnapping), bribery, blackmail, espionage, theft, fraud, and misuse of classified information. If existing domestic laws deter foreign intelligence activity ex ante and punish it ex post, why does it matter how international law treats such activity?

There are several ways in which international law can provide additional—and important—rules for interstate behavior in the intelligence area. First, reliance on domestic law alone (and criminal law in particular) to regulate foreign intelligence may produce insufficient deterrence. It may be hard for a target state to identify the individuals engaged in the intelligence activity against it, especially when that activity uses complicated, remote technologies. Second, some states may lack a sufficient range of domestic statutes to address these various behaviors, and may

have insufficient resources to prosecute such cases when they arise. Third, states may be more tolerant of foreign intelligence activity against disfavored groups (such as minorities) and less willing to pursue domestic remedies on their behalf. Fourth, international law serves an expressive function, and, in the human rights context, can signal a commitment to providing universal protections against certain troubling acts by states. An assertion that a state has violated international law conveys a different and more potent message than a claim that a particular foreign official violated another state's domestic law. Finally, international law opens up additional remedies by which states can resist and suppress violations, including through the use of international institutions and the doctrine of state responsibility. For all of these reasons, rules of international law that regulate and constrain intelligence activity can play an important role in shaping state behavior.

II. A CHANGING INTELLIGENCE LANDSCAPE

In the millennia-long history of state intelligence activities, the vast majority of those activities have been directed against other states. For example, states long have recruited foreign officials and conducted physical and electronic surveillance to gain insider access to the decision making of foreign governments; steal foreign military plans; ascertain the size of weapons arsenals; determine other governments' negotiating positions; and overthrow hostile governments, replacing them with leaders more friendly to the acting state. Today, we are at the crossroads of important changes that involve significantly increased access by both U.S. and foreign citizens to information about various states' intelligence activities, an expansion of intelligence missions, and an increasingly legalized culture inside intelligence communities. This confluence of changes has produced a greater number of actors who seek more robust application of international law constraints to intelligence activities and who face a more receptive audience for those claims inside rule-of-law-focused governments and their intelligence services.

This Part argues that even if the realpolitik view has been the correct one historically, it cannot endure in the medium term. Four important changes, coupled with the additional, specific pressures on states discussed in Part III, are stimulating a shift toward the formalist view.

A. Public Access to Information

The first critical change is an increase in access to information about intelligence activities. The general public has significantly greater information about actions the Central Intelligence Agency ("CIA"), National Security Agency ("NSA"), and other actors in the U.S. intelligence community have undertaken in the past ten years. Some of this information has emerged from leaks. Some has emerged from the intelligence agencies themselves, or from their overseers. Additional information has appeared in news reports because more of what intelligence communities are being asked to do now is publicly detectable.

This is not to suggest that intelligence activities never became public in the past. Professor Michael Reisman and Judge James Baker, for example, identified eight covert actions that became widely known, including the 1953 effort by the United States and United Kingdom to overthrow Iran's Prime Minister; the Israeli kidnapping in 1960 of Adolf Eichmann from Argentina to stand trial in Israel; and the CIA's efforts in 1970 to prevent Salvador Allende from taking power in Chile.[33] One important recent development, however, is that information about intelligence activities is coming to light in near-real time, rather than decades after the fact. That means that there are greater incentives to pressure governments (through litigation, among other means) to effect immediate policy changes, because the programs at issue may be ongoing.

1. Leaks

Edward Snowden's leaks of information about the activities of the NSA and its U.K. equivalent, the Government Communications Headquarters ("GCHQ"), revealed large amounts of classified information about state electronic surveillance programs, highlighting the breadth and depth of government capabilities. Although the leaks provided specific evidence that the United States and other states spy on the communications of each other's leaders, the leaks also disclosed that NSA and GCHQ programs collected large amounts of telecommunications and Internet information from average citizens, both U.S. and foreign.[34] The

[33] Reisman & Baker, supra note 5, at 49–52, 59–61.

[34] Ewen MacAskill et al., GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications, Guardian (U.K.) (June 21, 2013, 12:23 PM), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [https://perma.cc/L7S8-55HD].

United States and United Kingdom are not alone in collecting data (sometimes in bulk) on foreign citizens. States such as France, Spain, Germany, and Sweden also undertake bulk collection.[35]

Other types of intelligence activities have come to light as a result of leaks to journalists. U.S. government officials revealed that in 2001 President Bush authorized the CIA to use lethal force against, capture, and detain members of al Qaeda.[36] The media learned that in 2007 President Bush authorized the CIA to undertake covert action to destabilize Iran's government.[37] The U.S. executive branch authorized some of these revelations itself, as when former CIA Director Leon Panetta revealed, shortly after the U.S. action in Pakistan that killed Osama bin Laden, that the United States had undertaken the raid as a covert action.[38]

Different types of intelligence activities trigger different responses by the public. Most U.S. citizens are likely to support U.S. efforts to pres-

[35] Adam Entous & Siobhan Gorman, Europeans Shared Spy Data with U.S., Wall St. J. (Oct. 29, 2013, 7:31 PM), http://www.wsj.com/articles/SB10001424052702300804579165653105860502 [https://perma.cc/Y58K-JMGR]; Steven Erlanger, France, Too, Is Sweeping Up Data, Newspaper Reveals, N.Y. Times (July 4, 2013), http://www.nytimes.com/2013/07/05/world/europe/france-too-is-collecting-data-newspaper-reveals.html [https://perma.cc/QYZ6-7Z9A]; Benjamin Wittes, Mark Klamberg on EU Metadata Collection, Lawfare (Sept. 29, 2013, 1:03 PM), http://www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection. See generally Ira Rubinstein, Greg Nojeim & Ronald Lee, Ctr. for Democracy & Tech., Systematic Government Access to Personal Data: A Comparative Analysis 14–15 (2013) [hereinafter CDT Report], https://cdt.org/files/2014/11/government-access-to-data-comparative-analysis.pdf [https://perma.cc/FJ5Y-4RB4] (discussing revelations of French and German programs); Christopher Wolf, A Transnational Perspective on Section 702 of the Foreign Intelligence Surveillance Act, Testimony Before the Privacy & Civil Liberties Oversight Board 8–14 (Mar. 19, 2014), https://www.pclob.gov/library/20140319-Testimony-Wolf.pdf [https://perma.cc/TX72-7XEM] (describing the intelligence regimes of nations across the globe).

[36] David Johnston, At a Secret Interrogation, Dispute Flared over Tactics, N.Y. Times (Sept. 10, 2006), http://www.nytimes.com/2006/09/10/washington/10detain.html [https://perma.cc/TYD5-Z85C]; Jane Mayer, The Predator War, New Yorker (Oct. 26, 2009), http://www.newyorker.com/magazine/2009/10/26/the-predator-war [https://perma.cc/VG5H-NJQX].

[37] Brian Ross & Richard Esposito, Bush Authorizes New Covert Action Against Iran, ABC News: Blotter (May 24, 2007), http://blogs.abcnews.com/theblotter/2007/05/bush_authorizes.html [https://perma.cc/YZK8-DT4U] (describing covert action finding that authorized the CIA to use propaganda, disinformation, and currency manipulation to pressure Iranian regime).

[38] CIA Chief Panetta: Obama Made 'Gutsy' Decision on bin Laden Raid, PBS NewsHour (May 3, 2011), http://www.pbs.org/newshour/bb/terrorism-jan-june11-panetta_05-03 [https://perma.cc/4CUE-GEFJ].

sure the Iranian government using nonlethal tools. This is a traditional intelligence activity: One state covertly tries to influence the internal dynamics of another to achieve specific foreign policy goals. Other activities stimulate far more concern, however, particularly when those activities directly implicate the life, liberty, and privacy of individuals not associated with governments.[39] The recent leaks have illustrated—in ways that startled the general public—the prevalence today of that latter type of activity.

2. Voluntary Transparency

Leaks are not the only ways in which intelligence activity is coming to light. Some governments have chosen voluntarily to tell the public more about their activities. The United States has done so through a series of speeches by executive branch officials. In 2010, State Department Legal Adviser Harold Koh gave a speech stating that all U.S. operations involving the use of force are conducted in accordance with all applicable law, and that all U.S. targeting practices, including those undertaken using unmanned aerial vehicles, comply with the laws of war.[40] It was widely reported at that point that both the Defense Department and the CIA used force against members of al Qaeda and associated forces in various geographic locations.[41] As a result, Koh's speech was understood to apply to both agencies. Subsequently, then-CIA General Counsel Stephen Preston gave a speech detailing how the United States con-

[39] See Jaime Fuller, Americans are Fine with Drone Strikes. Everyone Else in the World? Not So Much., Wash. Post (July 15, 2014), https://www.washingtonpost.com/news/the-fix/wp/2014/07/15/americans-are-fine-with-drone-strikes-everyone-else-in-the-world-not-so-much [https://perma.cc/R8RU-J4B9] (noting that opposition around world to drone strikes is "sweeping"). For discussions of new roles for intelligence agencies, see Richard J. Aldrich, International Intelligence Cooperation in Practice, *in* International Intelligence Cooperation and Accountability 18, 20 (Hans Born et al. eds., 2011) (describing intelligence operations today as "more kinetic and more controversial"); id. at 31 (describing intelligence services as moving beyond passive intelligence gathering to "fixing, enforcing and disruption"); see also Detainee Inquiry, Report, 2013, ¶ 5.7 (U.K.) [hereinafter U.K. Detainee Inquiry], http://www.detaineeinquiry.org.uk/wp-content/uploads/2013/12/35100_Trafalgar-Text-accessible.pdf [https://perma.cc/64SV-8KPW] (describing the U.K. Secret Intelligence Service admission that it had little experience before 2001 in interviewing detainees in the field as a result of lack of prior operational need).

[40] Harold Koh, The Obama Administration and International Law, Speech at the Annual Meeting of the American Society of International Law (Mar. 25, 2010), http://www.state.gov/s/l/releases/remarks/139119.htm [https://perma.cc/C5D9-YPK2].

[41] See, e.g., Mayer, supra note 36 (describing in 2009 the existence of Department of Defense and CIA drone programs).

ducts its legal analysis of covert operations.[42] John Brennan, then serving as Assistant to the President for Homeland Security and Counterterrorism, publicly explained and defended the U.S. use of drones to kill members of al Qaeda.[43] Finally, President Obama gave a speech discussing the NSA's electronic surveillance and describing changes to U.S. policy intended to "provide greater transparency to our surveillance activities."[44]

Other forms of government transparency take the form of voluntary declassification. The Privacy and Civil Liberties Oversight Board, which President Obama tasked to review the U.S. government's surveillance programs, successfully urged U.S. intelligence agencies to declassify many facts surrounding the "Section 702" program by which the NSA collects email content from overseas targets.[45] The U.S. intelligence community also declassified a number of opinions from the Foreign Intelligence Surveillance Court ("FISC").[46]

Overall, the public now expects greater transparency about intelligence activities and some governments have begun to provide it. In presenting the U.K. Intelligence and Security Committee ("ISC") report on surveillance, a U.K. parliamentarian stated, "There is a legitimate public

[42] Stephen W. Preston, Gen. Counsel, CIA, Remarks at Harvard Law School (Apr. 10, 2012), https://www.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/cia-general-counsel-harvard.html [https://perma.cc/TN2Z-BX63].

[43] John O. Brennan, The Efficacy and Ethics of U.S. Counterterrorism Strategy, Remarks at the Wilson Center (Apr. 30, 2012), http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy [https://perma.cc/6YRY-RV8X]; John O. Brennan, Strengthening our Security by Adhering to our Values and Laws, Remarks at Harvard Law School (Sept. 16, 2011) [hereinafter Brennan Harvard Speech], http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an [https://perma.cc/U29X-7CKL].

[44] Obama NSA Speech, supra note 6; see also Robert S. Litt, U.S. Intelligence Community Surveillance One Year After President Obama's Address, Remarks at the Brookings Institute (Feb. 4, 2015), http://www.brookings.edu/~/media/events/2015/02/04-surveillance/20150204_intelligence_surveillance_litt_transcript.pdf [https://perma.cc/KSV9-NZ9R] (explaining how the United States implemented policy changes announced in President Obama's speech and associated Presidential Policy Directive).

[45] Privacy & Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 3 (2014) (noting that as a result of the Board's efforts, "many facts that were previously classified are now available to the public").

[46] See, e.g., Press Release, Office of the Dir. of Nat'l Intelligence, ODNI and DOJ Release Additional Declassified FISC Filings and Orders Related to Section 215 of the USA Patriot Act (May 14, 2014), http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1065-odni-and-doj-release-additional-declassified-fisc-filings-and-orders-related-to-section-215-of-the-usa-patriot-act [https://perma.cc/3HV4-ZLNG].

expectation of openness and transparency in today's society, and the security and intelligence agencies are not exempt from that. . . . This is essential to improve public understanding and retain confidence in the vital work of the intelligence and security Agencies."[47] Ironically, the Snowden leaks themselves prompted greater transparency from the U.S. intelligence community. The General Counsel of the Office of the Director of National Intelligence stated:

> The best way to prevent the damage that leakers can cause is by increased transparency on our part . . . . Public confidence in the way that we conduct our admitted secret [activities] is [essential] if we are to continue to be able to anticipate and respond to the many threats facing our nation.[48]

Although the U.S. intelligence community must continue to conduct many of its operations in secret, this increasing push for greater transparency aligns with an instinct in U.S. culture that is uncomfortable with secrecy.[49] As a former FBI official wrote, "What makes the United States unique is that we dislike the fundamentals of our own policy [of conducting covert action]. We take national pride in promoting self-determination, public disclosure, and public diplomacy. We dislike secrecy."[50] Producing more rigorous determinations about what must be kept secret can alleviate some of the cognitive dissonance between the national character of the United States and its intelligence operations.

3. Increased Physical Detectability

Some activities that intelligence agencies undertake today produce observable effects in ways that differ from traditional intelligence activi-

[47] Matt Dathan, Edward Snowden Report: MPs Call for Major Overhaul of Surveillance Laws, Independent (U.K.) (Mar. 12, 2015), http://www.independent.co.uk/news/uk/politics/edward-snowden-report-mps-call-for-major-overhaul-of-surveillance-laws-10103363.html [https://perma.cc/7U2R-R3UC] (U.K. parliamentarian Hazel Blears commenting on ISC's surveillance report).

[48] Josh Gerstein, Litt Lashes Leakers, Touts Transparency, Politico: Under the Radar (Mar. 18, 2014, 5:36 PM), http://www.politico.com/blogs/under-the-radar/2014/03/litt-lashes-leakers-touts-transparency-185327 [https://perma.cc/7KQR-SESN] (reporting Robert Litt's statement that officials are now paying close attention to the risks that secret programs will be disclosed and considering whether they should not be deemed secret in the first place).

[49] See Shulsky, supra note 13, at 144 (discussing how use of secrecy in a democracy can undercut legitimacy of intelligence services).

[50] M.E. Bowman, Secrets in Plain View: Covert Action the U.S. Way, 72 Int'l L. Stud. 1, 12 (1998).

ty. For example, the CIA is alleged to have conducted a significant number of rendition flights that transported al Qaeda detainees through European airspace. European parliamentarians and rights groups were able (after the fact) to identify what they claimed were the flight paths and aircraft used for the flights.[51] Likewise, journalists and nongovernmental organizations ("NGOs") have investigated targeted killings in Somalia, Yemen, and Pakistan.[52] Learning about the location, timing, and targets of these killings is simplified by the fact that drone strikes—unlike, say, efforts to recruit a foreign asset—produce visible physical damage. Stuxnet provides another example. Computer scientists discovered the Stuxnet worm, which destroyed about one thousand Iranian nuclear centrifuges, when it spread to computers outside of Iran.[53] These media and parliamentary reports highlight previously unknown aspects of intelligence activities, including their geographic location, scope, and targets. The Internet allows these reports to circulate widely.

In addition, those adversely affected by intelligence activities have incentives to reveal those activities in ways intelligence "victims" did not used to have. Historically, states and state actors have been the targets of foreign intelligence activity. State targets often have incentives not to reveal intelligence actions taken against them because they are embarrassed, fear revealing weakness, or seek to avoid a diplomatic clash. In contrast, individual victims who are not state actors have many reasons to reveal the fact and impact of intelligence activity, and few reasons not to. The victims may desire reparations, public condemnation of the intelligence activity, revenge, or action by their state of nationality to prevent repetition of the activity.

[51] Dick Marty (Rapporteur), Alleged Secret Detentions and Unlawful Inter-State Transfers Involving Council of Europe Member States, Committee on Legal Affairs and Human Rights, Council of Europe Parliamentary Assembly, AS/Jur (2006), ¶ 219 (June 7, 2006), http://assembly.coe.int/committeedocs/2006/20060606_ejdoc162006partii-final.pdf [https://perma.cc/GQ3P-Q76N].

[52] See, e.g., Human Rights Watch, "Between a Drone and al-Qaeda": The Civilian Cost of US Targeted Killings in Yemen (2013), https://www.hrw.org/sites/default/files/reports/yemen1013_ForUpload.pdf [https://perma.cc/52GU-XXVL] (Yemen and Pakistan); Helene Cooper, Somali Militant Leader Believed Killed in Drone Strike, N.Y. Times (Apr. 1, 2016), http://www.nytimes.com/2016/04/02/world/africa/american-strike-shabab-somalia.html [https://perma.cc/86EH-5WPV] (Somalia).

[53] David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, N.Y. Times (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [https://perma.cc/D55N-Z7MQ].

These two phenomena feed into a third element: an increased overall interest in what intelligence communities do. A U.S. career intelligence officer wrote, "In the course of twenty-five years of operational intelligence experience, where my task was to gather actionable intelligence information from individuals who ran the gambit from helpful to hostile, no one outside the profession seemed at all interested in either what I did or . . . how I did it."[54] This is no longer true. In the wake of recent intelligence leaks about interrogation, rendition, and surveillance, and in the face of new terrorist and proliferation threats to Western states, many more people are informed about and interested in intelligence activity. This amplifies the effect of reports about intelligence activities. The converse also is true: The greater the number of people who are interested in intelligence, the more likely it is that journalists, civil liberties groups, and others will pursue stories, litigation, and other actions that implicate intelligence—and seek to cabin its reach through the application of international law.

B. Expanded Missions

As a related matter, intelligence agencies (especially the CIA and NSA in the United States and MI6 and GCHQ in the United Kingdom[55]) are being asked to undertake a new set of missions. The missions are programmatic, lasting years rather than days or months. In the wake of the September 11 attacks, these missions included, for the CIA, targeted killings of members of al Qaeda[56] as well as detention, rendition, and interrogation;[57] and for both the NSA and GCHQ, electronic surveillance to detect activities of those engaged in terrorism and proliferation.[58]As President Obama has noted:

[54] Steven M. Kleinman, The Compatibility of Intelligence Gathering, Interrogation, and Preventing Torture, 11 N.Y. City L. Rev. 325, 325 (2008).

[55] MI6 is the commonly used name for the U.K.'s Secret Intelligence Service ("SIS").

[56] Earlier examples of comparable intelligence activities include actual and attempted assassinations. See, e.g., S. Select Comm. to Study Governmental Operations, Interim Report on Alleged Assassination Plots Involving Foreign Leaders, S. Rep. No. 94–465, at 1 (1975); CIA Historical Review Program, Soviet Use of Assassination and Kidnapping (Sept. 22, 1993), https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol19no3/html/v19i3a01p_0001.htm [https://perma.cc/3PVX-URPE].

[57] S. Select Comm. on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, S. Rep. No. 113-288 (2014).

[58] MacAskill et al., supra note 34.

> [E]merging threats from terrorist groups and the proliferation of weapons of mass destruction place new and in some ways more complicated demands on our intelligence agencies. Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence, as well as great good. . . .
>
> . . . .
>
> . . . [Our intelligence agencies] were now asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated by spies or informants.[59]

These new missions implicate non-state actors as never before. In the case of targeted killings, renditions, and detentions, the targets are not state actors or militaries. Rather, they are members of al Qaeda, ISIS, and associated forces—groups that are unaffiliated with a state and that employ tactics that include operating from within civilian populations. This increases the likelihood that innocent civilians may be affected by intelligence activities directed at these non-state groups. The nontraditional nature of the U.S. armed conflict with al Qaeda blurs military, intelligence, and counterterrorism actions. As a result, the CIA has been asked to perform acts that usually transpire in wartime, such as the noncriminal detention and interrogation of members of armed groups.

Although forcible intelligence activities are not the subject of this Article, the fact that the U.S. government has tasked the CIA to undertake these types of activities has stimulated interest in and concern about how intelligence activities affect individuals. In addition, if intelligence services are using force, they surely also are engaged in activities short of the use of force that also implicate non-state actors. Two reported examples include bribing or threatening members of the Taliban to switch their support to the Afghan government and supporting a fake vaccination drive to secure information about Osama bin Laden's location.[60]

---

[59] Obama NSA Speech, supra note 6.

[60] CIA's 'Fake Vaccine Drive' to Get bin Laden Family DNA, BBC News (July 12, 2011), http://www.bbc.com/news/world-south-asia-14117438; Joby Warrick, Little Blue Pills Among the Ways CIA Wins Friends in Afghanistan, Wash. Post (Dec. 26, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/12/25/AR2008122500931.html [https://perma.cc/GQ95-L3UJ].

In addition, counterterrorism and counterproliferation goals have grown in importance, with states such as the United States identifying terrorism, proliferation of weapons of mass destruction ("WMDs"), and transnational organized crime as among the top security threats.[61] This means non-state actors are now a significant focus of many intelligence communities. Further, to the extent that electronic surveillance is an important way to detect and ultimately halt those types of activities, surveillance agencies have turned to bulk collection, which implicates the communications of millions of private individuals. As President Obama noted, "[T]he same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach."[62] As a result, each of these missions increases the interactions between intelligence agencies and individuals not associated with foreign governments.

C. Legalized Culture

Third, an increasingly legalistic approach to intelligence is both caused by and is causing a change in intelligence culture. At least in several Western states, intelligence organizations are increasingly bound by significant quantities of law. The organizations also are becoming more attuned to the way law is used by outside actors to alter intelligence behavior; many intelligence services now understand the relevance of legal compliance to the organizations' perceived legitimacy. Formalist arguments are more persuasive to those who seek enhanced legitimacy through legal compliance; realpolitik arguments become less sustainable when the costs of a legal black hole become more tangible.

1. More Law, More Lawyers

Today—more so than fifteen years ago—many intelligence communities are bounded by detailed statutes. In examining the NSA, Professor Margo Schlanger has identified this phenomenon as "intelligence legal-

[61] James R. Clapper, Dir. of Nat'l Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Community (2014), at ii, http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf [https://perma.cc/9SUW-CGDF].

[62] Obama NSA speech, supra note 6.

ism."[63] The phenomenon has occurred in other U.S. agencies as well. Then-CIA General Counsel Stephen Preston stated, "[T]he rule of law is integral to Agency operations."[64] Preston described U.S. domestic legal constraints at length, but also noted that the executive branch takes into account international law. Foreign intelligence services also have experienced increased legalism over the past two decades.[65] These states had some intelligence-related statutes on the books before 2000,[66] but these statutes, and more recent amendments, have become increasingly dense and detailed.[67]

Not surprisingly, as intelligence services face greater quantities of regulation, they hire more lawyers to help them navigate and comply with those regulations. The number of legal officers within the CIA grew from ten in the mid-1970s to approximately 150 in 2010.[68] With that rise in numbers came a shift in mindset: "[T]he Agency transformed itself from being indifferent to the law to being preoccupied by it."[69] Professor Jack Goldsmith describes the "scores of legal restrictions on the executive branch" that are enforced by that "bevy of lawyers."[70] The U.K. services also appear to be infused with lawyers who provide direct guidance to intelligence operators. For example, the U.K. Parliament's

[63] David S. Kris & J. Doug Wilson, 1 National Security Investigations and Prosecutions, §§ 2.7, 3.4 (2d ed. 2012) (describing grafting of legal culture onto NSA culture); Margo Schlanger, Intelligence Legalism and the National Security Agency's Civil Liberties Gap, 6 Harv. Nat'l Sec. J. 112 (2015).

[64] Preston, supra note 42.

[65] Intelligence Services Act 2001 (Austl.) (establishing in statute the Australian Secret Intelligence Service and Defence Signals Directorate (now the Australian Signals Directorate), and imposing ministerial authorization and parliamentary oversight requirements); Anti-Terrorism Act, S.C. 2001, c 41 (Can.) (regulating the Communications Security Establishment of Canada (the NSA's equivalent) and its collection operations); General Security Service Law, 5766–2002, SH No. 1832 p. 179 (Isr.) (regulating its internal security service); Regulation of Investigatory Powers Act ("RIPA") 2000 (U.K.) (structuring how public actors may conduct surveillance, investigations, and the use of covert intelligence sources).

[66] The Canadian statute regulating Canada's equivalent of the CIA dates to 1985, for instance. Canadian Security Intelligence Service Act, R.S.C. 1985, c C-23.

[67] See Kris & Wilson, supra note 63, at §§ 2.3, 2.5 (citing earlier "culture of lawlessness" and flagrant disregard of law by CIA); Aldrich, supra note 39, at 35 ("In the 1990s, the European intelligence services went through a regulatory revolution during which many services were given a legal identity and in some cases the European Convention on Human Rights was written into their core guidance."); Bowman, supra note 50, at 6 ("Not until 1974 did Congress seriously begin to consider a role for itself in covert operations.").

[68] Jack Goldsmith, Power and Constraint: The Accountable Presidency After 9/11, at 87 (2012).

[69] Id.

[70] Id. at 107.

ISC Report on Rendition describes how intelligence operators receive legal briefings on both domestic and international law to ensure that sharing U.K. intelligence does not result in torture or mistreatment by other intelligence services.[71]

There are historical precedents for legalizing national security institutions. Intelligence communities' approach to law and lawyers today looks familiar to the transition that occurred within state militaries several decades ago. Many states determined that there was a significant benefit to increasing the role of law and lawyers in military operations. Post-Vietnam, U.S. military engagements involved "closer-than-usual contact with civilians and raised hard law-of-war issues—especially about detention, interrogation, and rules of engagement—that lawyers were vital in sorting out."[72] "[T]he continued rise in the influence of lawyers in the post-9/11 era reflects a judgment by the military establishment that having the lawyer in the targeting cell is a net-plus on balance."[73] Because more intelligence activities today involve "closer-than-usual contact with civilians," it is unsurprising that intelligence lawyers play an increasingly important role in helping operators navigate the law.

2. More Litigation

Litigation is helping to focus the attention of intelligence communities on the law and legal compliance. And as those communities face more leaks and voluntarily become more transparent, the quantum of litigation likely will increase. Disclosures about intelligence activities directly affect the likelihood that plaintiffs suing governments or government officials will succeed in litigation, because the disclosures may alter courts' assessments of jurisdictional issues such as standing and

[71] Intelligence and Security Committee, Rendition, 2007, at ¶¶ 172, 174, 53–54 (U.K.) [hereinafter ISC Rendition Report]. Additionally, in 2006 the U.K. Security Service (the FBI equivalent) and the Secret Intelligence Service (the CIA equivalent, which as previously noted is also commonly known as MI6) issued guidance about liaison relationships that recommended when to consult the Services' Legal Advisors. U.K. Detainee Inquiry, supra note 39, ¶ 5.81.

[72] Goldsmith, supra note 68, at 127.

[73] Id. at 146. Goldsmith adds, quoting General Mark Martins, "[W]e still have a lot of initiative, we still have forces that can win, we're still very effective, and we're made more effective by the legitimacy that comes from being law-governed; and that requires lawyers out and about." Id.

privileges such as the state secrets privilege.[74] The disclosures also reveal secret programs of which potential plaintiffs may not have been aware.

In the past ten years, individuals have, with increasing frequency, begun to challenge the legality of different forms of intelligence activity in court. This contemporary role for courts stands in contrast to the highly cabined role they have historically played in overseeing intelligence, although courts in the United States have been more reluctant to decide these cases on the merits than have foreign and international courts.[75] For instance, in the United States, a U.K. resident (and several others) who had been subject to rendition sued a CIA contractor, claiming that the company flew rendition flights on the CIA's behalf.[76] The plaintiffs invoked the Alien Tort Statute, alleging acts that constituted international law violations such as torture and cruel, inhuman, and degrading treatment, as well as forced disappearance. Although the U.S. Court of Appeals for the Ninth Circuit concluded that the state secrets privilege precluded the plaintiffs from proceeding with their case, the court admitted that it found the case difficult[77] and ordered the government to pay the plaintiffs' costs—something the plaintiffs themselves had not requested.[78] It is hard not to interpret this order and the opinion's dicta as signaling the court's displeasure about the executive's underlying rendition policy and its decision to invoke the state secrets privilege.[79]

In the United Kingdom, the son of a man allegedly killed by a U.S. drone in Pakistan sued GCHQ, claiming that GCHQ employees had abetted murder by providing locational intelligence to the CIA so that it could target the individual.[80] Another U.K. court allowed an individual

[74] See Ashley S. Deeks, Intelligence Services, Peer Constraints, and the Law, *in* Global Intelligence Oversight: Governing Security in the Twenty-First Century (Zachary K. Goldman & Samuel J. Rascoff eds., forthcoming 2016) (manuscript at 9).

[75] Goldsmith, supra note 68, at 83–84 (stating "[t]he courts played no role in monitoring CIA activities" during Allen Dulles's time as CIA Director from 1953–1961).

[76] Mohammed v. Jeppesen Dataplan, Inc., 614 F.3d 1070 (9th Cir. 2010) (en banc).

[77] Id. at 1073 (noting that the court reached its decision "reluctantly").

[78] See Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 8 (D.D.C. 2010) (expressing concern that the United States needed a warrant to wiretap an American citizen abroad but required no such judicial review to kill an American citizen alleged to be a high level al Qaeda operative).

[79] Ashley S. Deeks, The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference, 82 Fordham L. Rev. 827, 830 (2013).

[80] Ravi Somaiya, Drone Strike Prompts Suit, Raising Fears for U.S. Allies, N.Y. Times (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/world/drone-strike-lawsuit-raises-

to proceed with his claim that U.K. and U.S. intelligence services transferred him to the Libyan government, which he alleges tortured him.[81] Several civil liberties groups filed a legal challenge to U.K. surveillance practices in the European Court of Human Rights, claiming that bulk collection violates international law and U.K. domestic law.[82]

Some attempts to bring intelligence officials into court take the form of criminal cases. Several states have undertaken criminal investigations or prosecutions of those engaged in intelligence activities. Italy prosecuted a number of U.S. intelligence and military officials for allegedly rendering a radical sheikh from Milan to Egypt.[83] A German prosecutor investigated whether the NSA tapped Angela Merkel's cell phone, but has not found sufficient proof to initiate a case.[84] A Lithuanian prosecutor recently reopened an investigation of reports that Lithuania hosted a secret CIA detention facility; the focus is likely to be on senior Lithuanian intelligence officials.[85] The United States itself has filed criminal charges against five Chinese military officials for conducting electronic espionage against U.S. corporations.[86]

This litigation heightens intelligence services' awareness of the contested nature of their activities, as well as the potential legal exposure of

concerns-on-intelligence-sharing.html [https://perma.cc/L5EY-TYKP] (noting that case raised the prospect of legal liability for European officials by linking them to the U.S. drone campaign, which is widely seen as illegal in their home states). The U.K. Court of Appeal ultimately ruled against Khan. Khan v. Sec'y of State for Foreign and Commonwealth Affairs [2014] EWCA (Civ) 24, [53]–[54] (Eng.).

[81] Owen Bowcott, Abdel Hakim Belhaj Wins Right to Sue U.K. Government over His Kidnap, Guardian (U.K.) (Oct. 30, 2014), http://www.theguardian.com/world/2014/oct/30/abdel-hakim-belhaj-court-kidnap-mi6-cia-torture [https://perma.cc/CC4A-4R8D].

[82] Amnesty International Takes UK Government to European Court of Human Rights Over Mass Surveillance, Amnesty Int'l (Apr. 10, 2015), https://www.amnesty.org/en/articles/news/2015/04/amnesty-international-takes-uk-government-to-european-court-of-human-rights-over-mass-surveillance/ [https://perma.cc/CK7Z-VKVY].

[83] Craig Whitlock, Testimony Helps Detail CIA's Post-9/11 Reach, Wash. Post (Dec. 16, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/12/15/AR2006121502044.html [https://perma.cc/P2NE-PQKC].

[84] Alexandra Hudson, No Proof So Far that NSA Bugged Merkel's Phone: Prosecutor, Reuters, Dec. 11, 2014, http://www.reuters.com/article/2014/12/11/us-germany-usa-spying-idUSKBN0JP1QG20141211 [https://perma.cc/RC2N-TN9J].

[85] Andrius Sytas & Christian Lowe, Exclusive: Lithuanian Prosecutors Restart Investigation into CIA Jail, Reuters, Apr. 2, 2015,http://www.reuters.com/article/2015/04/02/us-usa-cia-torture-lithuania-idUSKBN0MT18Z20150402 [https://perma.cc/7QBH-TXZC].

[86] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/2QCP-MVW].

their officials. Such concerns will only increase their attention to applicable legal constraints and the desire to protect themselves from legal proceedings by complying with those constraints. Even when states have not traditionally viewed a particular body of international law as applicable, litigation is likely causing them to rethink that realpolitik view.

3. Increased Desire for Legitimacy

The final element changing the landscape in which intelligence communities operate is an increased interest within these communities in having the public perceive their actions as legitimate. In the constitutional context, Professor Richard Fallon has argued that legitimacy takes three forms: legal, sociological, and moral.[87] Intelligence agencies today seem most interested in garnering legal and sociological legitimacy. Legal legitimacy is associated with law-abidingness. Sociological legitimacy arises when others view one's actions as justified and appropriate.[88]

Intelligence communities have instrumental reasons to increase the public's sense that their activities are legitimate. As President Obama argued in a 2014 speech:

> [W]e have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require. We need to do so not only because it is right, but because the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon. . . . And for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.[89]

At least among Western democracies, a given intelligence agency will more readily be able to sustain cooperation with its peer intelligence services if those services (and the leadership of those foreign countries) view the agency as law-abiding (that is, legally legitimate) and engaged in justified and acceptable activity (that is, sociologically legitimate).

[87] Richard H. Fallon, Jr., Legitimacy and the Constitution, 118 Harv. L. Rev. 1787, 1790 (2005).
[88] Id. at 1794–95.
[89] Obama NSA speech, supra note 6.

There may be a second reason that intelligence communities—particularly in democracies—hope to increase their legitimacy.[90] That is simply to relieve the burden of feeling undervalued even though they are performing tasks their government has asked them to do.[91] Individuals who engage in difficult yet secret tasks and who believe that they are doing the "right thing" understandably wish to see their work valued appropriately. Recent criticisms of intelligence activities, particularly in the United States and United Kingdom, place intelligence services under a shadow from which they surely would like to emerge.

This changed intelligence culture, which is more attuned to the relevance of law and to the consequences of real or perceived noncompliance with law, produces constraining effects between and among intelligence services too. Using various mechanisms, one state's intelligence service can affect how another intelligence service conducts its activities and the amount and kind of intelligence the other service receives.[92] The nature of intelligence relationships can lead to second-order effects that result in one intelligence service being constrained not only by its own laws and rules but also by the laws and legal interpretations of other states with which it is cooperating. Legalism therefore can be contagious.

D. Humanization of International Law

The humanization of international law reflects a move away from a Westphalian understanding of international law, in which states are the central actors and interstate relationships are of primacy concern. Professor Theodor Meron has described the various ways in which international law has shifted its focus away from state-state relations and toward the protection of the individual in areas as diverse as investment, the environment, war-fighting, and intellectual property.[93] Humanization reflects that international law plays an important role in ensuring that

[90] For a discussion of the U.S. intelligence community's concerns about its own legitimacy, see Benjamin Wittes, The Intelligence Legitimacy Paradox, Lawfare (May 15, 2014, 6:14 PM), http://www.lawfareblog.com/2014/05/the-intelligence-legitimacy-paradox.

[91] See Bowman, supra note 50, at 2–4 (arguing that U.S. citizens "simply don't like secrecy. We like to consider ourselves as ingenuous, open, and honest. We prefer to regard deviousness and secrecy as the product of evil empires. . . . Covert action, which definitionally restricts participatory activity, seems somehow antithetical to these ideals").

[92] Deeks, supra note 74, at 2.

[93] Jacob Katz Cogan, The Regulatory Turn in International Law, 52 Harv. Int'l L.J. 321, 323–24 (2011).

states respect the integrity of the individual and in protecting him from excessive governmental control.[94] As Judge Thomas Buergenthal wrote:

> When we compare the position of individuals under international law as it existed before the Second World War with their status under contemporary international law, it is evident that a dramatic legal and conceptual transformation has taken place. This transformation has "internationalized human rights and humanized international law." . . . [I]ndividuals as such now have internationally guaranteed human rights . . . .[95]

In war-fighting, for instance, "'humanization' has profoundly modified states' conduct"[96] by emphasizing the need to decrease individual suffering, even in the absence of reciprocity among parties fighting the conflict. "[H]uman beings are being brought front and center, and thus displacing the state from its long unrivaled position as the principal actor and primary beneficiary of the legal regulation of international relations."[97] Several (though by no means all) recent domestic and regional court decisions have held that international human rights rules take priority over state-focused rules implicating state immunity and counterterrorism actions.[98] In addition, several secondary rules of international law protect individual rights at the expense of states' flexibility of action.[99]

[94] Id. ("The triumph of human rights as an idea—if not a fully effective tool—has only grown since. Whether the focus is war, trade, intellectual property, investment, the environment, or any number of other topics, human rights norms now influence, in varying degrees, international law and politics more than ever before." (footnotes omitted)).

[95] Thomas Buergenthal, International Law and the Holocaust, *in* Holocaust Restitution: Perspectives on the Litigation and Its Legacy 17, 21 (Michael J. Bazyler & Roger P. Alford eds., 2006) (footnotes omitted).

[96] Amrita Kapur, The Rise of International Criminal Law: Intended and Unintended Consequences: A Reply to Ken Anderson, 20 Eur. J. Int'l L. 1031, 1032 (2009).

[97] Mohamed S. Helal, Justifying War and the Limits of Humanitarianism, 37 Fordham Int'l L.J. 551, 554 (2014).

[98] Joined Cases C-402/05P & C-415/05P, Yassin Abdullah Kadi & Al Barakaat Int'l Found. v. Council of Eur. Union & Comm'n of Eur. Cmtys., 2008 E.C.R. I-6351, I-6509 (concluding that imposition of UN Security Council-mandated sanctions violated rights to due process and property contained in E.U. law); Al-Jedda v. United Kingdom, 2011-IV Eur. Ct. H.R. 308, 310 (concluding that the United Kingdom could not rely on a UN Security Council resolution to justify al-Jedda's noncriminal detention in Iraq, given U.K. obligations under ECHR article 5).

[99] See, e.g., Vienna Convention on the Law of Treaties art. 60(5), May 23, 1969, 1155 U.N.T.S. 331 (stating that states may not withdraw from or terminate treaty obligations in face of treaty partner's material breach of IHL treaty); Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 50 *in* Int'l Law Comm'n, Rep. on the Work of

This broader trend of expanding the reach of human rights to all areas in which states and individuals interact has altered the background expectations against which intelligence communities operate.

***

The preceding Sections set the stage for new thinking about whether, when, and how to apply international law to intelligence activities. We know more about more intelligence activities to which states conceivably could apply existing laws. A far greater number of private individuals are affected by these activities. And intelligence services themselves are becoming acclimated to legalism and perceive more keenly the connection between legal compliance and legitimacy.

At the same time that these background changes have occurred, members of the U.S. and foreign publics, elites, foreign leaders, corporations, and civil liberties groups have pressured the U.S. executive branch and Congress to terminate or limit some of these intelligence activities. Other states, including the United Kingdom and Australia, face similar pressures.[100] Those seeking to impose restrictions on actors often turn to all available arguments or sources of existing law. One area that has captured the attention of those who hope to constrain states is international law. As discussed in the next Part, these groups claim that international rules protecting the equities of both states and individuals do and should apply to intelligence. The realpolitik view thus is increasingly unsettled.

III. CONFRONTING INTELLIGENCE ACTIVITIES WITH INTERNATIONAL LAW

Notwithstanding the realpolitik tradition, invoking international law to criticize and challenge intelligence activities is not entirely new. States claimed that violations of international law occurred in a number of historical intelligence episodes, including the 1960 U-2 incident, in

Its Fifty-Third Session, U.N. Doc A/56/10, at 333 (2001) (prohibiting states from taking countermeasures that would affect obligations protecting human rights or obligations of a humanitarian character prohibiting reprisals).

[100] Sam Ball, UK Approves Mass Surveillance as Privacy Battle Continues, France 24 (Dec. 7, 2014), http://www.france24.com/en/20141207-uk-tribunal-approves-mass-surveillance-privacy-battle-continues-gchq-snowden [https://perma.cc/EE82-XURV]; Ewen MacAskill & Lenore Taylor, Australia's Spy Agencies Targeted Indonesian President's Mobile Phone, Guardian (U.K.) (Nov. 17, 2013), http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone [https://perma.cc/4FWB-KXTC].

which the U.S.S.R. shot down a U.S. spy plane,[101] and the Rainbow Warrior incident, in which French intelligence operatives sunk a Greenpeace ship in New Zealand waters.[102] Other intelligence cases exist in which the victim state invoked international law as part of its claim against the violator,[103] but examples are uncommon.

The Snowden leaks have evinced from states more explicit statements about their views of the relationship between international law and foreign surveillance, with states asserting that certain treaties or CIL rules prohibit elements of those programs.[104] Likewise, revelations about detentions, renditions, and cyber operations by the CIA have prompted states and other actors to argue that rules related to the *jus ad bellum*, the laws of war, and human rights law apply to those actions.[105] There is a lack of consensus about how, precisely, existing rules of international law regulate these activities. Nevertheless, the fact that more states have been provoked into stating their views on the relationship between intel-

[101] The U.S.S.R. stated, "'The integrity of the territory of all states has always been and remains . . . a major and generally recognized principle of international law,' observance of which is the 'backbone of peaceable relations between states.'" Quincy Wright, Legal Aspects of the U-2 Incident, 54 Am. J. Int'l L. 836, 841 (1960) (noting also that the U.S.S.R's draft Security Council Resolution asserted that "violations of the sovereignty of the state are incompatible with the principles and purposes of the Charter of the United Nations").

[102] See Reisman & Baker, supra note 5, at 66–67. France ultimately paid New Zealand $7 million and publicly acknowledged that "the attack carried out against the 'Rainbow Warrior' took place in violation of the territorial sovereignty of New Zealand and that it was therefore committed in violation of international law." Memorandum of the Government of the French Republic to the Secretary General of the United Nations at ¶ 5, U.N. Secretary-General: Ruling on the Rainbow Warrior Affair Between France and New Zealand, 19 R.I.A.A. 199, 209 (1986). See also Text of Goldwater's Letter to Head of C.I.A., N.Y. Times (Apr. 11, 1984), http://www.nytimes.com/1984/04/11/world/text-of-goldwater-s-letter-to-the-head-of-cia.html [https://perma.cc/54N6-YTLR] (accusing the CIA of violating international law by mining Nicaragua's harbors).

[103] Covert uses of force and nonconsensual renditions sometimes evoke claims that the covert actor violated the victim state's territorial integrity and national sovereignty. See Tom Ruys, The Meaning of "Force" and the Boundaries of the *Jus Ad Bellum*: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, 108 Am. J. Int'l L. 159, 193 (2014). For example, Argentina complained that Israel's covert abduction of Nazi fugitive Adolf Eichmann violated its sovereignty. Representative of Argentina, Letter Dated June 15, 1960 from the Representative of Argentina Addressed to the President of the Security Council, U.N. Doc. S/4336 (June 15, 1960).

[104] I leave for future work a deeper analysis of the sincerity of each state's claims, the incentives of the states making these various claims, and tangible practice by the intelligence communities of the states making these claims.

[105] As noted in Part I supra, I do not treat the realpolitik view as necessarily rejecting the argument that *jus ad bellum* rules regulate intelligence activities, even if some states and scholars nevertheless doubt the applicability of *jus ad bellum* constraints in this context.

ligence activities and international law—both about whether a state's intelligence activities should comply with international law and about which international laws are implicated—is prompting a reconsideration of the international law/intelligence relationship.

States are not the only actors using international law as a tool of argumentation. Efforts to impose more international law on intelligence activities are arising in different fora, ranging from litigation in domestic courts to human rights resolutions in the United Nations. Notwithstanding the disparate nature of actors who seek to alter the way governments conduct intelligence activities, a relatively unusual alignment of interests has formed among corporations, elite opinion, and many "ordinary citizens"—all of whom would like to see greater restraints on those activities.[106]

States have several incentives to argue that international law applies to the activities of other states, particularly now that so much detail has come to light. "Wronged" states may be motivated to issue their complaints in international law terms simply because they believe that international law does (or should) regulate these activities. But they often have other motivations as well: They may be responding to complaints from domestic constituencies who were adversely affected by the intelligence activity. They may seek an excuse to criticize the states conducting the intelligence activity, even if they themselves perform the same behavior. They may have nothing to lose, because they have weak intelligence services. Or they may believe that only if their partner intelligence services comply with international law can they continue to cooperate with those partners.[107]

NGOs and similar groups presumably want states to apply international law constraints to intelligence activities because they genuinely believe that, as a matter of legal interpretation, states intended international law to apply to these acts when they developed that law. The mission of human rights NGOs is generally to focus on the protection of individuals rather than on national security equities, and so these groups have been outspoken opponents of intelligence activities such as bulk data collection and renditions, while advocating for increased transpar-

[106] Deeks, International Legal Framework, supra note 11, at 328.

[107] See Soering v. United Kingdom, 161 Eur. Ct. H.R. (ser. A) at 44 (1989) (holding that the United Kingdom could not extradite criminal suspect to the United States because the amount of time spent by those on death row in the United States exposes that individual to a real risk of inhuman or degrading treatment); Deeks, supra note 74, at 16–17.

ency by intelligence services.[108] Some NGOs feel directly and adversely affected by surveillance, claiming that it has chilled their communications with foreign actors.[109] As a legal policy matter, these groups would argue that, more than any other activity, secret intelligence activities require rules to protect individual rights. Their broader goal is to try to force states to stop or modify the activities in question. Yet many of these actors recognize that existing international law must be "repurposed" in order for it to regulate these activities.[110]

This Part argues that not all intelligence targets are created equal. Nor is all international law that potentially implicates intelligence activities created equal. Pressures to employ international law to provide certain basic protections to individual intelligence targets are compelling. Pressures to use international law to protect the equities of target states against traditional intelligence actions are less persuasive. This is so because of the widely divergent power dynamics between states and individuals. Individuals are third-party beneficiaries of individually-focused international law, which states created to provide basic protections to individuals in their interactions with states. Individuals have limited means to contest state action. Target states, on the other hand, have a far greater ability to contest foreign intelligence action, and the harms they suffer from that action often are less immediate and direct than those felt by private individuals.

[108] Anthea Roberts, Righting Wrongs or Wronging Rights? The United States and Human Rights Post-September 11, 15 Eur. J. Int'l L. 721, 738 (2004).

[109] Human Rights Watch & Am. Civ. Liberties Union, With Liberty to Monitor All: How Large-Scale U.S. Surveillance Is Harming Journalism, Law and American Democracy 71–75 (July 2014); Tanya O'Carroll, Human Rights Groups Cannot Do Their Jobs in a Surveillance State, Amnesty Int'l (July 9, 2015), https://www.amnesty.org/en/latest/campaigns/2015/07/human-rights-groups-cannot-jobs-surveillance-state [https://perma.cc/7TF9-6K3J].

[110] For a recognition that the application of international law to surveillance currently is unclear and requires development, see Peter Margulies, The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism, 82 Fordham L. Rev. 2137, 2138 (2014); International Principles on the Application of Human Rights to Communications Surveillance, Necessary and Proportionate (May 2014), https://en.necessaryandproportionate.org [https://perma.cc/Z9BW-DNKM] (arguing, contradictorily, that law has not kept up with modern communications surveillance and that states "must comply" with a long list of principles in order to "actually meet their international human rights obligations"); Laura Pitter, Comments of Human Rights Watch, Testimony Before the Privacy & Civil Liberties Oversight Board 8 (Mar. 19, 2014), https://www.pclob.gov/library/20140319-Testimony-Pitter.pdf [https://perma.cc/PHH5-SCA7] (implicitly recognizing lack of clarity in law when stating that "[c]oncepts of jurisdiction based on control over territory and persons . . . can and should adapt to the reality of mass digital surveillance").

The following Sections identify two categories of pressure on intelligence communities to comply with existing international law. One category relates to efforts to protect *individuals* who may be affected by intelligence activities through the invocation of human rights rules and, where relevant, IHL. The other category focuses on *state-centric* concepts such as territorial integrity and diplomatic protection as a means to critique acts of foreign intelligence services. This Part then argues that states should be more attentive to the first set of pressures than the second.

A. Pressures to Respect Individual Rights

The first set of pressures urges intelligence services to act consistently with several bodies of international law that protect individual rights. Specifically, some states and many human rights groups have urged states to ensure that their intelligence activities comply with protections contained in the ICCPR (in particular, the right to privacy, humane treatment protections, and the protection against arbitrary deprivation of life), the Convention Against Torture ("CAT"),[111] and IHL. This pressure has manifested itself in public statements, litigation, action in the United Nations, and private interactions among intelligence services.

1. Naming and Shaming

Some states have responded to spying revelations by publicly accusing the spying states of violating human rights law. Specifically, certain states have asserted that electronic surveillance of the type undertaken by the NSA and GCHQ violates the right to privacy and other human rights obligations contained in the ICCPR (and, for the United Kingdom and other European states, the European Convention on Human Rights ("ECHR")).[112] For example, Brazilian President Dilma Rousseff called

[111] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, opened for signature Dec. 10, 1984, S. Treaty Doc. No. 100-20, 1465 U.N.T.S. 85.

[112] ICCPR article 17(1) states, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." International Covenant on Civil and Political Rights art. 17(1), opened for signature Dec. 19, 1966, S. Exec. Doc. No. E, 95-2, 999 U.N.T.S. 171. For states parties to the Council of Europe, the European Convention on Human Rights provides another potentially relevant international obligation. Article 8 establishes a right to respect for privacy and correspondence, subject to limited interference. European Convention on Human Rights art. 8, opened for signature Apr. 11, 1950, E.T.S. 5.

the NSA surveillance program "a breach of [i]nternational [l]aw" and a "situation of grave violations of human rights and of civil liberties."[113] She added, "The right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country."[114]

Human rights groups agree, though until recently few international actors viewed the ICCPR or CIL rules that draw on that treaty as regulating purely foreign intelligence collection.[115] States may begin to interpret the right to privacy in this way, especially when surveillance captures the content of communications, but the application and nature of that right is embryonic.[116] A former head of GCHQ stated, "As a result of pressure from civil rights organizations following Snowden, governments are rightly re-examining processes and legal frameworks for intelligence activity and seeking to improve oversight mechanisms."[117]

Human rights groups have been even more pointed in their public arguments that various treaties apply to (and prohibit) renditions,[118] the maintenance of secret detention facilities, and the use of enhanced inter-

[113] President Dilma Rousseff, Statement at the Opening of the General Debate of the Sixty-Third Session of the United Nations General Assembly, (Sept. 24, 2013), http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [https://perma.cc/Z9WL-GEMT].

[114] Tom Risen, Brazil's President Tells U.N. That NSA Spying Violates Human Rights, U.S. News (Sept. 24, 2013), http://www.usnews.com/news/articles/2013/09/24/brazils-president-tells-un-that-nsa-spying-violates-human-rights [https://perma.cc/MX4R-VFE2].

[115] Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, 56 Harv. Int'l L.J. 81, 108 (2015).

[116] Deeks, International Legal Framework, supra note 11, at 293–95. Current and former state leaders and human rights groups effectively concede as much. See Ryan Gallagher, After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty, Slate: Future Tense (Sept. 26, 2013, 2:16 PM), http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html [https://perma.cc/PQ9G-QK5E] (describing Germany's efforts to clarify that the ICCPR applied to electronic privacy); Jagland: International Spy Laws Necessary after Snowden Leaks, UPI, Nov. 20, 2013, http://www.upi.com/Top_News/World-News/2013/11/20/Jagland-International-spy-laws-necessary-after-Snowden-leaks/62701384960646 [https://perma.cc/5MLP-XBSK] (discussing the former Norwegian Prime Minister's argument for new international laws applicable to new surveillance technologies); Pitter, supra note 110, at 8.

[117] David Omand, Understanding Digital Intelligence and the Norms That Might Govern It 17 (Global Comm'n on Internet Governance, Paper No. 8, Mar. 2015), https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no8.pdf [https://perma.cc/QS56-6TWR].

[118] See, e.g., Margaret L. Satterthwaite, Rendered Meaningless: Extraordinary Rendition and the Rule of Law, 75 Geo. Wash. L. Rev. 1333, 1386–94 (2007) (arguing that human rights treaties apply to extraterritorial transfers of detainees by the CIA).

rogation techniques.[119] For these groups, there is no question that human rights law governs these actions against individuals, and that states should be held to account for their violations of this law.

Even a state's legislature may invoke international law as a means to control the intelligence community it oversees. For example, at least as of 1992, the Senate Select Committee on Intelligence's criteria for reviewing U.S. covert action programs include the following questions: "What is the character of those whom we support? Do they support democratic processes and human rights?" and "If [the program] were to become known, could it be justified under international law?"[120] Public calls for human rights compliance by intelligence services are now widespread.

2. Litigation

Another way human rights groups have attempted to hold states to account for their alleged international law violations is through litigation. These groups have helped individuals bring cases in U.S., U.K., and international courts related to renditions,[121] electronic surveillance,[122] and

[119] Amnesty Int'l, USA: Crimes and Impunity 133–34 (Apr. 21, 2015); Human Rights Watch, No Questions Asked: Intelligence Cooperation with Countries that Torture 1 (June 2010); Human Rights Watch, USA and Torture: A History of Hypocrisy (Dec. 9, 2014), https://www.hrw.org/news/2014/12/09/usa-and-torture-history-hypocrisy [https://perma.cc/AXB4-3ZPL].

[120] Reisman & Baker, supra note 5, at 122; see also Select Comm. to Study Governmental Operations, Final Report of the Select Committee to Study Governmental Operations With Respect to Intelligence Activities, S. Rep. No. 94-755, at 33 n.14a (1976) (noting that "norms of international law are relevant in assessing the legal and constitutional aspects of covert action"); Sen. Feinstein's Full Remarks on CIA Torture Report, USA Today (Dec. 9, 2014), http://www.usatoday.com/story/news/politics/2014/12/09/dianne-feinstein-cia-torture-report-full-remarks/20151977 (noting that the CAT's ban on torture is absolute).

[121] See Mohammed v. Jeppesen Dataplan, Inc., 614 F.3d 1070 (9th Cir. 2010) (en banc); Bowcott, supra note 81; Jamie Doward, Secrets of CIA 'Ghost Flights' to be Revealed, Guardian (U.K.) (July 25, 2009), http://www.theguardian.com/world/2009/jul/26/cia-rendition-guantanamo [https://perma.cc/9VR9-N7FV]; Factsheet, Eur. Ct. H.R., Secret Detention Sites, (Feb. 2016), http://www.echr.coe.int/Documents/FS_Secret_detention_ENG.pdf [https://perma.cc/5UP7-8TYB] (describing cases of *El-Masri v. Macedonia*, *Al Nashiri v. Poland*, and *Abu Zubaydah v. Poland*).

[122] See Privacy Int'l v. United Kingdom, [2014] UKIPTrib (Investigatory Powers Trib.) Case No. IPT/13/92/CH, [28] (U.K.); Owen Bowcott, Libya Rendition Victims Demand Disclosure of UK Surveillance Policy, Guardian (U.K.) (Oct. 17, 2014), http://www.theguardian.com/world/2014/oct/17/libya-rendition-disclosure-uk-surveillance-policy [https://perma.cc/UT8E-YFSF] (noting that rendition victims claimed denial of fair trial in their civil suit for kidnapping and torture because GCHQ eavesdropped on their attorney-

detainee mistreatment.[123] In some cases, courts have been amenable to holding intelligence communities liable for violations of international law. The European Court of Human Rights ("ECtHR") found Macedonia responsible for cooperating with the CIA in a way that resulted in the ill treatment by the CIA of a German national detained in Macedonia and transported to Afghanistan. The Court found that Macedonia violated Articles 3 (prohibition on torture and degrading treatment) and 5 (right to liberty and security) of the ECHR.[124] In a separate case, the ECtHR held that Poland violated the rights of two detainees whom the CIA allegedly held and mistreated in secret detention facilities in Poland.[125]

Even some domestic courts, which may be more reluctant to decide intelligence-related cases and may be more sensitive to national security issues than the ECtHR, have allowed these cases to proceed. For example, a U.K. appeals court has allowed Abdel Belhaj to proceed with his claim that MI6 and the CIA rendered him to Libya, where he was mistreated.[126] It reached this conclusion even though it recognized that allowing the trial would require a U.K. court to assess the wrongfulness of acts by U.S. and Libyan intelligence agents.[127] These types of cases produce both direct and atmospheric pressures on intelligence communities to take rights-focused international law into account when conducting their operations.

3. United Nations

The United Nations serves as another forum in which states and NGOs have pressured states to ensure that their intelligence communities act consistent with human rights treaties and IHL. For example, after Edward Snowden's leaks revealed that the NSA was monitoring Chan-

client discussions). U.S. plaintiffs have brought cases regarding NSA surveillance but have not invoked international law as a source of their complaints. See, e.g., Complaint for Declaratory and Injunctive Relief at 6–10, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-3994), 2013 WL 2492595 (claiming that NSA surveillance violated the First and Fourth Amendments and federal statutes, but not invoking international law).

[123] See Arar v. Ashcroft, 585 F.3d 559 (2d Cir. 2009) (en banc); El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007) (ACLU representing el-Masri); Binyam Mohamed v. Sec'y of State for Foreign Affairs [2010] EWCA (Civ) 65 (Eng.).

[124] Factsheet, supra note 121, at 1–2 (describing case of *El-Masri v. Macedonia*).

[125] Id. at 3 (describing cases of *Al Nashiri v. Poland* and *Abu Zubaydah v. Poland*).

[126] Bowcott, supra note 81.

[127] Id.

cellor Angela Merkel's cell phone, Germany and Brazil sponsored a U.N. General Assembly ("UNGA") resolution addressing the right to privacy in the electronic age.[128] In December 2013, the UNGA adopted the resolution, which "[a]ffirms that the same rights that people have offline must also be protected online, including the right to privacy,"[129] and calls on states "[t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy."[130] The resolution's preamble sweeps in overseas surveillance, noting "[d]eep[] concern[] at the negative impact that . . . extraterritorial surveillance . . . may have on the exercise and enjoyment of human rights."[131] At the same time, the fact that many states joined Germany and Brazil in supporting the resolution suggests that states thought it was important to clarify that the right to privacy in the ICCPR extends to foreign electronic surveillance.[132]

In a different U.N. channel, the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression criticized extraterritorial surveillance and expressed concern that such surveillance "raises serious concern with regard to the extraterritorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance,

[128] G.A. Res. 68/167, ¶ 3 (Dec. 18, 2013). The UNGA adopted the resolution by consensus. The U.S. Government joined consensus on the resolution with an Explanation of Position that affirmed its "longstanding" views of the ICCPR, including articles 2 and 17. That is, the United States reads the resolution as applying only to the extent that a state is acting on its own territory. U.S. Envoy at U.N., Explanation of Position on Draft Resolution L.26/Rev. 1 The Right to Privacy in the Digital Age (Nov. 25, 2014), http://iipdigital.usembassy.gov/st/english/texttrans/2014/11/20141126311471.html#axzz3xj47wbSn [https://perma.cc/Q345-9DM6].

[129] G.A. Res. 68/167, supra note 128.

[130] Id. ¶ 4(c).

[131] Id. at 2.

[132] Pressures on states to apply the ICCPR to their intelligence activities are new. I was able to find no examples before 2006 of cases in which anyone alleged that a particular intelligence activity violated the ICCPR or the ECHR. See David Weissbrodt & Amy Bergquist, Extraordinary Renditions: A Human Rights Analysis, 19 Harv. Hum. Rts. J. 123, 129 (2006) (arguing that extraordinary renditions violate the ICCPR, among other treaties). In 2006, Simon Chesterman listed four bodies of international law that arguably apply to espionage, and omitted a discussion of international human rights law entirely. Simon Chesterman, The Spy Who Came in from the Cold War: Intelligence and International Law, 27 Mich. J. Int'l L. 1071, 1081–87 (2006).

challenge decisions with respect to foreign surveillance, or seek remedies."[133] The U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism wrote a report emphasizing that states using drones must comply with IHL and human rights law.[134] At the same time, he recognized that "there is currently no clear international consensus" about the interpretation and application of international law on the use of deadly force in counterterrorism operations.[135] The prior Special Rapporteur compiled a summary of good practices on legal frameworks that ensure respect for human rights by intelligence agencies.[136] In his view, those practices include a requirement that intelligence services operate in a manner consistent with international human rights law.[137] These examples reveal both pressures to apply human rights law and IHL to intelligence operations and a recognition that ambiguity remains about whether, when, and how international law regulates those operations.

4. Peer Constraints

Finally, a far less public mechanism is in play among states' intelligence communities.[138] One state's intelligence community can impose logistical or substantive constraints on the activities of its counterparts, including in ways that rely on or implicate the first state's domestic and international legal obligations.[139] Through various mechanisms, one state's intelligence services can affect the way in which another intelligence service conducts activities such as interrogation, detention, and surveillance.[140] Many of these constraints derive from international hu-

[133] Frank LaRue, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, ¶ 64, Hum. Rts. Council, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).

[134] Ben Emmerson, Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, ¶ 23, Hum. Rts. Council, U.N. Doc. A/HRC/25/59 (Mar. 10, 2014).

[135] Id. ¶ 70.

[136] Scheinin Report, supra note 31, ¶¶ 9–50.

[137] Id. ¶ 11 (practices 4 and 5).

[138] For an extended discussion of these "peer constraints," see Deeks, supra note 74.

[139] One scholar has argued that intelligence communities may constrain each other based "almost exclusively by a shared professional ethos, rather than law." Elizabeth Sepper, Democracy, Human Rights, and Intelligence Sharing, 46 Tex. Int'l L.J. 151, 153 (2010). In my view, law itself provides direct and indirect constraints in this context.

[140] These influences broadly establish "accountability": *A* is accountable to *B* when *A* must inform *B* about *A's* actions and decisions, justify them, and suffer a penalty in case of mis-

man rights obligations. For instance, one intelligence service might insist on receiving diplomatic assurances that a detainee being transferred to another intelligence service will be treated humanely—an obligation that derives from the CAT.[141] Though not every interaction among intelligence services triggers these constraints, states that are attuned to the rule of law and already believe that at least some international law binds their intelligence activities will transitively impose comparable rules of behavior on their peer services in relevant cases in exchange for intelligence cooperation.

B. Pressures to Respect Rights of States

Human rights law and IHL are not the only bodies of international law potentially implicated by intelligence activities. States recently have alleged that other states are violating international rules related to diplomatic relations and sovereignty. Most of this state pressure has taken the form of public allegations and "naming and shaming," though one state brought a case in the International Court of Justice ("ICJ") against another state it accused of spying. The media has revealed many of these allegations to be hypocritical, however.[142] Additionally, at least some types of harms of which state targets are complaining, and against which relevant international law might protect, are harms to state dignity, which are less concrete than the more tangible harms imposed on individual non-state actor targets.

Certain states have recently levied allegations that other states' officials are spying on them from within foreign embassies. These accusing states appear to believe that it violates the VCDR for a sending state to conduct electronic surveillance from within its diplomatic facilities against government officials in the receiving state. The VCDR requires all persons receiving diplomatic immunity to "respect the laws and regu-

conduct. Andreas Schedler, Conceptualizing Accountability, *in* The Self-Restraining State: Power and Accountability in New Democracies 13, 17 (Andreas Schedler et al. eds., 1999).

[141] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment art. 3, opened for signature Dec. 10, 1984, S. Treaty Doc. No. 100-20, 1465 U.N.T.S. 85.

[142] David Francis, Germany's Hypocrisy on NSA Surveillance, Slate: Future Tense (Feb. 25, 2014), http://www.slate.com/articles/technology/future_tense/2014/02/angela_merkel_surveillance_proposal_germany_is_hypocritical_about_the_nsa.html [https://perma.cc/WBQ7-YEU2]; Matt Vasilogambros, Brazil's Moment of Hypocrisy: They Spied on Allies Too, Nat'l J. (Nov. 4, 2013), http://www.nationaljournal.com/s/67264/brazils-moment-hypocrisy-they-spied-allies-too?mref=scroll.

lations of the receiving State."[143] Likewise, the treaty requires receiving states to treat foreign missions and archives as inviolable.[144] One could interpret these provisions as an agreement that diplomats and receiving states will not spy on each other. However, recent (and historical) news reports are rife with descriptions of spying conducted from within and against diplomatic posts.[145]

For example, Germany's Foreign Ministry summoned the U.K. ambassador to Germany to demand an explanation of reports that the United Kingdom was spying on Germany from within the U.K. Embassy in Berlin. The German Ministry "indicated that tapping communications from a diplomatic mission would be a violation of international law."[146] It is unclear how the United Kingdom responded. Pakistan also appears to believe that certain U.S. foreign surveillance in Pakistan violated diplomatic law.[147] States have not proffered specific legal analyses of the question or attempted to wrestle with the longstanding historical practice of spying from within—and on—embassies. Indeed, as recently as 2008 a former CIA General Counsel stated that he could recall no instance in which a receiving state had alleged that a state official caught spying

[143] Vienna Convention on Diplomatic Relations art. 41, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95. As noted supra Part I, the domestic laws of many states criminalize espionage.

[144] Id. at arts. 22, 24.

[145] Jens Glüsing, Laura Poitras, Marcel Rosenbach & Holger Stark, NSA Accessed Mexican President's Email, Der Spiegel (Oct. 20, 2013), http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817-druck.html [https://perma.cc/2XLZ-ZGNB]; George Roberts, Indonesia Summons Australian Ambassador to Jakarta Greg Moriarty over Spying Reports, ABC (Austl.) (Oct. 31, 2013), http://www.abc.net.au/news/2013-11-01/indonesia-australian-embassy-spying-spies-espionage-jakarta/5062626 [https://perma.cc/9CCE-FXCN]; Spiegel Staff, Embassy Espionage: The NSA's Secret Spy Hub in Berlin, Der Spiegel (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html [https://perma.cc/Y9ZP-989H].

[146] Germany Calls in British Ambassador over Spying Reports, Deutsche Welle (Nov. 5, 2013), http://www.dw.com/en/germany-calls-in-british-ambassador-over-spying-reports/a-17204342 [https://perma.cc/2PJ3-GLBH]; Barbara Miller, Berlin Calls in British Ambassador over Spying Reports, ABC (Austl.) (Nov. 6, 2013), http://www.abc.net.au/am/content/2013/s3884802.htm [https://perma.cc/SM9G-6AKH].

[147] Pakistan Lodges Protest Against U.S. Surveillance, Kuwait News Agency (July 3, 2014), http://www.kuna.net.kw/ArticleDetails.aspx?id=2385965&language=en (quoting Pakistan Foreign Office release as stating, "The US Embassy in Islamabad was conveyed today that [reported U.S. surveillance] against Pakistani government departments or other organizations, entities and individuals is not in accord with international law and recognized diplomatic conduct").

was violating the VCDR.[148] In view of this practice, it would be a notable change to interpret the VCDR to prohibit such activities.

Other states have argued that the NSA and GCHQ surveillance programs violate CIL, particularly the rules of sovereignty and territorial integrity.[149] Though widely cited as foundational concepts in international law, the substantive content of these broad principles remains nebulous. One might argue that surveillance interferes indirectly with the internal affairs of another state by detecting communications related to those affairs.[150] One also might argue that the principle of territorial integrity "negates the general permissibility of strategic observation in foreign territory."[151] But the widespread and longstanding practice of (human or electronic) spying by many states during time periods that both precede and post-date the rules' development complicates arguments that these CIL principles were intended to prohibit espionage. Yet it is possible to see how such provisions have *some* relevance to physical intrusions into one state by another state's agents to gather intelligence or undertake other intelligence activities.

Brazilian President Rousseff called the NSA surveillance program a situation of "disrespect to . . . national sovereignty" and argued, "Meddling in such a manner in the lives and affairs of other countries is a breach of international law and, as such, it is an affront to the principles that should otherwise govern relations among countries . . . ."[152] In the wake of reports that the NSA was collecting all phone calls of individuals in the Bahamas, the Bahamian foreign minister stated,

[148] Smith, supra note 10, at 544.

[149] Professor James Crawford has defined sovereignty to mean "the collection of rights held by a state, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people." James Crawford, Brownlie's Principles of Public International Law 448 (8th ed. 2012).

[150] Quincy Wright, Espionage and the Doctrine of Non-Intervention in Internal Affairs, *in* Essays on Espionage and International Law 3, 12–13 (Roland J. Stanger ed., 1962).

[151] John Kish, International Law and Espionage 84 (David Turns ed., 1995).

[152] Maria Lopez Conde, Rousseff Denounces U.S. Espionage, Rio Times (Braz.) (Sept. 24, 2013), http://riotimesonline.com/brazil-news/front-page/rousseff-denounces-u-s-espionage [https://perma.cc/UN4U-J9HQ]. Notwithstanding Brazil's position, reports have emerged that Brazil itself spied on Russian and Iranian diplomats and monitored Iraq's embassy in Brazil in 2003. Brazil Admits Spying on Russian, Iranian Diplomats, Fars News Agency (Nov. 5, 2013), http://english.farsnews.com/newstext.aspx?nn=13920814000871 [https://perma.cc/E6QH-L3XB].

> The Bahamas wishes to underscore the most worthy principles of [the Organization of American States] charter: that international law is the standard of conduct of States, the primacy of sovereignty, maintenance of territorial integrity, [and] freedom from undue external intrusion and influence . . . .
>
> . . . .
>
> . . . [O]ur citizens are questioning what these high ideals of territorial integrity, sovereignty and respect for the rule of law actually mean in practice.[153]

Indonesia claimed that extraterritorial surveillance violates international law and the U.N. Charter (which reflects sovereignty and territorial integrity rules).[154] Given the relatively indeterminate nature of these rules, it is not surprising that states have not provided granular analyses of the ways in which surveillance implicates CIL, at least to date. But the references to international law violations are unmistakable.

Timor-Leste used the ICJ as a forum in which to argue that another state's foreign surveillance violated international sovereignty rules. Timor-Leste alleged that Australia raided the offices of Timor-Leste's Australian attorney and seized documents that implicated Australia in bugging Timor-Leste's internal negotiations about a treaty.[155] Timor-Leste asked the Court to "adjudge and declare . . . [t]hat the seizure by Australia of the documents and data violated (i) the sovereignty of Timor-Leste and (ii) its property and other rights under international

[153] Rashad Rolle, Lawyers to Act in N.S.A. Spy Row, Tribune (Bah.) (June 5, 2014), http://www.tribune242.com/news/2014/jun/05/lawyers-act-ns-spy-row [https://perma.cc/7PB6-E83G].

[154] Press Release, U.N. General Assembly, Third Committee Approves Text Titled "Right to Privacy in the Digital Age," as It Takes Action on 18 Draft Resolutions, U.N. Press Release GA/SHC/4094 (Nov. 26, 2013), http://www.un.org/News/Press/docs/2013/gashc4094.doc.htm [https://perma.cc/7VHN-URPK].

[155] See Ashley Deeks, Can the ICJ Avoid Saying Something on the Merits About Spying in *Timor Leste v. Australia*?, Lawfare (Mar. 12, 2014, 5:00 PM), https://www.lawfareblog.com/can-icj-avoid-saying-something-merits-about-spying-timor-leste-vs-australia [https://perma.cc/24JH-JEA6] [hereinafter Deeks, ICJ on the Merits]; Ashley Deeks, East Timor's Case in the ICJ: Will the Court Decide Whether Spying Violates International Law?, Lawfare (Jan. 22, 2014, 10:00 AM), https://www.lawfareblog.com/east-timors-case-icj-will-court-decide-whether-spying-violates-international-law [https://perma.cc/3DK3-93QK].

law."[156] It also demanded that Australia "not intercept or cause or request the interception of communications between Timor-Leste and its legal advisers whether within or outside Australia or Timor-Leste."[157] Although the parties subsequently asked the ICJ to suspend the case, the ICJ seemed sympathetic to Timor-Leste's claims in granting provisional measures.[158]

Even here, target state perspectives diverge: Some states paint their claims of illegality using a broad brush and loose legal concepts, while others identify particular treaty principles violated by the NSA, GCHQ, the CIA, and other intelligence agencies. This broad lack of consensus about which international rules govern—and how—will have longer-term effects on state practice, because different states will see their own intelligence services as limited by different bodies of international law. This should prompt all states to take more seriously their internal and public analyses about whether and how international law regulates their intelligence agencies.

C. Protecting the Individual

Although the two preceding Sections illustrate that states now face pressure to apply both individually-focused and state-focused rules, the merits of interpreting individually-focused rules robustly are more compelling. At least two theoretical justifications exist for a requirement that intelligence services should have less flexibility in interpreting international law that protects individuals than they should have when interpreting state-focused rules. These justifications are grounded in tacit consent by states and the idea of international law as a form of procedural due process. Both justifications support a rule that requires states to interpret international law obligations more stringently in the face of intelligence activities against non-state actors in contexts in which those actors may suffer readily identifiable harms.

[156] Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.), Provisional Measures Order, 2014 I.C.J. 147, 148 (Mar. 3, 2014), http://www.icj-cij.org/docket/files/156/18078.pdf [https://perma.cc/54ZY-P2KT].

[157] Id. at 149.

[158] Id. at 161.

1. Tacit Consent

The most compelling justification for approaching intelligence differently depending on whether the subject of the intelligence activity is a state actor or a non-state actor is the principle of tacit consent.[159] In the face of the longstanding practice by states of spying on each other and attempting to influence each other's policies with limited legal restraint, one can argue that states and their officials are on notice that they are subject to foreign intelligence activity and, where they have not objected to it, have tacitly consented to being the targets of that activity.[160] In the absence of such objections, acts that otherwise might constitute violations of international law become nonviolations by virtue of tacit consent. When a state's interests are adversely affected by another state's spying or covert influence, that state (at least in theory) has both the incentive and the capacity to unwind its tacit consent and vindicate its interests, including by prosecuting the spies, imposing sanctions, or spying in response. Unless and until states respond consistently in that manner, their tacit consent stands. Of course, as states assert more clearly that they object to certain intelligence activities (as several states have done with foreign electronic surveillance), this weakens a justification based on tacit consent.[161]

A related concept of "fair play" is also at work here. As Professor John Rawls has argued, the acceptance of benefits within a cooperative scheme can generate rights and obligations.[162] Some scholars have argued that spying helps maintain geopolitical stability and avoid unnecessary conflict.[163] We therefore might view spying as providing reciprocal

[159] See A. John Simmons, Tacit Consent and Political Obligation, 5 Phil. & Pub. Aff. 274, 279 (1976) (defining tacit consent as consent expressed "by remaining silent and inactive"); cf. L. Oppenheim, 1 International Law 22 (2d ed. 1912) (discussing tacit consent as a method by which CIL forms).

[160] ECtHR case law on freedom of expression provides a loose parallel. That court has held that public figures must tolerate wider criticism than the average citizen. Lingens v. Austria, App. No. 9815/82, 8 Eur. H.R. Rep. 407, 419 (1986).

[161] In assessing the validity of a tacit consent theory related to foreign surveillance, the complaining state's own surveillance practices would be relevant. A complaining state should not be allowed to withdraw its tacit consent if and so long as it undertakes the same type of activity against other states.

[162] John Rawls, Legal Obligation and the Duty of Fair Play, *in* Law and Philosophy 3, 9–10 (Sidney Hook ed., 1964).

[163] Baker, supra note 24, at 1092; Wright, supra note 101, at 842 (quoting Ambassador Lodge as arguing, "When such a government [i.e., the U.S.S.R.] insists on secrecy it is in effect also insisting on preserving its ability to make surprise attacks on humanity").

benefits, at least in a general sense, including when it is conducted outside the constraints potentially imposed by international law. States that take advantage of this cooperative scheme of spying, particularly by undertaking such spying themselves, should not be permitted to complain about being the victim of spying when committed by others. Even if some or all states do not affirmatively benefit from this cooperative scheme, those engaged in the activity should be estopped from objecting to it.

The posture of actors who are not associated with states looks different. These actors look much more like third-party beneficiaries of rights negotiated among states, and, unlike states, generally are unable to consent or object to foreign intelligence activities.[164] Indeed, in most cases the relevant international rules are explicitly nonreciprocal, imposing obligations on states to the advantage of individuals. The states of nationality of individuals directly affected by intelligence activities often lack incentives to protest that activity, leaving the individuals with little or no means by which to contest their treatment.[165] It is therefore difficult to find the same tacit consent by non-state actors. Further, individuals are not part of the same Rawlsian "cooperative scheme" and generally suffer adverse consequences, rather than accrue benefits, when states avoid potential international law constraints.

Further, when a given international rule is specific and detailed, it is easier to argue that states have affirmatively agreed to apply that international rule to their intelligence activities. There is less room for dispute about what the rule means and less room to argue that states implicitly intended to carve out intelligence activities from coverage. Compare, for instance, the text of the CAT to the language of the U.N. General Assembly's Declaration on Principles of International Law Concerning Friendly Relations, which captures many of the CIL rules discussed

[164] See Ecuador v. United States, Case No. 2012-5, Expert Opinion with Respect to Jurisdiction of Professor W. Michael Reisman, at 4 (Perm. Ct. Arb. Apr. 4, 2012), http://www.italaw.com/sites/default/files/case-documents/ita1061.pdf [https://perma.cc/Q9L3-AGG3] (arguing that "treaties for the benefit of third parties" merit special attention to ensure that "interpretation by one or both of the States-parties not undermine the rights and expectations of the third-party beneficiaries").

[165] One justification for the rule of lenity in the criminal context is that it ensures that individuals are on notice that particular actions are criminal. The rule therefore places the burden on the rule-creator (there, Congress) to be clear. In the intelligence context, a "rule of lenity"-like rule would ensure that those potentially impacted by intelligence activities are protected by rights-protective norms unless and until states clarify that they do not intend those rules to apply to their intelligence communities.

herein.[166] Among other things, the CAT provides, "No State Party shall expel, return (*refouler*) or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture."[167] This language is quite straightforward about what actions are prohibited, even if there is some ambiguity built into the "substantial grounds" analysis. In contrast, the General Assembly Declaration states, "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."[168] On its face, this would prohibit one state's leader from calling another to urge her to alter a state policy—the bread and butter of diplomacy. This language is so overinclusive that it is nearly impossible to discern what activities states genuinely intended to prohibit. As a result, it offers greater flexibility to argue that longstanding intelligence activities may not fall within its coverage.

2. Error Avoidance

A second justification for a more rigorous interpretation of individually-focused international law is to reduce errors ex ante.[169] As discussed above, intelligence activities pose increased risks of harm to non-state actors, whether because those actors are believed to be part of an organized armed group that engages in terrorist acts against a state, or because a state operates surveillance technology that collects information about millions of foreign citizens, or because foreign states steal information from or interfere electronically with private corporations. In the first case, there is a not-insubstantial risk that the government seeking to detain or render those actors may make a mistake about the actors' identity or actions.[170] In the second and third cases, the international commu-

[166] G.A. Res. 2625, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970).

[167] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment art. 3(1), opened for signature Dec. 10, 1984, S. Treaty Doc. No. 100-20, 1465 U.N.T.S. 85.

[168] G.A. Res. 2625, supra note 166.

[169] See James E. Baker, What's International Law Got to Do with It? Transnational Law and the Intelligence Mission, 28 Mich. J. Int'l L. 639, 657 (2007).

[170] See S. Select Comm. on Intelligence, Study of the Central Intelligence Agency's Detention and Interrogation Program, S. Rep. No. 113-228, at xxi (2014) (discussing individuals mistakenly detained or held for improper reasons); Dana Priest, Wrongful Imprisonment:

nity might wish to ensure that a state only collects this kind of information where security imperatives outweigh the costs to privacy.

One way to manage or reduce those risks is by interpreting international law to apply robustly to intelligence activities that may harm individuals. Many (though not all) of the potentially relevant individually-focused international laws serve as procedural checks on the decision making of an intelligence service before it acts against an individual. In this way, international law can provide some of the same protections that procedural due process provides, though in a more modest form. In the U.S. constitutional context, courts have held that procedural due process requires them to evaluate the private interest affected by the official action; the risk of an erroneous deprivation of such interest through the procedures used; and the government's interest, including the burdens that additional process might entail.[171] This formula is concerned with accuracy and aims to reduce the likelihood of error.[172]

Some international law achieves similar goals. IHL, for instance, which requires the state to take certain precautions before targeting and to distinguish between combatants and civilians, is structured to help avoid the erroneous targeting of individuals who play no role in the conflict and thus to reduce unnecessary civilian casualties. IHL and human rights law also provide guidance about the categories of people a state may detain without charge, including in armed conflict, and about the processes to which they are entitled.[173] The right to privacy in the ICCPR is structured to require states to assess whether a particular privacy deprivation would be arbitrary or unlawful, a requirement that forces a state to make certain factual and political assessments before conducting surveillance.[174] Although many of the relevant international

Anatomy of a CIA Mistake, Wash. Post (Dec. 4, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/12/03/AR2005120301476.html [https://perma.cc/8A26-CQGY].

[171] Mathews v. Eldridge, 424 U.S. 319, 335 (1976).

[172] Daphne Barak-Erez & Matthew C. Waxman, Secret Evidence and the Due Process of Terrorist Detentions, 48 Colum. J. Transnat'l L. 3, 49–50 (2009).

[173] See International Covenant on Civil and Political Rights art. 9, opened for signature Dec. 19, 1966, S. Exec. Doc. No. E., 95-2, 999 U.N.T.S. 171; Geneva Convention Relative to the Protection of Prisoners of War arts. 42–43, 78, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 287; Matthew C. Waxman, Detention as Targeting: Standards of Certainty and Detention of Suspected Terrorists, 108 Colum. L. Rev. 1365, 1380 (describing U.S. definitions of who may be detained, drawn by analogy from IHL).

[174] International Covenant on Civil and Political Rights art. 17, opened for signature Dec. 19, 1966, S. Exec. Doc. No. E., 95-2, 999 U.N.T.S. 171.

rules do not impose extensive procedural requirements on states, at the very least they serve as a threshold check on a state's decision making before it takes measures against a particular individual.

Both because states have tacitly consented to a range of intelligence activities against them and because international law can serve as an important way to reduce error and unintended harm to individuals, states should be prepared to interpret more robustly the protections contained in individually-focused international law.

IV. STATE REACTIONS TO THE CONFRONTATION

Part III argued that states face new pressures to apply international law to their intelligence activities, and that there are persuasive normative justifications for states to take seriously the interpretation and application of individually-focused international law. This Part considers how states are responding to that pressure in practice. Understanding state responses is as important as understanding the pressures themselves, if the goal is to assess whether states that are heavily engaged in intelligence activities are beginning to think differently about the relationship between international law and intelligence—that is, are gradually shifting from a realpolitik posture to a more formalist one.

Although it is difficult to locate information about how intelligence services approach international law, it is possible to examine the (apparently) disparate responses by the United States and United Kingdom to these new calls for rigorous application of international law.[175] The United Kingdom has embraced the application of international law—at least human rights law—to its intelligence activities. The United States has been more circumspect about the extent to which it believes its intelligence agencies must comply with international law, but it has publicly identified several bodies of international law with which it complies as a policy matter.

[175] I selected the United Kingdom and United States as representative of these contrasting approaches for two reasons: because they represent similar systems, such that their apparently different approaches to the application of international law to their intelligence services is relevant; and because we know the most about the intelligence practices of these states. For an extended comparison between the two approaches, see Deeks, Intelligence Communities, supra note 11. However, the approaches of these states undoubtedly differ significantly from states that conduct limited intelligence activities and from states that are relatively impervious to pressures from foreign states, citizens, and corporations (such as China and Russia).

A close examination of how these two states are responding to pressures to apply international law to their intelligence activities leads to two surprising conclusions. First, it appears that the United States has analyzed its intelligence activities through the lens of some international laws since at least the 1990s. Second, notwithstanding their disparate public postures, the U.S. and U.K. approaches do not produce dramatically different outcomes. Both states apply certain international rules that protect individuals against physical harm, and neither state seems to interpret the state-focused rules of sovereignty, territorial integrity, and noninterference as constituting significant legal constraints on intelligence activities. This supports Part V's goal of crafting a new relationship between international law and intelligence, based on interpretive principles that take into account the status of the individual being impacted by the intelligence activity, the potential harm that the individual faces, and the clarity of the rule in question.

A. United Kingdom

The United Kingdom explicitly accepts that international law applies to its intelligence activities.[176] For example, in guidance to intelligence and military officials regarding detention, the U.K. government stated, "When we work with countries whose practice raises questions about their compliance with international legal obligations, we ensure that our co-operation accords with our own international and domestic obligations."[177] The United Kingdom's Secret Intelligence Service ("SIS") believes that it must comply with international human rights laws, even when doing so might allow a terrorist act to proceed.[178] And GCHQ's

[176] Other states such as South Africa take this approach as well. South Africa's constitution states that its security services must act in accordance with CIL and treaties binding on South Africa. S. Afr. Const., 1996 arts. 198–99.

[177] Cabinet Office, Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas and on the Passing and Receipt of Intelligence Related to Detainees, July 2010, ¶ 7 (U.K.), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62632/Consolidated_Guidance_November_2011.pdf [https://perma.cc/ND64-E3RF].

[178] Duncan Gardham, Does MI6 Have a License to Kill?, Telegraph (U.K.) (Dec. 3, 2012), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9699795/Does-MI6-have-a-licence-to-kill.html [https://perma.cc/PWM2-Z932] (quoting MI6's chief as stating that the service is prepared to let terrorist activity proceed "in order to stay within British and international law"); see also Government Response to the Intelligence and Security Committee's Report on Rendition, July 2007, ¶ K (U.K.), https://fas.org/irp/world/uk/rendition-resp.pdf [https://perma.cc/E595-Z8WT] (discussing a cancelled 2005 antiterrorism operation).

website states, "GCHQ is subject to rigorous legal oversight, and complies with the European Convention on Human Rights."[179]

These statements suggest that the United Kingdom is committed to broad compliance with international law. However, it is not clear precisely what "international law" (other than human rights law and IHL) the United Kingdom interprets as relevant to intelligence activities. For instance, the United Kingdom may interpret concepts such as territorial integrity and respect for other states' sovereignty as excluding human intelligence collection and various non-forcible covert activities from their remit. At the very least, though, the United Kingdom views international human rights law and IHL as applicable to its intelligence services.

There are at least two reasons why the United Kingdom may have adopted this approach to international law compliance.[180] First, the United Kingdom presumably does not want to suggest that any part of its state actions violates international law. Few states choose to declare openly that they feel no need to comply with international law, but this is especially true in Europe, where international law is deeply integrated into domestic law and the ECtHR looms large over state actions.[181] Second, the United Kingdom is keenly aware that, if they came to light, many of its intelligence actions would face judicial review in U.K. domestic tribunals and the ECtHR. Even if the United Kingdom would prefer to be more oblique about its position on international law compliance, it gains little from failing to claim that its intelligence services comply with U.K. international legal obligations, given that it will have to take that position in litigation.

B. United States

In contrast, the United States is more circumspect publicly about whether its intelligence community uniformly complies with international law. The United States has shaped the relationship between its intelligence community and international law using four tools.[182] First, the United States interprets narrowly the geographic scope of some of the

[179] Gov't Commc'ns Headquarters (U.K.), GCH-Who?, http://www.gchq.gov.uk/pages/GCH-Who.aspx [https://perma.cc/58PD-3KL6].

[180] Deeks, Intelligence Communities, supra note 11, at 10.

[181] See Jed Rubenfeld, Unilateralism and Constitutionalism, 79 N.Y.U. L. Rev. 1971, 1986 (2004).

[182] Deeks, Intelligence Communities, supra note 11, at 12.

human rights treaties that would potentially regulate intelligence activities. For instance, the United States asserts that the ICCPR only applies to activities that take place on U.S. territory and fall within its jurisdiction.[183] This means that there are fewer occasions in which those U.S. human rights obligations conceivably might reach intelligence activity, which generally takes place outside the United States.[184]

Second, in some cases the executive branch is authorized, under U.S. domestic law, to violate international law. For example, the President may violate CIL when he is exercising his constitutional authorities, at least where statutes do not require otherwise.[185] Further, Congress arguably has authorized covert actions that violate CIL and, potentially, treaties. In the National Security Act of 1947,[186] Congress forbade the President from authorizing covert action "that would violate the Constitution or any statute of the United States."[187] The statutory language notably fails to prohibit the President from authorizing activity that may violate CIL or treaties to which the United States is a party.

Third—and perhaps as a result of the first two elements—the United States has issued carefully crafted statements about how international law applies to its intelligence activities. For instance, a May 2013 document delineating U.S. policies in counterterrorism operations, which presumably applies to the U.S. intelligence community, stated, "Capture operations are conducted only against suspects who may lawfully be captured or otherwise taken into custody by the United States and only when the operation can be conducted *in accordance with all applicable law* and consistent with our obligations to other sovereign states."[188]

[183] Concluding Observations on the 4th Periodic Rep. of the U.S., Human Rights Comm., 110th Sess., Mar. 10–28, 2014, ¶ 4, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014); Conclusions & Recommendations of the Comm. Against Torture: U.S., Comm. Against Torture, 36th Sess., May 1–19, 2006, ¶ 20, U.N. Doc. CAT/C/USA/CO/2 (May 18, 2006).

[184] Deeks, Intelligence Communities, supra note 11, at 12.

[185] The Paquete Habana, 175 U.S. 677, 708 (1900).

[186] National Security Act of 1947, Pub. L. No. 80-235, 61 Stat. 496 (codified as amended at 50 U.S.C.A. §§ 3001 et seq. (West 2015)).

[187] 50 U.S.C.A. § 3093(a)(5) (West 2015); see also 50 U.S.C.A. § 3231(a) (West 2015) (clarifying that no legislation enacted on or after December 27, 2000 that implements an international agreement can make unlawful an otherwise lawful U.S. intelligence activity).

[188] Press Release, The White House, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities (May 23, 2013) (emphasis added), https://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism [https://perma.cc/HTM7-QY56].

Likewise, in her nomination hearing to become CIA General Counsel, Caroline Krass stated, "*As a general matter*, and including with respect to the use of force, the United States respects international law *and complies with it to the extent possible* in the execution of covert action activities."[189] These statements avoid articulating what international laws may be applicable to a given set of intelligence activities and whether the United States will act consistently with those laws in a given case.

Fourth, the U.S. government has adopted *policies* that narrow compliance gaps, including by requiring intelligence officials holding detainees anywhere in the world to comply with the treatment rules in Common Article 3 of the Geneva Conventions and the CAT.[190] The government also has indicated that if its intelligence community participates in a transfer of an individual to another state, intelligence officials should ensure that the individual is subjected to proper treatment by the receiving state.[191] The United States does not seem to have claimed publicly that international law simply does not apply to intelligence activity. Instead, the U.S. approach narrows the jurisdictional reach of international rules that might conceivably apply to intelligence activity and tries to ensure that its intelligence activities comply with well-established, rights-focused rules such as those of IHL.[192]

C. Comparing the Reactions

In light of the competing approaches described in the previous two Sections, one might expect that the practice of the two states would look notably different on the ground. There are differences, to be sure, but the practices look similar in several ways. This is due in large part to the fact that the United States employs various compensatory techniques to

[189] S. Select Comm. on Intel., 113th Cong., Additional Prehearing Questions for Ms. Caroline D. Krass upon her Nomination to be the General Counsel of the Central Intelligence Agency 7 (2013) (emphasis added), http://www.intelligence.senate.gov/sites/default/files/hearings/krassprehearing.pdf [https://perma.cc/G9GV-E5YQ]; see also Stephen W. Preston, Gen. Counsel, CIA, Address at Harvard Law School: CIA and the Rule of Law (Apr. 10, 2012), *in* 6 J. Nat'l Sec. L. & Pol'y 1, 7 (2012) (describing "how an Agency program involving the use of lethal force would be structured so as to ensure that it satisfies *applicable* U.S. and international law" (emphasis added)).

[190] Exec. Order No. 13,491, 3 C.F.R. 199, 200 § 3(a), (2009).

[191] Press Release, U.S. Dep't of Justice, Special Task Force on Interrogations and Transfer Policies Issues Its Recommendations to the President (Aug. 24, 2009), http://www.justice.gov/opa/pr/special-task-force-interrogations-and-transfer-policies-issues-its-recommendations-president [https://perma.cc/6J6G-LQQH].

[192] Deeks, Intelligence Communities, supra note 11, at 12.

minimize overt international law violations. In fact, although rarely recognized in the literature, this U.S. effort to apply certain international rules to intelligence activity is not new.

1. Jus ad Bellum Rules

Notwithstanding the claims of some realists that covert uses of force are "extralegal," both the United States and United Kingdom appear attuned to international prohibitions on the resort to force, including when developing and executing intelligence programs.[193] (This supports this Article's use of the more modest "realpolitik" approach, which assumes that most states would not argue that their intelligence communities are unconstrained by Article 2(4) of the U.N. Charter.) Most obviously, the United States has appealed to international law in justifying the use of force in its targeted killing program. The United States asserts that it may target members of al Qaeda and associated forces because it is in an armed conflict with those forces and/or the individuals it is targeting outside of Afghanistan and Iraq pose an imminent threat of an attack on the United States.[194] Further, it has even acknowledged that its use of force in these contexts is limited by sovereignty concerns; it will only use force where the territorial state consents or is unwilling or unable to suppress the threat.[195]

Discussing the bin Laden raid in Pakistan, then-CIA General Counsel Stephen Preston stated,

> By the time the force was launched, the U.S. Government had determined with confidence that there was clear and ample authority for the use of force, including lethal force, under U.S. and international law and that the operation would be conducted in complete accordance

[193] International law regulating the use of force has both individually-focused and state-focused aspects to it. The use of force very often causes physical harm to people, but it also implicates major security issues for states.

[194] Koh, supra note 40; see also Dana Priest, CIA Killed U.S. Citizen in Yemen Missile Strike, Wash. Post (Nov. 8, 2002), https://www.washingtonpost.com/archive/politics/2002/11/08/cia-killed-us-citizen-in-yemen-missile-strike/f802eff3-a58b-4e74-a34f-94715f628680 [https://perma.cc/L6LY-9QAC] ("Officials further contend that Sunday's missile strike was an act of self-defense, which is also permitted under the international laws of war.").

[195] Brennan Harvard Speech, supra note 43.

> with applicable U.S. and international legal restrictions and principles.[196]

In a case in Lebanon, the United States determined before taking action that the CIA's killing of senior Hezbollah official Imad Mughniyah (in cooperation with Israeli intelligence) would be consistent with international law on self-defense.[197] Some scholars have speculated that even the September 17, 2001 Memorandum of Notification authorizing the CIA to engage in various covert actions against al Qaeda may contain a requirement that individuals against whom the CIA uses force pose an "imminent threat" to the United States—a standard that would be consistent with international law regulating national self-defense.[198]

Even before the events of September 11 and the appearance of the new pressures described in Parts II and III supra, the United States appears to have evaluated—at least in some cases—whether intelligence operations were consistent with the *jus ad bellum*. In 1998, President Clinton approved a covert action to kill Osama bin Laden only because lawyers had determined that a "wartime" paradigm applied, such that the killing would be lawful under international (and domestic) law.[199] The United States extended this interest in adhering to the *jus ad bellum* to its dealings with Israel: The United States agreed to share with Israel images from a U.S. satellite, but reportedly refused to give the Israelis any intelligence that could help them plan preemptive strikes on their

[196] Preston, supra note 42; see also Charlie Savage, How 4 Federal Lawyers Paved the Way to Kill Osama bin Laden, N.Y. Times (Oct. 28, 2015), http://www.nytimes.com/2015/10/29/us/politics/obama-legal-authorization-osama-bin-laden-raid.html [https://perma.cc/U26E-VN95] (discussing the Department of Defense General Counsel's analysis of the raid's consistency with international law).

[197] Adam Goldman & Ellen Nakashima, CIA and Mossad Killed Senior Hezbollah Figure in Car Bombing, Wash. Post (Jan. 30, 2015), https://www.washingtonpost.com/world/national-security/cia-and-mossad-killed-senior-hezbollah-figure-in-car-bombing/2015/01/30/ebb88682-968a-11e4-8005-1924ede3e54a_story.html [https://perma.cc/K9N3-YYSN] ("'The decision was we had to have absolute confirmation that it was self-defense,' the official said.").

[198] Benjamin Wittes, Whence Imminence in that Drone Memo? A Puzzle and a Theory, Lawfare (June 24, 2014, 11:19 AM), https://www.lawfareblog.com/whence-imminence-drone-memo-puzzle-and-theory [https://perma.cc/CS2L-627B].

[199] Baker, supra note 169, at 657; see also Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 132 (2004) (noting that administration lawyers concluded that it would not violate the assassination ban to act in self-defense under international law against an imminent threat of attack posed by bin Laden).

neighbors.[200] (Preemptive uses of force are generally seen as unlawful under international law.) This is not to argue that every U.S. covert action complies with the U.N. Charter. Rather, it is to argue that the United States treats the Charter as applicable to its forcible covert actions and attempts to minimize possible violations.

The United Kingdom seems to take a similar—and possibly stronger—approach to the Charter. U.K. intelligence teams are reportedly providing moderate Syrian rebels with logistical assistance to fight ISIS, and U.K. assistance seems carefully crafted to avoid facilitating the overthrow of the Assad regime.[201] The United Kingdom's statements suggest that it would only provide this assistance if it did not violate international law, including Article 2(4) of the U.N. Charter. The United Kingdom also has asserted that for decades it has not assassinated individuals overseas, and that its intelligence services only could do so in an "emergency or crisis which causes danger to the UK or its citizens."[202] This indicates that U.K. intelligence services are not using force abroad in ways that would violate Article 2(4).[203]

[200] Roy Pateman, Residual Uncertainty: Trying to Avoid Intelligence and Policy Mistakes in the Modern World 129 (2003).

[201] Ministry of Defence, UK Troops to Train Moderate Syrian Opposition, U.K. Government (Mar. 26, 2015), https://www.gov.uk/government/news/uk-troops-to-train-moderate-syrian-opposition [https://perma.cc/9T7B-U75K]; Julian Borger & Nick Hopkins, West Training Syrian Rebels in Jordan, Guardian (U.K.) (Mar. 8, 2013), http://www.theguardian.com/world/2013/mar/08/west-training-syrian-rebels-jordan [https://perma.cc/2JQ8-9FDR] (noting that the "Brits and the French . . . are much more forward-leaning than others" in interpreting what assistance is permissible). On the U.S. approach, see Ashley Deeks, Arming Syrian Rebels: Lethal Assistance and International Law, Lawfare (May 1, 2013, 10:00 AM), https://www.lawfareblog.com/arming-syrian-rebels-lethal-assistance-and-international-law [https://perma.cc/AR6U-6RHY] (speculating that Article 2(4) was inserting caution into U.S. decision making about such arming) and Adam Entous, Legal Fears Slowed Aid to Syrian Rebels, Wall St. J. (July 14, 2013), http://www.wsj.com/articles/SB10001424127887323848804578606100558048708 [https://perma.cc/S7NM-QXMD].

[202] Duncan Gardham, MI6 Told Agent They Could Not Kill al-Qaeda Leader, Telegraph (U.K.) (Dec. 3, 2012), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9699783/MI6-told-agent-they-could-not-kill-al-Qaeda-leader.html [https://perma.cc/Q6UG-BNBN] (quoting a security source).

[203] There is an ongoing investigation, however, about whether MI6 participated in a rendition of a Libyan to the custody of Libyan intelligence services.

2. Jus in Bello Rules

Jus in bello rules—also known as IHL—apply to a state's conduct when it is engaged in an armed conflict.[204] The United States has repeatedly applied IHL to targeting decisions by intelligence officials. In 1998, before the United States conducted strikes against an al Qaeda training camp in Afghanistan and a pharmaceutical factory in Sudan, CIA lawyer John Rizzo was told to draft a Memorandum of Notification ("MON") authorizing members of Afghan tribes to try to capture bin Laden, but Rizzo was also told to authorize the tribals to use force only in "self-defense." (It is not clear if this refers to individual self-defense or national self-defense.) Rizzo then was told to modify the draft MON to allow the tribals to kill bin Laden only if capture was "not feasible."[205] These limitations may flow from interpretations of IHL requirements or (possibly) widely accepted human rights standards (which allow state actors in peacetime to use force only in self-defense, as a last resort, and in response to an imminent or actual threat). Also in 1998, when President Clinton authorized U.S. intelligence officials and their proxies to attack bin Laden,

> he did so in a manner that was consistent with the law of armed conflict as it was understood to be implemented in U.S. criminal law at the time. Thus, the President's authorization included instruction that if bin Laden or his lieutenants surrendered or were captured, they were to be treated humanely, that is, not executed or tortured (acts prohibited by international law as implemented in U.S. criminal law).[206]

Even in the wake of the September 11 attacks, at a time in which many outsiders perceived the Bush Administration and the CIA as ignoring international law, the CIA appeared attuned to international law standards.[207] In 2007, the U.S. Department of Justice ("DOJ") produced a legal opinion examining whether the CIA's interrogation program was consistent with Common Article 3 of the Geneva Conventions. The CIA

[204] *Jus in bello* rules presumably also attach to isolated extraterritorial uses of force, even if no victim ever responds forcibly to that attack and no armed conflict results.

[205] John Rizzo, Company Man: Thirty Years of Controversy and Crisis at the CIA 161–62 (2014).

[206] Baker, supra note 169, at 657; see also Steve Coll, Ghost Wars: The Secret History of the CIA, Afghanistan, and bin Laden, From the Soviet Invasion to September 10, 2001, at 409 (2004) (discussing how international principles of self-defense shaped the Pentagon's attempts to capture bin Laden).

[207] Deeks, Intelligence Communities, supra note 11, at 13–14.

asked DOJ for the opinion because the CIA "intend[ed] for the program to comply with Common Article 3."[208]

In 2009, President Obama issued an executive order requiring that all U.S. officials (including intelligence officers) treat detainees humanely and consistent with Common Article 3 of the Geneva Conventions and the CAT.[209] The United States has made clear that contemporary CIA targeted killing operations comply with IHL, including the principles of distinction and proportionality. Then-CIA General Counsel Stephen Preston stated:

> [When using lethal force abroad], the Agency would implement its authorities in a manner consistent with the four basic principles in the law of armed conflict governing the use of force: Necessity, Distinction, Proportionality, and Humanity. Great care would be taken in the planning and execution of actions to satisfy these four principles and, in the process, to minimize civilian casualties.[210]

U.K. intelligence services are required to comply with IHL as well. In January 2002, SIS and the Security Service issued guidance to their employees in Afghanistan, stating that all detainees were entitled to some level of protection under the Geneva Conventions and the Additional Protocols.[211] A report by the U.K. Parliament's Intelligence and Security Committee on the handling of detainees in Afghanistan, Iraq, and Guantanamo Bay makes clear that U.K. intelligence officials considered themselves bound by the Geneva Conventions in their interactions with detainees in those conflicts.[212]

---

[208] Memorandum from the Office of Legal Counsel, U.S. Dep't of Justice, for John Rizzo, Acting Gen. Counsel, CIA, 48 n.34 (July 20, 2007), http://www.justice.gov/sites/default/files/olc/legacy/2009/08/24/memo-warcrimesact.pdf [https://perma.cc/ER3Z-F8TH].

[209] Exec. Order No. 13,491, 3 C.F.R. 199, 199 (2009) (listing as one of the purposes "to ensure compliance with the treaty obligations of the United States").

[210] Preston, supra note 42.

[211] U.K. Detainee Inquiry, supra note 39, at 11. Further guidance was provided in August 2004. Id. at 16; see also id. at ¶ 5.15 (stating that the SIS Head Office believed that detainees in U.K. control would be subject to Geneva Conventions).

[212] Intelligence and Security Committee, The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq, 2005, Cm. 6469, ¶¶ 47, 51 (U.K.) [hereinafter U.K. Detainee Handling Report].

3. Human Rights Treaties

During the Bush Administration, the United States resisted the application of the CAT to its activities overseas, regardless of which agency undertook them.[213] Notwithstanding this approach, and even though DOJ determined that the CAT did not apply jurisdictionally to CIA interrogations abroad, the CIA nevertheless asked DOJ to analyze whether the CIA's interrogations would violate the substantive standards in CAT Article 16 if that provision did apply.[214] In 2009, President Obama issued an executive order mandating that individuals detained by U.S. officers, employees, or agents be treated humanely, consistent with, among other laws, the CAT.[215] The executive order was a *policy* determination, but clearly required intelligence officials operating overseas to comply with Common Article 3 and the CAT. In 2014, the United States affirmed that its *legal* position was that torture and cruel, inhuman, and degrading treatment are prohibited by international law "at all times, and in all places."[216] The U.S. delegation defending the U.S. periodic report to the Committee Against Torture stated that U.S. obligations to *prevent* acts of torture and cruel, inhuman, or degrading treatment, take offenders into custody, and ensure the rights of victims to complain and have their cases examined by competent authorities "apply in places outside the United States that the U.S. government controls as a governmental authority."[217] In its report to the committee it also discussed CIA secret de-

[213] See Memorandum from the Office of Legal Counsel, U.S. Dep't of Justice, for William J. Haynes, II, Gen. Counsel, Dep't of Def. 1 (Mar. 13, 2002), http://nsarchive.gwu.edu/torturingdemocracy/documents/20020313.pdf [https://perma.cc/CS2F-S9ZN] (stating that the CAT does not apply extraterritorially).

[214] Memorandum from the Office of Legal Counsel, U.S. Dep't of Justice, for John A. Rizzo, Sr. Deputy Gen. Counsel, CIA 2 (May 30, 2005), http://www.justice.gov/sites/default/files/olc/legacy/2013/10/21/memo-bradbury2005.pdf [https://perma.cc/Y8AA-P4QV]. Of course, many saw DOJ's substantive interpretations of the CAT and torture as deeply flawed; the Office of Legal Counsel later withdrew some of these memos. Letter from Daniel Levin, Acting Assistant Attorney Gen., to Hon. William J. Haynes, II, Gen. Counsel, Dep't of Def. (Feb. 4, 2005) http://www.justice.gov/sites/default/files/olc/legacy/2009/12/30/aclu-ii-020405.pdf [https://perma.cc/FF4H-NF4Y].

[215] Exec. Order No. 13,491, 3 C.F.R. 199, 200 § 3(a), (2009).

[216] Sarah Cleveland, The United States and the Torture Convention, Part I: Extraterritoriality, Just Security (Nov. 14, 2014, 11:18 AM), http://justsecurity.org/17435/united-states-torture-convention-part-i-extraterritoriality [https://perma.cc/9XCZ-3MW6].

[217] Id. (quoting Bernadette Meehan, Spokesperson, Nat'l Sec. Counsel, Statement on the U.S. Presentation to the Committee Against Torture (Nov. 12, 2014), https://www.whitehouse.gov/the-press-office/2014/11/12/statement-nsc-spokesperson-bernadette-meehan-us-

tention sites and alleged torture by the CIA, suggesting that it views the CAT as extending to the CIA.[218]

(The United States has not made a comparable change in how it interprets the jurisdictional reach of the ICCPR.[219] As a result, the United States does not appear to treat the ICCPR as regulating its intelligence activities overseas. Thus, the ICCPR's right to privacy would not restrict U.S. electronic surveillance conducted overseas against foreign nationals.)

In addition to affecting its own behavior, the United States sometimes decides to limit or alter its intelligence cooperation with other states in light of human rights violations by the latter. When asked whether the United States takes the human rights records of foreign security services into account before collaborating with them, a spokesman for the Office of the Director of National Intelligence stated, "Yes. . . . [A]s a general principle, human rights considerations inform our decisions on intelligence sharing with foreign governments."[220]

The United Kingdom has stated clearly that its intelligence services must and do comply with international human rights law, including the ICCPR, the CAT, and the ECHR. Under the CAT, the United Kingdom cannot knowingly assist in sending a person to another country (including by rendition) where there is a real risk that he may be tortured.[221] Pursuant to the ECHR and the CAT, the United Kingdom may not treat detainees in an inhuman or degrading manner (which the ECtHR has interpreted to mean that "[t]he acts complained of [are] such as to arouse in the applicant feelings of fear, anguish and inferiority capable of humiliating and debasing him").[222] For the United Kingdom, this includes

presentation-committee-a, [https://perma.cc/Z5U8-YUZP]) (listing as examples Guantanamo Bay and U.S.-registered ships and aircraft)).

[218] See U.S. Dep't of State, Periodic Report of the United States of America to the United Nations Committee Against Torture ¶¶ 23–26 (2013) (CIA secret detention facilities); id. ¶¶ 107–11 (alleged torture by CIA).

[219] Ashley Deeks, Does the ICCPR Establish an Extraterritorial Right to Privacy?, Lawfare (Nov. 14, 2013, 12:00 PM), http://www.lawfareblog.com/2013/11/does-the-iccpr-establish-an-extraterritorial-right-to-privacy (discussing U.S. interpretation of ICCPR's jurisdictional provision).

[220] Glenn Greenwald & Murtaza Hussein, The NSA's New Partner in Spying: Saudi Arabia's Brutal State Police, Intercept (July 25, 2014), https://theintercept.com/2014/07/25/nsas-new-partner-spying-saudi-arabias-brutal-state-police [https://perma.cc/H94C-58X6].

[221] ISC Rendition Report, supra note 71, ¶ 13.

[222] Id. ¶ 15.

the use of hooding and "wall-standing."[223] The United Kingdom must also affirmatively act to forestall any act of torture it can foresee.[224] Finally, the United Kingdom may not participate in renditions to bring individuals to U.K. territory.[225] One ISC report asserts, "UK Agencies have always been mindful of human rights issues, particularly when engaging with countries that do not pay the same attention to civil liberties and human rights as the UK."[226]

Even GCHQ's surveillance must comply with international human rights law. For the United Kingdom, which is bound by the ECHR, that means its surveillance must be necessary and proportionate. U.K. parliamentarian Hazel Blears (who is a member of the ISC) stated, "We have seen the datasets [of GCHQ] and concluded they are necessary and proportionate. All of these issues in order to be lawful have to be necessary and proportionate and not indiscriminate."[227] The ISC report on GCHQ surveillance states, "The lack of clarity in existing laws and the lack of transparent policies beneath them has not only fuelled suspicions and allegations but has also meant the agencies could be open to challenge for failing to meet their human rights obligations."[228] This standard of transparency derives from ECtHR case law, which has interpreted ECHR Article 8 to require that interference with a person's right to privacy be "in accordance with the law" and that the legal rules regulating the state's interference provide citizens with an indication of the conditions under which the authorities may interfere with the protected rights.[229]

In short, the United Kingdom and United States have different human rights treaty obligations and interpret differently some of the treaty obligations they share. Importantly, however, both states apply certain human rights laws to their intelligence services.

[223] U.K. Detainee Handling Report, supra note 212, ¶ 26.
[224] ISC Rendition Report, supra note 71, ¶ 16.
[225] Id. ¶ 11.
[226] Id. ¶ 31.
[227] Patrick Wintour & Rowena Mason, UK Surveillance Laws Need Total Overhaul, Says Landmark Report, Guardian (U.K.) (Mar. 12, 2015), http://www.theguardian.com/us-news/2015/mar/12/uk-surveillance-laws-need-total-overhaul-says-landmark-report-edward-snowden [https://perma.cc/G7NM-R4FR].
[228] Id.
[229] Malone v. United Kingdom, 7 Eur. Ct. H.R. 14, 26–28 (1984).

4. CIL Rules

The U.S. and U.K. approaches to CIL rules stand in notable contrast to their approaches to the individually-focused rules discussed above. Neither state appears to treat the CIL rules of sovereignty and territorial integrity as imposing limits on their extraterritorial intelligence activities. It is clear that the CIA and MI6, like many other intelligence services, undertake intrusive operations abroad without the consent of the states in which they are operating.[230] Although it is possible to imagine certain overseas operations that do not implicate the sovereignty or territorial integrity of another state (such as those conducted on the high seas or from satellites), most operations surely do. Nor are these states surprised when other states conduct espionage against them: Current and former U.S. officials indicated that the hack of massive amounts of data about U.S. employees (allegedly by the Chinese) was to be expected, and was the kind of thing that the NSA would undertake if it could.[231]

The fact that the United Kingdom and United States do not seem to apply these state-directed CIL rules to their intelligence activities may mean one of three things. First, those states might believe that those rules simply do not apply to intelligence activities in the first place. The practice of spying abroad is widespread and longstanding, and many states in different regions of the world have engaged in spying during periods that both precede and post-date the U.N. Charter. In the U.S. and U.K. view, this may undercut arguments that these customary principles were intended to prohibit espionage at the time they developed or should be deemed to do so today.[232] Second, these states might believe that those rules technically apply to intelligence activities but must be disre-

[230] Reisman & Baker, supra note 5, at 123–29 (United States); Wintour & Mason, supra note 227 (United Kingdom).

[231] Ellen Nakashima, U.S. Decides Against Publicly Blaming Chinese for Data Hack, Wash. Post (July 21, 2015), https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html [https://perma.cc/MP5C-LB2Q] ("Director of National Intelligence James R. Clapper Jr. and others have even expressed grudging admiration for the OPM hack, saying U.S. spy agencies would do the same against other governments."). In contrast, the United States plans to impose sanctions on China for its cyberespionage against private actors. Ellen Nakashima, U.S. Developing Sanctions Against China over Cyberthefts, Wash. Post (Aug. 30, 2015), https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html [https://perma.cc/PCN3-R8ZX] [hereinafter Nakashima, U.S. Sanctions].

[232] Deeks, International Legal Framework, supra note 11, at 301–03.

garded as a policy matter because of the very nature of most intelligence activity.[233] Third, these states may privately concede that it is possible to interpret these rules as applying to certain intelligence activities but place significant weight on the fact that states rarely levy allegations of international law violations against each other in the intelligence context. That is, the states may believe that these rules, as they might apply to some intelligence activities, have fallen into desuetude.[234] It is difficult to know which of these versions is most accurate. At least some states recently have revived the second approach: that the rules apply, even if states mostly disregard them. However, one need not resolve this knotty debate if one accepts the interpretive sliding scale approach in Part V, because that approach allows states a significant amount of flexibility in determining whether and how sovereignty-related rules apply to the conduct of intelligence activity.

***

In practice, then, the United States and United Kingdom have chosen to apply similar categories of international law to their intelligence activities. The United States and United Kingdom apply human rights and IHL rules—those international rules that directly affect individuals.[235] They do not seem to be interpreting CIL rules related to sovereignty and territorial integrity as constraining their intelligence activities.[236] It is unclear how these states approach operations that fall somewhere between

[233] In support of this, members of the U.N. Security Council in 1960, while considering the U-2 shootdown incident, all agreed that the U-2 flight violated Soviet territory, but China and Italy "noted that in view of the flights of man-made satellites and their potentialities for observation, air sovereignty had become more or less a myth." Wright, supra note 101, at 842.

[234] See generally Michael J. Glennon, How International Rules Die, 93 Geo. L.J. 939 (2005) (arguing that rules that states violate excessively are replaced by rules permitting freedom of action).

[235] Nat'l Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities § 4.2.1, at 194 (William A. Owens et al. eds., 2009) [hereinafter NRC Report] ("According to Jeff Smith, former general counsel to the Central Intelligence Agency (1995-1996), traditional U.S. interpretations of the laws of armed conflict . . . require covert action, whether or not it involves violent activities, to be conducted consistent with [the law of armed conflict's] requirements.").

[236] Thomas J. Jackamo, III, Note, From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention, 32 Va. J. Int'l L. 929, 967–68 (1992) ("[T]he line separating improper, illegal intervention from legitimate interference is quite difficult to draw.").

these two extremes—acts that, for example, affect more tangible interests of a "victim" state (bribery of foreign officials, covert involvement in foreign elections) and may implicate other bodies of international law.

This conclusion reveals that the publicly stated approaches of both the United States and United Kingdom are unsatisfying. The U.K. approach is flawed because it overclaims. The United Kingdom's assertions leave the impression that its intelligence community complies with all potentially relevant international law—that it already is a formalist. But some would argue that territorial integrity and sovereignty are "relevant" rules of international law, and the United Kingdom surely does not strictly heed them. The far more realpolitik U.S. approach is flawed because it creates a significant "zone of exclusion" for international law constraints. Where it has filled in that zone, it has done so as a matter of policy, not law. A preferable way forward, taken up in Part V, is to draw from the best parts of each state's approach. Intelligence communities should follow the U.K. approach in rigorously applying international rules that implicate the treatment of non-state actors, and follow the U.S. approach in allowing intelligence communities to interpret flexibly the sovereignty-related rules at the other end of the spectrum.

D. Explaining the Results

The previous Sections illustrated, unexpectedly, that states such as the United Kingdom and United States *are* applying certain rules of international law to their intelligence operations. But they are not applying all rules equally. Why are they applying more robustly those aspects of international law that directly implicate the treatment of individuals and not applying (or applying very flexibly) rules of international law that implicate state interests? A confluence of several factors likely explains this outcome, though these factors are not identical to the normative justifications discussed supra Section III.C.

First, it is increasingly hard to make a legal argument that the individually-focused rules do not apply to intelligence operations.[237] This is true in part because human rights law and IHL contain rules that are clearer and more determinate than the less detailed CIL rules, at least in terms of the core behavior they intend to regulate. Especially where the CIA and the Department of Defense ("DOD") are working together, and

[237] Reisman & Baker, supra note 5, at 77 ("Covert measures must meet the requirements of the law of armed conflict such as proportionality and discrimination.").

where these rules clearly apply to the DOD, it is difficult to argue as an international law matter that these legal provisions apply to one agency's military operation and not the other's.

Second, it is politically unpalatable to say that IHL and rules prohibiting torture and cruel, inhuman, and degrading treatment do not apply to intelligence activities. Put another way, since the intelligence activities to which these rules would apply (including interrogation, detention, and rendition) are unpopular internationally, the United States may be attempting to mollify critics by assuring them that the U.S. intelligence community at least complies with basic rights-protective rules.

Third, external pressures on states to conform their intelligence activities to international law are greater when it comes to individually-focused rules than to state-focused rules. Human rights groups put pressure on states to comply with human rights and IHL rules but have far less interest in ensuring compliance with state-state rules. Virtually all of the litigation discussed in Part III relates to enforcement of individually-focused rules.[238] (This can only be part of the story, however, since the United States and United Kingdom applied some individually-focused rules before these recent pressures emerged.) States themselves—even when victims of another state's spying—are often hamstrung when trying to critique intelligence activities as violating CIL because they themselves are engaged in those activities.

Fourth, U.S. and U.K. domestic laws criminalize torture and war crimes committed by their nationals abroad, but do not criminalize the violation of another state's sovereignty.[239] States often incorporate these individually-focused prohibitions because the relevant treaties require states parties to enact implementing legislation. As a result, it would be much more costly for the United States or United Kingdom to authorize an intelligence official to engage in torture than it would be to authorize him to sneak across another state's border to recruit foreign agents or steal military secrets. Further, to the extent that state actors are more inclined to comply with domestic law than with international law,[240] that

[238] See supra Subsection III.A.2. Timor-Leste's ICJ case is the sole exception. See supra notes 155–58.

[239] 18 U.S.C. §§ 2340A, 2441 (2012). The United Kingdom has comparable provisions in its domestic laws. See International Criminal Court Act 2001, c. 17, §§ 50–57; Geneva Conventions Act 1957, 5 & 6 Eliz. 2, c. 52, §§ 1–2.

[240] Jack L. Goldsmith & Eric A. Posner, A Theory of Customary International Law, 66 U. Chi. L. Rev. 1113, 1175 (1999) (indicating that, in well-ordered societies, domestic law is more reliably enforced than international law).

would help explain why states might be more inclined to heed individually-focused rules that they have incorporated into their domestic laws.

Finally, spying states surrender less flexibility of action in admitting the application of individually-focused rules than they would if they acknowledged that sovereignty rules applied to their activities. Interpreting CIL rules as strictly applying to their activities would bring to a halt most spying and covert action, as so many of those activities violate other states' territorial integrity and sovereignty, broadly interpreted.

For these reasons, the United States and United Kingdom (and possibly other states) have taken variable approaches to different types of international law. As discussed in Part III, there also are theoretical justifications for making this distinction. Part V takes up the challenge suggested by this bifurcated approach. It develops a set of concrete factors that states should use to assess how a particular set of international legal rules should constrain a given intelligence activity.

V. A SLIDING SCALE FOR INTERNATIONAL LAW

Underlying changes in the intelligence landscape have laid the groundwork for an altered international law/intelligence relationship. Diverse pressures, particularly from those focused on protecting individual non-state actor targets of intelligence activities, are challenging the longstanding realpolitik approach to intelligence. And several Western states themselves have structured their intelligence services to be responsive to individually-focused international laws such as those regulating armed conflict and protecting certain human rights.

Yet few guideposts exist on how to proceed. Past efforts to situate intelligence activities within an international law framework have proven unsatisfying. The analyses generally have taken one of the two approaches set forth in Part I. That is, some take a starkly realist approach to intelligence and assess that international law constraints are not (and will never be) relevant to the conduct of intelligence activities.[241] A second, strongly prescriptive and formalist approach insists that all of a state's international law obligations apply in their entirety to intelligence activities, just as they apply to other actions by that state.[242]

A handful of scholars have taken a more nuanced approach to the question, recognizing that international rules constrain intelligence ac-

[241] See supra text accompanying notes 10–28.
[242] See supra text accompanying notes 31–32.

tors in some (but not all) locations in some (but not all) situations.[243] Michael Reisman and James Baker have proffered a detailed way to analyze whether particular types of covert action violate international law. They argue for a deeply contextual and subjective approach that gives almost unfettered discretion to the state analyzing the issue.[244] Reisman and Baker conclude that

> the legality of any proactive covert operation should be tested by whether it promotes the basic policy objectives of the Charter, for example, self-determination; whether it adds to or detracts from minimum world order; whether it is consistent with contingencies authorizing the overt use of force; and whether covert coercion was implemented only after plausibly less coercive measures were tried.[245]

While their recognition that there is not a one-size-fits-all approach to intelligence in international law is laudable, an analysis that requires a state to assess whether an action advances "minimum world order" and "promotes the basic policy objectives of the Charter" offers insufficient guidance to states making difficult decisions in the real world. This Part proposes and details a sliding scale approach that would require states to consider specific factors to assess how rigorously they should interpret international rules that arguably apply to their intelligence activities. The goal is to provide more structured guidance to states that are contemplating how to conduct different categories of intelligence activities, while retaining an adequate level of state flexibility.

---

[243] Reisman & Baker, supra note 5, at 27; Forcese, supra note 8, at 209 (stating that international law on spying is a "checkerboard of principles, constraining some practices in some places and in relation to some actors, but not in other cases in relation to other actors").

[244] Reisman & Baker, supra note 5, at 77. A former head of the United Kingdom's GCHQ has proposed drawing from Just War principles to regulate intelligence activity on the Internet. See Omand, supra note 117, at 16–17. This approach, like Reisman and Baker's, seems exceedingly flexible and difficult for states to apply consistently.

[245] Reisman & Baker, supra note 5, at 77; see also id. at 25 ("Accordingly, we submit that lawfulness is, and should continue to be, determined by contextual analysis: who is using a particular strategy, in what context, for what purpose, and in conformity with what international norm, with what authority, decided by what procedures, where and how, with what commensurance to the precipitating event, with what degree of discrimination in targeting, and with what effects as a sanction and what peripheral effects on general political, legal, and economic processes.").

A. Parameters of an Interpretive Sliding Scale

This Part proposes a sliding scale approach that anticipates and accepts *gradations of interpretation* of international law, rather than an unsatisfying and self-defeating insistence on all or nothing. This proposal, which recalls the rule of lenity in criminal law,[246] would require states to interpret strictly both the applicability and substance of their obligations vis-à-vis individually-focused rights (treatment protections, data privacy) and vis-à-vis non-state actors, but would tolerate a more flexible interpretation of the applicability and content of state-to-state rules such as nonintervention, territorial integrity, and sovereignty. A flexible interpretation of a rule could include a determination, based on credible evidence, that states did not intend that rule to cover a given situation in its entirely. It also could mean that a state deems a rule generally applicable to intelligence operations but not applicable to a specific factual scenario. This preserves for states a less-constrained zone of action for "traditional" intelligence activity such as espionage against foreign government officials, but places greater constraints on intelligence activities that will impact private citizens.

A well-established principle in regional international law provides a structural precedent for this type of interpretive sliding scale. The ECtHR has firmly established in its jurisprudence an interpretive tool that it calls the "margin of appreciation." The doctrine reflects that the ECtHR will afford states parties to the ECHR a certain amount of flexibility in interpreting and implementing some ECHR rights, and thus allow them to take into account their states' particular history, culture, and circumstances.[247] "The margin of appreciation . . . enables the Court to balance the sovereignty of Contracting Parties with their obligations under the Convention."[248] One scholar described this as "breathing space" for

[246] See Orin S. Kerr, A Rule of Lenity for National Security Surveillance Law, 100 Va. L. Rev. 1513, 1514–15 (2014) (arguing for a rule of lenity-type approach to electronic surveillance statutes). Scholars also have argued that the rule of lenity applies in international criminal law. Allison Marston Danner & Jenny S. Martinez, Guilty Associations: Joint Criminal Enterprise, Command Responsibility, and the Development of International Criminal Law, 93 Calif. L. Rev. 75, 84 (2005).

[247] Yutaka Arai, The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR 2–3 (2001).

[248] R. St. J. Macdonald, The Margin of Appreciation, *in* The European System for the Protection of Human Rights 83, 123 (R. St. J. Macdonald et al. eds., 1993).

Member States.[249] The concept of a margin of appreciation has spread, and now appears in other human rights bodies and in other substantive areas of E.U. law.[250]

In general, the ECtHR has granted states a greater margin of appreciation (that is, has upheld a state's domestic law against challenge) (1) where there is less consensus among Member States about the importance of the right or how to protect the right; and (2) where the case does not implicate a right that the ECtHR itself views as fundamental.[251] The Court stated,

> Where . . . there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider. This is particularly so where the case raises complex issues and choices of social strategy . . . .[252]

In evaluating whether a particular restriction on a right is "necessary," the Court will grant a state more flexibility when these elements are present.[253] The Court also has employed a *narrower* margin of appreciation where the rights at issue are set forth in detail in the Convention itself—as with the right to a fair trial.[254]

Although not technically applicable to the interpretation of the vast majority of treaties and CIL that potentially confront intelligence communities, the margin of appreciation offers support for a sliding scale approach that grants states greater room to maneuver in interpreting international obligations that do not implicate fundamental human rights and that have not garnered widespread consensus about their meaning. As a result, states should be entitled to a greater margin in interpreting

[249] Howard Charles Yourow, The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence, 3 Conn. J. Int'l L. 111, 118 (1987).

[250] Arai, supra note 247, at 4; Yuval Shany, Toward a General Margin of Appreciation Doctrine in International Law?, 16 Eur. J. Int'l L. 907, 907–08 (2005).

[251] Jeffrey A. Brauch, The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law, 11 Colum. J. Eur. L. 113, 126–27 (2005).

[252] Dickson v. United Kingdom, 2007-V Eur. Ct. H.R. 99, 128.

[253] Eleni Frantziou, The Margin of Appreciation Doctrine in European Human Rights Law, Univ. Coll. London Policy Briefing (Oct. 2014), https://www.ucl.ac.uk/public-policy/public-policy-briefings/European_human_rights_law [https://perma.cc/98LB-ZDRB].

[254] Jeroen Schokkenbroek, The Basis, Nature, and Application of the Margin-of-Appreciation Doctrine in the Case-Law of the European Court of Human Rights, 19 Hum. Rts. L.J. 30, 34 (1998).

state-focused rights and a narrower margin in interpreting individually-focused rights.

B. Operationalizing the Scale

This Section demonstrates how states might operationalize this approach. It sets forth key factors that states should consider when evaluating where on the scale a particular intelligence activity falls, and then tests the approach by applying those factors to some common intelligence activities.

1. Factors

In view of the normative justifications for paying close attention to the target of the intelligence activity, the following factors focus primarily on the identity of and impact on the individual implicated in a state's foreign intelligence activity. This focus on the individual stands in contrast to the Reisman and Baker approach. Reisman and Baker take a broad, multifactor approach that is heavily weighted to the "rightness" of the cause and that admits to serious U.S. exceptionalism. This Part's approach does not favor any particular state;[255] rather, it attempts to provide more objective factors against which states should measure their intelligence actions. There will remain cases that fall in the middle of the continuum, where the factors cut different directions and offer no clear answer about the extent to which states should interpret international law to constrain their actions. But more than any other test proposed to date, this approach provides objective guidelines to states as they structure their intelligence activities with an eye toward international law.

a. Risk of error and quantum of harm. A primary consideration that states should take into account is the risk of error that may result from pursuing the wrong individual, from pursuing the correct individual in a way that implicates innocent actors, or from technological malfunctions. The higher the risk of error, the more important it is to stringently apply potentially relevant international laws as a form of due process. In addi-

[255] To be sure, the approach generally favors states with robust state-to-state spying capabilities. Even though it would permit all states to interpret more flexibly norms such as territorial integrity, that interpretive approach inherently favors states in a position to employ it—that is, states actively engaged in intelligence activities against other states. On the other hand, the proposed approach limits the flexibility of these same states when their activities implicate individual non-state actors.

tion, states should consider the amount of harm that will flow from the intelligence operation. The easiest cases are those where the harm will be physical—as with detention or rendition. Harder cases include those where a person is transferred to another state to face interrogation or criminal prosecution, or where an intelligence service recruits a non-state actor to perform an intelligence operation (such as stealing weapons plans from a military contractor), or where the harm is significant but purely economic. Where the action is likely to have a direct impact on an individual's freedom or treatment, a state should interpret international law and its ambiguities in favor of the individual. The more serious and direct the harm that may result, the less leeway a state should have in interpreting provisions of potentially applicable treaties or CIL.[256]

In some cases, an intelligence activity will affect the entire population of a state, most of whom are non-state actors, though it will not produce physical harms. Consider covert actions in which one state's intelligence officers bribe a foreign official to pursue a policy favorable to the bribing state, or introduce counterfeit foreign currency into another state's financial system to destabilize it, or tamper with elections to ensure a victory by the tampering state's preferred candidate. These are difficult middle cases, in that they produce conceptual harms to many non-state actors in another state but few tangible, direct harms. On balance, a state might conclude that the harms likely to result are too diffuse and low-level, and the potential prohibitions insufficiently on point, that it is reasonable to interpret international law not to apply to these types of operations. But other factors discussed in this section may point in a different direction.

b. Nature of the target. Another key factor is the identity of the individual at whom the intelligence activity is directed. Is the intelligence activity directed at another state or at a non-state actor? Is the person affected a government official (or a friend or relative thereof), or someone who has no associations with a state? States should be entitled to greater freedom to interpret international constraints when directing their operations against those with a close relationship to the government. The state/non-state distinction serves as an important proxy for whether

[256] See Kerr, supra note 246, at 1514 (arguing that when a government's power under existing law is ambiguous, the actor interpreting the law should adopt a construction that favors the individual rather than the government).

someone has assumed the risk that he may be the target of foreign intelligence activities. It is fair to assume that individuals who choose to work for a government (or for an international organization such as the United Nations) do so with an understanding that their activities and conversations will be of greater interest to foreign powers than the communications of their fellow citizens in the private sector. Government actors often have access to foreign policy decisions, classified information, and negotiation strategies that private citizens do not. Thus, a state conducting electronic surveillance of a foreign government official's cell phone should be entitled to greater flexibility in interpreting the right to privacy contained in the ICCPR. This might mean that a state could interpret more narrowly what an "arbitrary" deprivation of the right to privacy means in ICCPR Article 17, or more readily determine that such interception is necessary and proportional. In contrast, a state collecting the content of millions of calls of individuals not suspected of wrongdoing would need to interpret the requirements of the ICCPR more liberally in favor of the affected individuals.[257]

It often will be possible for intelligence services to identify affected individuals as clearly falling on one side or the other of the official/non-official line. Others, however, may fall into a gray area. How should states treat individuals who work for private companies that produce military hardware or intelligence-related software for their governments? What about non-state actors that a state uses as proxies to achieve its military goals? In cases such as these, a foreign intelligence service may treat these individuals, whose communications may well be of strong interest to those services, like government officials. In both of these examples, the non-state actors have assumed the risk that their close association with, and measures effectively taken on behalf of, a state renders them appropriate and predictable targets of foreign intelligence activity.

The first factor—the level of harm to the target—may overcome the fact that the person being targeted is indisputably a state actor. In other words, even where we believe that a person has assumed the risk of being subject to various types of foreign intelligence activity, that person may not have assumed a risk that he will be subject to significant harm such that the harm would be permissible under international law. For ex-

[257] Only states that interpret the ICCPR as applying extraterritorially presumably would be willing to take this approach, though many do interpret the ICCPR this way.

ample, the prime minister of a state might assume the risk that he will be the target of many forms of intelligence activity by virtue of his senior, high profile government position, but we would not say that international law should tolerate his assassination.

c. Rule specificity. States also should consider the level of specificity of the international rule at issue and how clearly the international rule covers the contemplated activity. It is more credible to extrapolate agreement to apply a rule of international law to intelligence activities when that rule is specific than when it is vague. The idea is that states intentionally have left themselves less flexibility in arguing about the content and application of specific rules. States therefore should ask whether there is a specific and clear provision of international law directly on point.[258] For example, the VCDR specifically prohibits assaults on or the detention of diplomatic agents.[259] The Chicago Convention explicitly prohibits states from flying state aircraft into another state's airspace without permission.[260] States should apply these types of provisions to all of their intelligence activities. Even here, though, a state should take more seriously the VCDR provision because it implicates harm to individuals, where the Chicago Convention rule primarily implicates harm to state sovereignty.

This factor may have particular import for the application of U.N. Security Council Resolutions to intelligence activities. Security Council Resolutions are usually quite specific, particularly when adopted under Chapter VII. Resolutions that impose obligations such as arms embargos, travel bans, and asset freezes should reach both overt and covert activities by states. All states (and in particular the permanent members of the Security Council, who by definition have not vetoed the resolution and who can take into account their intelligence needs and policies when shaping the text) should interpret these limitations as applying to their intelligence activities.

d. Overt parallels. Finally, a state should consider whether the intelligence activity it is contemplating has parallels in generally accepted,

[258] Of course, it is relevant whether there are any indications in the treaty text or the *travaux preparatoires* that states intended the treaty to cover (or not cover) intelligence activities.

[259] Vienna Convention on Diplomatic Relations art. 29, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95.

[260] Convention on International Civil Aviation art. 3, opened for signature Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

overt state conduct. Where a state can identify an accepted overt activity that appears comparable to the nature and goal of the covert activity, states should feel less constrained in undertaking the intelligence activity, even if that activity might otherwise be limited by potentially applicable international law. For instance, the U.N. Security Council has urged states to aggressively suppress the proliferation of WMDs to non-state actors.[261] Consider a covert action by an intelligence agency to interdict diverted nuclear material by using an agent to acquire that material in another state's territory without its knowledge. While the overt Security Council authorization does not affirmatively provide that one state may violate another's territorial integrity to accomplish the nonproliferation goal, a covert action that achieves the goal with limited impact on the territorial state seems relatively unproblematic. Or consider the process and goal of recruiting human sources. Intelligence services recruit foreign sources in an effort to obtain information about foreign governments, including their military capabilities and strategies and foreign policy goals. Diplomats and military officials expend significant energy doing the same overtly. As a result, states undertaking activities such as recruiting foreign officials as sources and obtaining information from them could interpret permissively in their own favor any relevant constraints under international law.

2. Applying the Factors

Having identified relevant factors that states should consider when assessing how to interpret international law that potentially applies to a given intelligence activity, this Subsection illustrates how states might apply the factors to different activities along the spectrum. There are undoubtedly dozens of contexts and variations in which these activities arise, and many other activities that intelligence services undertake. As a result, the following discussion is necessarily framed at a certain level of generality.

a. Actions that result in physical constraint (rendition, detention, interrogation). These activities fall squarely on the end of the scale of international law interpretation that offers less flexibility to states. The activities are directed at non-state actors, they can result in physical harm to those non-state actors and others who happen to be in their vicinity, the risk of error (due to faulty intelligence or technological malfunction)

[261] S.C. Res. 1540 (Apr. 28, 2004).

is significant, and the international rules regulating these activities are specific. As a result, intelligence services would need to rigorously interpret the full set of international legal rules applicable to this type of activity—including the treaties to which their states are a party and applicable individually-focused CIL. Relevant law could include IHL, the CAT, the ICCPR, and the Refugee Convention.[262] IHL would be relevant when an intelligence service is undertaking one of these activities during an armed conflict. The CAT would be relevant, for instance, when a service detains someone or intends to transfer an individual to another state where he might be mistreated. The ICCPR provisions regarding treatment, arbitrary deprivation of life, and, outside armed conflict, the right of a detainee to appear before a court would be relevant to forcible intelligence activity of this type. States also could derogate as necessary from specific ICCPR obligations pursuant to Article 4 of the treaty. The Refugee Convention would be relevant when an intelligence agency is contemplating turning a detainee over to a state in which his life or freedom would be threatened on account of his or her race, religion, nationality, membership in a particular social group, or political opinion.[263] However, the intelligence service could transfer a refugee if there are reasonable grounds for regarding the refugee as a danger to security or the community.[264]

b. Bulk collection of data. By definition, bulk acquisition of information using electronic surveillance (including both content and metadata collection) implicates millions of communications by non-state actors. This surveillance does not produce physical harm, though content collection, at least, can produce other harms (whether psychological, emotional, or intellectual).[265] If "risk of error" in this context means that

[262] For a survey of the international laws that may be relevant to rendition, see, e.g., Meg Satterthwaite, Al-Liby: "Rendition to Justice" Under Human Rights and Humanitarian Law, Just Security (Oct. 8, 2013, 12:20 PM), https://www.justsecurity.org/1767/al-liby-rendition-justice-human-rights-humanitarian-law [https://perma.cc/7VQY-W4LC].

[263] Convention and Protocol Relating to the Status of Refugees art. 33(1), opened for signature July 28, 1951, 19 U.S.T. 6259, 189 U.N.T.S. 150.

[264] Id. art. 33(2).

[265] Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1945–46 (2013). Scholars and NGOs debate whether ICCPR Article 17 would regulate the state's collection and use of bulk metadata, because of the limited information that such surveillance provides. Additionally, at least in the United States, constitutional doctrine provides that the government collection of metadata from third-party holders such as telecommunications companies does not trigger Fourth Amendment protections. Individuals therefore have a reduced expectation of privacy about their metadata, as opposed to content.

states are collecting the content of communications of people who are not engaged in terrorism or other criminal acts, then the risk of error is pervasive. To even call it a risk of error seems misplaced: It is a feature, not a bug, of this type of collection that it sweeps in wide swaths of data. The international rules regulating this type of privacy interference are moderately clear as applied to domestic action, but it is contested whether they extend to extraterritorial action.

On balance, the quantum of individuals affected suggests that states would likely need to interpret the privacy protections in the ICCPR or comparable CIL as applicable to their foreign surveillance of the content of communications, though not to metadata collection. The United States maintains its argument that the ICCPR does not apply extraterritorially, but states that admit to the ICCPR's extraterritorial application and accept that the treaty (or a comparable customary rule) applies when a state exercises "authority over a person or a context" would need to interpret these protections as reaching intelligence activities that constitute interference with communications.[266] States would therefore have to assess whether their actions constitute arbitrary or unlawful interference with individuals' privacy.

c. Economic espionage. Some states engage in widespread theft of trade secrets and other sensitive data from foreign companies, usually in order to provide advantages to their domestic companies. By definition, this activity is directed at non-state actors, including corporations that are developing advanced technologies. Although there is some risk that the state undertaking this type of espionage will capture some private information inadvertently, the economic espionage that has come to light recently appears to be quite intentionally targeted at selected victims.[267] The quantum of economic harm the theft produces, however, can be immense. General Keith Alexander, then-commander of U.S. Cyber Command, estimated in 2012 that computer hacking costs the U.S. economy $250 billion a year, calling it "the greatest transfer of wealth in history."[268] Although not all hackers are state-based, states such as China

[266] See Deeks, International Legal Framework, supra note 11, at 309 (emphasis omitted).

[267] Dep't of Justice Press Release, supra note 86 (listing as victims U.S. steel and solar companies).

[268] Josh Rogin, NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History," Foreign Pol'y (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history [https://perma.cc/XS8T-JKT4].

and Russia clearly are engaged in this activity.[269] Congressman Dana Rohrabacher stated, "I would say that the American people would be outraged to understand that tens of billions of dollars that have been taken from them in order for research and development in our country [have] ended up in the hands of an economic and military adversary like Communist China."[270] These factors cut in favor of giving states less flexibility to interpret any international laws that facially might constrain this activity.

The "rule specificity" factor cuts the other way, however. It is deeply unsettled whether existing rules of international law prohibit states from engaging in economic espionage.[271] The United States and United Kingdom have disclaimed this activity, arguing that the international community *should* prohibit this type of activity, even if it currently does not.[272] Indeed, the United States has indicated a willingness to impose economic sanctions on China for its role in cyberespionage against U.S. companies.[273] Until very recently, states such as China and France would

[269] Dep't of Justice Press Release, supra note 86 (China); Craig Whitlock & Missy Ryan, U.S. Suspects Russia in Hack of Pentagon Computer Network, Wash. Post (Aug. 6, 2015), https://www.washingtonpost.com/world/national-security/us-suspects-russia-in-hack-of-pentagon-computer-network/2015/08/06/b80e1644-3c7a-11e5-9c2d-ed991d848c48_story.html [https://perma.cc/N526-P8HY] (Russia).

[270] Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Foreign Affairs, 112th Cong. 47 (2011) (statement of Congressman Dana Rohrabacher, Member, Comm. on Foreign Affairs and Chairman, Subcomm. on Oversight & Investigations), http://fas.org/irp/congress/2011_hr/china-cyber.pdf [https://perma.cc/78L2-RQLR].

[271] Compare David P. Fidler, Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies, ASIL Insights (Mar. 20, 2013), https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving [https://perma.cc/G4PA-V3DB] (arguing that international law does not regulate economic cyberespionage and that the Obama administration has not asserted that cyberespionage violates international law, though it may wish to develop this norm), with Christina Parajon Skinner, An International Law Response to Economic Cyber Espionage, 46 Conn. L. Rev. 1165, 1171 (2014) (arguing that economic cyberespionage violates principles of sovereignty and nonintervention).

[272] David Feith, The Weekend Interview with Timothy Thomas: Why China is Reading Your Email, Wall St. J. (Mar. 29, 2013), http://www.wsj.com/articles/SB10001424127887323419104578376042379430724 [https://perma.cc/G4XB-DD3J].

[273] Ellen Nakashima, U.S. Sanctions, supra note 231. Notably, the United States is not contemplating imposing sanctions on China for recent cyberthefts of U.S. government-held data. This supports this Article's argument that some states are treating intelligence activities against private actors differently from similar activities directed against government actors.

have objected to the idea that economic espionage was problematic.[274] Part of the source of the disagreement is a divergence of views on whether this type of espionage furthers a state's national security goals. A state that believes that economic espionage advances its national security will see this activity as consistent with the traditional goals of espionage. However, China may be softening its view in this regard; it recently concluded memoranda of understanding with the United States and United Kingdom that disclaimed the use of economic espionage in cyberspace.[275] If and as states develop international rules constraining commercial espionage, they should not be given much flexibility in interpreting those norms.[276] Until such rules arise, however, states will assert broad freedom of action in this area.

d. Bribery and election influence. Attempting to influence the outcome of foreign elections or bribing foreign officials falls in the middle of the interpretive spectrum, because the intelligence activity affects both state officials and private individuals, but does not cause physical harm and poses little risk of error (though it might produce unpredictable outcomes). Other examples in this category of activity include covertly financing one party in an election or counterfeiting currency and introducing it into that state's monetary system to destabilize the government. Influencing elections, bribing officials, and counterfeiting currency share certain characteristics with metadata collection: The harms are nonphysical and diffuse, but may affect large parts of a population.

It is less clear than in the surveillance context, however, what rules of international law might regulate bribery and election interference.

[274] Jack Goldsmith, Why the USG Complaints Against Chinese Economic Cyber-Snooping Are So Weak, Lawfare (Mar. 25, 2013, 9:01 AM), https://www.lawfareblog.com/why-usg-complaints-against-chinese-economic-cyber-snooping-are-so-weak [https://perma.cc/B3YB-42WP].

[275] UK-China Joint Statement 2015 (Oct. 22, 2015), https://www.gov.uk/government/news/uk-china-joint-statement-2015 [https://perma.cc/5UG4-F8XB] ("The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage."); Ellen Nakashima & Steven Mufson, The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace, Wash. Post (Sept. 25, 2015), https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html [https://perma.cc/4MMW-R84A].

[276] One potential international rule that this activity could violate is the right to not be arbitrarily deprived of property. See G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 17 (Dec. 10, 1948). Whether this right is customary, applies extraterritorially, and includes theft of data is open to debate.

Scholars disagree about whether international law prohibits one state from bribing another state's officials.[277] Interfering with foreign elections by funding or training one's preferred candidate could violate ICCPR Article 25, which guarantees the right to vote in genuine periodic elections so as to "guarantee the free expression of the will of the electors." Article 25 might be read to prohibit interference in another state's elections, if one (a) reads the provision to apply extraterritorially; (b) interprets "respect" to mean "not alter or influence"; and (c) interprets "to vote and to be elected at *genuine* periodic elections" to prohibit attempts to influence elections. Some would interpret the customary rule of noninterference as prohibiting such influence as well.[278] But the language in these treaties and rules is not clear about whether states intended it to reach state activities of the type contemplated here, whether committed covertly or during a public course of dealings.

Further, influencing elections has certain parallels in regular diplomacy (which includes meeting with and otherwise supporting opposition groups and journalists but generally avoids direct financial contributions to candidates in foreign elections).[279] Bribery has more direct parallels in overt activity: One state often provides foreign assistance to another state with the goal of influencing (directly through that assistance or more generally through the creation of good will) the policies of the recipient state.

These types of activities present one of the hardest cases for the test set forth in this Part, because the factors cut in different directions. States presumably will either fall back to being guided by their assess-

[277] Reisman and Baker do not believe that the U.N. Charter (which contains norms requiring respect for other states' sovereignty) prohibits bribery. Reisman & Baker, supra note 5, at 29 (noting there is no international prohibition on engaging in covert economic coercion such as bribery). Professor Quincy Wright, on the other hand, argues that bribery clearly violates the territorial integrity and political independence of the other state. Wright, supra note 150, at 5. The U.N. Convention Against Corruption, to which many states are party, requires states to criminalize the bribery of foreign public officials "in order to obtain or retain business or other undue advantage in relation to the conduct of international business." G.A. Res. 58/4, United Nations Convention Against Corruption art. 16, U.N. Doc. A/RES/58/4 (Oct. 31, 2003). The bribing of a foreign official by one state's intelligence service does not seem to fall within that provision.

[278] Professor Loch Johnson argues that covertly influencing truly democratic elections violates the rule of nonintervention but that covert operations directed against self-interested autocratic regimes do not. Loch K. Johnson, On Drawing a Bright Line for Covert Operations, 86 Am. J. Int'l L. 284, 288 (1992).

[279] Damrosch, supra note 1, at 20–21 (describing various foreign involvements in elections).

ment of the policy costs and benefits to engaging in this activity, or interpret these provisions of international law as inapplicable, because it is insufficiently clear that states intended these international rules to regulate state action in these contexts.

e. Recruiting human sources. Recruiting a foreign human source falls on the far end of the spectrum from rendition and detention. Quite frequently an intelligence service will try to recruit a foreign source with ties to (or intimate knowledge of) his government. Even where an intelligence service tries to recruit a source unconnected to the government, the primary equities at issue are those of the state being penetrated. This is not to say that the person being recruited faces no risk—he could face harsh criminal penalties if caught—but the recruitment activity itself does not inherently produce the harm. Here, too, the prevalence of this activity among states suggests that states impliedly have consented to this activity, subject to the ability to prosecute those who agree to spy for other governments.[280] This is particularly true where the intelligence agent recruiting the source is in the source's country lawfully; this minimizes the scope of any sovereignty violation. As a result, states should be able to interpret flexibly (including by interpreting as inapplicable) CIL rules that could, on their face, be read to prohibit this kind of activity. The justification for that interpretation would need to be based on historical state practice and some signals by states that they believe this activity to be lawful under international law.

C. Consistency with Existing Practice

If Western, democratic states adopted this sliding scale, it would require them to change some of their practices, but less so than many would expect. As discussed in Part IV, a number of states require their intelligence services to interpret IHL as directly applicable during wartime and apply it accordingly. Most, if not all, Council of Europe member states presumably also prohibit their intelligence officials from engaging in torture or cruel, inhuman, or degrading treatment overseas. The United States has for decades complied with a self-imposed assassi-

[280] Wright, supra note 150, at 13 ("Intervention by unlawful acts in another state's territory may be divided into direct or open intervention, such as armed invasion, and indirect or subversive intervention involving secret activity. Since the government responsible for the latter type of action seldom acknowledges its responsibility but allows the agent, if caught, to be punished without protest, such incidents are not usually the subject of international discussion.").

nation ban, as has the United Kingdom. States seem to interpret U.N. Charter Article 2(4) as relevant to their intelligence activities.[281] The United States and United Kingdom have analyzed their covert efforts to arm rebels to fight the Assad regime in Syria under international law, which almost certainly would include Article 2(4) of the Charter.[282] The idea of requiring states to interpret arms embargoes as reaching all of their activities seems consistent with the U.K. and French approaches to the E.U. embargo in Syria, where those states waited until the E.U. lifted the embargo before their intelligence services started to supply the rebels.[283]

That said, adopting a sliding scale surely would prompt changes with regard to activities such as mass electronic surveillance. Most states currently do not appear to believe that bulk surveillance constitutes an interference with privacy, or they believe that they are not exercising "effective control" over an individual, so that the jurisdiction of the human rights treaties would not be triggered. But this argument may be hard to sustain in the long term, as the scale of the surveillance becomes clearer.

In short, the sliding scale interpretive approach to intelligence is a normative proposal, but it contains positive elements as well, because it reflects the general direction rule-of-law states are heading. The same cannot be said for states that are under no external pressures to "legalize" their intelligence services or for states that do not consistently heed their international obligations more generally. These states will be less willing to apply a sliding scale approach to international law, preferring to disregard the potential application of that law to any intelligence activities. For them, the realpolitik approach remains dominant.

[281] Entous, supra note 201 (describing the U.S. evaluation of Article 2(4) in supplying weapons to anti-Assad rebels).

[282] Id; see also Deeks, supra note 201 (analyzing how U.S. government might try to reconcile Article 2(4) with covert provision of support to rebels); Arming Syrian Rebels a Breach of International Law, Russia Says, France24 (Mar. 13, 2013), http://www.france24.com/en/20130313-russia-foreign-minister-arm-syria-rebels-breach-international-law [https://perma.cc/9TDL-W85T] (describing how Britain was considering whether to arm rebels while maintaining that "any action we take will be legal, will be clearly with a strong basis in international law").

[283] Ian Traynor, UK Forces EU to Lift Embargo on Syria Rebel Arms, Guardian (U.K.) (May 27, 2013), http://www.theguardian.com/world/2013/may/28/uk-forced-eu-embargo-syria-rebel-arms [https://perma.cc/P364-VU99].

D. Implications and Challenges

Adopting the type of sliding scale approach set forth here would have a number of positive implications for international law and international relations, though it would also have some ambiguous or negative implications.

The primary implication of the sliding scale is that states would need to act more carefully and cautiously when undertaking nontraditional intelligence activities, where individuals not associated with governments are likely to face harm and are generally without diplomatic, judicial, or other recourse. This means that states will have less leeway when interpreting legal limits on intelligence activities against non-state actors such as al Qaeda, ISIS, and Boko Haram. On one hand, this seems perverse, because state actors are more likely to comply with basic rules of IHL and general principles of decency. On the other, some of the non-state actors who get caught up in intelligence activity are innocent of wrongdoing. Further, it often is difficult to identify which non-state actors are and are not engaged in terrorist or criminal acts. Interpreting a certain body of international law strictly in favor of the target does not necessarily mean that the intelligence action could not be undertaken. Instead, the application of applicable international rules typically requires a state to make certain assessments before a state can take action.

This sliding scale will alter state incentives ex ante. For example, employing a sliding scale approach may affect states' incentives during treaty negotiations. Some states might press for explicit carve-outs for their intelligence services (or may insist on including "national security exceptions" to substantive rules). Alternatively, if states are permitted to interpret more flexibly vague international provisions that could implicate intelligence activities, some negotiators may press for increasingly abstract or nonspecific provisions in treaties.

The existence of a sliding scale may increase the quantity of verbal state practice related to intelligence. A more overt and straightforward discussion during negotiations about whether and how international law applies to intelligence might ultimately improve states' abilities to anticipate how other states will react to a given intelligence activity. This, in turn, may reduce political and military tensions or reactions. However, nonverbal state practice (especially in state-state intelligence operations) seems likely to remain largely secret. A state's interpretations of the limits, if any, imposed on a given intelligence activity that implicates a CIL rule such as sovereignty remains self-judging and, in most cases, un-

known to other states. Thus, it will take a long time for nonverbal state practice in this area to coalesce around common understandings of these customary rules.

To the extent that states view the sliding scale as inhibiting their freedom of action, they will only adopt this approach in their relations with other states that adopt it. That is, they will decline to unilaterally disarm. This might mean, for example, that discrete groups of states that feel the pressures of legalism described herein would agree among themselves to adopt a sliding scale approach in relation to each other's nationals and territory.[284] However, many of the constraints that arise in a sliding scale approach only attach to situations involving non-state actors, not to state-state interactions. Therefore, a state's freedom to conduct traditional intelligence activities against other states is less inhibited; states may conclude that they can adopt the sliding scale without unilaterally surrendering notable advantages to other states.

Further, adopting a sliding scale approach in the intelligence context might create a slippery slope. That is, if states should give more weight to individually-focused rules in this context than they give to the state-focused sovereignty norms, why should they not do so in other areas of international relations? The answer lies in history and secrecy. Historically, outside the realm of intelligence, states have not tried to argue that international law constraints are inapplicable. Intelligence has been the exception, not the rule; states must believe that the state-focused sovereignty norms are largely advantageous in virtually all of the other contexts in which they attach. Second, states generally seek to keep secret their violations of the state-focused norms. This helps guard against a slippery slope problem; if states do not publicly flout sovereignty rules in the intelligence context, it will provoke less interest in doing so outside of that context.[285]

Finally, even when a state concludes that a particular rule of international law is properly interpreted as inapplicable to its activity, it does not mean that the state undertaking the activity will face no consequences. A state that decides to undertake an intelligence activity always runs the risk that other states, especially the victim states, will impose politi-

[284] For a comparable problem, see Deeks, International Legal Framework, supra note 11, at 339–41.

[285] Perina, supra note 25, at 511 (arguing that covert violations may do less damage to legal rules than overt violations because they do not "constitute a legal precedent that legitimates future conduct").

cal, moral, or domestic legal costs on it. And to the extent that the victim states believe that the acting state has improperly interpreted international law, the victim states may impose countermeasures on the acting state. The language and form of the critiques and responses will differ, but they will emerge just the same.

CONCLUSION

Intelligence activity used to be the last bastion of international relations untouched by international law. That is changing; the realpolitik, anything-goes approach is on the wane and the impulse to apply at least some bodies of international law to intelligence activities is strengthening. That is as it should be, in light of changing intelligence missions and a new legal landscape. Just as U.S. courts are beginning to "normalize" foreign affairs, so too are we starting to see the "normalization" of intelligence.[286] Intelligence activities are no longer perceived as a special domain unconstrained by law, particularly when those activities implicate non-state actors. The pressures on Western intelligence communities to interpret international law more strictly and apply it more robustly are only beginning. This Article proposes a way to meet those pressures in a principled way.

[286] Ganesh Sitaraman & Ingrid Wuerth, The Normalization of Foreign Relations Law, 128 Harv. L. Rev. 1897 (2015).