International Political Sociology (2020) **14**, 323–344

Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon

Hager Ben Jaffel
CRESPPA/LabTop, Centre National de la Recherche Scientifique (CNRS)
Alvina Hoffmann
King's College London
Oliver Kearns
School of Sociology, Politics and International Studies, University of Bristol, UK
and
Sebastian Larsson
Stockholm University

This collective discussion proposes a novel understanding of intelligence as a social phenomenon, taking place in a social space that increasingly involves actors and professional fields not immediately seen as part of intelligence. This discussion is a response to the inherent functionalism in Intelligence Studies (IS) that conceives of intelligence as a cycle serving policymakers. Instead, our interventions seek to problematize and break with this notion of the cycle and show what an alternative study of intelligence would look like. In the first part of the discussion, we situate our intervention in the broader fields of IS and International Political Sociology. Espousing a transdisciplinary approach, we build our four interventions as transversal lines cutting through a social space in which agents with differing stakes participate and reframe the meaning and practice of intelligence. Intelligence professionals not only have to reckon with policymakers, but also increasingly with law enforcement agents, representatives from the science and technology sector, judges, lawyers, activists, and Internet users themselves. Each move takes a step further away from the intelligence cycle by introducing new empirical sites, actors, and stakes.

Intelligence stands as one of the last fields of "high politics" whose study is disciplined by those most invested in it, remaining wedded to restrictive functionalist modes of analysis and practiced by members of the "intelligence community" itself. In this respect, the actions of Edward Snowden, in leaking classified US National Security Agency documents in 2013, provide ample opportunity to rethink Intelligence Studies (IS). As a NSA sub-contractee, he detailed not just the expansive scope of surveillance, as scholars have pointed out, but the evolving social life of intelligence itself: dispersed across and maintained by people with varying relations to the intelligence services, an everyday aspect of different professions. Snowden

Ben Jaffel, Hager et al. (2020) Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon. *International Political Sociology*, doi: 10.1093/ips/olaa015
Corresponding author e-mail: hager.benjaffel@yahoo.fr

has insisted that this is what intelligence practice today looks like: "I was trained as a spy . . . [and] I developed sources and methods for keeping our information and people secure . . . So when [the US government] say I'm a low-level systems administrator, that I don't know what I'm talking about, I'd say it's somewhat misleading" (NBC 2014).

This collective discussion piece takes Snowden at his word, theorizing intelligence as a social phenomenon. This phenomenon constitutes a non-contiguous social space made up of a diversity of actors who breach the limits of the supposed "intelligence community." Snowden's insistence that his whistle-blowing aims to reorient intelligence toward legitimate ends—that, to follow his Twitter byline, where once he served the government, now he serves the public (@snowden)—ruptures the dominant ontology of intelligence work. Snowden provided vital intelligence, not to state officials and governing politicians, but to their populations. His analyses have detailed surveillance operations seemingly far exceeding "national security," reflecting how various parties have different stakes in intelligence, producing a heterogeneous social space where the meaning and practice of intelligence is being ceaselessly reframed.

We argue that conventional conceptualizations of intelligence cannot provide adequate insight into these social dynamics. As we argue below, the common notion of an "intelligence cycle" does not do justice to intelligence's existence within, and shaping of, social reality, both inside and outside the traditional "community." Put simply, intelligence isn't what its predominant scholars think it is, nor does it do only what is theorized of it. This has been largely overlooked due to the deep-rooted intellectual remit of IS scholarship, whereby intelligence theorizing is conceived functionally as serving policymaking; only by subverting this framework can scholars trace intelligence's international political sociology.

In making this argument, the article proceeds as follows: first, a critique of IS, making the case for a non-functionalist conceptualization; second, an overview of IPS's contributions to this research area; and finally, a series of interventions that analyses intelligence as a social phenomenon. Each move takes a step further away from the decision-making realm of the "cycle" by introducing new issues—from epistemology to international cooperation, to law enforcement, to science and technology, to lawyers, activists, and Internet users.

Theory "Of" or Theory "For"? "Intelligence" in Intelligence Studies

It is crucial to first address the IS sub-discipline itself, for those very social dynamics that interest us here have shaped IS so as to foreclose such analysis.

IS' relationship to "intelligence" is a long and fraught one. The field's understanding of what intelligence *is* and *does* has been shaped by its founding relationship with Anglo-American state intelligence practice. Developing in the 1950s out of the perceived need in the United States for literature that would aid the professionalization of state espionage and strategic analysis (Kent 1955), the intelligence research agenda was first structured by US political scientists and British historians, with archival releases and official investigations prompting interest in intelligence's global dynamics and relationship to governance (Gill and Phythian 2016, 6–8). This nascent field of scholarship was gradually institutionalized as a sub-discipline of International Relations (IR) (Andrew and Dilk 1984). Despite minor clusters in Europe (Khan 2008), IS continues to be overwhelmingly dominated by Anglo-American scholars, positioned as "an academic complement to the practice of [US] national security intelligence" (Marrin 2016, 266). This Anglo-American centrism has been further institutionalized in research centers, teaching courses and dedicated journals across Britain and the United States (Glees 2015; Van Puyvelde and Curtis 2016).

This strong Anglo-American state-policy lineage has fundamentally shaped IS' research agenda. Scholars have primarily investigated the intelligence services of their home countries and Five Eyes allies, serving them up as institutional exemplars (Aldrich and Kasuku 2012). IS' methodological debt to Anglo-American policymaking is reflected in access and crossover: the common practice of academic "secondment" to intelligence agencies in the United States, a "policy of indoctrinating academics"; and the British complement of commissioning "sponsored histories" of the intelligence and security services from historians (Goodman 2007; Baxter and Jeffery 2013, 294). Indeed, those who constitute IS have historically been acting and former US and UK intelligence professionals (Goodman 2007), some holding academic positions; their modes of thought and analysis have cleaved to their professional experience. These interdependencies are accompanied by strongly state-centric epistemologies (Gill and Phythian 2018).

Within this intellectual lineage and sociological context, the conceptual question of intelligence has been given narrow and uninquisitive answers. As recently discussed by Mark Phythian,[1] interrogating what intelligence *does* in the world has involved scholars defining intelligence's social dynamics by the relationship between state agencies and policymakers. This has led to theories *for*, rather than *of*, intelligence. Thus, IS' core function becomes improving intelligence services' ability to assist security and policymaking (Gill and Phythian 2018). Intelligence is considered socially significant insofar as it supports the "government machinery" around "the nature of security threats" (Scott and Jackson 2004, 143, 148).

This intellectual backdrop has determined the debate about what does and does not count as intelligence. Interrogating what intelligence *is* has led inexorably to ideas of "knowledge management," with intelligence being "a sub-set of surveillance" whose object is "security" (Gill 2010). This has spearheaded efforts to determine "best practice," concentrating on the supposed "intelligence cycle" of collection, analysis and dissemination (Van Puyvelde and Curtis 2016). Despite myriad criticisms of its inaccuracy (Hulnick 2006), scholars have clung to the model of the cycle since its culmination, "communication to the decision-maker(s)," conceptually defines "the value of the intelligence project" (Breakspear 2013, 681). Together with secrecy in terms of practitioners' target and methods (Warner 2012), this process is the primary means by which intelligence is defined and against which it is judged, feeding back into IS' mission of assisting policymaking.

This conceptualization of intelligence as secret knowledge-making (Scott and Jackson 2004) has, however, been put under strain. The perceived transnationalization of threats has incentivized services to lower their secrecy barriers and cooperate through intelligence exchange (Svendsen 2008). Such changes reflect both uncertainty surrounding intelligence's analytical boundaries and reservations about the traditional lenses of studying it.

A handful of dissenting voices have therefore tried to expand IS' conceptual possibilities. Scholars have offered a more flexible conception of intelligence as "simply what services do" (Stout and Warner 2018, 521), contesting the narrow conception of intelligence as a fixed cycle by acknowledging other practices, such as record keeping (Ehrman 2009) and data storage (Hammond 2010). Scholars have moved beyond secretive institutional settings to appreciate the multiplicity of actors with a stake in intelligence practice, including police forces (Foley 2013) and non-state actors (Martin and Wilson 2008; Stout and Warner 2018). Aldrich and Kasuku (2012) have sought to "escape" from the Anglosphere, addressing patterns of intelligence outside Anglo-American experiences. And the new *Journal of European and American Intelligence Studies* espouses a "vision of inclusiveness beyond mainstream approaches," giving greater visibility to research outside an Anglospheric framework (Baches-Torres and Torres-Baches 2018, 22).

[1] Mark Phythian. "Critical Intelligence Studies?" Paper Presented at CERI, Sciences Po Paris, September 19, 2019.

Others have initiated "Critical" approaches to intelligence. Hamilton Bean (2013, 498) proposes a "rhetorical and critical/cultural perspective" focused on the knowledge-power nexus underpinning intelligence practice, integrating power into intelligence's conceptualization. By combining the examination of rhetoric with critical and cultural theory, Bean demonstrates that discourse transforms intelligence categories into authoritative "knowledge claims" allied to identities and relationships (Bean 2013, 518). Peter De Werd, attending to intelligence's "socio-political context," examines the (de)securitization moves of intelligence discourse among various actors, from producer to consumer (De Werd 2018, 109).

If these initiatives have the merit of pointing to alternative research avenues, they are nonetheless insufficiently geared toward a transdisciplinary and critical view of intelligence *as a social phenomenon*. Initiatives within IS remain prisoner of its state-professional lineage. Critical IS still aims to inform debates on process and policymaking by reaching a "more visible and influential position within [IS]" (Bean 2018, 528). Such endeavors fail to break free from being theories *for* intelligence, reiterating the conceptualization of intelligence labor as merely subordinate to decision/policy-making. This functionalist outlook—that intelligence simply *is* state security—conceptually reduces what intelligence *does* in the world to those practices that explicitly bear on this rationale. If intelligence is embedded within larger, historical-sociological phenomena, then one is hampered by delimiting intelligence to a 'cog' of government 'machinery.'

In assuming, rather than scrutinizing, the government-security rationale, this literature fails to see intelligence's social existence *outside* the policymaking framework. It bypasses questions of who and what constitutes intelligence in the world. And it does not consider intelligence independent of theories *for* intelligence improvement.

Conceptualizing intelligence as a social phenomenon allows for a truly transdisciplinary research agenda, by situating practices of information-production-through-surveillance within their broader social sphere of influence and co-production, a social space wider and more diversified than the supposed cycle.

Breaking the Doxa: "Intelligence" in International Political Sociology

For us to study intelligence as a social phenomenon involving a multitude of actors, we need to break with the IS doxa. Doxa, in the work of Pierre Bourdieu, refers to the ideas and norms that represent the "commonsensical view" within a given field (of research or practice) on what should be at all thinkable or doable therein (Bourdieu and Wacquant 1992, 96). Doxa is not an explicit consensus but rather a largely implicit shared understanding among social agents regarding how the game is supposed to be played, as a form of pre-reflexive "agreement on legitimate disagreements" within their field (Loughlan, Olsson, and Schouten 2014, 32). Breaking the IS doxa means developing an approach that is not only transdisciplinary, but also sensitive to the actual social relations constituting intelligence as a practice.

Existing work in IPS helps us to this end. IPS scholarship identifies issues that "seem to be simultaneously social, political and international, but not quite in ways that make sense to analysts committed to the academic disciplines specializing in the social, the political or the international" (Walker 2016, 16). It insists on the detrimental effects of disciplinary gatekeeping and that analyses (and particularly "critiques") of social, political, and international phenomena demand a transdisciplinary perspective including methodological and theoretical experimentation across disciplines.

How have intelligence issues been approached in IPS along these lines? The Snowden revelations were a watershed moment, providing not only empirical evidence for mass surveillance practices that could previously only be assumed by activists or in court cases, but showing their normalization, digitized manifesta-

tion, and truly global reach (Bauman et al. 2014). It became clear that the involvement of intelligence agencies in mass surveillance had become a new normal, involving the mass collection of personal data of all citizens. It also became clear that intelligence today is tightly linked to police work, including profiling and preemptive practices (Bigo 2016) as well as notions of "extraordinary rendition," including torture and other coercive measures. These shifts have been reflected in IPS work.

First, IPS-inspired scholarship has strived to make sense of the social-digital entanglements of data extraction, mass surveillance, and secrecy in intelligence gathering, approaching these sociologically rather than as pre-given. Aradau (2017) introduces the notion of non-knowledge as a pertinent way to exemplify the controversies and stakes in mass surveillance from the perspective of knowledge construction and ignorance studies. She shows how different "regimes" of knowledge compete with one another, providing an analysis of the fragility of legal knowledge that is challenged "by digital technologies and future-oriented security practices" (*ibid.*, 329). This happens through the enactment of non-knowledge by means of vocabularies such as "risk, . . . uncertainty, ambiguity, error, surprise, complexity, confusion, omission, fallacy, or contingency" (*ibid.*, 331). Reasoning through the notion of uncertainty in legal cases on security issues has decreased the scope for resistance against surveillance. Thus, Aradau proposes to view secrecy as generative of a spatial-epistemic regime, separating "spaces of knowledge and knowers from spaces of non-knowledge" (*ibid.*, 336). Enacting this boundary increases the credibility of those who know and delegitimizes those located outside the boundary of this "community of secrets." This insight is important as it centers secrecy's production of particular kinds of subjects.

Bigo (2019) approaches secrecy through the notion of "*shared secret information,*" which captures the transnational condition of "national" security in the digital world. To him, secrecy is an internal hierarchical architecture that is organized around actors' claims to the right to access information (*ibid.*, 382). He centers the practices of exchange and information sharing among national intelligence services, therefore making secrecy not about withholding information but about the criteria of suspicion and techniques to circulate information within a "certain "circle" of people with authority to maintain the others in ignorance" (*ibid.*, 379). While these practices are not new, digitization has profoundly changed the scale of secret information sharing that now affects millions of individuals all around the globe. "National security" becomes projected outside national frontiers through a transnational alliance of security professionals and intelligence agencies, all the while transforming Internet users into subjects of suspicion, "destabilizing the protection for national citizens if they are communicating with foreigners" (*ibid.*, 384). Blurring the legal categories of foreigners and citizens has profound effects for claiming rights and protections.

Second, IPS scholarship has examined the everyday aspects of intelligence cooperation, for example by shifting focus from high-level bureaucracies and senior government analysts, to how intelligence works through mundane practices of policing, surveillance, and vigilance. Here, intelligence becomes organized around the role of the *public* as a space, target, and actor for intelligence work. For example, it has been studied how the collection of intelligence on potential threats and terrorist suspects has come to involve not "undercover" sources, but increasingly the citizen itself. Reconfiguring intelligence work into a "shared responsibility" (Petersen and Tjalve 2013), citizens are encouraged by state agencies to engage in a form of "participatory policing" and report people, behaviors, or objects that appear "suspicious" or "out of place" (Larsson 2017). This radically shifts the question of what intelligence means and does, since subjective and prejudiced citizen reports are treated as perfectly legitimate intelligence for police-driven operations. "Once the work of an insular and carefully select few," as Petersen and Tjalve (2018, 30)

argue, "intelligence production is now a networked, partially open and extensively public–private enterprise."

In IPS, the study of intelligence thus not only raises questions around secrecy, knowledge, ignorance, and gated communities of intelligence professionals, but also prompts us to consider practices of information sharing and withholding, conducted in a variety of social, digital, and everyday spaces and in relation to other actors.

Intelligence as a Social Phenomenon: Four Moves

Exploring intelligence as a social phenomenon opens up space for a critical and transdisciplinary approach, one that avoids falling into the trap of functionalism, allowing for theoretical innovation to analyze the transformations of intelligence, rather than taking its scope for granted. Approaching intelligence as a social phenomenon thus means situating intelligence in a social space of relationships that expand beyond intelligence services alone and involve other actors embedded in struggles to speak for, perform, and contest intelligence. In the following, we will give a sense of the constitutive relations and transformations that take place in a social space of intelligence. How does the practice and expansion of the field of intelligence manifest itself and what does it mean for intelligence professionals, other practitioners and those who oppose it? The first move analyses the discursive effect of IS' functionalism on the social existence of the state, opening up space for the subsequent interventions to examine intelligence as a social phenomenon evolving far beyond an insular statism.

Intelligence, the State, and the Success of Failure (Oliver Kearns)

What are intelligence analysts doing when they do their analysis? In conceptualizing intelligence beyond state-policymaking, we do not intend a simple swing from one empirical field to another. A key site where intelligence-as-social-phenomenon yields insight is that (in)famous organization, the state intelligence agency. Sociologically, this goes beyond examining actors' positional struggles; tracing this phenomenon means exploring social dynamics that are undetermined, that shape rather than follow interests (Guzzini 2016, 3–4). By contrast, IS bounds its subject's dynamics within a deeply interest-led relationship to government, specifically how agencies contribute to clear-sighted decision-making.

Or at least, how they *should* do so. IS scholars have clung to the model of the "intelligence cycle"—from requirements-setting to collecting and analyzing data to disseminating results—as it defines intelligence's value. Whether as decision-advantage or risk-shifting, intelligence emerges as a fundamentally interactive component of elite statecraft (Hillebrand and Hughes 2017, 5–6). Breakspear paraphrases former GCHQ officer Michael Herman: "intelligence must reach its clients in useable forms and in time. *The key question is what use they make of it*" (Breakspear 2013, 686, emphasis added).

Unfortunately, IS has found itself grappling with the very real possibility that intelligence is rarely used by policymakers to either guide or inform state strategy (Immerman 2008; Marrin 2008). In addition to studies that demonstrate that state leaders ignore or dismiss analyses when it suits them (Dahl 2013; Roberts and Saldin 2016), figures crossing that thin line between scholar and practitioner attest that much of intelligence "tradecraft" "doesn't have much to do with policy at all," with policymakers unlikely to notice or care about those analytical procedures designed precisely to improve usability (Treverton 2018, 476). Woodrow Kuhns, formerly of the CIA's Centre for the Study of Intelligence, laments that when policymakers do take notice, they attend to intelligence as "provid[ing] the facts" about the world that they themselves can "interpret" as befits their policy aims (Kuhns 2003, 94–95).

So the question returns: what exactly are intelligence analysts doing? If state intelligence's social dynamics are not consistently or even primarily about enriching policymaking through convincing self-explanatory guidance, what are these dynamics doing within and beyond intelligence agencies? How do practices of collection, analysis and dissemination impact this social field?

It is instructive here to return to the intelligence cycle. Besides valorizing elite dissemination, the key sociological effect of this model is to produce a self-contained schema for a broad positivist research agenda: under what conditions does the cycle produce its intended outcome, and when does it go wrong? Unpicking past "intelligence failures," particularly around predicting and pre-empting foreign actors (Marrin 2004, 657–658), is "perhaps the most academically advanced field in the study of intelligence" (Kuhns 2003, 80). Scrutinizing the causes of failure has emerged as IS' main theoretical thread, with these efforts "serving a similar functional purpose as explanations of war in an IR theoretical context" (Marrin 2018, 481).

The parallel is revealing. Remaining the assumed prerogative of realist and liberal theory, explanations of war in IR take the international structure of states, and the conditions that lead those states into security dilemmas, as a given, even inevitable (Raschi and Zambernardi 2018). Paradoxically both "taken for granted in its meaning" and "radically underdeveloped" conceptually, a commonsensical notion of "war" has been placed within "an analytic terrain defined in advance" by "the sovereign state and the state system," being "reduced primarily to an effect of the states system" (Barkawi 2011, 709). IR's study of war thus rationalizes a model of geopolitics structured (unevenly) by states of normative equivalence; for these theories, "state sovereignty is not merely a descriptive fact, but also a normative claim" (Morkevičius 2015, 13), one perpetuated through "war" as an object of study.

If the question of intelligence failure plays a functional role echoing the one of war in IR, might this IS research agenda similarly restrict insight into its object's origins? IS theory on failure shares a key orientation with these IR traditions: inevitability. Just as war is assumed to be an outgrowth of the state system, intelligence failure is conceived of as resulting from attempts to navigate that system. Thus, Richard Betts, in a paradigmatic article, traces failure to the excesses of fragmentary data collected on other states' intentions and military capabilities. This informational overload can never be mitigated: to assume the worst in response to ambiguity, or to subject data to multiple analyses, merely increases the likelihood that statespersons will be unable to discern others' intent, or that suspected adversaries will react to pre-emptive actions in kind (Betts 1978, 73–78). Since Bett's article, "a consensus appears to have developed . . . that the causes [of failure] are immutable" (Marrin 2004, 661). What remains uninterrogated is how the relative positioning and consequent adversarialism of state actors prompts them to each discern potential "threats."

Despite the lack of theoretical innovation since Betts' piece, what keeps this research agenda going is the functionalist motivation that IS has inherited from the "strategic surprise" literature: to improve the state's ability to predict military or other attack (Marrin 2004, 658). Events that IS deems failures are overwhelmingly those that bear upon the outcome of strategic planning vis-à-vis "rivals." It is for this reason that misapplied collection resources can remain invisible in IS theory if state policy goes unaffected; by contrast, blunders due to statespersons' neglect of agency reports will often be characterized as a failure *of* intelligence (Jensen 2012, 276–278). As Jensen succinctly summarizes, "[f]rom the perspective of a decision-maker . . . an intelligence failure results simply when the intelligence input into the decision-making process is lacking or unsatisfactory" (*ibid.*, 263). Despite the glorification of accuracy among scholars and analysts, or the lament that accuracy is

unachievable, failure under the above definition can occur quite independently of any inaccuracy; the failure will be one of not contributing to security policymaking.

If the real theoretical issue, then, is state strategy, what is the image of the state underlying IS' research agenda? Here, we identify a major lacuna in IS theory—the lack of a theory of the state, that very entity which supposedly necessitates intelligence and the reduction of strategic surprise. Even the most sophisticated and comprehensive accounts of failure, tracing its potential across the intelligence cycle, from process to product to institutional organization (e.g., Pastorello and Testa 2017, 50–53; Gill 2019, 3–7), rely foundationally upon an unspoken image of "the state" as a sociological entity within which process is rationalized, product feeds into policymaking and organization forms a structural component.

Outside IS, political sociology has long understood that "state" works ordinarily as a distorting abstraction from political practices (Abrams 1988); the task has therefore been to determine the concept's potential utility as an ontology that elucidates those practices' interrelations (Hay 2014, 468). To the extent that IS attempts such theorizing, it centers the relative influence and autonomy of intelligence agents and agencies within national governance. What results are typologies based on security-influenced governing logics—the garrison state, the surveillance state, etc.—and on the domestic power of agencies (Gill 2010, 47). Yet as Peter Gill identified a decade ago, insofar as intelligence relates to state power, "we need to specify how that relationship *defines the state in general*" (*ibid.*, emphasis added), that is, defines those social practices associated with the state *as* state. This can be conceptualized as "the statization of social life," the ways that such practices materialize a comprehensible entity called "the state" within social relations (Painter 2006, 759). While the "statizing" practices typically studied in sociology are those that materialize a "domestic" sovereign sphere (Hay 2014, 469–476), intelligence agencies concerned with "foreign threats" articulate the state *within* the international, explaining the latter and its relations *to* the former. The statization of social life here is also its internationalization.

Critically approaching intelligence as a social phenomenon makes a significant contribution to this research area. Consider a British intelligence assessment from January 2003 that Saddam Hussein is "misreading the international scene" by refusing to back down in the face of a threatened invasion of Iraq (Joint Intelligence Committee 2003, 2). This practice of explaining Saddam's "misperceptions" imagines international relations as an immutable social field, one beyond policy consideration. The "international scene" is a fixed social force that one either "gets" or misreads. The British state, moreover, is irreducibly constitutive of that unexamined field, part of a "coalition" whose elemental dynamics a racialized Saddam has simply failed to appreciate. Such assessments, being written and disseminated among multiple social groups, articulate "[t]he state . . . as an imagined collective actor" through their "telling of stories of statehood and [their] production of narrative accounts of state power" (Painter 2006, 761). This reporting socially reiterates Britain's geopolitical position in the international as a priori, its interests coherent, all validated in a circular logic by the "nature" of the international.

Telling stories exceeds the written word. Taught IS now regularly includes analytical exercises modeled on state-institutional practice. These exercises have a clear socializing effect, instantiating the Anglo-American state as an irreducible political actor whose sovereign pre-eminence across bounded social fields localizes intrinsic geopolitical insecurities. An exercise that asks whether a regional organization constitutes a "threat to . . . United Kingdom and Western security" and/or "regional stability" prompts students to assess whether political actors are "enem[ies]" of one's state or "benign"; "Western security," what it would look like and how to measure its acquisition, goes unexplored (Davies 2006, 728, 731). Another, simulating a "ticking clock" terrorism threat, may make students reflect on "just how hard analysts'

jobs are" (quoted in Shelton 2014, 276), but in so doing it invites them to embody the lived international experience of "the state" as entirely without antecedent, occupying a given present that *necessitates* gaining advantage over others. This makes force in the state's name a foregone geopolitical conclusion.

Such intelligence practices articulate the state as having a self-dependent validity within the international—a natural right to retain its geopolitical position—and as therefore acting legitimately in investigating foreign adversaries. This is the paradoxical success of "intelligence failure." The notion of "accuracy," as proxy for strategy, normalizes the international circumstances of an analyst's polity as having no political past—only an objective facticity that must be maintained and cannot be reconfigured, even to reduce threats. International social dynamics which tie that polity to "adversaries'" actions are repeatedly reinscribed as inveterate "failures" of information. This supposed inevitability forecloses any study of how "failure" may be conditioned by the above normalization. What possibilities for understanding these global dynamics are abnegated by a narration of one's state as an irreducible geopolitical force? What possibilities for improving the security of national populations?

Studying intelligence as a social phenomenon therefore needs to do more than breach a tool-of-governing analytic. Tracing intelligence's transnationalization also means tracing its continued implication in state-making practices, accounting for how those things that intelligence analysts do all day work to reassert the state, and its place within the international, as both real and unquestionable.

Intelligence Cooperation: Europe, Police Forces and Everyday Practices (Hager Ben Jaffel)

What does intelligence look like when the point of departure is not policymaking but the "ground"? How those who practice intelligence cooperation understand their work? This second intervention grounds intelligence in its social space, which is not confined to intelligence services alone and is not necessarily driven by the demands of policymakers. I show how the everyday of representatives of police forces involved in intelligence cooperation in Europe contradicts the core assumption about intelligence as a cycle for policymakers.

Even when unfolding at the international level, intelligence remains informed by a strategic reasoning that gives primacy to intelligence services, American intelligence and policymaking. On the one hand, scholars have situated intelligence cooperation in the functionalism of the cycle, elevating it as the predominant conception to understand intelligence in practice (Marrin 2017). For Johnson (2009) and Phythian (2009), the cycle best explains how intelligence professionals understand their work. It accurately reflects the "professional world of intelligence" (Phythian 2009, 55). Hence, for some scholars, intelligence cooperation is grounded in one or more stages of the intelligence cycle (Westerfield 1996; Johnson 2009; Svendsen 2009a). The practice of intelligence and, by extension, intelligence cooperation, is thus dictated by policy-makers' necessities.

On the other hand, this understanding of intelligence is further reinforced by explaining intelligence cooperation according to threats and American intelligence-driven perspectives. The fight against terrorism is identified as the main cause of change in the practice of intelligence cooperation, which is typified by increased intelligence sharing between intelligence services and police forces and a logic of action where secret services are increasingly oriented at actions, for example enforcing and disruption (Rudner 2004; Svendsen 2009b). This reasoning ontologically places American intelligence as the condition of, and force behind, cooperation but also understands intelligence in the world through the lenses of the American experience (Aldrich 2002; Rudner 2004; Svendsen 2009b).

If this Anglo-Saxon dominant conception of intelligence has been challenged by some of its advocates for not being relevant for examining "intelligence else-

where" (Aldrich and Kasuku 2012; Davies and Gustafson 2013), they have, however, further deepened its main assumptions. They have taken for granted American intelligence as the organizational particularism that explains intelligence in universal terms. In sustaining the focus on secret services (Aldrich and Shiraz 2019), they have not sufficiently paid attention to the differences with other arrangements where services involved in intelligence are not secret services but police services, as seen in many European countries (i.e., France and Spain) and in the EU. They have devalued and downplayed other patterns of intelligence that are not about secret services. Compared to their activities, law enforcement intelligence is viewed as "pedestrian" (Aldrich 2004, 741). Similarly, the EU's cooperation institutions are neither strong nor fast enough to keep up with counter-terrorism activities nor fit for intelligence sharing (Aldrich 2004, 2009a; Walsh 2006). Moreover, they have also approached European intelligence from the perspective of the challenges raised for the main players in intelligence cooperation, for example Britain and the United States (Aldrich 2006; Svendsen 2009b).

Because existing studies have given primacy to a conception of intelligence as country-specific and secret services over one of intelligence as people and practices, they have been unable to see that those who "do" intelligence cooperation are not irremediably spies but state bureaucrats from the Ministry of the Interior, such as border guards, immigration officers or police liaison officers (Bigo, 1996, 2014; Block 2010). When examining intelligence from the perspective of the experiences of the professionals themselves, a different picture emerges, even within IS. Professionals have, indeed, contested the tools that are intended to improve their own performance by understanding differently what IS scholars say constitutes intelligence production (Hulnick, 1986, 2006; Marrin 2017). This echoes a similar contradiction raised by Kearns in his contribution. As he notes, supporting policy-making does not constitute the core work of intelligence analysts. The writings of IS scholars bear the effect of the assumptions of the field, in that they are unable to mobilize the contributions of professionals to shift from a priori definitions to a research line that takes the analysis of practices as the starting point. This analytical neglect is also compounded by the fact that little, if no, dialogue is in place with other studies from the "outside" that are less cited, yet more useful to refocus the lens on Europe and extend intelligence cooperation to law enforcement.

Scholars from EU studies have examined the *effective* role of Europol, and of the EU more generally, in counter-terrorism intelligence (Bures 2008; Argomaniz 2011; Den Boer 2015; Monar 2015). Equally, research on policing has shed light on police liaison officers as central actors in transnational police cooperation (Block 2010; Lemieux 2010; Block and Den Boer 2013). The sociology of policing has, however, gone the deepest in examining police labor in Europe. Building upon ethnographic fieldwork of police liaison officers, Bigo (1996) and Sheptycki (2003, 2011) demonstrate how practices in contact with information-communication technologies and interpersonal solidarities across European police forces enabled and embedded intelligence sharing into a European internal security field.

The present move expands on these sociological investigations to ground the analysis of intelligence cooperation into a line of inquiry that is informed by a Bourdieusian political sociology, one that has remained "outside" IS debates until quite recently (Ben Jaffel 2019, 2020). The sociology of practices and habituses renders a critique of IS's conception of intelligence cooperation possible. This is supported by fieldwork involving thirty-five in-depth interviews conducted between 2014 and 2016 with acting and retired police liaison officers deployed in European capital cities and Europol. As indicated by their areas of expertise that span across the continuum of (in)securities, intelligence cooperation increasingly bears on counter-terrorism and crime control abroad. The analysis of their everyday experiences is helpful for framing two moves that indicate that they have another understanding

of their daily job that is neither about the cycle nor the United States but about crafting cooperation with Europe.

First, exploring the habituses of police liaison officers suggests that intelligence practices and relations abroad are not generated by the functionality of the cycle, let alone by threat perceptions, but through a social process over time and spaces, which is the habitus. The habitus is a system of durable and transposable dispositions that frame schemes of perceptions, appreciations and actions (Bourdieu 1972, 256; 1980, 88). The "practical sense" of liaison officers, that is the way they practice, and understand, intelligence cooperation is acquired through a long process of socialization to cooperation craft and incorporated in their habituses.

What does "doing" intelligence cooperation mean to liaison officers? How do they practice cooperation? Their testimonies do not mention the cycle or assistance to policymakers. Rather, they stress the intricacies that make up intelligence sharing with their counterparts. For liaison officers based in capital cities, most of their time is taken up by processing incoming and outgoing requests for information between home services and host country services (for a similar argument, see also Block 2010). They handle and rank requests on the basis of operational criteria that they define themselves. For instance, requests that are "urgent" are processed first. These are usually related to national security matters, such as counter-terrorism. Their time is also absorbed by constructing and fostering ties with local counterparts. "Small little things," that is routines that are usually neglected by functionalist approaches, are of considerable significance to liaison officers in creating a solid network of contacts and ensuring cooperation is up and running. "When in Rome, do as the Romans do" neatly sums up ways of acting as an "insider." This is not about going native, hence a period of assignment not exceeding four years, but about adjusting to the local customs and way of living of the host country. For instance, it's about going out for a beer in a pub in Britain or having a meal at a restaurant in France.

Second, and in return, in learning the tricks of the trade, liaison officers are able to address their most immediate concerns. Their daily concern is not "policy related intelligence" (Aldrich 2002, 55) but to be "seen" and position themselves vis-à-vis other players. The expansion of intelligence cooperation beyond intelligence services alone has indeed attracted other players such as police forces and EU internal security agencies (for a similar argument, see Bigo 2001), multiplying the routes of communications through which intelligence is exchanged. The corollary is that none of the players have control over all connections overseas. Liaison officers are not a "mandatory" crossing point between countries. Intelligence sharing operates against the background of parallel and concurrent liaisons, in this regard. To make a place for themselves and be "seen" by local counterparts, liaison officers design strategies of distinction by playing out, and framing, their functions in at least two ways.

To the extent that they have *intermediary* positions between home services and local counterparts, liaison officers play a supportive role by "smoothing" the circulation of incoming/outgoing requests in both directions (see also Block 2010). Like switchmen, they help orienting requests to the "right" recipient and contact. They also play a role in exchanging intelligence at speed. The performance of these roles is constructed through the socialization to cooperation craft. As recalled by a French liaison officer posted to London, living as a local has contributed to him being recognized by his counterparts as a "partner": "I didn't come to the United Kingdom to live like a Frenchman in France. I was like an Englishman, and I bought myself a second-hand Jaguar. So, I was identified as an Anglophile and I think it helped me in making a place for myself" (Interview, June 5, 2014). As they are in daily contact with their partners, liaison officers develop their own "who's who," a hands-on knowledge about who is the "right" and "most appropriate" contact to place a *specific* demand to. They develop a "flair" for determining what they can and cannot

request or who they can contact first. Because they acquire competences derived from their experiences on the ground, they claim to share intelligence faster and more effectively than Europol that they label as "slow" and "bureaucratic."

This move indicates that attending to practices generated by the habitus gives a different complexion of what and who constitute intelligence cooperation. It moves away from notions of intelligence that ignore the agency of intelligence professionals and see them as inevitably "replying" to necessities dictated by policymakers to a perspective that emphasizes their daily routines and how they interpret them. The doxa of IS field means that the literature is marked by a discrepancy between practices on the ground and the analytical tools that are said to "understand" them. The next intervention will continue to explore intelligence but where it is not supposed to be, taking intelligence further away from policy making.

Intelligence Cooperation through "Science and Technology" (Sebastian Larsson)

What does it mean to do intelligence, but to call it something else? How is the exchange of secret information and counterterrorism strategies taking place far from traditional intelligence agencies, and instead in the ambiguous social space of "security research"? How are certain carefully framed and technically oriented research collaborations around homeland security representing a novel form of intelligence cooperation, involving not dedicated spies and analysts working under the government, but agency bureaucrats and tech-savvy scientists? As Kreissl (2017) notes, "mission-oriented" security research programs may sometimes work like a "Trojan horse" for silently introducing other forms of collaboration. This third intervention makes the case that applied security research should be seen as a key dimension of contemporary intelligence cooperation—and vice versa.

For this purpose, I draw on the bilateral "science and technology"-agreement between the United States and Sweden in the area of homeland security. Although framed primarily as a "research and development" (R&D) relationship, it was legally designed to be as far-reaching as possible, as an "R&D Plus"-form of cooperation facilitating activities not limited to "science and technology," but also including information sharing, laboratory collaborations, staff exchanges, counterterrorism exercises, and more. In contrast to the controversial transatlantic cooperation involving the Swedish National Defence Radio Establishement (FRA), the NSA, and GCHQ (Eakin 2017), the R&D partnership between Sweden and the Department of Homeland Security (DHS) has remained largely unscrutinized due to its "scientific" appearance.

The Swedish defense minister and the US secretary of homeland security signed the bilateral research agreement in April 2007, to be overseen by the Swedish security agency MSB and the DHS' "Science and Technology Directorate" (DHS S&T), respectively. Since then, DHS has established similar agreements with eleven other countries, and uses them to identify the "strengths" of each country in terms of counterterrorism innovations (Larsson 2019, 113–123). DHS spokespersons were attracted by Sweden's widespread reputation as a "strong innovator" (due in large part to its long history of arms production), and sought to seek out new Swedish technologies for surveillance, border checks, cybersecurity, and particularly CBRN(E) detection (in response to the series of anthrax attacks after 9/11) (Kleja 2007a, 2007b).

The signed R&D agreement states as its objective: ". . . to encourage, develop, and facilitate bilateral Cooperative Activity in science and technology that contributes to the homeland security capabilities of both Parties." More specifically, projects should focus on "the prevention and detection of, response to, and forensics and attribution applied to, terrorist or other homeland security threats and/or indicators" as well as "crisis response and consequence management and mitigation for high-consequence events" (DHS S&T and KBM 2007, 6; see also MSB 2011). The agreement thus conceives of "research" rather narrowly, as what Cox (1981, 103)

calls "problem-solving": applied studies that seek to instrumentally "improve" or "solve" some (security) issue by serving—much like traditional intelligence—as "a guide to tactical actions" for politicians and bureaucrats.

In more detail, the agreement consists of so-called "project arrangements" (PAs). Drafted by US and Swedish agency directors and attorneys, the purpose of PAs is to frame the general practical area wherein research cooperation may be initiated (either now or in the future, since PAs have no end-date). The content of a PA is regarded as "controlled unclassified" information (reviewed and censored before release); however, according to the Swedish agreement director, "there are some project arrangements that "don't exist, that are secret" (Larsson 2019, 117). Together, the PAs constitute the general legal framework for research, testing, and exchange of "information or equipment and material" (up to "top secret" level) in areas like surveillance, counterterrorism, policing, CBRN(E) detection, cybersecurity, and infrastructure protection. Some PAs facilitate professional networks for specific tasks like forensics or lab work, whereas others are far more open-ended and seek to facilitate the "gathering, analyzing, managing, sharing, and protecting [of] information related to all hazards including terrorist threats" (DHS S&T and KBM 2007, 15; Larsson 2019, 118).

As noted, the R&D agreement encourages research that overlaps strongly with security practice. Indeed, the different scientific "products" that are generated (facts, models, systems, data sets, programs) acquire a social and political life as they are designed to immediately leave the scientific field, to "perform a function" elsewhere for security practitioners (Berling 2011, 393–394). Thus, the researchers involved here—like Mills' "abstracted empiricists"—are supposed to "serve whatever ends its bureaucratic clients may have in view" (Mills 2000, 101). They are not urged to work independently; more like conventional intelligence analysts, they must work instrumentally and under strict supervision and "formulate problems out of the troubles and issues that administrators believe they face" (*ibid.*, 96).

Which other practices, that are not strictly defined as "research," are covered by the agreement? Some activities are framed as "reciprocal education and training," "field exercises," and "joint task forces" (DHS S&T and KBM 2007) and have, more specifically, referred to joint terrorism exercises in urban environments; for example, when Swedish first-responders and police trained together with US police and FBI staff in a staged terrorist bombing inside a Stockholm subway station. Other activities are framed as "visits and exchanges" between "technical experts" and "other appropriate personnel" who may make "joint use of laboratory facilities and equipment and material" (DHS S&T and KBM 2007). This refers to how the DHS in fact moved much of its counter-bioterrorism operations to the Defence Research Institute (FOI) in Sweden. In addition to nuclear and radiological testing facilities in underground caverns, Swedish authorities also possess the biological agent of myxomatosis ("rabbit fever"), a highly infectious disease with a deadly effect on humans, which the DHS suspects may become used as a potential bioterrorism weapon (Larsson 2019, 113–123).

In order to harbor these and related forms of collaboration, the legal text is written purposely vague, with so many hypothetical openings that "R&D" is able to mean far more than simply "research." According to MSB attorneys, PAs should work as "open avenues for cooperation" designed not to regulate or restrict but, on the contrary, to stimulate expert exchanges and information sharing. As put by MSB's director, the partnership is seen as "very wide-ranging," as an "R&D plus"-agreement including "that which is not exactly "science" but perhaps more innovation" (*ibid.*, 122). As formulated by the agreement director,

> the idea was an R&D agreement, but we always had in the back of our minds that it was "R&D plus." The core and the foundation is research, which is harmless and nothing to worry about, but "R&D plus" means that we need to have other forms of cooperation … The "plus"-part has been growing over the years. (*Ibid.*)

Agency attorneys admit that phrasings like "cooperation," "collaboration," "includes but is not limited to," and so on, are used precisely because PAs should not be delimited to only "research projects," but again, work more as "practitioner channels": "It is not so much "researcher-to-researcher," but more expert [-exchange] . . . all of this can be covered by the umbrella that is the agreement" (*ibid.*).

In fact, the agreement formalizes the cooperation not only between the DHS S&T and MSB, but between *all security agencies* in the two countries. It is designed more as "gateway," allowing any interested Swedish agency (e.g., security services, police, border guards) to draw out sensitive information and work methods from any DHS agency (e.g., FBI, CIA, FEMA, ICE), and vice versa. MSB spokespersons have sought to actively exploit this function: "We are trying to wipe out this label of an 'S&T deal' that people use, since DHS S&T is merely an entry point in the same way as MSB is [one] here" (*ibid.*, 123). As observed by both Kearns and Ben Jaffel above, we may here too see how contemporary intelligence is about *cooperation*: its gated logic (defending from breaches into national information silos) has shifted to a channeled logic (formalizing networks for transnational information flows).

Bearing in mind the agreement's gateway-function, the highest level of classification for the "information or equipment and material" that may be exchanged in the partnership is "top secret." Elsewhere in the agreement, the notion of "information exchange" is blown up to include all kinds of "practices, laws, regulations, standards, methods, and programs relevant to cooperation" (DHS S&T and KBM 2007, 10). The PA for "countering terrorism . . . within the critical infrastructure protection domain," moreover, makes a staggeringly wide definition of "information":

> *knowledge that can be communicated by any means, regardless of form or type,* including, but not limited to, that of a scientific, technical, business, or financial nature, and also including photographs, reports, manuals, threat data, experimental data, test data, computer software . . . algorithms, designs, specifications, processes, techniques, inventions, drawings, technical writings, sound recordings, pictorial representations, and other graphical presentations, whether in magnetic tape, optical disc, integrated circuitry, computer memory, or any other form and whether or not subject to Intellectual Property rights. (DHS S&T and MSB 2009, 4–5 [emphasis added])

A PA quite strikingly entitled the "Master Information Sharing Arrangement" reinforces this open-endedness by stating that "successful collaboration is dependent on the fullest possible exchange of information" across the "entire range of potential areas of cooperation" (DHS S&T and MSB 2015, 3–4).

In conclusion, this intervention illustrates how security R&D is not "only research," but a messy activity involving a myriad of processes, actors, and interests that in various ways cross into and expand the notion of "intelligence." On the one hand, the US-Swedish agreement represents a novel form of intelligence cooperation by means of its technical orientation. It concerns sharing policing methods, co-developing forensics and detection solutions, visiting testing laboratories, conducting joint counterterrorism exercises; or, more generally, attaining very specific skills and data sets beyond the conventional realm of intelligence. PAs harbor a "new" and technical form of intelligence that informs not governments or secret agents, but the new generation of security practitioners doing counterterrorism and surveillance mainly through technological solutions. On the other hand, due to its channel-function and open-ended phrasings, the agreement may work like a "vessel" for potentially extensive forms of information sharing that may in different ways—either now or in the future—broaden and complement the formal (and more scrutinized) intelligence collaboration involving the NSA and Swedish FRA.

The ambiguous role of "problem-solving" and "mission-driven" research may have serious implications. Whereas the EU's security research program is largely transparent in terms of participants and outcomes, the Swedish-US collaboration is a more secretive arrangement set up in the name of "science and technology." When

a certain practice is framed "scientific," it becomes inscribed with a form of societal acceptance and trustworthiness, making whatever activities taking place in its name difficult to unpack. As Bourdieu explained, science draws heavily on symbolic capital; that is, the ability to create the appearance of "disinterestedness" (Bourdieu 2004, 34; see also Berling 2013, 70–71). Quite contrary to the production of conventional "intelligence knowledge," the production of scientific knowledge must be "based on the obligatory denial of interest," and so security research can be framed as an ascetic exercise "with nothing received in return . . . masking, even from the person who performs it, the ambition of securing a power" (Bourdieu 2004, 53). Thus, to perform intelligence through security research, in the name of "science and technology," is an elusive strategy.

Intelligence Agencies, Internet Users, and Human Rights: Boundaries of the Social Space of Intelligence (Alvina Hoffmann)

We began this article with Snowden, whose spectacular act of resistance profoundly challenged the unhindered and evermore expansive transnational practices of intelligence agencies. This opened up possibilities for other forms of contestation. In this part, I focus on Internet users' claims to their collective rights in legal courts which provides a different perspective on the social space of intelligence and where to locate its contested boundaries. The social space of intelligence aims at colonizing the Internet, and this attempt is limited by actors and (unexpected) alliances between judges, human rights lawyers, digital rights activists and politicians through international law. The second move emphasized the central role of police liaison officers in intelligence, and hence the increasing space of law enforcement in intelligence. Here, we take this legal logic in the opposite direction and show how resistance to the field expansion of intelligence professionals takes place in the case of the Internet. Contrary to the logic of the cycle, the stakes are centered on ensuring human rights on the Internet against intrusive intelligence operations.

At stake is the unequal treatment and application of safeguards toward citizens and foreigners regarding the interception of their data and respect of privacy. As Bigo et al. (2013, 3) note, the ideal solution lies in granting all data subjects the same rights, either by changing US laws or negotiating an international treaty. It is vital to insist on the figure of the data citizen because of the extraterritorial nature of mass surveillance operations and the transnational flow of personal data across international borders (Guild 2019). Data protection and the right to privacy need to be granted through this same extraterritorial logic by means of international human rights law (Cole and Fabbrini 2016).

The Snowden revelations pushed EU institutions toward safeguarding the rights of their citizens that are enshrined in both the European Convention on Human Rights and the EU Charter on Fundamental Rights. Under European law, individuals own their own data. For the purposes of this intervention, I will read the Court of Justice of the EU (CJEU) case—*Maximilian Schrems v. Data Protection Commissioner* (*Schrems I*)—not only as setting standards for delineating boundaries between lawful and unlawful surveillance activities based on principles such as strict necessity and proportionality, or as balancing fundamental rights and national security concerns, but also as steps toward enshrining the legal subject of the data citizen. This is not only important in light of the individual levels of protection that apply in our daily interactions on the Internet. As Bigo et al. (2013, 5) emphasize, "it is the purpose and the scale of surveillance, however, that fundamentally differentiate democratic regimes and police states." Our collective forms of political organization and association are at stake. This is why the fight is now waged by human rights NGOs and data activists, placing themselves firmly as actors to be reckoned with amongst politicians, judges, intelligence professionals and technical experts (*ibid.*, 11).

Mass surveillance programs have collective implications for fundamental rights. There is a shared, almost taken-for-granted notion that the responsibility and solution to these rights violations lie with the individual, encouraged to refrain from sharing personal data and to stay vigilant at every step through the logic of digital hyperindividualism (Bigo, Isin and Ruppert 2019, 5–6). This is no surprise when analyzing the dominant practices centered on individual Internet users: Personalized algorithms, the creation of digital profiles and specifically targeted advertisements transform the experience of being online into an atomized, self-centered event (see Lake 2017 for a discussion of Big Data's hyperindividualist foundational ontology). I contend that claiming human rights on the Internet can be seen as a collective practice through which all Internet users benefit.

What does a conceptual shift from data subject to data citizen entail? Article 4(1) of the GDPR, succeeding the EU Data Protection Directive 95/46, defines the data subject with reference to personal data: "'personal data' means any information relating to an identified or identifiable natural person ('data subject')." (General Data Protection Regulation (GDPR), 2018) Data subjects are granted rights with regards to the controller, which in Article 4(7) is defined as "the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data," while data processors, recipients of processed data and third parties are not included in these legal terms (ibid).

To Guild, the data subject is "the object of state measures to protect the subject's right to privacy" (Guild 2019, 267). It can be seen as one aspect of what it means to be a (data) citizen, putting the onus of protection on the state in processes of data collection, processing and sharing with others. Recognizing data citizens entails enshrining the rights in international law as its central source, meaning that rights claims of data protection and privacy are not limited within a state jurisdiction, where only citizens enjoy this privilege. Following Guild, we can locate the data citizen's practices of rights claims at the intersection between national and international law that gradually transforms the category of data subjects into citizens in this field of struggle, characterized by legal, political and other forms of contestation. This fight mobilizes "the human rights principle of consent to use of personal data," centering the fact of data ownership (*ibid.*). She offers the example of the UN General Assembly resolutions and OHCHR projects concerned with the right to privacy in a digital age that challenges the citizen/foreigner distinction through the language of the universality of human rights and states' human rights obligations (*ibid.*, 276, 282).

Gabrys (2019) describes another account of the data citizen, centered on their practices of data production for the purposes of public knowledge, rather than just being a passive object on whom data is collected. She analyses this through a case-study on monitoring air quality and changing urban environments in southeast London (*ibid.*, 249). The right to data becomes inseparably linked to the right to the city. Reading Guild's and Gabrys' intervention in conversation, we see the many intertwined sources for data citizens and rights, emergent from legislation, court cases and everyday practices. The *Schrems I* case at the CJEU becomes central in this regard, as Maximilian Schrems has been challenging the Irish Data Protection Commissioner and Facebook Ireland as an Austrian national and a Facebook user, hence claiming the right to privacy and data protection not in relation to his own state of Austria. Thus, how can we understand *Schrems I* through the lens of the data citizen, a spokesperson for all Facebook users in the EU and a collective achievement for Internet users? As both the Judgment and the Opinion of the Advocate General show, the implications of the case, based on the evidence of mass surveillance practices, go far beyond the personal effects on Schrems.

The ruling was issued on October 6, 2015 at the CJEU, a landmark case that invalidated the Safe Harbor agreement between the EU and United States from the

year 2000, which allowed unhindered data transfers between the two legal regimes. Max Schrems, a privacy advocate and data rights activist, challenged the transfer of his data, and hence the data transfer of all EU citizens, to Facebook Inc. in the United States via its subsidiary Facebook Ireland. The proceedings began on June 25, 2013 when Schrems issued a complaint to the Data Protection Commissioner in Ireland in which he asked the Commissioner to make use of his investigatory authority to prohibit Facebook Ireland from transferring data to the United States. In light of the Snowden revelations, the Court had to establish whether US law provides for adequate protection of EU citizens' data. The data transfer regime was based on a 2000 decision by the Court that deemed the US data protection regime as "adequate." This prompted the Irish supervisory authority to claim that there was no need to further investigate the complaints. In *Schrems I,* the Court ruled that existing decisions do not cancel investigatory powers of national supervisory authorities. All complaints must be examined with due diligence. In addition, the Court acknowledged the "mass and undifferentiated accessing of personal data" (para. 33), that data subjects have the right to effective legal remedies, and that in all data transfer regimes adequate levels of protection need to be in place that are "essentially equivalent to that guaranteed in the EU legal order" (para. 96). EU citizens have no judicial remedies once their data has been transferred to the United States where the law applies to US citizens only.

How is *Schrems I* more than an individual case? As the Advocate General noted in his observations, it is not about proving specifically how Schrems was affected by mass surveillance activities, or how "he was at imminent risk of grave harm owing to the transfer of data between Facebook Ireland and Facebook USA" (para. 59) (Opinion of Advocate General Delivered on september 23, 2015). Instead, he emphasized the "general and abstract nature" of US surveillance programs (*ibid.*). What is more, in his argumentation, he drew from existing asylum case law (*N.S. and Others)*, in which the Court had previously ruled that no asylum seeker should be transferred to a Member State where they "would face a real risk of being subjected to inhuman or degrading treatment" (para. 103) (ibid). As such, the Advocate General highlighted existing principles under which all Directives and secondary law must be interpreted in light of fundamental rights, not based on conclusive or irrebuttable presumptions (paras. 101, 104) (ibid). The evidence presented shows the "wide-ranging" and "extremely serious interference" with the private data of a "large number of users concerned" (para. 171) (ibid). He further notes that the US intelligence authorities may have access to data transfers that cover "all persons and all means of electronic communication and all the data transferred" without any limitations or exception (para 198) (ibid). Hence, "all persons using electronic communications services" are concerned and there is no need to establish whether or not they actually constitute a potential threat to national security (para. 199) (ibid).

Schrems and other claimants challenging mass surveillance activities are enormously important in taking on seemingly all-powerful and unimpeachable tech companies and intelligence agencies. The Court recognizes this fight as part of a broader movement, highlighting the general implications on all Internet users. After Snowden's revelations, this should be read as part of a new imaginary and set of resistance practices, in which data citizens claim their rights with regards to regional human rights frameworks, not just as citizens of their own country. Safe Harbor has been replaced by Privacy Shield, a new data transfer regime, which shares many of the same shortcomings in which US companies can self-certify whether they have adequate data protection rules in place. Indeed, this agreement has been challenged directly in the CJEU by the French digital rights group *La Quadrature du Net*, linked to a second challenge by Maximilian Schrems contesting standard contractual clauses as a means of transferring data to the United States under the EU GDPR. The logic of inevitability of these data transfer regimes linked with mass

surveillance programs can be disrupted through strategic alliances and contestations through rights claims.

Conclusion

As our four individual interventions moved further away from intelligence as practiced by intelligence officers, we encountered a social space of intelligence that is increasingly intrusive and implicates more and more actors, including all of us as Internet users. We analyzed intelligence as a social practice of "state-making," rather than subservient to the state; intelligence as an everyday practice of law enforcement officers situated in a transnational context; intelligence as it is practiced covertly through transnational science and technology research agreements in the context of Sweden and the United States; and finally how its intrusion is resisted through legal contestation in regional courts. As we conclude this piece, we would like to pose a question that can animate further research in this area, employing some of the tools we used. Leading on from our final intervention, we wonder: Where are the boundaries of the social space of intelligence? How can we make these boundaries visible? As we showed, mobilizing legal resources enabled an alliance between Internet users and activists and judges in regional courts to overthrow political and legal infrastructures that had authorized transnational flows of data between vastly different privacy protection regimes.

We proposed a transdisciplinary research program to study the dynamics of expansion, retreat and contestation that constantly redefine the boundaries of a social space of intelligence. Resistance and contestations are not limited to the legal sphere. Other creative forms of resistance exist, such as facemasks, which limit the operational ability of facial recognition software, or more recently the refusal of some citizens to install a coronavirus digital contact tracing application on their phones. In a sense, this reverses the logic of suspicion that states and intelligence gathering imposed on every citizen and applies it back at the state. Therefore, we produce ourselves and are produced as new kinds of subjects, counter-acting the imagery of subjects of suspicion in surveillance regimes through other possibilities as digital citizens, giving us room for contestation and creativity. As the subjects change, so does the social space of intelligence, which is in need of tools to analyze its reach and transformations. In light of this, we need to ask specific questions: Who has the power to change it and how? Naming the actors and dissecting their central practices of information sharing, withholding and creation, but also ways to resist these practices and break the natural flow are central imperatives. A transdisciplinary lens allows us to change perspectives, make visible logics of cooperation and alliance building, as well as the ongoing transformations, the extent of which is not always immediately grasped. This piece is very much an invitation to think with, and beyond, our interventions.

Acknowledgments

The authors want to thank Didier Bigo, two anonymous peer reviewers, and Kerry Goettlich for their insightful comments on various drafts of this article.

References

Abrams, Philip. 1988. "Notes on the Difficulty of Studying the State." *Journal of Historical Sociology* 1 (1): 58–89.

Aldrich, Richard. 2002. "Dangerous Liaisons: The United States and Intelligence Alliances After 9/11." *Harvard International Review* 17 (1): 135–52.

———. 2004. "Transatlantic Intelligence and Security Co-operation." *International Affairs* 80 (3): 331–55.

———. 2006. "The UK-US Intelligence Alliance in 1975: Economies, Evaluations and Explanations." *Intelligence and National Security* 21 (4): 557–67.

———. 2009a. "US-EU Intelligence Cooperation on Counter-terrorism: Low Politics and Constraint." *British Journal of Politics and International Relations* 11 (1): 122–39.

ALDRICH, RICHARD J., AND JOHN KASUKU. 2012. "Escaping from American Intelligence: Culture, Ethnocentrism and the Anglosphere." *International Affairs* 88 (5): 1009–28.

ALDRICH, RICHARD, AND ZAKIA SHIRAZ. 2019. "Secrecy, Spies and the Global South: Intelligence Studies Beyond the "Five Eyes" Alliance." *International Affairs* 95 (6): 1313–29.

ANDREW, CHRISTOPHER, AND DAVID DILKS, eds. 1984. *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*. Basingstoke: Macmillan.

ARADAU, CLAUDIA. 2017. "Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World." *International Political Sociology* 11 (4): 327–42.

ARGOMANIZ, J. 2011. *Post-9/11 European Union Counter-terrorism: Politics, Polity and Policies*. London: Routledge.

BACHES-TORRES, DANIELA, AND EFREN TORRES-BACHES. 2018. "Intelligence Studies: An Ironic Tale of Politicization, Failure of Imagination, Lack of Collaboration and Exclusion." *Journal of European and American Intelligence Studies* 1 (1): 15–24.

BARKAWI, TARAK. 2011. "From War to Security: Security Studies, the Wider Agenda and the Fate of the Study of War." *Millennium: Journal of International Studies* 39 (3): 701–16.

BAUMAN, ZYGMUNT, DIDIER BIGO, PAULO ESTEVES, ELSPETH GUILD, VIVIENNE JABRI, DAVID LYON, AND R.B.J. WALKER. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44.

BAXTER, CHRISTOPHER, AND KEITH JEFFERY. 2013. "Intelligence and 'Official History'." In *Intelligence Studies in Britain and the US: Historiography since 1945*, edited by Christopher R. Moran and Christopher J. Murphy, 290–305. Edinburgh: Edinburgh University Press.

BEAN, HAMILTON. 2013. "Rhetorical and Critical/Cultural Intelligence Studies." *Intelligence and National Security* 28 (4): 495–519.

———. 2018. "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had." *Intelligence and National Security* 33 (4): 527–40.

BEN JAFFEL, HAGER. 2019. *Anglo-European Intelligence Cooperation: Britain in Europe, Europe in Britain*. London: Routledge.

———. 2020. "Britain's European Connection in Counter-terrorism Intelligence Cooperation: Everyday Practices of Police Liaison Officers." *Intelligence and National Security* (Online first).

BERLING, TRINE VILLUMSEN. 2011. "Science and Securitization: Objectivation, the Authority of the Speaker and Mobilization of Scientific Facts." *Security Dialogue* 42 (4–5): 385–97.

———. 2013. "Knowledges." In *Bourdieu in International Relations: Rethinking Key Concepts in IR*, edited by Rebecca Adler-Nissen. London: Routledge.

BETTS, RICHARD K. 1978. "Analysis, War and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31 (1): 61–89.

BIGO, DIDIER. 1996. *Police en réseaux, l'expérience européenne*. Paris: Presse de Science Po.

———. 2001. "Internal and External Security(ies): The Möbius Ribbon." In *Identities, Borders, Orders: Rethinking International Relations Theory*, edited by David Jacobsen, Mathias Albert, and Lapid Yosef, 91–116. Minneapolis: University of Minnesota Press.

———. 2014. "The (In)securitization Practices of the Three Universes of EU Border Control: Military/Navy—Border Guards/Police—Database Analysts." *Security Dialogue* 45 (3): 209–25.

———. 2016. "Rethinking Security at the Crossroad of International Relations and Criminology." *British Journal of Criminology* 56 (6): 1068–86.

———. 2019. "Shared Secrecy in a Digital Age and a Transnational World." *Intelligence and National Security* 34 (3): 379–94.

BIGO, DIDIER, SERGIO CARRERA, NICHOLAS HERNANZ, JULIEN JEANDESBOZ, JOANNA PARKIN, FRANCESCO RAGAZZI, AND AMANDINE SCHERRER. 2013. "Mass Surveillance of Personal Data By EU Member States and Its Compatibility with EU Law." CEPS Paper in Liberty and Security in Europe, no. 61.

BIGO, DIDIER, ENGIN ISIN, AND EVELYN RUPPERT, eds. 2019. *Data Politics: Worlds, Subjects, Rights*. London: Routledge

BLOCK, LUDO. 2010. "Bilateral Police Liaison Officers: Practices and European Policy." *Journal of Contemporary European Research* 6 (2): 194–210.

BLOCK, LUDO, AND MONICA DEN BOER. 2013. *Liaison Officers: Essential Actors in Transnational Policing*. The Hague: Eleven International Publishing.

BOURDIEU, PIERRE. 1972. *Esquisse d'une théorie de la pratique*. Genève: Edition Droz.

———. 1980. *Le sens pratique*. Paris: Les éditions de minuit.
———. 2004. *Science of Science and Reflexivity*. Chicago: University of Chicago Press.
Bourdieu, Pierre, and Loïc J.D. Wacquant. 1992. *An Invitation to Reflexive Sociology*. Cambridge: Polity Press.
Breakspear, Alan. 2013. "A New Definition of Intelligence." *Intelligence and National Security* 28 (5): 678–93.
Bures, Oldric. 2008. "Europol's Fledging Counterterrorism Role." *Terrorism and Political Violence* 20 (4): 498–517.
Cole, David, and Federico Fabbrini. 2016. "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders." *International Journal of Constitutional Law* 14 (1): 220–37.
Cox, Robert W. 1981. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millennium: Journal of International Studies* 10 (2): 126–55.
Dahl, Erik J. 2013. "Why Won't They Listen? Comparing Receptivity Toward Intelligence At Pearl Harbour and Midway." *Intelligence and National Security* 28 (1): 68–90.
Davies, Philip H, J. 2006. "Assessment BASE: Simulating National Intelligence Assessment in a Graduate Course." *International Journal of Intelligence and CounterIntelligence* 19 (4): 721–36.
Davies, Philip H.J., and Kristian Gustafson, ed. 2013. *Intelligence Elsewhere: Spies and Espionage outside the Anglosphere*. Washington DC: Georgetown University Press.
Den Boer, Monica. 2015. "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis." *Intelligence and National Security* 30 (2–3): 402–19.
De Werd, Peter. 2018. "Critical Intelligence Studies? A Contribution." *Journal of European and American Intelligence Studies* 1 (1): 109–48.
DHS S&T and KBM. 2007. "Agreement on Cooperation in Science and Technology for Homeland Security Matters." *Swedish Civil Contingencies Agency*.
DHS S&T and MSB. 2009. "PA 009–2009 Critical Infrastructure Protection." *Swedish Civil Contingencies Agency*.
———. 2015. "PA 021–2015 Master Information Sharing Arrangement." *Swedish Civil Contingencies Agency*.
Eakin, Hugh. 2017. "The Swedish Kings of Cyberwar." *New York Review of Book*s, January issue.
Ehrman, John. 2009. "What Are We Talking about When We Talk About Counterintelligence?" *Studies in Intelligence* 53 (2): 5–20.
Foley, Frank. 2013. *Counter Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past*. Cambridge: Cambridge University Press.
Gabrys, Jennifer. 2019. "Data Citizens: How to Reinvent Rights." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert. London: Routledge.
General Data Protection Regulation (GDPR). 2018. Accessed July 20, 2020, https://gdpr-info.eu/.
Gill, Peter. 2010. "Theories of Intelligence." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 43–58. Oxford: Oxford University Press.
———. 2019. "Explaining Intelligence Failure: Rethinking the Recent Terrorist Attacks in Europe." *International Journal of Intelligence and CounterIntelligence* 33 (1): 43–67.
Gill, Peter, and Mark Phythian. 2016. "What Is Intelligence Studies?" *The International Journal of Intelligence, Security, and Public Affairs* 18 (1): 5–19.
———. 2018. "Developing Intelligence Theory." *Intelligence and National Security* 33 (4): 467–71.
Glees, Anthony. 2015. "Intelligence Studies, Universities and Security." *British Journal of Educational Studies* 63 (3): 281–310.
Goodman, Michael S. 2007. "Studying and Teaching about Intelligence: The Approach in the United Kingdom." *Studies in Intelligence* 50 (2): 57–65.
Guild, Elspeth. 2019. "Data Rights: Claiming Privacy Rights Through International Institutions." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert. London: Routledge
Guzzini, Stefano. 2016. "International Political Sociology, Or: The Social Ontology and Power Politics of Process." *DIIS Working Paper* 6: 1–13.
Hammond, Thomas. 2010. "Intelligence Organisation and the Organisation of Intelligence." *International Journal of Intelligence and Counterintelligence* 23 (4): 680–724.
Hay, Colin. 2014. "Neither Real Nor Fictitious But "as If Real"? A Political Ontology of the State." *The British Journal of Sociology* 65 (3): 459–80.
Hillebrand, Claudia, and R. Gerald Hughes. 2017. "The Quest for a Theory of Intelligence." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael S. Goodman, 1–24. London: Palgrave.

HULNICK, ARTHUR S. 1986. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach." *Intelligence and National Security* 1 (2): 212–33.
———. 2006. "What's Wrong with the Intelligence Cycle?" *Intelligence and National Security* 21 (6): 959–79.
IMMERMAN, RICHARD H. 2008. "Intelligence and Strategy: Historicizing Psychology, Policy and Politics." *Diplomatic History* 32 (1): 1–23.
JENSEN, MARK A. 2012. "Intelligence Failures: What Are They Really and What Do We Do About Them?" *Intelligence and National Security* 27 (2): 261–82.
JOHNSON, LOCK K. 2009. "Sketches For a Theory of Strategic Intelligence." In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 33–53. London: Routledge.
JOINT INTELLIGENCE COMMITTEE. 2003. "Iraq: The Emerging View from Baghdad." *The Iraq Inquiry*, February 29. Accessed July 20, 2004, http://www.iraqinquiry.org.uk/the-evidence/declassified-documents.
JUDGMENT OF THE COURT (GRAND CHAMBER) OF OCTOBER 6, 2015. "Maximillian Schrems v Data Protection Commissioner." C-362/14. EU:C:2015:650.
KENT, SHERMAN. 1955. "The Need for an Intelligence Literature." *Studies in Intelligence* 1 (1): 1–11.
KHAN, DAVID. 2008. "Intelligence Studies on the Continent." *Intelligence and National Security* 23 (2): 249–75.
KLEJA, MONICA. 2007a. "Michael Mohr—vår Säkerhetskontakt i Washington." *Ny Teknik*, August 28.
———. 2007b. "Sverige Hjälper USA Med Terrorforskning." *Ny Teknik*, February 27.
KREISSL, REINHARD. 2017. "Predicaments of Policy-Oriented Security Research." *OpenDemocracy*. Accessed January 20, 2017, www.opendemocracy.net/reinhard-kreissl/predicaments-of-policy-oriented-security-research.
KUHNS, WOODROW. 2003. "Intelligence Failures: Forecasting and the Lessons of Epistemology." In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, edited by Richard Betts and Thomas Mahnken, 80–100. London: Frank Cass.
LAKE, ROBERT W. 2017. "Big Data, Urban Governance, and the Ontological Politics of Hyperindividualism." *Big Data & Society* January–June: 1–10.
LARSSON, SEBASTIAN. 2017. "A First Line of Defence? Vigilant Surveillance, Participatory Policing and the Reporting of "Suspicious" Activity." *Surveillance & Society* 15 (1): 94–107.
———. 2019. *In the Name of Society: The Branding of Swedish Civil Security Technologies and Their Exclusionary Effects*. PhD Thesis, King's College London.
LEMIEUX, FREDERIC, ed. 2010. *International Police Cooperation: Emerging Issues, Theory and Practice*. London: William Publishing.
LOUGHLAN, VICTORIA, CHRISTIAN OLSSON, AND PEER SCHOUTEN. 2014. "Mapping." In *Critical Security Methods: New Frameworks for Analysis*, edited by Claudia Aradau, Jef Huysmans, Andrew Neal, and Nadine Voelkner. Hoboken: Taylor and Francis.
MARRIN, STEPHEN. 2004. "Preventing Intelligence Failure By Learning from the Past." *International Journal of Intelligence and CounterIntelligence* 17 (4): 655–72.
———. 2008. "Intelligence Analysis and Decision-making: Methodological Challenges." In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 131–50. London: Routledge.
———. 2016. "Improving Intelligence Studies As an Academic Discipline." *Intelligence and National Security* 31 (2): 266–79.
———. 2017. "Why Strategic Intelligence Analysis Has Limited Influence on American Foreign Policy." *Intelligence and National Security* 32 (7): 725–42.
———. 2018. "Evaluating Intelligence Theories: Current State of Play." *Intelligence and National Security* 33 (4): 479–90.
MARTIN, ALEX, AND PETER WILSON. 2008. "The Value of Non-Governmental Intelligence: Widening the Field." *Intelligence and National Security* 23 (6): 767–76.
MILLS, C. WRIGHT. 2000. *The Sociological Imagination*. Oxford: Oxford University Press.
MONAR, JÖRG. 2015. "The EU as an International Counter-terrorism Actor: Progress and Constraints." *Intelligence and National Security* 30 (2–3): 333–56.
MORKEVIČIUS, VALERIE. 2015. "Power and Order: The Shared Logics of Realism and Just War Theory." *International Studies Quarterly* 59 (1): 11–22.
MSB. 2011. "Sverige Och USA: Gränsöverskridande Risker Och Gemensamma Lösningar." *Swedish Civil Contingencies Agency*.
NBC. 2014. "Edward Snowden's Motive Revealed: He Can 'Sleep At Night.'" *NBC News*, May 28. Accessed June 20, 2017, https://www.nbcnews.com/feature/edward-snowden-interview/edward-snowdens-motive-revealed-he-can-sleep-night-n116851.
OPINION OF ADVOCATE GENERAL DELIVERED ON SEPTEMBER 23, 2015. Case C-362 /14.

Painter, Joe. 2006. "Prosaic Geographies of Stateness." *Political Geography* 25 (7): 752–74.

Pastorello, Mauro, and Marianna Testa. 2017. "Intelligence Failures: Between Theories and Case Studies." *Sicurezza, Terrorismo e Società* 5 (1): 49–68.

Petersen, Karen Lund, and Vibeke Schou Tjalve. 2013. "(Neo) Republican Security Governance? US Homeland Security and the Politics of 'Shared Responsibility'." *International Political Sociology* 7 (1): 1–18.

———. 2018. "Intelligence Expertise in the Age of Information Sharing: Public–Private "Collection" and Its Challenges to Democratic Control and Accountability." *Intelligence and National Security* 33 (1): 21–35.

Phythian, Mark. 2009. "Intelligence Theory and Theories of International Relations: Shared World Or Separate Worlds?" In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 55–72. Abingdon: Routledge.

Raschi, Francesco, and Lorenzo Zambernardi. 2018. "Was Anybody Ever a Realist? A Sceptical View on the Distinction Between Political Realism and Liberalism." *History of European Ideas* 44 (3): 370–83.

Roberts, Patrick S., and Robert P Saldin. 2016. "Why Presidents Sometimes Do Not Use Intelligence Information." *Political Science Quarterly* 131 (4): 779–802.

Rudner, Martin. 2004. "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism." *International Journal of Intelligence and Counterintelligence* 17 (2): 193–230.

Scott, Len, and Peter Jackson. 2004. "The Study of Intelligence in Theory and Practice." *Intelligence and National Security* 19 (2): 139–69.

Shelton, Allison M. 2014. "Teaching Analysis: Simulation Strategies in the Intelligence Studies Classroom." *Intelligence and National Security* 29 (2): 262–81.

Sheptycki, James. 2003. *In Search of Transnational Policing: Towards a Sociology of Global Policing*. London: Ashgate.

———. 2011. *Transnational Crime and Policing: Selected Essays*. London: Routledge.

Stout, Mark, and Michael Warner. 2018. "Intelligence is As Intelligence Does." *Intelligence and National Security* 33 (4): 517–26.

Svendsen, Adam. 2008. "The Globalization of Intelligence Since 9/11: The Optimization of Intelligence Liaison Arrangements." *International Journal of Intelligence and CounterIntelligence* 21 (4): 661–78.

———. 2009a. "Connecting Intelligence and Theory: Intelligence Liaison and International Relations." *Intelligence and National Security* 24 (5): 700–29.

———. 2009b. *Intelligence Cooperation and The War on Terror: Anglo-American Security Relations after 9/11*. London: Routledge.

Treverton, Gregory F. 2018. "Theory and Practice." *Intelligence and National Security* 33 (4): 472–8.

Van Puyvelde, Damien, and Sean Curtis. 2016. "'Standing on the Shoulders of Giants': Diversity and Scholarship in Intelligence Studies." *Intelligence and National Security* 31 (7): 1040–54.

Walker, R.B.J. 2016. "Only Connect: International, Political, Sociology." In *International Political Sociology: Transversal Lines*, edited by Tugba Basaran, Didier Bigo, Emmanuel-Pierre Guittet, and R.B.J. Walker. London: Routledge.

Walsh, James. 2006. "Intelligence Sharing in the European Union: Institutions Are Not Enough." *Journal of Common Market Studies* 44 (3): 625–43.

Warner, Michael. 2012. "Fragile and Provocative: Notes on Secrecy and Intelligence." *Intelligence and National Security* 27 (2): 223–40.

Westerfield, Bradford. 1996. "America and the World of Intelligence Liaison." *Intelligence and National Security* 11 (3): 523–60.