Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society

Petersen, Karen Lund; Rønn, Kira Vrist

Published in:
Intelligence and National Security

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Petersen, K. L., & Rønn, K. V. (2019). Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society. Intelligence and National Security, 34(3), 311-16.

Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society

Karen Lund Petersen & Kira Vrist Rønn

To cite this article: Karen Lund Petersen & Kira Vrist Rønn (2019) Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society, Intelligence and National Security, 34:3, 311-316, DOI: 10.1080/02684527.2019.1553365

To link to this article: https://doi.org/10.1080/02684527.2019.1553365

Published online: 12 Feb 2019.

INTELLIGENCE AND NATIONAL SECURITY
2019, VOL. 34, NO. 3, 311–316
https://doi.org/10.1080/02684527.2019.1553365

Routledge
Taylor & Francis Group

INTRODUCTION

Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society

Karen Lund Petersen and Kira Vrist Rønn

ABSTRACT

This special issue is based on the observation that today's intelligence services stand before a difficult task of, on the one hand, having to manage the uncertainties associated with new threats by inviting civil actors in to help, while also, on the other hand, having to uphold their own institutional authority and responsibility to act in the interest of the nation. In balancing this task, we show how today's intelligence practices constantly contests the frontiers between normal politics and security politics and between civil society and the state. In this introduction we argue that these changes can be observed at three different levels. One is at the level of managerial practices of intelligence collection and communication; another is in the increased use of new forms of data, i.e. of social media information; and a third is the expansion of intelligence practices into new areas of concern, e.g. cybersecurity and the policing of (mis-) information.

Complex and uncertain threat environments, with terrorism, cybersecurity and global financial crisis, have made many traditional management tools unfit and profoundly transformed the ways in which intelligence services deal with threats to the nation and its citizens. In this special issue, we argue that intelligence agencies today stand before a defining gap between an increasing demand from society and politicians to provide security and the organization's ability to fulfil those demands and needs. In order to manage this gap between expectations and possibilities for management, new methods, coalitions and partnerships are considered pertinent.

These practices include the use of new technologies for collection and analysis as well as arrangements to increase cooperation and partnerships between national and foreign intelligence and security services, between intelligence and police services, between intelligence and security services and the public, and between intelligence and private companies and 'other potentially uneasy bedfellows'.[1] While these practices help to manage the gap and thus meet public expectations, they also confront and challenge a long-established role of intelligence agencies in society: as institutions which are able to make well-informed judgements and decisions on how to protect national interests.

The engagement of new methods might seem an unavoidable consequence of having to meet new challenges and manage uncertainty; however, some of these methods challenge both our vision of democracy and privacy and the organizational identity of the services. The organizational identity is challenged by the inclusion of new partnerships and collaborations. Almost paradoxically the intelligence services need on the one hand to manage uncertainties and in the course of that to invite new actors in to help, while they also need to assume authority and responsibility to act in the interest of national security. This organizational reality, the articles in this special issue argue,

CONTACT Karen Lund Petersen klp@ifs.ku.dk

creates not only new managerial concerns but – and far more importantly – it also challenges our most fundamental democratic values, namely freedom and protection.

The articles in this special issue analyse this new role of intelligence services and show how today's management practices and alliances contest the frontiers between normal politics and security politics and between civil society and the state. As Rune Saugmann Andersen argues in his analysis of the intelligence use of amateur photographs, images taken by civilians are increasingly turned into military imagery and used for the purpose of conceptualizing conflicts zones. Yet, in doing so, the 'normality' associated with that of taking private photos and sharing these on social media becomes an object of security politics. Thereby, security comes to invade the very idea of 'citizenry' and privacy. In similar terms, Adam Diderichsen shows how intelligence work has come to define core tasks in what we used to think of as 'normal' bureaucratic governmental institutions, challenging the bureaucratic logic of governmental agencies.

In a broad perspective, this special issue raises the most intrusive question of them all: namely what role intelligence services have or should have in a globalized democratic society, where threats are hard to pin down and manage by normal means of control and where new means of control are deemed necessary. In the words of Didier Bigo, we ask, 'What happens when intelligence services are demonopolized?'

The de-monopolizing of intelligence practices

Within the larger aim of understanding current attempts to demonopolize intelligence, the articles especially focus on three dimensions. First, the managerial practices of intelligence collection and communication and how those new practices redefine the role of the public in security affairs and affect the management structures and the organizational identity of intelligence services. Second, how the performance of different forms of data mining, i.e. of social media information, challenges fundamental rights of citizens – e.g. the right to privacy – both nationally and globally. Third, the expansion of intelligence practices into new areas of concern, e.g. cybersecurity and the policing of (mis-) information in the context of the EU.

The term 'civil society' is generally applied in a broad sense, as a gathering of concepts of non-state actors, including individuals, groups and private companies. While 'the public' has similar connotations, traditionally referring to the role of individual citizens in the national political community, the articles also show that the concept of public becomes more blurry when addressing new types of security threats. Accordingly, Christensen and Liebetrau argue that when it comes to cybersecurity 'it becomes much more opaque who has a right to security and a legitimate say in holding those responsible to account'. Hence, a main aim of the issue is to flesh out and question how the public is currently being put into play in new and different ways in the context of security. Later, we will specify the three dimensions/themes and group the articles under the following sections.

New practices of communication and intelligence collection

The first theme concerns the communication between intelligence services and the wider public. Communication is here understood as a way to cope with pressing public and political expectations and thus a way to *manage management* that prescribes certain roles for the public. Two articles address the issues of organizational identity of intelligence services by discussing how new forms and means of communication render the public active actors in the identification and collection of intelligence. This inclusion of the public raises some new democratic and managerial dilemmas.

In her article 'Three concepts of intelligence communication: awareness, advice or coproduction', Petersen shows how the role of communication vis-à-vis the public has changed from being primarily concerned with creating awareness and advice to that of finding an institutional form that supports communication for the purpose of co-production. This change, she argues, assigns an

active role to the public where they are made co-responsible for identifying security threats and risks to society. Hence, Petersen argues that this communication strategy functions as a way to manage the uncertain threat and risk environment facing society and the intelligence services as such. Hence, including the public in the reply to the often illusory public demand for security in an absolute sense can be viewed as a legitimacy-enhancing endeavour on the part of the services. By navigating the complexity facing the services via increased public inclusion, the services seem to manage the 'performativity gap' which arises when organizations face complex, if not impossible, tasks such as the management of current security risks and uncertainties on one hand and the political and public demands for (absolute) security on the other hand.

Co-production of intelligence is likewise a keyword in the article 'From madness to wisdom: intelligence and the digital crowd'. In this piece, Cavelty and Jaeger scrutinize how crowd sourcing increasingly becomes a crucial part of intelligence practices. They understand crowd sourcing as an element of the Big Data wave influencing an ever-increasing range of societal functions, and they argue that the inclusion of the crowd raises new types of question concerning how voluntary and involuntary security communication is changing the relationship between intelligence agencies and the public due especially to Internet and Communication Technologies (ICT). The authors argue that whereas the crowd was previously something to be neutralized and controlled, the crowd increasingly participates in the coproduction of security and of a resilient society. This new endeavour and role of the crowd raises new dilemmas such as increased inclusion of privately owned and designed social media platforms in security governance. Hence, the privately mediated information from and on the crowd potentially creates conflicting interests between the ICT companies, the intelligence services and the public.

Social media, the Internet and privacy

A second group of articles study how the mere idea of 'privacy' is challenged in a world where new technologies allow for a different engagement with citizens. Thus, by considering the frontiers between public and private in the current security landscape, we also hint to the emerging discussions concerning ownership, control, access and exploitation of personal information and photos on social media platforms in the name of security and public safety. Hence, the importance of open sources and information from social media is increasing rendering discussions on the nature and exploitation of such information pertinent.

Saugmann Andersen argues in his article 'Open-source intelligence and individual security' that photos taken in conflict and war zones by citizens are extensively exploited by intelligence services via social media platforms. He argues that the use of such images 'changes not only media practices and the representation of conflict, but are increasingly part of the logics of conflict itself'. Furthermore, this undertaking potentially turns citizens into active actors in a specific conflict. Along with this usage of online amateur photos in conflicts, the citizens providing such images unwillingly become endangered, since the photos can be tracked back to the specific individuals by digital traces. Saugmann Andersen explores how open-source intelligence was used in the context of investigating the downing of MH17 over eastern Ukraine and argues that this investigation relied heavily on citizens' images. Saugmann Andersen concludes that this new tendency 'creates a new kind of individual security dilemma in which citizens are endangered if they voice everyday concerns visually because the digital traces of their everyday visual practices are appropriated by conflict actors.'

In line with the paper by Saugmann Andersen, Rønn and Søe argue in their article 'Is social media intelligence private?' that the exploitation of social media information in the name of security and public safety is often regarded as unproblematic by the services themselves, since the majority of such information is publicly available. In this article, Rønn and Søe however argue against this claim also reflected by Omand, Bartlett and Miller (2012) stating that openly available SOCMINT is non-intrusive. Social media platforms are similar to public spaces; however, this in the

view of the authors does not mean that governmental bodies should randomly access such information in order to provide societal security and public safety. The authors argue that the concept of privacy is somewhat unfit for the context of social media due to difficulties concerning control over information and the flaws concerning an adequate concept of informed consent. Hence, the authors argue that systematic exploitation of social media platforms potentially creates a negative chilling effect where citizens will avoid certain types of communication via such platforms due to the fear of being watched. Thus, Rønn and Søe conclude that the services should take the democratic virtues (freedom of speech and expression) rendered possible by social media platforms into account before randomly exploiting information from such platforms.

On the practice of data mining in the context of intelligence, Bigo likewise provides a comprehensive and thought-provoking analysis of the logics embedded in the cross-national sharing of secret information, especially between national SIGINT bodies. Bigo argues that 'marginal' digital behaviour often becomes the marker for suspicion for the intelligence services and the warrant for the inclusion of individuals on lists which are shared between a large number of security authorities worldwide. Bigo calls this phenomenon a 'mass production of "shared secrets"'. He further argues that a range of challenges arise in the wake of such sharing of secret digital information, which is further boosted by this cross-national sharing of such information. First of all, the individuals have no right to know why they are included in such lists and thus why they became suspects, which in his words 'creates a problem regarding the rule of Law and democratic principles, and suppose new discussions about the boundaries between secrecy, security, publicity and scrutiny.' Secondly, the cross-national sharing of secret SIGINT leads to a destabilizing of the dichotomies 'public and private, internal and foreign, shared and (national) secret distinctions.' Bigo calls for further attention on the fact that the increased sharing of secrets between states, leads to a new type of global suspicion where individuals can also be followed worldwide via digital traces, due to 'marginal digital behaviour' and this, Bigo argues, creates new challenges regarding the legal certainty concerning these individuals.

New conceptual practices: intelligence, misinformation and cybersecurity

The third and final group of articles look at how new conceptual developments work to establish an identity of security management within the intelligence services, which enforces old structures of secrecy and authority in a range of new domains, which challenge those same structures of knowledge and fundamentally redefines the mere meaning of the public. Hence, this part of the issue is organized around a concern about what happens when the traditional area of expertise of intelligence services expands and furthermore what happens when fundamental democratic conventions are challenged by seemingly new security needs.

The traditional notion that some intelligence work is 'inherently governmental' is more challenged now than ever. As Petersen and Tjalve state, even 'the collection of intelligence has drifted outside the purview of the agencies themselves'.[2] New actors such as partners in banks, industry, social institutions, hospitals, prison guards and citizens are main players in the intelligence context. Hence, the relationship between the state and civil society is radically different now and this is especially obvious in the context of cybersecurity where the public/private dependency is somewhat turned around.

In the article 'A new role for "the public"?', Christensen and Liebetrau argue that the relationship between state and civil society, i.e. private companies, is not simply characterized by 'mutual cooperation and mutual benefit'. On the contrary, the state is becoming more and more dependent on the companies and their willingness to inform, cooperate, etc. Furthermore, companies are not, like most intelligence services, delimited by national borders and often they may simply consult cooperate security departments instead of state security agencies when they face security challenges. In the article, Christensen and Liebetrau introduce some of the new challenges related to accountability and oversight in the context of cybersecurity. Applying WannaCry as the starting

point for discussions, they argue that 'the public' in the case of cybersecurity cannot be neatly defined in terms of 'a national political community'. Furthermore, they argue that who has a right to security and a legitimate say in holding those responsible to account becomes much more opaque in the context of cybersecurity. They call for a redefinition of 'security publics' in the context of cybersecurity, since these publics become more context sensitive and in-flux in the case of cybersecurity. This fact affects the notion of whom intelligence services are accountable towards and to some degree also the task of identifying responsible and accountable actors in the case of cybersecurity.

The second article in this part of the issue is titled 'Spreading intelligence', and here Diderichsen addresses another context where traditional intelligence practices are changing. Diderichsen argues that by increasingly applying the concept 'intelligence' to, for example, policing, public administration or risk management, the institutions adhere to what could be termed a specific 'intelligence' or 'adversarial logic', where the presence of an enemy is presumed. The general endorsement and spreading of intelligence could intuitively be understood as unproblematic since it simply reflects an urge to be increasingly knowledge-based. Diderichsen, however, argues that more is at risk in the spreading of intelligence, and his analysis shows that the adoption of intelligence in traditional non-intelligence practices entails a problematic transformation in the nature of 'the social relationships founded in and by these various institutions', for example, in the presumption of an enemy instead of a client, a colleague, a citizen, etc.

Finally, in the article 'Deferring substance', Ördén provides a comprehensive analysis of EU policies addressing so-called 'information threats'. Such threats are understood as threats from misinformation and fake news and in the article Ördén argues that it is not clear what the subject of these policies are – that is – who is considered relevant for protection and against what? Furthermore, the article shows how intelligence and security practices of the EU are expanding into new areas not previously understood as in need of protection by EU bodies. Hence, in this sense Ördén scrutinizes how 'information threats' are being *securitized* and considered as an urgent issue of EU security policies even though the main concepts – information threats, security etc. – are unclear and diverging in the chosen EU policies. The complexity of the threat spelled out by Ördén in her search for a 'referent object of security' in current EU policies addressing 'information threats' seems to suggest that there is no clear understanding of what security means in this regard and thus neither of who and what should be protected and by whom.

Generally, this special issue seeks to create a stronger dialogue between intelligence and security studies; two disciplines which increasingly share readers. In security studies, many of the security practices we have just described have been captured by the term 'management of unease' – describing a seeping spread of the security logic to the everyday risk practices of bureaucracies, governmental agencies and companies.[3] Where security traditionally was considered an exception to the law, today's politics of 'resilience' seem to rewrite or even suspend the difference between 'normal politics' and 'security politics' – between war and peace – altogether. This development is in many ways troubling as it fundamentally calls into question the classical understanding of the sovereign state as the guarantor of security and thereby individual freedom (cf. Skinner 1989). By bringing this perspective into intelligence studies, we aim and hope to spur a wider debate about the role of intelligence services in society; a debate on managerial realities that are co-constitutive of our wider society and its values.

Notes

1. Richards, "Intelligence Dilemma," 773; Aldrich, "Global Intelligence"; Petersen & Tjalve, "Intelligence Expertice"; and Petersen, *Coporate Risk*.
2. Petersen and Tjalve, "Intelligence Expertice," 23.
3. Huysmans, *The Politics of Insecurity*; Bigo, "Globalized In-Security" & "Liason Officers in Europe"; Neal, "Normalization and Legislative Exceptionalism"; and Petersen & Tjalve, "(Neo)Republican Security Governance".

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Karen Lund Petersen is Professor (with special responsibilities) at the University of Copenhagen and Director of the Centre for Advanced Security Theory. Her primary research interests are security and risk governance, with a particular focus on political risk, corporate security management and intelligence. As member of the so-called Copenhagen School within security studies, she has furthermore contributed to the debate on securitization and widened concept of security. Among her most recent publications are 'Intelligence expertise in the age of information sharing', *Intelligence and National Security* 2017, and 'Private–public partnerships on cyber-security: a practice of loyalty?', *International Affairs* 2017.

Kira Vrist Rønn, PhD, is Lecturer at the University College Copenhagen and her primary research interests concern policing and security studies.

Bibliography

Aldrich, R. "Global Intelligence Co-Operation versus Accountability: New Facets to an Old Problem." *Intelligence and National Security* 24/1 (2009): 26–56. doi:10.1080/02684520902756812.

Bigo, D. "Liaison Officers in Europe: New Officers in the European Security Field." In *Transnational Policing*, edited by J. W. E. Scheptycki, 67–99. London and New York: Routledge, 2000.

Bigo, D. "Globalized-In-Security: The Field and the Ban-Opticon." In *Translation, Biopolitics, Colonial Difference*, edited by N. Sakai and J. Solomon, 109–156. Hong Kong: University of Hong Kong Press, 2006.

Huysmans, J. *The Politics of Insecurity. Fear, Migration and Asylum in the EU*. London: Routledge, 2006.

Neal, A. W. "Normalization and Legislative Exceptionalism: Counterterrorist Lawmaking and the Changing Times of Security Emergencies." *International Political Sociology* 6, no. 3 (2012): 260–276. doi:10.1111/j.1749-5687.2012.00163.x.

Petersen, K. L. *Corporate Risk and National Security Redefined*. London: Routledge, 2012.

Petersen, K. L., and V. Schou Tjalve. "Intelligence Expertise in an Age of Information Sharing: Public-Private "Collection" and Its Challenges to Democratic Control and Accountability." *Intelligence and National Security* 33/1 (2018): 21–35. doi:10.1080/02684527.2017.1316956.

Petersen, K. L., and V. S. Tjalve. "(Neo)Republican Security Governance? US Homeland Security and the Politics of "Shared Responsibility"." *International Political Sociology* 7, no. 1 (2013): 1–18. doi:10.1111/ips.12006.

Richards, J. "Intelligence Dilemma? Contemporary Counterterrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (2012): 761–780. doi:10.1080/02684527.2012.708528.