Selected Papers of AoIR 2016:
The 17th Annual Conference of the
Association of Internet Researchers
Berlin, Germany / 5-8 October 2016

FROM THE 'FIVE EYES' TO THE 'SIGINT SENIORS EUROPE': THE INTELLIGENCE COMMUNITY AS A TRANSNATIONAL FIELD

Ronja Kniep
WZB Berlin Social Science Center

Introduction

Technology and the practices of intelligence agencies have long been closely intertwined. During World War II, the intelligence community encouraged the invention of computers in its effort to decrypt and access the communications of foreign enemy states (Corera, 2015). It was out of this effort that the intelligence alliance 'UKUSA' between the US-American and the British intelligence services was born as early as in 1943. Today, this alliance forms the so-called 'Five Eyes' together with the foreign intelligence agencies of Canada, Australia and New Zealand, who joined the circle of the National Security Agency' s (NSA) 'second party partners' shortly after in 1946.

Until today, the core of this agreement has been the development of signals intelligence (SIGINT) capabilities, i.e. the process of accessing, collecting and analysing of electronically transmitted communications. During the period of the Cold War, Western security actors wished to more efficiently surveil the Soviet Union. Hence , around 1982, another multilateral intelligence alliance was formalised which exists until today: a secret club called the 'SIGINT Seniors Europe' (SSEUR) (cf. Rosenbach & Stark, 2014, p. 366). This multilateral network is comprised of the 'Five Eyes' and a selection of European intelligence agencies. The series of internal NSA documents that has been published since 2013 has revealed the identity of the SSEUR's member states[1]. The documents also offer insights into the interaction, the institutional setting and the practices of the highly secretive SIGINT community and they inform about the modalities of bi- and multilateral intelligence alliances.

I examine these SIGINT alliances with a focus on the SSEUR and I interpret the findings with regard to the nexus of technology and transnational intelligence communities. The paper makes a conceptual and an empirical contribution to recent

[1]'SSEUR members are the Five Eyes nations (Australia, Canada, New Zealand, United Kingdom and United States) and the following Third Party partners: Belgium, Denmark, France, Germany, Italy; Netherlands, Norway; Spain, Sweden' (First-Ever Formal SIGINT Development, 2010).

Suggested Citation (APA): Kniep, Ronja. (2016, October 5-8). *From the 'Five Eyes' to the 'SIGINT Seniors Europe': The intelligence community as a transnational field.* Paper presented at AoIR 2016: The 17th Annual Conference of the Association of Internet Researchers. Berlin, Germany: AoIR. Retrieved from http://spir.aoir.org.

debates on surveillance, and it adds to theorising socio-technical developments related to the internet. On the conceptual level, the paper argues that Pierre Bourdieu's field theory, and specifically Didier Bigo's application of it to transnational fields, provides a useful heuristic to analyse the internet's role in the transnational field of intelligence. On an empirical level, the paper proposes to combine the analysis of internal NSA files, witness statements made by intelligence personnel and historical research in order to shed a light on previously secret intelligence communities that go beyond the 'Five Eyes'. It shifts the focus from the practices of single agencies to their embeddedness in transnational fields. In addition, the paper illuminates what we have learned about the activities of European intelligence agencies since the 'Snowden revelations' in June 2013.

Method and data

It is vital but at the same time challenging to study secretive organisations (cf. Monahan & Fisher, 2015). This paper advocates that academia should use and make sense of the data made publicly available by whistleblowing, but under the condition of reflecting on the data's selectivity, ethicality, and authenticity. This paper draws on two main sources, the former being composed of leaked material: internal NSA files and witness statements by personnel of the German foreign intelligence service, the *Bundesnachrichtendienst* (BND). Publications based on historical archives complement and contextualise the findings of the qualitative document analysis (e.g. Frost & Gratton, 1994; Aid & Wiebes, 2013; Corera, 2015).

The internal NSA reports were accessed by the author via the searchable database provided by the *American Civil Liberties Union* (ACLU)[2]. The search mask makes it possible to select those documents that provide information on foreign intelligence partnerships in general, the actors involved in European networks (e.g. SSEUR, BND, DGSE), and the joint programmes conducted by the 'Five Eyes' together with third party partners in Europe (e.g. RAMPART-A, EIKONAL, ORANGECRUSH). The keywords were identified in an iterative process of reading NSA documents as well as news coverage, and by examining the institutional structures of the different intelligence agencies. Yet, for the purpose of understanding transnational intelligence alliances, the information made available through the database remains fragmented. Like most leaked documents, the NSA files are highly selective, not least because the picture of alliances is drawn through the lens of the NSA. In order to address this aspect of selectivity, the paper also draws on witness statements by personnel of the BND. Here, the analysis focused on the statements made by (former) employees of the division 'Technische Aufklärung' (TA) who were invited as witnesses to an inquiry panel by the German government[3]. The division TA is responsible for SIGINT, and the analysis of the NSA files provided evidence that it is the direct partner unit of the NSA in both bilateral and

[2] In June 2013, The Guardian had published the first series of documents released by the former NSA subcontractor Edward Snowden. The ACLU has collected all documents that have been published since 2013 in one archive.

[3] In 2014, the German government established a committee of inquiry which was tasked with investigating the way and the scale the intelligence services of the 'Five Eyes' have been collecting data on communication activities, and how the German BND has been involved for the period from 2001 onwards.

multilateral SIGINT agreements. All transcripts of witness statements in the public part of the hearings have been made accessible by the blog *netzpolitik.org,* and partly via the platform *WikiLeaks*.

The world of secret intelligence as a professional field of struggle

Semi-autonomous fields, e.g. journalism, art or politics, are the product of historical differentiation and are basically small worlds governed by their own 'rules of the game' (Bourdieu & Wacqant, 1992, p. 127). This analogy of games, invoked by Bourdieu, highlights important assumptions of field theory: The field's structure and its dynamics are shaped by struggles among the players, who share a collective belief in the game's meaning, a common *illusio* that the game is worth playing (Bourdieu, 1996, p. 360).

In the intelligence game, actors jointly but antagonistically struggle over the prerogative of interpretation related to security threats. In this struggle, power relations are defined by the agencies' competencies in terms of access to data and communications ('informational capital'), besides other forms of capital like personnel and financial resources. Yet, actors in a field do not only compete over capitals. The very definition of what is at stake in the field is contested. Dominant players, i.e. actors with a relatively high amount of (symbolic[4]) capital, shape the rules that are considered to be legitimate or as given in the intelligence field. The agencies' shared sense of providing a crucial service in the fight against crime and terror contributes to the field's specific *illusio*.

Fields differ with regard to their degree of autonomy, i.e. the degree of domination by external forces. While journalism, for example, can be considered a weakly autonomous field because of its structural dependence on the market and its audience, mathematics is a strongly autonomous social space because of very specific rules and a highly exclusive expertise. Like in mathematics, participants in the intelligence field hardly discuss concrete practices with anyone outside their peers. The habit of secrecy facilitates the intelligence field's autonomy, as internal practices and interpretations are mostly exchanged within a very limited circle in the same social universe. In addition, the right to secrecy makes it harder to challenge intelligence agencies' claim to hold the truth about security threats. Thus, the special right to secrecy potentially increases their symbolic capital vis-à-vis less secretive organisations in the security domain.

Analysing intelligence communities as fields has at least two advantages. Firstly, by describing intelligence as a socially constructed and contingent social space which is shaped by specific institutional histories, the sociological theory counters the narrative that the surveillance practices of intelligence agencies are simply a natural response to a given technological development. Secondly, field theory offers an analytical perspective that does not demonise (nor heroise) intelligence agencies, while it maintains a critical potential. Rather than framing the intelligence field as a homogenous alliance that is jointly struggling against terrorism, or vice versa as a united front

[4]Symbolic capital refers to the prestige, reputation or fame of certain actors in a field (Bourdieu, 1991, p. 230). Symbolic capital translates into symbolic power, which is 'a power of constituting the given (…) a power that can be exercised only if it is recognized, that is, misrecognized as arbitrary' (ibid., p. 170).

infringing privacy rights, the notion of a field uncovers internal struggles and competitions among intelligence services and potentially other security actors. Like other professional fields, the intelligence field is a site of bureaucratic infighting among actors with different resources. Thus, field theory illuminates that surveillance practices are the product of both internal struggles and processes of the field's autonomisation. The surveillance practices and the specific rules they follow may well be criticised. But they are better understood in the light of characteristic field dynamics - and not as products of rational choice or conspiracy.

Changing the rules of the game? The internet and the transnational intelligence field

In the following, I briefly discuss selected results of the analysis in the light of two assumptions which characterise the role of the internet in the intelligence community as a transnational, Bourdieuian field:

1. The internet has modified the rules for the intelligence agencies' struggle over the prerogative of interpretation related to security threats.

Like in other professional fields, the commercialisation of the internet in the 1990s has challenged established practices in the intelligence field. The interception of internet communication travelling via fibre-optic cables turned out to be more complex than the interception of satellite communication, and the sheer volume of data required new ways of collection and analysis. Despite these challenges, the analysis of leaked NSA files shows that the programmes aimed at the global surveillance of satellite communication (such as ECHELON) have been complemented by interception programmes that target fibre-optic cables with and via third party partners (e.g. RAMPART-A). In the self-proclaimed second 'golden age of SIGINT', access to internet communication has become an essential motive for the agencies' partnerships with private companies and other intelligence agencies. The co-operations between the NSA and the European states that have been growing or maintained on a high level in recent years are structured by the goal of accessing internet cables and the exchange of technologies for large-scale analysis. This is the case for the alliances with Germany, Sweden, the Netherlands, France and a relatively new SIGINT programme with Poland. As the analysis of witness statements suggests, for the German BND, the joint programme with the NSA called 'EIKONAL' that was initiated in 2002, has been 'the door opener' for cable access. Yet, the analysis also shows that the technological development is not sufficient to characterise intelligence partnerships and their practices. Historical ties between agencies as well as expertise on high-priority targets, e.g. in the form of relevant language skills or regional analytical expertise, are also important criteria for the establishment of SIGINT alliances.

2. The autonomisation of the transnational intelligence field sets rules for the internet.

The institutionalisation of a transnational field of security professionals has led to the autonomisation of '(…) "specific experts" acting for a certain cause' (Bigo, 2011, p. 253). Thus, professional guilds of (in)security, including their ideas and practices, are

characterised by a certain degree of isolation “from the professionals of politics and the public” (ibid.). An important finding of the document analysis is that this is specifically the case for the transnational, secret SIGINT alliances, where ‘specific experts’, the ‘ SIGINT Seniors’, negotiate the exchange of sensitive data and the technologies for accessing and analysing them. This specific group of actors in the intelligence field has formalised agreements, introduced practices and interpreted national law independently from politicians. However, the (semi-)autonomously produced interpretations and missions potentially influence both law- and policy-making related to the internet *as well as* the internet as a socio-technical institution, acknowledging that

> *‘(…) the problem of integrating the machine in society is not merely a matter of making social institutions keep in step with the machine: the problem is equally one of altering the nature and the rhythm of the machine to fit the actual needs of the community’ (Mumford 1934, p. 367).*

Field theory elucidates that the ‘ actual needs of the community’ are field-specific. They are often inward-looking and to a certain degree detached from other fields of the society. While Pierre Bourdieu tended to see a field’s autonomy as being something desirable, the application of field theory to the intelligence community illuminates that autonomously produced practices also imply normative challenges.

References

Aid, M. M., & Wiebes (2013). *Secrets of Signals Intelligence During the Cold War: From Cold War to Globalization (Studies in Intelligence)*. Hoboken: Taylor and Francis.

Bigo, D. (2011). Pierre Bourdieu and International Relations. Power of Practices, Practices of Power, *International Political Sociology,* 5(3), p. 225–258.

Bourdieu, P. (1991). *Language and symbolic power.* Cambridge: Harvard University Press.

Bourdieu, P., & Wacquant, Loïc J. D. (1992). *An invitation to reflexive sociology*. Chicago: University of Chicago Press.

Bourdieu, P. (1996). *The rules of art: Genesis and structure of the literary field*. Meridian. Stanford Calif.: Stanford Univ. Press.

Corera, G. (2015). *Intercept: The secret history of computers and spies.* London: Weidenfeld & Nicolson.

First-Ever Formal SIGINT Development (2010, October 25). Retrieved from https://www.aclu.org

Frost, M., & Gratton, M. (1994). *Spyworld. Inside the Canadian and American Intelligence Establishments*. Toronto, Ont.: Doubleday Canada.

Monahan, T.; Fisher, J. A. (2015). Strategies for Obtaining Access to Secretive or Guarded Organizations, *Journal of Contemporary Ethnography,* 44(6), p. 709-736.

Mumford, L. & Langdon, W. (1934). *Technics and civilization*. New York: Harcourt.

Rosenbach, M. & Stark, H. (2014). *Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung* (German). Deutsche Verlags-Anstalt.