3. Beyond national security, the emergence of a digital reason of state(s) led by transnational guilds of sensitive information: the case of the Five Eyes Plus network

Didier Bigo

1. A CHANGE OF PARADIGM OF NATIONAL SECURITY: TOWARDS THE EMERGENCE OF A DIGITAL REASON OF STATE(S)?

I argue in this chapter that the scale and scope of surveillance and the transnationalization of secret intelligence services we have witnessed over the last few years require a renewed investigation of contemporary world security practices. Reflexively, it means also we need a careful mapping of our very own categories of analysis, especially the one of national security. National security had a stabilized meaning during the Cold War, but has been gradually challenged by the idea of a global security agenda and by the argument that cooperation between intelligence services to trace transnational threats was a necessity, especially in matters of terrorism. The destabilization of meaning is not specific to national security as such. Sovereignty, security communities, territory, border control, surveillance, technology, intelligence and rule of law have also ended up meaning different things for different people with different normative and political judgements. Is security, protection of the people or mass surveillance? Is rule of law a danger for an adequate prevention in need of efficiency and high-speed action? Are border controls an effective tool for intelligence purposes if suspects are already on the territory? The list can continue. What is under question is not the transformation of one of these categories over another one, but how all these categories have simultaneously changed. This supposes to move away from the mainstream of intelligence and security studies and to develop an International Political Sociology (IPS) of freedom and security inspired by surveillance studies and human rights legal knowledge, in addition to the legacy of critical security studies.

Following this IPS approach, I will argue that national security is no longer national as such, nor does it correspond to a traditional understanding of security as protection from war. This change in national security practices is what I call 'the emergence of a digital reason of state(s)' based on the possibility for intelligence services to cooperate and compete to extend their goals of prevention of crime, terrorism or espionage by the inclusion of technologies collecting traces of human activities.

As I will claim in the first section, national security, because of the structural changes in technologies at distance including the use of Internet and smart-phones, of the huge exchange of data between different intelligence services in order to give sense to events via global interconnected information, and of the current forms of neoliberal management, is

no longer political, national and public in its making. In the second section, I will develop by showing that in the current state of the game, the very idea of a 'national' security is the result of the power struggles of a field of actors who want to control the management of sensitive data. These actors, that I call guilds of management of sensitive information, are now one of the key components of this transnationalization of the *Raison d'Etat* (Reason of State) in a digital age, which is still called national security but is in need of a different name. Then, I argue that this boils down to an argument over the digitization and heterogenization of *Raison d'Etat* which national security expresses poorly. Thus, in a third section, I will argue that these inner struggles within a transnational guild of professionals are creating the current series of paradoxes of situations after the Snowden disclosures of the practices of the US National Security Agency (NSA) and the 'Five Eyes Plus' network. This explains, for example, the current paradoxical status of some European national laws on intelligence which gave to these secret services more personnel, technologies and rights after 2013 than before, even if the necessity of oversight has been recognized. The follow-up to the debates about surveillance and democracy have by the same token created interventions of 'intelligence non-professionals or amateurs' into the very heart of the control of data management by introducing references to data protection, encryption, privacy, democracy. But it is not clear that they succeed to destabilize the idea of an inevitability of surveillance in a technological world, justifying an extension of intrusive intelligence, often because a confusion between intrusive intelligence and pervasive forms of everyday surveillance has occurred, including inside the academic literature.

1.1 Methodology

Key to my argument is therefore to first understand and to analyse how the classic Raison d'Etat and its contemporary iterations, such as national security during the cold war, have undergone profound mutation with the process of digitization leading to the emergence of 'datafication' of our societies in everyday life, the development of transnational exchange of data between secret services, and the extension of the personnel involved in intrusive intelligence beyond police and intelligence services.[1] This increase in gathering digital communication and data has nurtured a wider transnational collaboration amongst national intelligence and security professionals and resulted in an extension of the category of foreign intelligence in order to share data that could be of national concern more specifically. The Reason of State is becoming shared between a group of states that elaborate strategies, responding unequally to their own interests. Therefore, by projecting their national security 'inside out', via a transnational alliance of the professionals of national security and sensitive data, they have in return an 'outside in' effect of suspicion fors all Internet subjects; a situation which destabilizes strongly the categories of 'foreign' and 'domestic' by dispersing them and transforming the line that separated

[1] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, CEPS Liberty and Security in Europe No. 61 (6 November 2013); Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R.B.J. Walker, 'After Snowden: Rethinking the Impact of Surveillance' 2014) 8(2) *International Political Sociology* 121–44.

them into a Möbius strip.[2] The national-foreigner divide that organizes both the cleavage between military and police services, as well as the difference of targeting between citizen and foreigners, is therefore blurred and becomes highly intersubjective and discretionary, creating new forms of discrimination different from the traditional national security argument. The mode of acquisition changing as well as the objectives, the nature of the groups in charge change also. The groups in charge of national security are now transnational groups of experts, both public and private, both security and data 'bureaucrats', obeying both their national politicians but also their transnational allegiances. This is rendered possible by the accelerated growth of interception and intrusive collection of data that these intelligence services extracting information at distance can perform, and by the ease with which they can perform these extractions on a large scale, because of the digitization of the formats of data and metadata. Those who manage this information have a socio-technical capital on information at distance which allows them to claim a relative autonomy, challenging the national monopoly of the politicians in assessing who is the enemy and what are the objectives of national security.

Hence, national security now encapsulates practices which, first, are a mix between national and transnational objectives; second, are organized more bureaucratically than politically; and third, are assembled by a hybrid form of grouping of different public services and private companies interested in the management of sensitive information in police and intelligence matters.

To integrate in the reasoning these three key elements of metamorphosis of national security, I propose a Bourdieusian-inspired analysis of the contemporary international sphere, insisting on the transnational fields of power, their dynamics, and the dispositions that the actors enact when what is at stake is the management and extraction of data for purposes of constituting watch lists of suspects.[3] In this approach, the positions of the field inform the struggles in terms of symbolic power between the actors, their position-takings and the regime of justifications they use. The dynamics in the field, and the emergence of scandals by disclosure of secret practices creating turbulences, are therefore less determined by one main actor than by the results of the field interactions which play a central role for understanding the compliance and resistances of large parts of the public.

At the core of this grouping of actors connecting many tools of surveillance with intelligence purposes of prevention is what I call a 'guild' of actors having their specific know-how, their specific dispositions, sense of order, truth rituals, at the transnational scale.[4] This notion transposes and clarify the ones used by previous Bourdieusian

---

[2] Didier Bigo, 'Internal and External Security(ies): The Möbius Ribbon' in Mathias Albert, David Jacobson and Yosef Lapid (eds), *Identities, Borders, Orders*, (Minneapolis, MN: University of Minnesota Press, 2001) 91–116; Didier Bigo and R.B.J. Walker, 'Political Sociology and the Problem of the International' (2007) 35(3) *Millenium Journal of International Studies* 725–39; Didier Bigo, 'Sécurité intérieure, sécurité extérieure: séparation ou continuum?' in Sébastien-Yves Laurent and Bertrand Warusfel (eds), *Transformations et réformes de la sécurité et du renseignement en Europe* (Presses Universitaires de Bordeaux, 2016) 316.

[3] Didier Bigo, 'International Political Sociology: Rethinking the International through Field(s) of Power' in Tugba Basaran, Didier Bigo, Emmanuel-Pierre Guittet and R.B.J. Walker (eds), *Transversal Lines* (Routledge, 2016).

[4] Didier Bigo, 'Sociology of Transnational Guilds' (2016) 10(4) *International Political Sociology* (1 December) 398–416.

approaches about the role of power elites and professional expertise. Specifying the activities of intelligence services in the general management of unease by security professionals, the idea of a guild of management of sensitive information is proposed to analyse the current composition and roles of the SIGINT (signals intelligence) and Internet agencies more well-known under the name of 'Five Eyes', which are the US NSA and its private contractors, plus the UK GCHQ, the Australian ASD, the Canadian CSEC, and the New Zealand GCSB. These so-called 'Five Eyes' have in addition asymmetrical ramifications in different regions, including Europe, where other services play an important role in producing information and intercepting data. The various segments of this guild (often referred as 'Five Eyes Plus') have different capitals, be they socio-technical or symbolic, which give them different assets and allow them to enter, or not, into the competition for defining and prioritizing the tools, budgets, personnel who have to be in charge of the world control of management of sensitive information. The actors of this guild extracting data and building profiles of suspects are now as much technical experts coming from the digital industry as they are policemen or military. Often, they straddle competencies and move back and forth between public and private positions. Having the double competencies of security agents and strong knowledge in informatics is one of their characteristics. The apparent heterogeneity of the different trajectories is nevertheless mitigated by the fact that they all share a common know-how in the management of sensitive data, and that they consider that they are more experts in this domain than the politicians themselves and the high spheres composing their national security councils. The feeling of power connected with the shared secrecy of data in a small world of experts reinforces the solidarity beyond national ties and reinforces the transnational dimension of professional expertise. But they are not, in fact, all powerful, even when they think so. The field of their inner struggles creates centrifugal dynamics destabilizing the secrecy of their universe, and whistle-blowers are not exceptional in this universe. They often resist the doxa of the field to be beyond the reach of the rule of law and democratic scrutiny and reintroduce other actors, security amateurs, into the debates about what is at stake in this field. It is essential to take into account these characteristics in order to understand the public controversies around the legitimacy of large-scale surveillance by intelligence services in the name of anti-terrorism, the counter-claims of the necessity of democratic controls, and counter-technologies like encryption. The latter element may paralyse in some ways traditional forms of protests and mobilizations by the quick acceptance that current technologies are inevitable and necessary. But this form of doxa regarding the social effects of digital technologies impacts on the public at large and many academics, which reinforces *a priori* compliance, but also generates alternative behaviours, and reframes the field dynamic in a way that the core actors do not control.

2. NATIONAL SECURITY IN A DIGITAL WORLD: A SHRINKING NOTION OR A PHOENIX RESURRECTION?

2.1 When National Security was Meaning National First

National security is a terminology often taken for granted and considered almost universal. Certainly, we do not lack for definitions, and Arnold Wolfers has given a definition

largely accepted by the United States during the Cold War by capturing the older formula of Walter Lippman (1943) in condensing it as: 'a nation is secure to the extent to which it is not in danger of having to sacrifice its core values'.[5] The work of national security is therefore to produce the means to identify who or what can endanger these values and to define the threats to these core values in order to protect them. As long as the enemy is seen as another state whose forces are mainly outside of the territory, the horizon of deterrence and military war can be used to be sure that the balance of power is sufficient to avoid any attacks, but if the intelligence services have to cope with more complex elements coming from social changes, decolonization, revolution or attempts of destabilization by a spectacular form of political violence, the 'national' character is already not completely synchronous with the one of territory. Nevertheless, if one adds to military intelligence services more police and criminal-justice oriented services, it is possible to fill the gap, or at least to believe it. National security means national interest for the government of a specific territory and is an instrument of sovereign power. The web of international laws, regulations and organizations is not penetrating the national logic.

Even after the end of the Cold War, the idea of national security has not been challenged; on the contrary, national security has been extended, via societal security or environmental security to new domains.[6] But, nevertheless, the introduction of the will to control different threats and global risks began to change the 'national' game, and in-depth cooperation is considered as a necessity for the different national intelligence services to 'connect the dots' at a global reach. Agreements which were signed against a precise common adversary are therefore extended to a more common appreciation of what is a threat or a risk, with nevertheless contradictions and competitions in different forecasts about the risks to come. This happens even if the sharing of information limits discrepancies, with the possibility that some crucial ones, the most important ones, have not been shared. Coopetition (cooperation and competition) is officially the rules between countries, but theoretically not inside the national agencies. This will change.

The 'war on terror', launched on 14 September 2001 and presented as the only possible answer to the 11 September attacks, will facilitate this shift by enforcing a 'coalition of the willing' who consider that a global civil war is at stake and justify a total information awareness and the extraction of information by secret services by whatever techniques they want to use. The CIA will be put in charge of 'extracting information'. It seems, then, that national security has never been so important and has justified exceptional and emergency measures in the fight against terrorism. But, whose national security is reinforced? At what costs? Is cooperation for the benefit of all countries or only for some? Is national security still defined by core values or by a politicization of one agenda imposed on a coalition unaware of it or complicit in it? By considering national security as potentially unlimited, with a doctrine of security first, where human rights are secondary, national security will succeed for a period to see a return to a police state at the global stage, but with major criticisms.

---

[5] Arnold Wolfers, '"National Security" as an Ambiguous Symbol' (1952) 67(4) *Political Science Quarterly* 481–502.

[6] Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis* (Lynne Rienner Publishers, 1998).

The delegitimization of some modalities of extraction of information via extraordinary rendition in countries torturing on the behalf of the CIA or complicit in the transportation will create in fact a 'denationalization' of national security. Different modes of acquisition will emerge in competition for a better legitimacy and will oppose de facto previous transnational networks of services organized along their technical specificities: human intelligence, security intelligence, defence intelligence and signal intelligence. But this time the competition turns into a struggle for symbolic power over security and growth of budgets and missions, with the real possibility that some services disappear as such.

SIGINT intelligence will win the fight for national security by reframing the game around digitization, large-scale surveillance and cyber(in)security as the main threat for the future. This is not to say that it is forever. Many current tensions in the transatlantic domain regarding extrajudicial killing, extraordinary rendition, indefinite detention, which were almost settled by the Obama Administration, are back again, the elite in the US Administration considering that their national security imperatives give them an 'imperial right' to act as they wish (a position nevertheless not shared by the practitioners).

However, if one looks at what national security has done effectively to justify practices of exception, it is obvious that in a less contentious way (but far more important for everyday practices), the controversy has focused from 2013 on the management of sensitive data and especially (but not only) personal data. The first target has become the NSA and the Five Eyes network, while the CIA's practices now appear as an error from the 'past'.

2.2 Turning Digital? Re-opening the Competition Around the Control of National Security, Meaning Privileging a Different Set of Actors: SIGINT Agencies

The digitization of the means of acquisition of information for intelligence purposes redesigned as the tool by excellence for national security will change the possibilities of large-scale surveillance and the idea of national security itself, by inversing priorities and going outside in to follow the suspects. The core of the activity is then no longer turned towards external attacks but also turned internally towards potential infiltrations and a generalization of suspicion. Global security replaces national security and transforms the latter into a form of 'egoist' practice.

This is one of the first paradoxes inherited from the transformations of the practices of national security. The strong boundaries made between totalitarian regimes and democracies was on the moderate use of intelligence services, but after the end of the Cold War and the argument of a global war against terrorism, this argument is no longer a strong currency for many Global North (previously called Western) states.[7] It is still important to differentiate from Russia and China or Iran, but the cybersecurity discourse is framed more by filling the gap against them than by a self-restraint on the use of intrusive software. For many years, non-democratic regimes have dreamed about having

[7] The terminology of Global North includes the United States, Canada, Australia, New Zealand, European countries, Japan, South Korea, Israel; a list which is not far from the configuration of the full Five Eyes Plus network.

instruments to undertake this general surveillance of the regime's opponents, but the ratio between surveillance and surveillees was of four to one. Now, it is said that preliminary investigations can be done 'at a click of the mouse' and that 'data collection' is an easy task if collaboration between secret services exist (e.g. ICREACH between the Five Eyes Plus), or if one has built specific spy software for browsing the Internet and the social media, often bypassing the restrictions that the Internet providers have put in place to limit such easy collection.

China has recently been very efficient, as well as Russia and even Iran, in setting up intrusive means of collecting data, but what is at stake in democracies? Do they behave differently or not? Are these countries still in a position to outlaw intrusive practices against Internet users? To paraphrase Allen Dulles quotation, are the secret services of democracies protected from the temptation that the easiness of technology pushes them to collect data not because 'they need to do it' but because 'it is just nice to do it'?

Clearly, since the mid-1990s, technological transformations resulting from increased digitization of everyday life have changed the way in which these SIGINT (and later on) Internet intelligence agencies operate at a distance. It already existed during the scandal of Echelon, where it was known that the Five Eyes had intercepted communication of their allies in order to take advantage in commercial competition, but it has changed in scale with the surveillance of the Internet. Today, digital traces left by almost all transactions and mundane actions are stored and collected for commercial or security purposes. Besides, from their offices, acting at distance, the specialists of intrusion have had the capacity to trace almost all of the online activities that an Internet user was undertaking during the day, at least before 2013. After this date, corresponding to the Snowden disclosure of the practices of the NSA and its network regarding intrusive capture of Internet users' data, as I will show, it has become more complicated and a fight between encryption and decryption will give a certain density to the losses and the gains in the digital realm, but it will not stop the practices of secret services putting at risk fundamental rights of Internet users and democratic scrutiny of their own countries.

It is these latest evolutions that most authors of security and intelligence studies have not taken into account, mostly because of the proximity between the analyses they produce themselves and those of the practitioners; the convergence of the two narratives is building a very strong form of power knowledge relation inside and forming a doxa almost impossible to challenge, but also a very weak interpretation in terms of understanding of global transformations, obliging a reconsideration of the basic notions at stake.

2.3 Power-Knowledge of National Security: Assumptions at Stake

Security and intelligence studies have often refused to take into account these changes in the paradigm of national security that we have discussed. They continue with the idea that a cycle of intelligence exists; that the distinction between data and information is clear; that the work of intelligence services is under the control of politicians; that national allegiances always take primacy over any other one. More importantly, they have even continued to defend the idea that secret services are outside the boundaries of normal jurisdiction and democratic accountability. They have spent their time confirming the impression of the agents of this field of secret actions that they had a special code of conduct; that they have, by contract, immunity regarding the right to carry out

forbidden activities as long as they obey a hierarchical order. Certainly, some among them have insisted that national security is no longer the emanation of a police state, of the old '*Raison d'Etat*', but a way to defend democracies against their enemies, and that consequently the secret services need a new contract making clear the boundaries between secrecy and publicity, detailing their actions, as well as establishment of rules of accountability supposing a more powerful and independent oversight verifying the behaviours of the agents.[8] But, for the vast majority of practitioners and academics who were former practitioners, and for a large part of the realists in international relations, to admit that secret services come within the realm of legality is a threat to their existence as such; they therefore claim that agents are most of the time carrying out 'a-legal' actions (not directly illegal as they have orders, or actions which are located outside of the current legal order and by which they benefit from holes in the positive legislation of the technical realm not yet controlled).[9] However,, it seems that even if they have easily convinced politicians and Members of Parliament to accept this rhetoric, they have had far more difficulties with the judges, who consider that what is not legal is by definition illegal and susceptible to be condemned.

More in line with the judicial vision, surveillance studies and critical security studies have insisted on the imposition of democratic limits on the secret services, which shows the transformations by which national security is now a field of forces, in the Bourdieusian sense of a magnetic field attracting more and more actors, including technical and private ones, around the formation of a legitimate definition of what national security means, and simultaneously a field of struggles between the transnational groupings of a specific kind of secret services (e.g., the Five Eyes network) opposing other transnational groupings (e.g., the CIA and the other external services) not only in international politics, but also and perhaps mainly in national politics, where budgets and missions are crucial to obtain, as well as the power to define the priorities of the threats and risks.

It is this field, now populated by different actors, but all interested to fight for a say on the digital Reason of State that is emerging, and which is more transnational than national, more hybrid than public, more bureaucratic than political, that I will describe in more detail in the next section.

3. FIVE EYES PLUS CONFIGURATION: EMBODIMENT OF THE DIGITAL REASON OF STATES AND ITS FIELD EFFECTS

Edward Snowden has described the Five Eyes network as a 'supra-national intelligence organisation that doesn't answer to the laws of its own countries'.[10] This is an important

---

[8] Richard J. Aldrich, 'Transatlantic Intelligence and Security Cooperation' (2004) 80(4) *International Affairs* (1 July) 731–53; David Omand, *Securing the State* (London: C. Hurst & Co. Publishers Ltd, 2012).

[9] Sébastien Laurent and Bertrand Warusfel, *Transformations et réformes de la sécurité et du renseignement en Europe* (Presses Universitaires de Bordeaux, 2016).

[10] Edward Snowden, 'Testimony Submitted to the European Parliament', Brussels, European Parliament, 2014.

point of departure. The question is not about technology or surveillance in general, the question is not about Big Data in our lives, it is about rule of law and secrecy, reason of state or more exactly reason of 'states' that consider they may have shared interests, constructed by the chains of interdependencies of their secret services and the associated public and private bureaucracies acting inside and outside the territory in a transnational context.

Too many works have confused intelligence with surveillance, and it has created some misunderstanding of the current situation. Without an industry developing intrusive intelligence technologies and working for the secret services, openly or not, the situation would be different. This is also the case of the structure of the relations between the different secret services specialized in SIGINT and Internet management of sensitive data. They are not a form of meta-policing acting against global terrorism by sharing confidential intelligence, and their mutual 'trust' is certainly not highly developed. They are as much in competition than in collaboration, and they have created their own word of 'coopetition' to express it. This is why the Bourdieusian notion of field of struggles is so important to describe what is at stake in this domain of intrusive intelligence, and why the understanding of the logic of distinction between the agents, as well as what capitals they can mobilize, explain their current strategies internationally and locally simultaneously.

Therefore, this approach is reluctant to take for granted the common narrative regarding the cultural ties of democracies in the Anglo-American world, and the special relation between the United States and the United Kingdom forming a unique security community. The power relations and asymmetries are deep inside the Five Eyes network, as well as the competition for specific tools enhancing the capacities of secret services.

3.1 Mutual Trust Narrative and its Culturalism

Nevertheless, most frequently, the history of the 'Five Eyes' as an organization emerging from the collaboration during the Second World War and the struggle against communism has a cultural narrative set up by the first books on the NSA and which have been repeated again and again without a serious second examination.[11] Intelligence studies create a continuity in the collaboration between the different Anglophone members and do not speak of the strong conflicts of the mid-1970s, with Australia, for example. They want a progressive development from the origins during the Second World War to now which is supposedly based on the mutual trust between these partners, more difficult to obtain if they include the Swedes, the Germans or the French. This may have been true at the beginning, but deference to NATO and the United States has been de facto the essential political factor and has played a role regarding countries who wanted a strong European defence pillar independent from the United States. If the United Kingdom was recognized as a special partner, it was more because its socio-technical

[11] James Bamford, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization* (New York: Penguin Books, 1983; Chuck Darwin and James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (Doubleday, 2002); James Bamford,*The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (Doubleday, 2008).

capital in term of research has been higher than other countries with specific innovations (decryption of the Enigma machine by Alan Turing, better encryptions during the mid-1970s, and Tempora software with the Internet). The specific location of the United Kingdom as the prime receiver of transatlantic cables has also assured a necessity to collaborate with the UK government, even during disagreement. Australia and New Zealand have been much more subordinate and considered as outposts more than as partners. So, beyond the story of the great 'fraternity' between the Anglo-American people, it may be useful to look in more detail at the structure of the network and its asymmetry.

The network has changed profoundly and is not based on an Anglo-American core which will have some marginal partners. The more robust partners, and sometimes simultaneously adversaries, inside the Five Eyes Plus are the ones placed in strategic locations in relation to the network cables through which Internet connections are possible, downgrading the previous key role of satellites. They are also the ones who have invested in technological research, and have their own software or 'niche' in the markets of intrusive surveillance via their (so-called) private industry. Germany, Sweden, France and Israel, are key players. Research into the so-called SSEUR or 'SIGINT Seniors Europe' (Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain and Sweden) is showing the importance of this network, beyond the Five Eyes as such.[12] Their activities range from active collaboration on counter-terrorism matters and geopolitical analysis of the Middle East, to competition and struggles around collections of data intercepted via computer access, border mobility and/or financial transactions for economic and business advantages for their own firms. The existence of this 'coopetition' with different rules and forms of trust between the agencies structures an asymmetrical transnational system of exchange of 'sensitive' information in intelligence and police matters that have to be checked, and implies a reflection on oversight mechanisms when transnational activities are at stake. SSEUR analysis shows that key positions gained by Sweden, Germany and France are related to their structural positioning, and that the United Kingdom, Australia and New Zealand are not privileged as the so-called 'first circle'. They are only privileged if they add material support to the large-scale collection or retention of data. The internal divisions in almost every agency seem to confront the denizens of a 'Wild West' Internet where no rights exist and where the most powerful can intercept what they want if they have an interest to do so, versus a group led by an alliance of lawyers, inside the services and inside private companies, pleading for a more systematic collection of information allowing a reduction in false rumors and to minimize the size of information.

It seems also that the specificity of the NSA network is to have all over the world a series of specialized agencies in signals intelligence acting 'regionally', and that a series of them coming from the Western alliance and its clients around the world are exchanging some of the data they intercept, in competition with other networks, which seems more correlated with national structures, but may also have connections with Russia, China, or even Kazakhstan, Iraq and Pakistan.

---

[12] See Ronja Kniep, forthcoming.

3.2 Forms of Capitals which are Mobilized to Play into the Field of Management of Sensitive Information

The hybrids constituted by the secret services and their private partners have different forms of capitals, some of which materialize easily, others are more symbolic, but nevertheless very effective. I will here describe the part of the field known as the 'Five Eyes Plus' network, which plays the most important role now that national security is digitized, but a full picture would need to analyse the various other intelligence services, the CIA's network, the FBI's policing counterparts, and for each of them their links with the private companies, the politicians, the judges, the media. The first criteria is the size of the personnel and their socio-technical capacities, which means here that it is not the amount of technology they have which is important, but how they use it. The second criteria is the location of these services in relation to the Internet cables infrastructure. The last one is the socialization of their agents and their trajectories

3.3 Number of Personnel Enrolled into Intrusive SIGINT and Internet Intelligence and Their Socio-Technical Capacities

In the United States, with approximately 100,000 people employed at the NSA, of which 'about 30,000 are military and the rest private contractors', the NSA is 'by far the biggest surveillance agency in the world'.

The NSA has primarily used a platform named UPSTREAM which operates, where a request from the Five Eyes alliance cannot obtain permission to obtain information, to bypass this by an intrusive form of 'monitor any communication it engages in', tapping directly into the infrastructure – undersea fiber-optic cables.[13]

The other program that has made news worldwide is PRISM, also run by the NSA. Its main idea is simple: it essentially means a 'program where people in corporations or non-profits of any kind, are complying in helping the government, because they are forced under the FISA Amendments Act'.[14] Basically, PRISM receives information from the Internet or social network providers such as Google, Apple, Facebook, Amazon, but also Microsoft, Yahoo and Netflix, which are intermediaries in the process of intrusive interception by facilitating, or with various degrees of resistance limiting, the easiness of the intrusion, depending on the history of the company, the socialization of their personnel, the strength of their legal teams.[15]

The NSA therefore has seven times more personnel than the UK GCHQ and eight

---

[13] Known as 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data). Upstream collection includes programs known by the blanket terms FAIRVIEW, OAKSTAR and STORMBREW, under each of which are individual SIGADs. Each data processing tool, collection platform, mission and source for raw intelligence is given a specific numeric signals activity/address designator, or a SIGAD. The NSA listening post at Osan in Korea has the SIGAD USA-31. Clark Air Force Base is USA-57. PRISM is US-984XN. Source: file://localhost/wiki/SIGAD.

[14] See www.revolvy.com/topic/Upstream%20collection&item_type=topic (accessed 8 September 2018).

[15] See Felix Treguer, 'Intelligence Reform and the Snowden Paradox: The Case of France', *Media and Communication*, 1 March 2017, 5, available at https://doi.org/10.17645/mac.v5i1.821.

times more employees than the French Directorate-General for External Security (DGSE) and German Federal Intelligence Service (BND). In addition, the NSA employs private contractors to do part of the job, so it could be considered that the number of employees could be to 12 to 16 times superior to that of any other agency. This is the same for the budget. The NSA has a budget of 7 billion Euros a year. Within Europe, the GCHQ, with a budget of 1.2 billion Euros, is well below that of the NSA but has nevertheless over twice the yearly budget of other agencies, such as the BND, DGSE or Swedish National Defence Radio Establishment (FRA).

Nevertheless, another important actor is the UK GCHQ, which has a program of its own design, different in execution, but similar in purpose and focusing on the capacity to retain data for analysis, the Tempora project, previously known as 'Mastering the Internet'. It allows the GCHQ to collect any data that passes through Great Britain and store it for several days, the necessary time to filter the data with specific selectors, a technology that all other intelligence services including NSA want to use.

Beyond the NSA and GCHQ, the other powerful actors are services which were not part of the initial agreements but have a key role because of their positions in the circulation of data through the cables, and/or their own capacities in having the personnel and the technologies giving them something to 'exchange', to 'sell' to the other services. What has been called the Five Eyes 'Plus' is this network, which is theoretically composed of 18 eyes, and where clearly some SIGINT services in Europe and in the world exchange more information than the United States and Canada or New Zealand (supposedly in the core group).[16] The BND in Germany, DGSE in France, are in this first circle of strong actors because they have these capacities in personnel and technologies, and for them, the disclosures of Snowden have played a positive role in seeking to recruit more personnel and to have more investment in technologies, as we will see later. Their increased role, which was not clear in 2013, is also connected with their strength in the second criteria, which is their location and capacity to intervene in the building, management and capacity of interception in the Internet cables.

3.4 Position in the Internet Infrastructure

The NSA has constructed a network of relations that in practice follow the routes of the international infrastructure of submarine cables and the places of exchange into the main terrestrial networks, without forgetting satellite communications.[17] The Internet is therefore not immaterial or in the 'clouds', it is a subterranean infrastructure that has its main roads and its small pathways, as shown by the many maps of submarine and terrestrial Internet cables.

Looking at these maps, it becomes clearer why the NSA collaborate more with some agencies than with others. The transatlantic cables in Europe are distributed with important nodes beginning with the United Kingdom (GCHQ), Sweden (FRA),

---

[16] Some journalists have spoken of the Nine Eyes, with the addition of Denmark, France, the Netherlands and Norway; or the 14 Eyes, with Germany, Belgium, Italy, Spain and Sweden.

[17] Ronald Deibert, 'The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace' in Andrew Chadwick and Philip N. Howard (eds), *Routledge Handbook of Internet Politics* (Routledge, 2009) 323–36.

Germany (BND), France (DGSE), the Netherlands, Italy and Spain. Each of these places are important for intercepting Internet data, especially Sweden regarding Russia, and France for the Middle East. Germany is central for all EU networks. In North America, the Canadian Communications Security Establishment (CSEC) has been important to intercept data discreetly from Latin America and Brazil in particular. The connection on the Austral hemisphere bypasses Australia and New Zealand and maybe also Japan. In Asia, the secret services of Singapore, South Korea and also Pakistan are involved, plus in the Middle East a strong connection with Israel and Jordan, and France for North Africa.

Obviously, despite the extension of the network and the lengthening of the chains of interdependence between each point of the network, the structural power of the NSA is still very strong because of the concentration in its hands of the combination of the different modalities of acquisition of data via hundreds of specialized programs unified under various platforms of integration, and specific software for data mining and profiling. As long as the NSA has the most important personnel, be it its own agents or contractors, has constructed specific software allowing intrusion, and has obliged the intermediaries to operate or to allow them to carry out this intrusion, its pre-eminence cannot be challenged. Nevertheless, as in any form of interdependence, brute power is much more complex to use in practice, and some local actors may impose local agendas on the full network.

3.5 Socialization of the Agents, Dispositions, Trajectories

Many things have been said about the culture of trust and mistrust, and the limitations of this explanation are obvious. The relations to the geopolitics of the cables and the analysis of capacities of man- and socio-technical power are certainly more telling, but this may be too mechanistic. What is at stake to understand the relations between the individual agents, their willingness or not to collaborate, their solidarities and allegiances in case of contradiction between national and professional imperatives, is less well known. Investigations about the style of intrusive intelligence techniques, the respect of limitations, attitudes towards the rule of law and oversights are in progress, but still lacking comparative evidence. Nevertheless, it seems important to notice that the sharing of information is better with foreign intelligence services that have the same kind of skills and know-how than with national intelligence services that have different kinds of know-how, even if they theoretically participate in the same mission, or even are in a coordination or fusion centre. Studies of the professionals involved in policing anti-terrorism has shown that the professional training, the socialization via Euro-Atlantic meetings, the digital nature of exchange of information beyond one dossier, the 'geek' attitude of some of these agents, the belief in predictive software and preventive solutions, are all criteria playing into enhancing the so-called necessity of an increased amount of digital technologies of surveillance in all the operations of intelligence and the necessity to be both a technological and a security person.

I would suggest that the different agencies are hierarchized, as were the guilds in the Middle Ages with their rituals, their codes, their rules of strict hierarchy, obedience and solidarity, and that is why coopetition is possible at the transnational scale because professional solidarities sometimes trump national interests and political games of the moment. And just like these old guilds, these transnational professional organizations

confer symbolic power on a specific know-how, which can be strong enough to challenge some politician players and compete against them regarding the truth concerning threats and risks.

The national security game played by the politicians in charge, and sometimes by their national security councils, is not the same as the one that the transnational guild of sensitive information is playing. It may create serious confrontations. For example, the asymmetry is obvious in favour of the NSA but this is not in direct correlation with the US policy at a certain period of time. Transnational solidarities partly escape the international political games.

Then, the NSA is at the core of the guild structuration, and often imposes its own interests onto other ones, to the point that the other SIGINT services seem to have sometimes privileged the interests or needs of information of the NSA over the interests and alliances-organizations they are in: for example, the UK GCHQ spying on EU institutions for the NSA, or BND spying on their own aeronautic industry for the benefit of the NSA and Boeing, or Australia conducting espionage on Indonesian high officials for the NSA, directly hurting the Australian foreign policy and national interests.

The description of these inner struggles and the different capitals and strategies of the central actors who are carrying out intrusive intelligence using techniques to capture the flows of information that are now part of our everyday life, is in my view central to understand how global effects are sometimes paradoxical, for example, when the disclosure of NSA practices has helped the so-called victims, i.e., the other secret services, to make play with it, in order to claim more budgets, personnel and legal power. It will also allow us to understand the emerging common doxa of the inevitability of surveillance on the public, the problematic confusion of surveillance and intrusive intelligence.

4. CONTEMPORARY FIELD OF POWER IN THE DIGITAL REASON OF STATE AND ITS EFFECTS OF COMPLIANCE AND RESISTANCE

4.1 Five Eyes Contemporary Structure and the Snowden Paradox: Recent Intelligence Laws and Recent Judgments

The disclosures in 2013 by Edward Snowden of the secret US NSA program PRISM, and of more than 1,000 intrusive software systems with genuinely hush-hush codenames, have raised serious concerns about the scope and scale, the qualitative and quantitative dimensions of surveillance of everyday Internet users for intelligence purposes. What has been done by the NSA and the Five Eyes network during the previous ten years, in secret? Is it possible in democracies to act in such a way, certainly less directly violent than the CIA's networks, but nevertheless problematic for democratic forms of states?

Quite clearly, Snowden's disclosures of NSA practices have sparked significant public and political concerns. Some concerns about security to start with – security for whom? – were identical with the critique of the war on terror, but they were followed by questions about technological progress and a sense of the ineluctability of the deprivation of confidentiality and privacy in our modes of communication, wrapped around by an overall argument about the inherently violent, unsecured and dangerous state of the world.

There certainly lies a change in the regime of justification of national security within this argument. First, a justification has been expressed and presented openly, because the scandal provoked by the disclosure of large-scale surveillance was too strong to return to opacity, to the traditional: 'no comment, no denial' policy. But, the national security argument has been connected centrally with the large-scale intrusive data interceptions the press has called mass surveillance and bulk collection, while the services and the Internet providers have considered that their methods were necessary, appropriate and proportional.

The controversy has implied, on the technological side, a branching out of existing rhizomatic commercial surveillance for profit and intrusive methods of interception and collection of personal information by specialized intelligence services and their contractors. It has also opened a legal conflict with the judiciary on many fronts, and the national security terminology, which was in many countries a doctrine coming from the United States and the United Kingdom, has nevertheless entered the national legislations by the mid-2000, even if for most of them (France, Germany, Spain, Italy) the notion of 'secret defense' is still more relevant in a legal context than that of national security. A reaction will take time, but will nevertheless transform the US approach and its pervasiveness in the EU, and will eventually turn the United States' approach back in favor of human rights activists.

4.2 A Counter-Move: Rule of Law, Human Rights Countering Technological Arguments and Necessity of Intrusive Intelligence?

National courts and European Courts have been more and more clear in their judgments post-2010 that, if it is for the government to decide the content of national security, this cannot be completely discretionary. This has been and still is the main challenge theoretically for the concept of 'national security' and the encapsulated practices of human and technological intelligence. National security (and the secrecy around it) cannot be transformed into a cover for arbitrariness of the executive that other powers and citizens cannot check. Even when citizens believe that, in general, agents of secret services are also good citizens, they nevertheless want to have the capacity to differentiate inside the group, to punish those who act against inviolable rights, like the prohibition of torture, and to know who has given these orders. Since 2010, in a not yet stabilized doctrine, a framing, which has been developed in Europe via the role of Courts (European Court of Justice and European Court of Human Rights), but also national courts in the United Kingdom and Germany, has contradicted the US NSA's approach following the war on terror based on a more military and strategic vision justifying the President's power and its own practices. It seems that in Europe, legally, national security cannot trump the rule of law and democracy for political opportunist interests; the derogations have to be necessary and proportional to the threat. The threat itself cannot be the product of a flourishing imagination, it needs some evidence of an actual project of realization. Prevention is not fiction; anticipation has to have grounds.

Nevertheless, the reactions of the highest courts, acclaimed by activists and lawyers challenging the government, have not transformed the everyday practices of Internet users, and pushed them to defend by themselves their rights of data protection, privacy and forms of freedom endangered by intrusive intelligence. The argument of the necessity

of struggle against terrorism has been quite powerful, as well as the argument that the traces left by the use of the Internet and the limitations of privacy are the normal counterpart of more communication at distance, as Zuckerberg once bluntly said.

4.3 Resistances and Compliance: Contemporary Situation

Since Snowden's disclosures, one has certainly witnessed the end of a monopoly by the different intelligence services and the circles of experts of national security of what is the legitimacy of the practices enacted in the name of this national security. Competing discourses on intelligence services coming from non-professional circles (the 'amateurs' of security), and numerous NGOs of Internet activists discussing national security and surveillance, have emerged and have used the Internet and the social networks to claim their disagreements with these practices. These coalitions between these Internet activists (hacktivists as they call themselves) and human rights lawyers, as well as privacy lawyers, have set up a counter-discourse on the legitimacy of intelligence services in democratic regimes, which has given the judges of the highest courts the impression that they were not obliged to be completely deferential to the executive branch, and that their defiance was welcome.

This coalition has also sometimes been supported by major Internet providers accused of participating in the large-scale surveillance, or at least complicit and silent about what had happened over more than ten years before Snowden disclosed it. Public controversies occurred between those who, in light of the revelations, were claiming the necessity to improve intelligence oversight, and those who simply favored the public denunciation of the intelligence services who have covertly colluded and used the worst and most arbitrary means to arrest and detain suspects, first with the CIA, secondly with the NSA (and in some case killer drones abroad).

Yet, the world of intelligence remained quasi-untouched by the different scandals and has been moving even faster towards a more globalized cooperation among Western democracies, the implementation of alliances with non-democratic regimes, and the automation and digitization of their tasks and tools with the blessing and legitimizing authority of some of the new laws on surveillance.[18]

But here also, it is important to understand the 'fracturing' of the positions between actors. If this happened, it is because some Western governments (Germany, Brazil, France, Sweden) have played a specific game due to their ambiguous position in claiming initially, after Snowden, that they were themselves the first victims of these intrusive surveillance of the Anglo-American Five Eyes. The different SIGINT services have therefore lobbied their own governments to show the discrepancy between their tools and the ones that the NSA used, as if it came as a surprise to them. The efforts towards more means of 'defensive' digital technologies for cybersecurity purposes have been their first argument. By that move, some governments have 'modernized' their laws on intelligence, introducing some official possibilities of better oversight, but simultaneously reinforcing the possibilities for the intelligence services to use more capacities of interceptions, not less.

---

[18] Didier Bigo, *The Paradox at the Heart of the Snowden Revelations*, Open Democracy (10 February 2016); Félix Tréguer, 'Intelligence Reform and the Snowden Paradox: The Case of France' (2017) 5(1) *Media and Communication* (22 March) 17–28.

The paradox has consequently been that the post Snowden national legislations have not followed the approach hoped for by the NGOs. They have been a way for some services in need of technical capacities, first, to ask for more funding to acquire them, to develop also their own segment of surveillance industry, and ultimately to combat their Parliaments and especially their courts, which were motivated on the contrary to limit the intrusiveness of any techniques applied by intelligence services. They have nevertheless provided a way for the courts to identify the main violations of rights that such interceptions imply, beginning with the length of data retention and its use for profiling, the unnecessary large-scale collection of data, the function creep in access to databases and data mining.

The structure of the game has therefore reinforced the initial contradictions, and all the central players may claim that they have won, while at the same time the general debate initiated in 2013 is, five years later, inaudible in mainstream media and traditional political arenas.

The fact that the orientation of the debate on large-scale surveillance and personal data has been connected with the question of the struggle against terrorism by electronic means has certainly created a very different landscape around the claim of what national security can perform, and what is open in terms of operational practices when carried out by a government and its secret services. There has been a dual effect, especially after the Paris attacks of 2015, with, on one side, the revival of a discourse about the necessity of large-scale surveillance in order to prevent bombings before they happen, and justifying some of the public emergency measures and even their routinization. But, on the other side, it has also transformed the common understanding of national security by affirming that its definition, organization and means were not the exclusive domains of a national security council, and that these intellectual activities of interrogating the purposes of national security have to be shared by the other branches of power (to use the metaphor of Montesquieu), in particular the judicial, in opposition to the arguments that law has to follow and accept technology.

Indeed, the fate of different reforms of intelligence laws in the United Kingdom, Germany and France is currently suspended awaiting courts' decisions. This is also the case of a series of agreements between the EU and North America (Canada and the United States) on passenger name records (PNR) and on transfer of personal data by private companies. They now depend on assessments by judges of the impact of the practices enacted in the name of national security by intelligence and law enforcement services, as well as private companies, upon privacy, data protection, right of access and correction to personal data, and ownership of data by the data subject. The UK Investigatory Powers Act 2016 was repealed on 30 January 2018, the EU-Canada Agreement on PNR has also been blocked, as well as different Directives of the European Commission on data retention, to mention only a few cases, showing that while an argument on national security grounds still provides a government the possibility to open a right to exceptional practices, it will be under the gaze of judges.

4.4 The Inevitability of Surveillance: An Effect of the Doxa of a Transnational Field? Position Takings and Controversies

The story on the inevitability of surveillance has been constructed based on the potentiality of the system. We have to live with it and to forget privacy. The game is changing,

but it accelerates always in the same direction. Privacy is an old idea, laws are always late regarding technologies. Nothing can be done politically and collectively. Only a clever strategy may shift the trend at its margins. But it will come from those who know the technology. The belief that hackers are more important than judges to save what is left of privacy is of great currency in some circles. Efficient encryption is more useful than a law on the right to be forgotten. As surveillance is almost the only route, only smart individuals are equipped for the winding road of privacy. In any case, if counter-technologies can block technologies of surveillance, this is only for a short period of time. The ones without technology merit their fate as victims. Technological individualism is a form of 'Darwinian' survival.

How has this discourse of 'lassitude' in the face of battles known to be lost in advance, emerged? As I have said previously, it is certainly related to the fact that the capacity to act at distance has certainly increased the traceability of data; the possibility of data retention; the capacity to build software that enables complex relations between databases, and to deduct from these data emerging trends, statistical categories of behaviors or individuals; but it has created the belief that these emergent and minority trends give intelligence services a decisive advantage in conducting their various activities, such as espionage, economic intelligence, and the struggle against terrorism and crime.

This has been advertized as the key role of Big Data in algorithmic analytics. For many popular newspapers, but also in different important journals, future prediction, in the form of scientific prediction, is no longer a fantasy, but an 'advanced knowledge'. *Minority Report* is for tomorrow and begins already today. Nevertheless, I will contend (playing the novel of Philip K. Dick against the end of the movie) that the last point is not certain at all. The prediction of the secret services looks more like violent sacrifice to the omens than to scientific knowledge of future human actions.[19]

The lack of debate is astonishing. Why are so many actors saying that surveillance is a fatality and a necessity? When the debates exist, it seems that they concentrate on its efficiency and its proportionality from a legal point of view, forgetting the very first argument of possible lack of necessity; in technological debates, the main discourses look like a religious faith in Big Data analytics and the capacity of artificial intelligence to change our modes of reasoning by anticipating the future of individual actions.

A paradoxal conclusion is therefore that the inevitability of surveillance comes from very different actors, and constitutes in some ways the new doxa of all the actors, including the critical ones.

Of course, against the narrative of a scientific frame of predictive behavior of terrorist suspects that justified any increased measure of surveillance, some investigative journalists and academic books have been central to address key issues and to demonstrate the false pretence of this predictivity (e.g. works by Bauman *et al.* (2014), Lyon (2014) and Greenwald *et al.* (2013)).[20] Coming from different disciplines, they have raised a number

---

[19] Didier Bigo, 'Sécurité maximale et prévention? La matrice du futur antérieur et ses grilles' in Barbara Cassin (ed.), *Derrière les grilles: sortir du tout évaluation* (Paris: Fayard, Mille et une nuits, 2013).

[20] Zygmunt Bauman *et al.*, 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8(2) *International Political Sociology* 121–44; David Lyon, 'Surveillance, Snowden, and Big Data:

of other issues challenging the main story telling. First, they have asked why the question of the role of surveillance in a democracy has been reduced to one about the limits of the rights to data protection and privacy. Second, they have questioned the discussion around the balance of power and why it has been reframed as one about the exaggerated power of the courts, especially the regional and international courts that can more readily challenge the legitimacy of presidential powers. And third, they have asked why the question of secrecy in a democracy has been silenced, limited to a question of transparency, leaving aside the rights of persons accused of crimes based only on accumulated suspicions, and caricatured by the discourse that real innocents have nothing to fear if they have nothing to hide from the police.

But, because this alone does not seem sufficient, and because they have not seen mobilizations and demonstrations against the practices of the SIGINT Internet intelligence services, their hope has faded. For example, Bernard Harcourt has beautifully described the emergence of a society of exhibition insisting on our own weaknesses, our self-surveillance tendencies, our will to serve instead if it is too complicated in terms of satisfaction of a desire to wait. Many other books and articles have followed the same line of thought.[21] Zygmunt Bauman has spoken of a do it yourself (DIY) surveillance.[22] And these arguments are certainly not without validity, but, in my view, they contribute to avoiding the analysis of the formidable strength of these transnational guilds of management of sensitive information. This is perhaps because too many of the same authors have confused in their theoretical framework surveillance and intrusive intelligence practices, and in some paradoxical ways, have reinforced the positions of the most powerful actors of the game by validating the idea that we cannot escape the new world of surveillance and that we have only the choice to adjust to it.

So, I would like to finish with a focus on some elements that seems already well-known, but which are not taken sufficiently seriously. It is important to remember that the modalities of these SIGINT and Internet intelligence services are not equivalent to commercial profiling, even if those are also a problem. Here, the perpetrators of intrusive forms of intelligence do not ask you on Facebook to become your electronic friend; on the contrary, they capture what you have been concerned not to give away, even to your best friends.

The tacit contract of adherence to the newly established order of the digital Reason of State and its confusion with practices of surveillance and self-surveillance therefore defines the doxa of a field of power, but to recognize its existence is not to deconstruct this doxa. Heterodox positions, heretical subversions are not by themselves sufficient to break up this established order, as long as it has not experienced objective crisis.

Capacities, Consequences, Critique' (2014) 1(2) *Big Data and Society*, 2053951714541861; Glenn Greenwald *et al.*, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Macmillan, 2013).

[21] Bernard E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge, MA: Harvard University Press, 2015).

[22] Bauman *et al.*, 'After Snowden: Rethinking the Impact of Surveillance', n. 20 above; Zygmunt Bauman *et al.*, 'Repenser l'impact de la surveillance après l'affaire Snowden: sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance' (2015) 98 *Cultures and Conflits* (15 October) 133–66.

Nevertheless, these heretical positions challenging the authorized discourses on a digital national security, on the key role of secret services, may point out the dialectic between the authorized language of inevitability of surveillance and the disposition of the groups authorizing it by the configuration of their struggles.[23]

[23] Paraphrasing Pierre Bourdieu in *Language and Symbolic Power* (Cambridge, MA: Harvard University Press, 1993) 127.