# The socio-genesis of a guild of "digital technologies" justifying transnational interoperable databases in the name of security and border purposes: a reframing of the field of security professionals?

Didier Bigo. Professor of International Political Sociology, Sciences-Po Paris- CERI.
Professor of War Studies at King's College London
Email: didier.bigo.conflits@gmail.com

ABSTRACT
Smart borders, intelligent systems of filtering travelers by detecting suspects of crime and terrorism through interoperable national data bases and regional agreements are proliferating. In the European Union it began with the Schengen Information System. SIS-VIS-EURODAC, EES, ETIAS, ECRIS are acronyms for different realizations and projects of Entry and Exit Systems, of pre-frontiers zone, of policy checks regarding police, immigration and asylum, tracing people and scoring the degree to which they can be suspected to be illegal or criminal. Security stakes have been technologized. This is a profound reconfiguration of the different regional fields of security professionals with the emergence of a transnational guild regrouping data analysts, civil engineers on IT systems and border controls, changing de facto who is deciding the limits between security and insecurity, risk and fate. This importance of the online -virtual regarding the off-line- actual is affecting freedom and criminal justice.

KEYWORDS
Security; securitization; information technology; smart borders; border controls; policing; interoperability; IT systems; transnational guild; international political sociology; bourdieu;

# The socio-genesis of a guild of "digital technologies" justifying transnational interoperable databases in the name of security and border purposes: a reframing of the field of security professionals?

This article wants to show that the digitization of control in the European Union which is happening with the interoperability proposals of the EU commission and the trialogue with the Council and the European Parliament needs to be questioned by addressing the root causes which have transformed digitalized technologies of data base management into "solutions" for trans-border control activities and preventive-predictive logics.

This importance of datafication for control and surveillance in security and trans-border activities has been presented as a natural answer from new threats: terrorism of Daech, transnational crime, migration and refugee arrivals, and more generally surveillance of anomalies in the patterns of travelers. Critiques have certainly been addressed regarding

the side effects of a culture of surveillance and the impact on privacy, but they have often accepted that digitization was beneficial in itself and that interoperability was welcoming.

The public controversy opposing interoperability to privacy, which has raised in the aftermath of the interoperability proposals, presented by the EU commission as a response to terrorism in Paris and Brussels and Nice of 2015-16-17, as well as a solution to the so-called refugee crisis due allegedly to a lack of control of freedom of movement inside the area and a lack of surveillance of who is entering and exiting, has a multifarious series of causes that we explore later, but it is recognizable that these digital technologies for security purposes are the result of a move from "integrated border management" to "integrated data management', which is neither recent, nor a techno solution to so-called new external and transnational threats[1].

It is therefore necessary to challenge this vision of a neutral improvement of technologies by showing that it introduces de facto new "players" in the (in)security field in Europe who have their own politics, connected with their own visions of the world order, their own interests, and specific habitus or dispositions different from the military, the police or the border guards. This is why it may be important to do a socio-genesis of these practices of datafication and digitization in security matters in order to signal that they are centrally the results of a path dependency originating from Schengen with the SIS (Schengen Information System) as a solution for managing security "technically", "beyond political disagreements" between governments (Burgess 2009)(Broeders and Dijstelbloem 2016)).

Today, this trend to abandon political judgement on violence, order, freedom and justice, is reinforced by the fact to consider that digital technologies are improving previous technologies and are key in the achievement of successful preventive politics of security. The recent multiplication of narratives regarding digitization as the ultimate solution for terrorism, crime and border controls, has flourished in different spheres, largely beyond security, but providing them a certain kind of credibility.

Freedom of movement which was at the core of the European Single Act and the change of the Common Market into a European Union, and which was also allegedly the root of the Schengen Agreements, is now almost forgotten, and replaced by so-called "smart borders" technologies developing in the name of speed and easy freedom to move, increasing tools of surveillance and goals of prevention of suspicious acts ending up with lists of data-suspects.

In addition to the objective of surveillance of movement, digitization (artificial intelligence, predictive analytics, algorithms having the capacity to learn from the flows of data to become more and more accurate via machine learning) is also seen as a central capacity to produce scientific prediction about these lists and to achieve a "real" prevention of threats. A belief that the future can be read as a future perfect, a future already there and known, evading most of uncertainties is accompanying this faith on digital technologies and algorithms. These different assumptions about the links between the digital space and the taming of the future, as well as the easiness of mass surveillance have certainly to be assessed, especially in the cases where targets are aware to be under surveillance and can outmaneuver easily stereotypical behavioral patterns.(Bernard E. Harcourt 2007)

[1] A second co-authored paper discuss in detail the recent events post 2015 and the correlation between attacks of Daech, counter terrorist policies, and EU proposals of interoperability. It analyses the positions of the different actors and their logics of distinction as well as the different fields they come from. It tries to explain why the pressure to do something from the politicians has helped to choose and to justify interoperability at that moment in time. This paper wants to distantiate itself from the controversy and to show that interoperability as a vision of the world is the result of the emergence of specific specialists of IT systems in the domain of internal security.

To reinforce the strength of the values of digitization in terms of speed of calculus and scientific prediction of behavioral patterns, arguments of emergency and exception have in addition evoked "new" form of terrorism as the ultimate permanent threats against democratic regimes. Professionals of intelligence and specialized policing (terrorism, organised crime) have seen an advantage to develop the argument of the necessity of digitization and to comfort the legitimacy of the reasoning of these civil engineers, specialist of IT systems in matters of security. The fight for transformation of the who decides about the boundaries of security has put digital technology first and has trumped the more traditional discussion on security and privacy, on human beings right to change their mind until action, and even on the basic assessment of necessity, proportionality and adequacy of the measures proposed regarding their declared objectives.

If the debate is back again on privacy in 2018 and if some challenges emerge from the EU civil society organizations[2], this article claims nevertheless that the proposals of interoperability have silenced one of the most important question that Europe, but also Australia, Canada, the US have, concerning the management of their different entry and exit systems, pre-frontiers zone, policy checks regarding police, immigration and asylum, i.e; a profound reconfiguration of the different regional fields of security professionals with the emergence of a transnational guild regrouping data analysts, civil engineers on IT systems and border controls. This is changing de facto who is deciding the limits between security and insecurity, risk and fate, importance of the online -virtual and of the off-line- actual.

My argument goes therefore beyond the traditional acceptance that interoperability, if implemented in a well-thought manner and in full compliance with the fundamental rights, is acceptable as it is a neutral technique. On the contrary, I insist here that what is at stake is a strong political move where digital technology is depoliticizing questions and transforms who becomes in charge of security and who are the key targets of these policies (see introduction of this special issue). We have to understand that the dispossession of today political judgement and human values has been a consequence of this trend towards always more technologies of surveillance and identification each time politicians disagree about the politics to follow and feel they are obliged nevertheless to pretend they do something.

Taking the European Union as an example of this transversal tend which affects also Australia and North America, I want to demonstrate that interoperability mechanisms between data bases and the key role of digital analysts in the management of these systems of border controls and police at distance, are not an answer to new external threats of terrorism or risks of migratory flows invasion, they are *the sign of a push for more power of decision* in terms of risk analysis by data analysts, IT systems engineers profiting from a dromopolitics to challenge the police establishment, and large segments of border controls agencies . This is what I call the *emergence of a guild of "digital technologies" managing security*.

To makes sense of it, I consider in a first part that it is necessary to avoid presentism and the common sensical approach of analysing security as a reaction to threats. For me security professionals construct what is insecurity, security and fate (Bigo 2016). Only an historical perspective analyzing the overall development of the different data bases in police and migration matters as well as the projects to expand them, may therefore give a first answer in terms of power relation and its articulation with the digital. The interest on border

[2] The discussion on privacy is also detailed in the co-authored paper following this one.

controls and control of foreigners by policemen in addition to the forces in charge of passports and visa is consubstantial from the beginning of national policing (Noiriel, Gérard, 1991) but the idea to stop systematic control and to connect freedom of movement with filtering of who is travelling via technologies is more recent. I will study how these specialists of IT systems have become important actors in security-freedom dilemmas from the beginning of the Schengen agreements in the mid-eighties (1985) with the introduction of a Schengen Information System as an instrument for collaboration on external border controls and police collaboration. I will also explain its evolutions in the 1990s correlated with the enlargement to Eastern European Countries, and its reconfiguration as a series of search tools creating a function creep giving police access to data bases constructed initially only for the management of border controls or for the management of refugees inside the EU. The creation of multiple databases protected by purpose limitations in terms of access has been at the core of the functioning of the area of freedom, security and justice during the last twenty years, even if after 2004, under the pressure of the US administration some purpose limitations had been already removed. Only a small group of specialists coming from some private companies linked with governmental authorities and even rarest policemen knowledgeable on IT systems will be involved in the development of the SIS, and will fight between them on conceptions of IT system (centralization or not in relation to federalization or sovereignty of EUMS; border controls on site or preventive approach of policing at distance; freedom of movement, privacy and retention of data). The change between SIS1 and SIS2 has been crucial and the preventive vision has favored strongly the trend to digitization. SIS2 has de facto created a continuum of (in)security by gathering into the same data base information concerning crime, migration control and cross border activities, even if the conditions of access have been carefully separated. But when registration has been transformed into logs searchable by police organizations into the SIS2, and when police succeed to have access to other data bases like Eurodac and VIS, the question of transformation of criminal police into intelligence and surveillance for prevention purposes had become crucial. Security was not seen any more as a protection of an area of freedom of movement but as a necessity to have a “continuity” of surveillance anticipating danger coming from abroad before they actualized (risk calculation of overstay, score of suspicion based on contacts with persons knowing themselves terrorists or criminals).

In the second part, I analyze the key moments of this contemporary reconfiguration of the European field of power concerning the boundaries of freedom, security and justice, by looking at the different actors having a controversy around the efficiency of digital technologies and their impact on privacy, examining in detail what are the logics at stake in terms of *interoperability* at the EU level. I will especially investigate the opposition in the European Union between, the central principle of *purpose limitations* and the one of *interoperability*. Purpose limitations create the democratic boundaries of what the exceptional measures can do without destroying what they claim to protect. They relate to privacy but not only. They are crucial for delineating the limits of liberal and illiberal regimes. But nowadays, politicians and data managers see purpose limitations as an obstacle to the success of preventive policies; prevention which, for them, depends from the fluidity of data and their easy interconnection. This is why, as we will see, a tremendous change will happen between a SIS1+ enlarging territorially the capacity of the system to the new member states but keeping the philosophy of border controls, and the will to have a SIS radical change by organizing search tools and interlinks of alerts which will de facto introduce the idea of developing a scientific predictive and preventive police into the EU via technology and

digitization. The agencification of the group in favor of this trend via EU-LISA in 2011 will materialize an "intelligencification" of policing, its digitization and its dependence from the interests of hybrid public private firms developed from 2004. The interoperability proposals in the EU of 2015-2017 which are presented as the solution to efficiency and speed against all forms of threats, and a way to prevent transnational violence, along the same narrative than the one which was used by the Homeland Security Department of the US in 2000's, have been in fact the by-product of this rise in Europe of this guild of data managers and their interaction with the specialized police of antiterrorism and "serious" crime police squads who wanted to control at distance, a trend which was accelerated by the War on Terror in the US, especially after the Madrid bombings of 2004. The proposals on smart borders and interoperability are the sign of the influence of data managers in security in the last ten years.

Interestingly, EU-Lisa and the Commission in 2015 have re-used the terminology of logic of *silos* blocking communication and cooperation, in the same way that the post 9/11 Commission has done to criticize the purpose limitation and the separation of information between internal and external services launched in the 80s by the Church Commission after the evidences of intrusive and disruptive practices of FBI and CIA against the civil right movement. The parallel between the neo-conservative narrative of the US government of Georges Bush and the today commission's narrative may look too harsh to the reader and certainly the EU has not entered into a militarized option after 2015, but on both case they have proposed the same underpinning logic of a relaxation of democratic rules in the name of efficiency and among these rules at stake, purpose limitation has been perceived as a threat to interoperability, speed and efficiency of preventive antiterrorist policies.

So, my overall argument is not to deny the importance of the attacks of 2004-2005 or the ones of 2015 to 2017 and the sense of emergency they have created for the politicians to do something, but I argue that if the latest attacks of 2015 and 2016 have played a role in the push for digitization of controls, it is because they have created a *window of opportunity for the guild of digital technologies* to link strongly digital technologies and prevention of terrorism coming from abroad via the so-called need of interoperability. And, if digital technologies have been reinforced, it is centrally because the technologization and especially the digitization of the border controls has become a prime objective concerning the large-scale surveillance of the mobility of persons and an economy of data suspects( Author 2015) ). Only in this vision of the world, data analysts can control more and more the field of security, or so it seems.

As I will demonstrate in the last part, cooperation on border control via digital data sharing is not anymore, a means for the goal of enhanced security to protect the area of freedom of movement of the EU as it was presented in the beginning of the Schengen agreements, but it has become a goal in itself, serving the interests of the ones developing the technologies associated with it. Importantly, this "objective", which is more the result of a field effect than a strategy by a specific dominant group, is nevertheless the drive that all professionals of security, including the "stake holders", consider crucial: i.e. to "govern" travelers globally, via data management and ironically beyond border controls (Walters 2002)(Amoore 2006).

## The sociogenesis of the professional guild of digital technologies for security purposes and its agencification via EU-LISA

To make sense of the contemporary struggles around the digital technologies in security matters, it is necessary to analyze what is contributing to or affecting the course of the social development of technologies of border controls, and not to rely in the argument that they are only the reaction, the products of the most recent threatening events. The idea of interoperability is engrained into the history of Schengen in the European Union, and especially on the practices of actors connected with the Schengen Information System.

### At the origins of the Schengen Information System and its competitors: building an IT system efficient and politically acceptable, using a multi-purpose data base managing crime and entry of foreigners.

The initial configuration of police data bases has been set up by Interpol in the mid - seventies, and many intelligence services were sharing information by fax, satellites, or encrypted phone technologies, but the routines of using information systems began with the project in the European Union (still at that time called European Community) to manage in common the borders of a series of member states (Benelux, France, Germany) by accepting freedom of movement for citizen and third country nationals living there, but to create "safeguards", "compensatory measures" by "reinforcing" together the control at the "external" borders with the countries non-members of the common area. (see article on the origins of Schengen in this issue).

To connect the different police and immigration authorities it was decided to develop both police liaison officers, common police stations at the borders, and to dedicate policemen to learn informatics to share information through data bases on a bilateral or multilateral bases.

The Schengen Information System or SIS comes from the recruitment or contracting of a hybrid of persons in police and border guards having knowledge as data base skill users, and persons coming from high tech companies like Honeywell Bull, Siemens, Hewlett Packard or later on Steria (which became SOPRA-STERIA), who were IT specialists. The creation of the SIS tool was therefore also the creation of a specific field of professionals of (in)security management specialized in data management and IT security. This introduction of new players has, in the European Union, transformed the way policing and intelligence were done, and the way sovereignty and freedom were exercised. Beyond the juridical formulation of an area of freedom, security and justice, and its strong legal component, a specific logic of (in)securitization has prevailed, not only via discourse but via material design on border control technologies, visa and passports servers and biometric tools in various databases, but it was certainly not done in a monolithic way as we will see.

This move and redefinition of the boundaries of the field of European security has been and still is the result of multiple struggles between specific transnational guilds whose solidarities are related with specific know-how and communication at distance that have been described as different social universes or guilds populating the traditional forms of security agencies (law enforcement agencies, police with military status, liaison magistrates, police intelligence services, border guards and immigration management services)(Bigo 2013). These traditional actors have been challenged in the 1990s by the enlargement logic and in the 2000s by previous outsiders entering into the field of internal security with force

and coming from adjacent fields (military and signal intelligence services, private security firms connected with defense, customs agents, consulate agents and importantly for this research data scientists and engineers specialized in technologies and digital capacities of systems whose are designed for control and surveillance of mobility). These later actors are still heterogeneous groups but, by working together into specific places or formal agencies, they may form themselves a specific guild based on the digital capital and acting for the justification of human mobility surveillance, by the production of lists of data-suspects, largely beyond the argument of antiterrorism, and targeting all the "undesirable" subjects (Richmond and Valtonen 1994), the ones to ban in order to normalize the others.

The emergence of these new players who do not come from the police or military worlds, or even from customs and consulates, but from private civil engineers and data specialists, reframe the scope of the missions by introducing the digitization of data as the ultimate and perhaps unique tool of preventative security (the history of the group SOPRA and its merging with STERIA is telling about this entanglement of private interests https://www.soprasteria.com). Traveler surveillance beyond terrorism risk seems also to offer to this group an entry into the game of military intelligence and sigint intelligence agencies, as well as the capacity to impose some of their views to more powerful actors coming from defense.

As it has been discussed by Sebastian Larsson in his article on this issue, most of the material production, beyond the services of data analysts, is concerned with IT systems for security but also for different dual-use technologies which straddle between internal security (policing- societal security) and external security (defense and foreign intelligence), lethal and non-lethal armament, defensive and offensive cyber actions. The people specialized on IT systems and interoperability between these systems as well as the ones constructing border technologies are therefore a specific part of a larger group where all the actors are using their knowledge to build the connections between tracking, intercepting (legally or not) data, building risk indicators, channeling travel routes, and eventually exploiting mass of personal data to construct profiles of suspicion. In an ironic way, this end product of list of data suspects to check after risk profiling by scoring interlinked alerts on individuals, may be the best definition for the "smart borders" initiative. They are smart for their builders and help them via automation, but they are not really smart for their end-users despite the discourse that they help them to move faster and so to enhance their freedom (Author 2011).

It is impossible to do a detailed historical account of the birth and development of the SIS, but three major elements are worth noticing. First the emergence of the SIS has been presented as a condition of "success" of the Schengen agreement, replacing the idea of an area of freedom of movement, and the current dispute around Schengen concentrates also on the "survival" of the SIS. Second, the transformation of the SIS1 into a SIS2 via the transition of the SIS1-for-All at the period of the enlargement of Schengen to Eastern European countries is not a technical but a highly political move which has disrupted for a brief moment the trend toward preventative policing. However, SIS2 is de facto a new system which is not the follower of SIS1-for-All or SIS1, as it has developed beyond border controls checks, search tools giving the possibilities to run multiple searches and generating potential function creep in favor of police services regarding data bases on asylum, migration and borders. This is this logic which has been at the core of the discourse of the necessity of interoperability. Third, the impact of preventative arguments has justified in

2001-2004 and later on in 2015-2017 the use of large-scale IT systems based on data collection, retention and predictive profiling, putting at the very heart of the discussion on security, the digital technologies as “mediator” of the values of freedom, privacy, protection, security.

## The beginning of the SIS

Different researchers have considered from the very beginning of the Schengen Information System that the forms taken by policing foreigners and doing border controls were reframed by the technological modalities given priorities of the digitization of documents over face to face relations at the border. In relation with the intense debate about national sovereignty and fear of a function creep in favor of a neo-federalist view advantaging a European bureaucracy in the making, the computer scientists had to manage the degree of centralization of the management of information in a very political way (Georgakakis, Didier 2012). The vivid nationalist reactions obliged them to create a central system interconnecting the different national systems but containing no data in itself. It created a politics of securitization via the policy tools which will continue all along the development of an area of justice and home affairs (De Hert and Vandamme 2004; Michael and Michael 2008; Balzacq 2008). In addition, the development of digital borders and their implications in terms of privacy were explored by lawyers and IR specialists criticizing already a tendency to associate crime, terrorism and migration together via the argument of illegality (Bevers 1993; W. Walters 2006; E. Brouwer 2008; Guild and Bigo 2010).

The characteristics of computerization and the facilities to exchange data internationally, as well as the struggle around the codes and the formats of data have not been ignored, and the SIS has not been seen by everyone as a progress in the management of borders, despite the multiplication of advertisement for its efficiency. Tony Bunyan of Statewatch and many other NGOs have insisted from the very beginning about the problems arising from this type of computerization of data, in terms of error, of safety of the system itself, of data protection, of privacy regarding the individuals. ( Bunyan, Tony 1993)

But the message was not listened. The decoupling of state borders’ logics of control from the territorial border initiated by the Schengen agreement in the name of freedom of movement of persons – tempered by the fear of the rise in crime related to this freedom – exacerbated previous tensions concerning the narratives of national sovereignty and global insecurity. It destabilized the idea of what was internal and what was external to a national state inside the European Union. The internal security of a unique European space (or area) has been conceived as the coalescence of different national internal security spaces including, de facto, an external dimension for each national state that the limited effect of European citizenship has not succeeded in solving fully. It has therefore created ambiguities, raising new questions about controls and surveillance in the entire European zone and accepting the need to trust other police forces and to share responsibilities between these forces, as well as accepting the existence of some coordination points.

Typically, the creation of a horizontal group of informatics in Schengen to set up the characteristics of the SIS has been the place for many of these quite confidential discussions going far beyond the technical specifications. The precise history of this group and his legacy to set up the foundations of what we call European police collaboration through digital means is still to be done, but it makes no doubt that these actors have been central to build the “pre-history” of the EU-Lisa agency and the idea that they have to make choices which

will impact the next twenty or thirty years of the relations between freedom and security, just by the way they set up a path dependency organized around a specific technological choice (see Time Line Annex). They have also integrated the refusal of a federal Europe in their technical choices and have presented centralization as a danger and interoperability as the best solution, giving a specific tone to the debate of computerized technologies in security matters, different from other areas.
Mathieu Deflem has been one of the rarest to integrate this technological element in his history of policing (Deflem, Mathieu, 2000, Deflem, M. 2007). On my side, I have given different resumes of this emergence of a European guild specialized on the management of computerized exchange of information in police matters which appears in the mid-eighties, but become more powerful with the enlargement process of the EU and the number of participants to Schengen on one side and with its formalisation as an agency EU-LISA on the other side. (Author 1996a; Infantino et al. 2013; Author 2013)

The strong argument in favor of computerized information systems was to turn collaboration between different foreign services doing the same task into a routine. Collaboration needed to be an everyday task, and marginally, it was also for some countries a way to centralize the data on serious crime or terrorism in national bureau and not at the local level. Different Information Systems were discussed, on terrorism inside the Trevi group, which will give birth to Europol, on border controls, asylum, and visa (CIREA-CIREFI) groups in addition to the specific Schengen initiative. The European Information System, competitor of the SIS, collapsed, leaving the place to the private companies coming from a consortium led by Germany and France (Bull and Siemens). This created an advantage into the technical competition and oriented the system towards a “multi-purpose” data base but organized in “silos” to respect specific access of data; a policy which has been more and more combatted by police and border guards authorities.

Among these purposes, the most disputed was the article 95 of the Schengen Information System allowing to have a more “personalized” approach of control gathering the different elements of information towards a specific person. Privacy actors and the then EDPS have fought immediately this idea, but IT specialists saw lawyers negatively, anti-technologists, and they were keen to support the security actors, especially among them, the persons working for private companies. The SIS was therefore seen as a great way to settle the dispute in a “balanced” manner creating the conditions for a freedom of movement by removing internal border checks but, keeping the borders of the different member states safe by exchanging information electronically and by enhancing communications and “trust” that the other polices will work for the safeguards of all member states.

The SIS became the key argument to enter into the Schengen agreements in most of the Member states debates, and some countries refused to enter into Schengen but wanted nevertheless to be part of the SIS for police purposes. Operationalized in 1995, the Schengen Convention was seen as a success, mainly because of its computerized information system as the celebrations shown at the time and twenty years after (just before the Paris attacks). It derived from this long history of technologisation of police matters and border controls that the link between computerized technology, digital approach and security was strongly set up, while the objective of freedom of movement was almost forgotten.

## The SIS a digital technology translating crime and migration into “fields” for security matters: when registration becomes a search for linking crime and migration together.

If the SIS1 had been conceived as a system connected with the area of Freedom, Justice and Home Affairs, especially after the failure of the European System of Information as a competitor, its central goal was to coalesce the different spaces of the national organizations, initially five, into a functioning entity without hole in space or laps in time. The goal was to create a virtual boundary giving a sense of identity of all the persons inside and to promote practically “their” freedom. With the SIS2 twenty years after, it was not anymore, the core of the system. Identity has been turned into fear of otherness regarding transnational political violence, and even about “their” mobility, as migrants, “poor tourists” or “potential terrorists”. Suspicion of illegality became more important than the experiencing of freedom and the economic dynamic resulting of it. A transatlantic wind blows importing the argument that if the dots were not connected, intruders will certainly come, both on the territorial space or even worst into the IT system itself through cyber wars. Security was not seen as a protection of an area of freedom but as a necessity to have a “continuity” of surveillance anticipating danger, on both the spatial dimension and the virtual one (illegal migrants and hackers becoming almost identical in this regard of troubling the system). But, in such a political imaginary, continuity was even not the reproduction to the same, it was designed technically as a system of systems conceived as a permanent extension for managing more spaces and having more police functions available in order to anticipate in the future not only threats but also accidents. The argument that the present system was a blue print for the next step, for the future (perfect) system became a mantra organizing all the discussions. Therefore, the efforts have been about maintaining and developing the system for future extensions in order to secure the full space of all the EU members, while not creating one space controlled by one centralized entity. Future oriented action has not been set up to forecast multiple futures, but to avoid at the present time a worst-case scenario imagined by the police.

This trend reinforcing police powers and their willingness to pretend that they can be preventative if technologies are interoperable and data are searchable through predictive analytics has created this political move towards “interoperability”. Far from being something new, post 2015 it was already the argument in order to extend the initial Schengen to all the other member states, and to accept Italy (who has many terrorist and organised crime mafia like data bases) despite the reticence of the 5 other different ministries of Interior among the initial members, and it was then the same argument to accept Spain, Greece, as well as the Nordic states which had already an area of freedom of movement between themselves (including non EU members: Norway and Iceland). The accumulation of data in order to connect the dots of transnational crime has been the leit motiv of the permanent geographical extension as well as the functional one. This has, by the same token, isolated the UK, and only Ireland was obliged to join the UK to stay outside the Schengen area in the name of the struggle against IRA (a still dividing problem, as Ireland succeeded in other domains to have its autonomy, like with the euro). This disjunction between EU borders and “Schengenland” has nevertheless reinforced even more the fact that border controls national agencies needed to create a virtual system where they can be permanently in touch.

## The formalization and institutionalization of the role of data managers in the field of security professionals, the emergence of a new guild?

The drive towards digitization suggested by the initial discussions but not really implemented beyond police cooperation in terms of major crime and terrorism, became central to manage borders in an "integrated" way. Less visible than the coordination of the border guards via Frontex, the central move was to organize a virtual space managing the digital connections and all the IT apparatus necessary for the establishment of a common management, both technical and political (by avoiding centralization). Rapidly, the number of agencies by countries and the number of countries using the SIS for the purpose of border controls for TCN entering the external borders exploded. It was not anymore, an add-on, but became a central piece in the networks of data bases, especially for Germany, France and later on Italy, even if some countries like Portugal were continuing to prioritize for most of their actions Interpol links instead of the possibilities of the SIS. To convince national forces to use the SIS was a permanent fight obliging a strong lobbying.

Contrary to the natural history of a consensus to go forward, political struggles with other digitized systems (like Interpol) existed, and the reluctance of national and local forces were also strong, especially with the UK outside trying to propose other solutions. Nevertheless, digital Information Systems on Foreigners were considered more and more significant for border controls, and the securing of documents (especially passports and visa) as well as the systematization of biometrics in these documents became a way to extract, collect, share, transmit quickly information between national databases, at a speed superior to the speed of a plane travel. The UK went on to build the same kind of system.

The entry of the intergovernmental agreement of Schengen into EU law with the Amsterdam Treaty as well as the enlargement process with the accession of new member states into the Schengen area have been complex steps. Schengen and its SIS were not any more at the margins, or in advance, they became the core of the functioning of the area of freedom, security and justice. It became almost impossible to enter the EU without accepting the "Schengen acquis" integrally. This created a lot of resentment in many Eastern countries during the first enlargement and even more for Romania and Bulgaria in the second eastern enlargement when they were left outside despite their efforts to reorganize their police and border forces[3]. Once again, the argument of the necessity of interoperability of the data bases was used against their will to re-discuss the basis of the Schengen logic. They had to comply first at tests that they were up to date, even if at the same moment, the number of countries part of the SIS obliged to revisit almost completely the architecture of SIS (1) by developing a, by far, more sophisticated software, first by accelerating the speed of the system as well as the number of participants, and secondly on allowing searches on the Schengen database even if the searches were nevertheless restricted to specific national authorities whose conditions of access were depending on the motives described in the specific articles of the Schengen agreement.

[3] On 21 December 2007, the Schengen border-free zone was enlarged to include Estonia, the Czech Republic, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia.

Not much has been written about these key transformations of purpose, but it has propelled the idea that interoperable search between different national authorities was effectively useful for all national investigations and identification purposes. But this narrative was in fact a cover up for strong political disagreements regarding the entry of the new 10th into the SIS and a fight about the purpose of the SIS: border controls or prevention of terrorism and illegal migration. In a nutshell, the SIS called "one for all" and later, in an even more effective manner, the SIS-2, have modified the logic of digitization of border controls that was initially with the SIS1 activated to verify documents only into the current tools for identification and control of persons at the borders and beyond.

The period of the Portuguese presidency was crucial as the Portuguese destabilized for the first time the path dependency on digital technologies created by the EU Commission division of Frank Paul who was in charge of creating a SIS with search functions and platform of integration (SIS2), and the private companies (consortium of German-French companies) which were building the IT Systems. A small Portuguese start up presented in 2007 a cheap way to replicate SIS1 and offered its clone for a small price to the Eastern countries[4].

Largely sufficient for border controls, it was blocking the ambitious SIS2 project and its de facto function creep function in favor of intelligence and law enforcements that the new "features" were preparing.

The major member states and companies' reaction (France-Germany, their consortiums and some key members of the commission from these nationalities) was to oppose strongly to this impediment of digital technologies created by this simple solution of SIS1forall, and to insist even more on the creation of a SIS2 with searchable criteria through a strong coalition of private financial interests with the Commission and later on with the new EU antiterrorist coordinator, supported also by US interests. The first success of these tenants of a strong interoperability was to succeed to obtain that police officers and other law enforcement agencies (including prefectures administrative services dealing with foreigners) has access to the specific database on asylum seekers applying in Europe: Eurodac in 2011, despite the strong resistance of the European Data Protection Supervisor and its national counterparts, as well as the UNHCR. It was also simultaneously to have the creation of a "technical" EU-agency called EU-LISA set up in 2011, explicitly to run all the different existing data bases and their future projects, in order to be sure that no more other option can really emerge blocking the different smart borders projects They also insisted of the necessity of a creation of a Visa Information System (VIS) and to develop PNRs and entry exit systems that can be compatible both inside the EU and within the Global North area of civil aviation.

The fight between the two visions of the role of Information System and especially between the differentiation of access between police and border controls continued during at least three years. The Portuguese vision to maintain limitation purposes and cheap development was eliminated and the SIS 2 arrived in force after almost six years of delays in 2013. The new system changed the way police was working. The prevention discourse of the politicians of the time was sustained by a technique of multiple alerts creating what was called reasonable suspicion on some individuals and groups of population. Even if some police organizations were not keen to have so much data to look at, the drive to connect the dots, if necessary, in case of emergency, succeeded and the European Parliament accepted this "neutral" technology while insisting on the privacy question.

[4] In 2007, while developments were in progress, Portugal had offered the use of a version called "SISone4ALL" developed by SEF (Portugal's Border and Foreigners Service) and Critical Software.

But, they did not realized that what was initially a reporting system has been transformed with the SIS2 into an investigatory tool about organized crime and terrorism which has used the registration of foreigners entering the EU into art 95 and the one of asylum seekers applying for refugee status via Eurodac, as privileged “pools” to look for suspect, because they were built with the same formats and easy to search (Vavoula, Niovi. 2017). This so-called integrated border management has lowering the threshold for registering alerts. “Automaticity that was prevented through the insertion of a proportionality clause has been deployed at the national level, and progressively endorsed at EU level in a bottom-up process with minimum transparency and scrutiny “(Vavoula p134). “Crucially the interlinking of alerts has created the possibility of the merging of purposes, whereby a person’s data becomes relevant in multiple contexts” (Vavoula p136).

In addition, the authorities granted access to the system were directly linked to the introduction of collecting biometric data. This means, at the very least, that third-country nationals who have in some way attracted the attention of national administrative or law enforcement authorities due to their misconduct becomes privilege targets for serious crime and terrorism suspicions. And this suspicion through creation of list of individuals that emerge from the multiple signals of risk that they carry will be often merged and analyzed as one profile as if to have been illegally in the EU was transforming you into a potential drug dealer or terrorist.

The access of law enforcement authorities to Eurodac and their access to the Visa Information System (VIS), in order to check the stored information on all short-stay visa applicants who are, in principle, unsuspected of any misbehavior, have worked to create potential associations of a person with a series of danger by interlinked alerts. Interoperability has finally changed of logic, abandoning the sole purpose of border check for the ones of creating lists of data suspects. But what is the legitimacy of this new purpose? Is it not a danger in itself, a solution that fails by successfully implementing more of its initial mistakes?

To say it more crudely, is the fact that missions of consulates decide about visa refusal, could be considered as a good indicator to find unknown criminals or terrorists? Are all the people suspected of crossing borders illegally more susceptible to be criminals or terrorists than others who have not move? These assumptions that violent and criminal networks are merged with the networks of forced migrants and people who want to visit Europe, are certainly not validated by statistical facts. Most of terrorists who died in operations were born in their own country, had the citizenship of it, and did not travel abroad frequently. Despite a lot of noise in the media, almost none of them where returning from places of conflicts, they were inserted into the society they fought. In effect, these assumptions about foreignness and enmity create breaches of privacy on one topic and by their modes of interlinking alerts, are transforming specific alerts into a mode of creating scores to build data suspects, a procedure which will become even more a problem after the 2015 Paris attack. The process of creating an (in)security continuum through association of risks transversal to different subjects despite the restriction of access which is still at work, is therefore creating a way to govern all mobile populations entering into the area by a form of electronic surveillance based on their digital traces and the guess that authorities may have about their future activities.

## EU-LISA and Smart Borders: from Integrated Border Management (IBM) to Integrated Data Management (IDM).

Smart border has been a terminology in use for a while. It has taken a different take when applied, as explained by Julien Jeandesboz and Susie Allegre, to the introduction of an EU travel authorization scheme for persons who are *not* subject to visa requirements. This was first considered in the 2008 Commission communication on 'Preparing the next steps in border management in the European Union' (Jeandesboz, Julien, Allegre, Susie. 2009). The proposed measure was dubbed 'EU-ESTA' in reference to the Electronic System for Travel Authorization that US authorities eventually introduced in 2009 for travelers from countries participating in the Visa Waiving Program (VWP). In 2011 plans for EU-ESTA were discarded after the Commission communication on 'Smart borders – options and the way ahead' raised doubts about the necessity of such a measure by the resistance of the EU parliament. Despite this assessment, and less than five years later, the European Commission announced nevertheless its intention to return to this matter in its April 2016 communication on 'Stronger and Smarter Information Systems for Borders and Security', but this was after the 2015 Paris attacks and the series of events connected with the Daech attacks on France and Belgium and elsewhere during 2015 to 2017, and before their defeat on their soil in Syria. The interoperability argument was relaunched and white washed of its defaults regarding privacy and discrimination and used against the key notion of purpose limitation, in order to develop a "collect it all "data logic.[5]

As we have just seen, we cannot see a "grand strategy" into this reconfiguration. In fact, various heterogeneous networks of actors have worked on the building of data bases for security purposes from the mid-eighties to the 2010s and they had not in mind to build a system of inadequate suspicion, but the result is there, as a field effect wanted by nobody, but having discriminatory effects. The IT specialists are not innocent and neutral in that game and share responsibility for these effects. If they were almost invisible and marginal as players in the beginnings, they have been more and more efficient to impose their technical design as substitute for political agreements, now they have to assume. From the creation of EU-LISA in 2011, they have finally played the same strategy than the other security professionals by lobbying to have their own "operational" agency and after by justifying their agenda as the best way to keep safe the population from "all sorts of threats and risks".

## The agencification of the providers of technologies, private IT specialists and data analysts specialized on border security: a transatlantic information awareness in the making?

All the new proposals that EU-LISA has proposed under the terminologies of "smart borders" have been set-up in this effort to connect more agencies of different purposes all together in order to better "identify" individuals entering the EU, not via their narratives or documents given by their own states, but by an inner shared knowledge about them, even if

[5] The EDPS has criticized the proposals on this very specific line: As he says "facilitating the access by law enforcement authorities to non-law enforcement systems (i.e. to information obtained by authorities for purposes other than law enforcement), even to a limited extent, is far from insignificant from a fundamental rights perspective. Routine access would indeed represent a serious violation of the principle of purpose limitation. The EDPS therefore calls for the maintenance of genuine safeguards to preserve fundamental rights of third country nationals."

it is the first time they are coming. They have therefore reinforced the argument that they can predict via big data, patterns of abnormal behaviors, even for persons they do not know. It has had a central effect by transforming the locus of borders as a locus for checking data suspects against specific profiles, and to change the nature of the border guards' role. They share now more and more the habitus of intelligence services or they want to. They think of themselves as risk profilers and not as "guards". They know also that they have the possibility to be the intermediary point of contact between the virtual world of data and the physical presence of individuals who want to enter a country, and that he gives them by far more importance than before, revalorising their positions regarding specialized police forces[6]. Be it the EES, the ETIAS or the ECRIS-TCN proposal, it seems that all the proposals that EU lisa and the Commission have proposed are increasing a reliance on mass data processing as well as on automated processing, interoperability between information systems, and data mining and profiling characterised as 'risk assessment' located at the "virtual" pre border area of the registering for entry exit system[7]

We cannot develop all examples but a key element on this reconfiguration has been the discussion of the ETIAS proposal. This ETIAS proposal foresees that all travelers to the Schengen area not subject to visa requirements shall be obliged to obtain authorization prior to their departure through an online application. The travel authorization requirement does not concern EU citizens, holders of a valid residence permit or a local border traffic permit, among others, but applies to *third-country nationals enjoying the right of free movement who do not hold a residence card, including third-country nationals who are family members of a Union citizen* and to whom Directive 2004/38/EC applies. The delivery of an authorisation to travel under the ETIAS scheme is conditional upon the automated processing (comparison) of applicant personal data held in existing information systems, such as the Schengen Information System (SIS), the Visa Information System (VIS), Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), the EES, Eurodac, the European Criminal Records Information System (ECRIS), and the Interpol Travel Documents Associated with Notices database (TDAWN); in the ETIAS-specific watchlist established by the ETIAS proposal; and specific risk indicators that are kept secrets.

If we consider the volume of personal data it will process, ETIAS should be conceived as a platform for mining and profiling personal data rather than a platform for issuing automated or manual travel authorization decisions. "The ETIAS screening rules aim to identify persons who are otherwise unknown to responsible authorities of the Member States but are assumed to be of interest for irregular migration, security or public health purposes". These persons are flagged not because of specific actions they have engaged in, but because they

[6] The PHD of Georgios Glouftsios details the different steps of this move from Integrated Border Management by EU-LISA. He explains the link between the interoperability logic and the project of a form of Transatlantic Information Awareness based on connecting the dots and of predicting behaviors and trajectories of mobile people. This is one of the rare piece available on the importance of digitization of data regarding security in Europe and the key role of engineers, IT specialists and data analysts in framing what is security, not so much through discussion about security limits, but through the technical "design" on the exchange of communication between the different agencies and the permanent argument of the necessity of the continuity of the maintenance of the digital network, and the extension of functions perform by the system as well as the number of agencies to be connected. The PHD is not yet available but elements are on Glouftsios G (2018) Governing Circulation Through Technology Within EU Border Security Practice-Networks. *Mobilities.* 13(2): 185-199.

[7] EES : Entry/Exit System

display particular category traits. While not directly a data mining and profiling measure, the ETIAS watchlist is nevertheless future-oriented by aiming to deny travel authorisation to individuals whose authorities believe they are likely to commit criminal offences in the future (Vavoula 2017). This created a strong mobilization of the privacy and fundamental rights authorities as well as Ngo's activists working for the Courts to condemn these projects. The climate created by the Snowden disclosures on the NSA was also important to put a stop to this "collect it all" logic.

But as a variety of attacks occurred around Europe and with particular force in France, the push towards coordination and in the end interoperability of (some) databases, those containing personal data on third country nationals, became once again seen as "the" solution to solve all problems (see the specific article on interoperability after 2015 in this issue).

For the people willing to cross borders it has created a ban-opticon normalising most of the travelers but abnormalizing a small minority on dubious criteria obtained by correlations of data and no real causalities (Author 2007). Now, the individuals at the borders, or in front of their computers asking for an entry, are more and more reduced to a data subject potentially suspect and-or a body waiting on queue to be check again, not any more considered as an individual asked to give proof to its own identity but as a container of its own digital and physical traces.

The system at work is operationalized for dialogues between the bureaucracies of control at distance and is de facto inattentive to the interactions with the human being in front of the controllers; the identification of a "data subject" has become a "test" to pass for avoiding being categorized as a "data suspect". This data-suspect logic therefore supersedes the control into an entry of freedom of movement to become a tool of management of physical objects by the correlation existing between this object and the traces left in the digital world. The professionals of computerization by what they call "interoperability" have succeeded the operation to transform the physical world into an "off-line" world which has to obey to the logic of the "online" world. Data analysts and IT specialists had gained a way to frame the boundaries of security through technology competing directly with the traditional security professionals coming from police organizations and from specialized EU bureaucrats, and in addition they have been granted to have their own "agency" to develop this program of governing all mobile people via digital information, welcoming them in the so-called world of "smart borders"

In conclusion, the phenomenon of a digitization of control played out with the role of data-bases in the management of mobility is therefore the trend which explains how the debate between freedom and security has been technologized during almost thirty years and are now let in the hands of "solutionist" managers who act by default of political in-depth discussions. I have, therefore, insisted on a long-term perspective, on a socio-genesis of the conditions of possibilities that have made this transformation of the field of security professionals now more and more dependent on digital technologies.

The willingness to connect the dots by doing large scale data collection and retention, screened through profiles of risk analysis on degree of foreignerness and dangerosity and scoring all passengers traveling in order to focus on the 1 to 5% considered as the "most suspects", is profoundly irrealist. It is supposed to solve, by risk calculation based on

algorithms, the questions of violence and illegal migration without the necessity to reach a political agreement between EU member States and their transatlantic partners, who have very different visions regarding migration. Technology is therefore seen as a solution to avoid major political disagreement by desecuritizing , depoliticizing the issue itself; issue reduced to the problem of "efficient border controls". This way of "mediating" security and freedom via technologies of interoperability and to present them as "inocuous" and non political, ("neutral") is therefore a powerful tools in the hands of the EU bureaucrats to be in charged as much as the national politicians (Papilloud, Christian 2005). It tends to present alternatives to the conflictual relations between different political and ethical orientations towards foreigners and national identity, under the label of expertise, neutrality and science. The so-called move from Integrated Border Management (IBM) to Integrated Data Management (IDM) is ultimately the marker of the rise of these computer and databases specialists who are the producers of these numerical technologies and who are populating the EU-LISA agency of the EU as well as the recipients of the EU-funds given to some very specific private companies.

They want to become the cunning reason of mobility control by the way they activate the virtual reality of data and computers in order to manipulate space and time at will around a series of bodies moving and by producing "data-suspect".

They claim that security is done by channeling space, by anticipating time, by speed of movement, in a "neutral way" independent from the unique person, that only a group profile makes sense. However, they are not necessarily effective outside of physical coercion by other means. For them the body of the individual is less important than the *data suspect*. The body is just "its emulation". The tools of surveillance and control which are operating follow and stop the bodies, touch them, detain them. The data suspect logic is therefore different from the detention of the physical person and is configured to erase the hope of the latter to resist via narratives of its own identity and even the allegations of documents provided by other states. These techniques do not work anymore. The identification of biometric recognized by all the different systems through interoperable connections replaces the written and oral identities 'claims on the moment of the encounter.

The results of the move from an integrated border management model to a model based on Integrated Data management are no longer directly targeting border control, they manage digital information system at the transnational scale to "immobilise preventatively" what has been called the escape of individuals and what Emma Mc Cluskey has investigated in Morocco in terms of resistance to this data management program that always fail, but always justify that the failure is the proof of a "not enough" and not a "too much" technology of connecting the dots digitally for a better awareness (see this issue).

The ways the system is constructed by the influence of this guild of digital technologies, as well as its goals, are at the end related to the constitution of a *data politics integrating security as one sector only of a more general management of the coordinates of space, time and life by algoritmic calculations*; calculations which need to be evaluated for the distribution of good and harms they provoke (Bigo, Isin, Ruppert. 2019).

# Bibliography


Amoore, Louise. 2006. ‘Biometric Borders: Governing Mobilities in the War on Terror’. *Political Geography* 25 (3): 336–351.

Balzacq, Thierry. 2008. ‘The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies’. *JCMS: Journal of Common Market Studies* 46 (1): 75–100.

Bevers, H. 1993. ‘Police Observation and the 1990 Schengen Convention’. *European Journal on Criminal Policy and Research* 1 (4): 83–107. https://doi.org/10.1007/BF02249467.

Bigo, Didier. 1996. ‘Frontiers and Internal Security in the European Union : New Stakes of the Eastward Enlargement’, November, 20.

Bigo, Didier. 2011. ‘Freedom and Speed in Enlarged Borderzones1’. In *The Contested Politics of Mobility: Borderzones and Irregularity*, edited by Vicky Squire, 87:31.

Bigo, Didier. 2013. ‘The Transnational Field of Computerised Exchange of Information in Police Matters and Its European Guilds’. In *Transnational Power Elites: The New Professionals of Governance, Law and Security*, 155. Niilo Kauppi, Mikael Madsen.

Bigo, Didier. 2015. ‘Electronic Large-Scale Surveillance and Watch Lists: The Products of a Paranoid Politics?’ *REMHU: Revista Interdisciplinar Da Mobilidade Humana* 23 (45): 11–42.

Bigo, Didier. 2016. ‘International Political Sociology: Rethinking the International through Field(s) of Power.’ In *Transversal Lines*, edited by Tugba Basaran, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker. Routledge.

Broeders, Dennis, and Huub Dijstelbloem. 2016. ‘The Datafication of Mobility and Migration Management: The Mediating State and Its Consequences’. In , 242–60.

Brouwer, E. 2008. ‘Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System’. *Immigration and Asylum Law and Policy in Europe* 15: 1–596.

Brouwer, Evelien. 2005. ‘Data Surveillance and Border Control in the EU: Balancing Efficiency and Legal Protection of Third Country Nationals’. *Working Paper - WP14*.

Bunyan, Tony. 1993. *Statewatching the New Europe. A Handbook on the European State.*

De Hert, Paul, and Luc Vandamme. 2004. ‘European Police and Judicial Information-Sharing Cooperation: Incorporation into the Community, Bypassing and Extension of Schengen’. In *ERA Forum*, 5:425–434. Springer.

Deflem, Mathieu. 2000. ‘Bureaucratization and Social Control: Historical Foundations of International Police Cooperation’. *Law and Society Review*, no. 34.3: 739–78.

Deflem, Mathieu. 2007. ‘International Police Cooperation Against Terrorism: Interpol and Europol in Comparison’. In *Understanding and Responding to Terrorism*, edited by Huseyin Durmaz, Bilal Sevic, Ahmet Sait Yayla, and Siddick Ekici, 17–25. NATO Science for Peace and Security Series. E. Human and Societal Dynamics, v. 19. Washington, DC: IOS Press.

Guild, Elspeth, and Didier Bigo. 2010. ‘The Transformation of European Border Controls’. *Extraterritorial Immigration Control: Legal Challenges* 21: 257.

Infantino, F., S. Carrera, E. Guild, and D. Bigo. 2013. ‘Bordering at the Window: Schengen Visas Policies and Allocation Practices at the Italian Embassy and Consulate in Morocco’. *Foreigners, Refugees or Minorities? Rethinking People in the Context of Border Controls and Visas*.

Jeandesboz Julien, Alegre, Susie. 2009. « External Dimension of the Area of Freedom, Security and Justice ». Report. European Parliament.

Michael, Katina, and Michael G. Michael. 2008. 'Schengen Information System II: The Balance between Civil Liberties, Security and Justice'. *Australia and the New Technologies: Evidence Based Policy in Public Administration*, 247.
*Noiriel, Gérard. 2006 - Introduction à La Socio-Histoire. Gallimard, Paris*.
Richmond, Anthony H., and Kathleen Valtonen. 1994. 'Global Apartheid: Refugees, Racism, and the New World Order'. *Refuge: Canada's Journal on Refugees* 14 (6).
Vavoula, Niovi. 2017. « European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications ». *Queen Mary School of Law Legal Studies Research Paper*, nº 256.
Walters, W. 2002. 'Mapping Schengenland: Denaturalizing the Border'. *Environment and Planning D: Society and Space* 20 (5): 561–80. https://doi.org/10.1068/d274t.