MSc Thesis DRAFT

Athens, June 2020

"The technopolitics of smart borders"

by Vasilis Argyriou
Graduate Program in History and Philosophy of Science and Tcehnology
Department of History and Philosophy of Sciences
National and Kapodistrian University of Athnes

Contents

Introduction

Objectives and argumentation of this thesis

Chapter 1

1.1 Border and migration studies

1.2 History of Technology and STS

1.3 Bringing border and technology studies together

1.4 Methodology

Chapter 2

2.1 European migration policy and the case of Greece

2.2 Defining ‘Smartness’ in technological assemblages

2.3 Placing the Smart concept in European borders

Chapter 3

3.1 The ongoing case of ‘Smart Borders Package’ in EU

3.2 Technical overview of Entry/Exit system, ETIAS and interoperability

3.3 Efficiency and feasibility through rhetorics: A critical assessment of the results on test pilots in Greece

3.4 Moving beyond biometrics. The case of iBorderCtrl

Conclusion

Introduction

Borders have always been around us throughout history; either visible with the form of fences around homes and institutions, either with the form of concrete walls and checkpoint hotspots around countries defining territories and nation states, either hidden and integrated in our social formations. While open society declarations as well as the Schengen Agreement among European states presuppose the free flow of people, goods and capital, at the same time we face a seemingly paradox phenomenon, that of the multiplication of borders both physical and virtual. The ongoing bordering process that takes place in 'high risk areas' incorporates more information technology and military management in compliance with the C4i dogma (command, control, communication, computing, Intelligence). The EU confronted "with a serious migration and asylum crisis, a brutal wave of terrorist attacks and increased foreign interference" (European Council, 2020:2) as well as to better facilitate 'bona fide travellers urges the development and implementation of digital surveillance and control policies, initiating programs such as "The Smart Borders Package", entrusted by the Commission to the Agency for the Operational Management of large-scale IT Systems in the area of Freedom, Security and Justice (eu-LISA). Initiated and funded by Seventh Framework Program (FP7) for research and innovation and the Horizon 2020 agenda, the agency's plans are to implement more sophisticated and interoperable systems to optimise the border control management of the external Schengen borders. Automation of identification and verification procedures with the help of machine learning applications, deployment of biometric systems including facial recognition detectors, fingerprint readers and potential future installments such as Artificial Intelligence lie detectors.

The Commission initiated a technical study to identify and assess more suitable and promising options and solutions for the legislation proposal, followed by a Pilot project based on this Study in selected countries-members of the EU. Aim of the pilot project was to examine the feasibility of the proposed techniques implementing them in specific 'high risk' areas around the EU, and was conducted under the "Agency for the Operational Management of large-scale IT Systems in the area of Freedom, Security and Justice (eu- LISA)".

Under these administrative agencies, biometric technologies are presented as necessary for "addressing the need for the Schengen Area to move towards more modern and efficient border management by using state-of-the-art technology" (Smart Border Pilot Manual, 2013:2). Apart from the already traditional biometric techniques that have undergone heavy critiques regarding violations of basic human rights as well as feasibility and efficiency concerns, there are other programs that have just completed their test pilot phase promising to move beyond biometrics. The iBorderCtrl consists among others subsystems, of a lie detection system, that operates algorithmically and by machine learning, to detect deceptive behaviours by examining micro expressions of the face (iBorderCtrl, 2018a). It is considered among the possible deployments alongside the general smart border assemblage to help facilitating mobility and prevent terrorism.

Aim and objectives

One important aspect of the EU visa regime as Parusel and Schneider has argued, is that fulfils the strategy to control the mobility of third country nationals prior to their entry into the country, i.e., extra-territorially (2012). This practice, among others, allows and steers the ongoing dislocation of borders in space and time. Following these assumptions I attempt to argue that the ongoing digitalisation of borders is expanding further a technopolitical regime. A process that incorporates

state of the art technologies such as biometrics and AI lie detectors, software based-virtual environments for sorting and controlling mobility, dislocating borders around space and time but also managerial practices on site, military and police deterrence and deadly push backs, as well as 'old school' borders such as walls, razor wired fences, fishing nets across sea borders and hot spot centres for detention. This "strategic practice of designing or using technology to constitute, embody, or enact political goals" (Hecht, 2011:19) appears in the technical proposals of the 'smart borders' system, and on the role and impact of the agents and the stakeholders that are related with the process and the overall process of shaping European identity.

One aim of this paper is to study the smart borders assemblage through their test pilots, as complex technological installation that interacts with the emergent socio-political discourse and public policy making, using tools from the STS field such as the technopolitics, border studies and migration studies. One main argument is that or the ongoing smartification of borders though the project of 'smart borders' and 'iBorderCtrl' is expanding further a technopolitical regime for european mobility. The 'Smart Borders Package' should not be seen as a mere linear process of anticipated technological progress or modernisation but as a way of flexible state intervention for managing 'crises', invoking new disciplines that require new legislative proposals to tackle an emergency situation, and the implementation of innovative devices and systems.
This technopolitical regime paves the way for more robust surveillance, migration management and a way to the ideal of integrated Europe that fulfils Schengen provisions, while reshaping its identity and tackling (bio)political concerns for managing population movements inside its area. This study is meant to become part of the general literature attempts for better understanding the sociotechnical character of the border phenomenon, its constitutional contingency as an apparatus and the bio-political power that holds, using theoretical concepts from History of Technology and the STS field, border and migration studies. It can contribute as an analysis of public policy for security matters and as an analysis of power distribution through technologies, useful for border studies, governance and security studies, political science, critical studies of geography and the STS field.

Chapter 1
Literature review. Embedding into academic literature

Border and migration studies

Border studies have been very productive explaining the nature, and the constitution of the borders, their historical origin and their general functionality inside society. (Bigo, 2008; Houtum & Naerssen, 2002; Lyon, 2003, etc.) Earlier scholars used to give great attention to the role of the nation-state in its sovereign territory and the focus of research was more geographical. The State had been a profound answer for all the questions concerning the border phenomenon, but as Chris Rumford argued, developing the idea of a cosmopolitan border, this is not a satisfactory answer as an explanation for our times, because borders are woven into the fabric of our society, able to provide at the same time insights in networked connectivity as well as in questions of identity, political conflict and societal

transformation (2014). One main conceptual shift in recent academic literature, lies in an understanding of borders as something inherently social and cultural rather than exclusively political (Scott and van Houtum 2009). In this sense, movement of people is rendered as a central political concern through discourses about management of migration (documented or undocumented), internal security, organised crime and terrorism, technological progress and digital transformation of governance, protection of the European way of life and asylum rights. Thomas Nail goes even further arguing 'Material border technologies are the concrete conditions for the principles and ideas of social life' (2016:5).

Governing the circulation of populations is one of the top priorities in political agendas since the dawn of modernity maybe even earlier, but nowadays, global mobility is considered as a constitutive condition for the 21st century along with the flow of goods and capital, while at the same time as the main source of insecurity for the so called first countries and advanced nations. One thing is certain, mobility of people and things must be predicted, acknowledged and controlled. Didier Bigo has offered an analysis and a concept for this kind of political intervention, termed as 'the politics of unease' and resumed into one principle: 'the obligation to choose who the enemy is and to declare it publicly' (2008:3). For Bigo the actual process of bordering is driven by security professionals in a globalizing world capable of creating systems of justifications for their activities.

The EU's reliance to scientific technologies and managerial expertise in the politics of border management indicates and confirms Bigo's analysis for managerial expertise in borders and mobility but also indicates the exercise of a bio power in which "the bodies of migrants and travellers themselves become sites of multiple encoded boundaries" (Amoure, 2006:336).

The proposed security regimes or what we can call as 'bordering' seems and even presented as an alternative way towards an integrated and interoperable EU. As Scott has pointed out, this process may be considered "as a laboratory of political, social, economic and cultural modes of bordering" (Scott, 2012:84).

The homeland security discourse is used for the intensification of the external borders of the EU, following the rationale of the United States security policy that was taking place at least two decades earlier. That was also a call for a globalised security policy which translates to more complex surveillance policies; technologies of governance in the sense that Michel Foucault has argued, are constituted from political discourses and scientific management but also from the governmental practises themselves and both the materiality and technicality that they need to get into action (2007). In this context, we feel no surprised about the proliferation of the war paradigm and war practices embracing the plethora of borders, walls, wired fences and detention centers that are endlessly constructed around us. They may be physical or digital or hybrid; either way, as Irma van der Ploeg has stressed "External borders are reconstructed in ways that can be summed up as fortification, militarization, and informatization"(van der Ploeg 2013:178). Informatization applies also to the bodies; they constitute machine-readable bodies through their transformations to digital codes (2005). Mezzadra and Neilson argues on the border as method 'the border is for us not so much a research object as an epistemological viewpoint' (2013: 18) and Dijstelbloem has coined the term of the 'migration machine' as a metaphor that helps to evaluate the role of technology, combines social and

technical reality and consists not only of high-tech, but of politicians, policy makers and military police (2011); one important aspect in migration technology policy is that "the spotlight is much less often focused on what happens during implementation, let alone the specific role of the type of technology used"(2011:13). Trauttmansdorff has studied the emergence of digital borders, focusing in the first proposal of the 'Smart Borders Package' which was proposed in 2013 and argued that "technologically mediated European borders are not only envisioned to facilitate control, but also to allow circulation" (2017:122). He points out, "that governing mobility in efficient ways does neither require a border as a wall or a fence, nor does it attempt to arrest movement entirely, but aims to function rather as a filter" (2017:117)

Border studies have come a long and productive way to analyse many of the complexities of the bordering phenomenon and their relations with emergent sociopolitical discourses and materialities.

Migration studies

Research on migration does not necessarily pays attention on questions of movement but also on the power of discourses, practices and infrastructures that both facilitate as well as hinder, halt and prohibit movement (Sheller, 2011). As Skeggs points out,"Mobility and control over mobility both reflect and reinforce power. Mobility is a resource to which not everyone has an equal relationship" (2004:49). The modern world market relies on rapid and incessant mobility; on one hand the bona-fide travellers of all kinds, state and business representatives, carrier services for transporting products around the global and the rapidly expanding tourist industry and on the other hand the asylum seekers, refugees struggling to escape wars or environmental disasters and migrant workers. There are certainly many other social groups on the move although they may fit in one of the two categories or somewhere in the middle and the fact is that the scale of mobility is massive. For all these bodies on the move new technologies are designed and implemented that improve the mobility of some groups and halts it for others, strengthening their immobility. It is also through the process of this movement that that bodies are marked as `different' in the first place (Ahmed, 2000). One interesting aspect as Sheller and Urry indicate is that these kinds of mobility show little sign of abating ever after 9/11, the outbreak of severe acute respiratory syndrome (SARS) due to coronavirus, multiple suicide bombings of transport networks, and other global catastrophes (2006).Terrorists and spies are on the move as well as legalised and illegalised products and materials are, like guns and drugs or alcohol and petrol. A 'new mobility paradigm' has emerged for the social sciences as Sheller and Urry has argued in their seminal and homonymous article that include contributions from cultural studies, anthropology, science and technology studies, migration studies transport and tourism studies. De Genova has written about "the legal production of illegality" (2002, 2005), processes of illegalisation come along with regimes of borders and 'unauthorised' migration and law practices that render migrants as 'illegal

aliens', and must be seen as a tactic that produces conditions for the production of new categories of minorities vulnerable to the recriminations of the law.
Baas,& Yeoh also point out, the systems that govern or facilitate mobility are deeply infused with notions of il/legalities that in themselves are constructed upon sociocultural and political ideas of belonging and what the nation-state is imagined to stand for (2018). Technological and managerial

Science and technology studies

One important aspect of the EU visa regime as Parusel and Schneider has argued, is that fulfils the strategy to control the mobility of third country nationals prior to their entry into the country, i.e. extra-territorially (2012). This practice, among others, allows and steers the ongoing dislocation of borders in space and time. Considering borders as method as Neilson and Mezzadra argued and not only as a research object, provide an 'epistemic' angle that allows insights about its productive power that filter and sorts flows, labor, goods and information (2013). Following these assumptions I attempt to argue that the ongoing digitalisation of borders is expanding further a technopolitical regime. A process that incorporates state of the art technologies such as biometrics and AI lie detectors, software based-virtual environments for sorting and controlling mobility, dislocating borders around space and time but also managerial practices on site, military and police deterrence and deadly push backs, as well as 'old school' borders, such as walls, razor wired fences, fishing nets across sea borders and hot spot centres for detention. This "strategic practice of designing or using technology to constitute, embody, or enact political goals" (Hecht, 2009:19) appears in the technical proposals of the smart borders system, on the role and impact of the agents and the stakeholders that are related with the process and the overall process of shaping European identity.
The term of technopolitics refers "to the strategic practice of designing or using technology to constitute, embody, or enact political goals"(p.19) As Hecht clarifies, "Opening the black boxes of culture and technology simultaneously can give us insight into how technologies constitute a terrain for transforming, enacting, or protesting power relations within the social fabric. Taking politics and culture seriously as objects of analysis greatly deepens our understanding of technological change" (10). Different policies even contradictory at a first glance can be inscribed at the moment of technological system design and their reconfigurations can be dynamically depended on political and institutional, scientific and sociocultural networks. Technopolitics pays attention to the historical importance of technoexpertise and their capacity to shape political ideas by embedding them upon technical proposals and design. Technoscientific neutralness is publically presented as a safe pathway for tackling certain important and often controversial political matters; by 'black boxing' crucial

elements of technical configurations, many capabilities or potentialities of the technological systems are concealed. The technopolitical regime concept, proposes that political, cultural and technical problems are not distinct and none of them is given in advance; instead their intertwined relations co-construct political, cultural and technical issues as well as national identities.

1.4 Methodology

Textual analysis, literature search, media research will be used.

During the study several conference reports of associated agencies, executive summaries, reports on the public consultation, regulations of the EU were examined. Official documents of the eu-LISA agency such as technical studies on smart borders, technical report annexes on the pilot project alongside with the legislative proposals of the European Committee and its socio-political discourse for matters of security, mobility and human rights. Public policy manifestations regarding securitization and migration control in Europe are collected and examined the public discourse (political manifestations, articles/interviews from the media, regarding securitization in the EU

Chapter 2

2.1 European migration politics and the case of Greece

Greece is regarded to be on war for one more time but this one is of a different kind; it is considered as an asymmetric warfare while the migration crisis an 'asymmetric threat'[1] for the borders of Europe, as the prime minister has noted. This special kind of warfare takes place along the borderlines with Turkey which"has turned into an official migrant trafficker" using its prisoners-migrants as 'bullets' and as a pressure technique for negotiating with the EU. The borderline territories are rapidly transforming through managerial expertise and cooperation of the National Army, Police forces, Frontex teams and groups of xenophobic individual locals that patrol voluntarily the area around Evros borders for 'intruders'. Nearby the conflict area, a huge concrete wall 10.3 km long that required more than 6.000 q.m of concrete and longer than 140 km of concertina and razor wire[2] was built in 2012 to deter the migrants coming from the turkish coasts. After the erection of the wall, the so called 'balloon effect' as it is known in policing and crime prevention studies or in migration scholars has taken place. Building the wall has simply rerouted the migration flows through the Aegean Sea, leading to unequalled refugee deaths from drowning. Almost eight years later, the greek government reacted once more with the deployment of surprisingly simple in design, yet unfeasible and offensive bordering techniques; in 2020 they announced their technical considerations of placing anti-migrant[3] floating barriers nearby Chios and Lesbos islands along with the turkish coasts to prevent the illegal boats from entering the greek territorial waters. Having a closer look to the technical requirements of the sea fence, it becomes clear that in normal operations what was ordered by the Greek government are plain sea garbage collector nets that can be also used for preventing medusas, plankton, oil slicks or other unwanted sea creatures[4].
In March 2020, Frontex agreed to launch a rapid border intervention to assist Greece in dealing with the large numbers of migrants at its external borders after official request of the Greek government.

> "Given the quickly developing situation at the Greek external borders with Turkey, my decision is to accept to launch the rapid border intervention requested by Greece. It is part of the Frontex mandate to assist a Member State confronted with an exceptional situation, requesting urgent support with officers and equipment from all EU Member States and

1 For more details see: https://www.ekathimerini.com/250159/article/ekathimerini/news/mitsotakis-says-migrant-crisis-has-become-asymmetrical-threat
2 https://www.kathimerini.gr/1055479/article/epikairothta/ellada/to-empodio-poy-alla3e-ta-dedomena
3 https://www.theguardian.com/world/2020/jan/31/greece-defends-anti-migrant-floating-barrier-amid-growing-criticism
4 https://www.scribd.com/document/444884904/P1Γ16-PX6#download&from_embed
For further reading about the technical requirements see the call announcement "Συμβάσεις-Διαγωνισμοί [Η Υπ'Αριθμ.02/20 Πρόσκληση Συμμετοχής σε Διαπραγμάτευση, για την Προμήθεια Πλωτών Προστατευτικών Συστημάτων (ΠΠΣ) προς Κάλυψη Κατεπείγουσας Ανάγκης Οφειλόμενης σε Γεγονότα Απρόβλεπτα

> Schengen Associated Countries," Frontex Executive Director Fabrice Leggeri., (FrontexNews release, 2020)

Surveillance capacity is already increased at the Greek borders but under the new urgent and exceptional situation' the updated "core mission is to protect the common borders of the European Union in support of Member States. In Greece, we contribute to this goal by supporting the registration of migrants and security screenings, which are also important for returns" (Frontex, News release, 2020).

Except for the operational activities, the agency also handles research and innovations activities; exploring technical solutions to address the operational needs, establish their readiness to be integrated and tested in a real operational scenarios, organises demonstrations of technology, conducts technical feasibility studies and runs pilot projects at all types of border. Frontex handles also reports on current practices for technology acquisition and deployment as well as presenting recommendations for EU-sponsored research (Frontex, 2019)[5]

While the agency studies the availability and readiness of technology for integrated border management, the Greek government has already adopted almost a decade ago, the Integrated Border Management Program for Combating Illegal Immigration 'for the protection of both the EU and national borders and the reduction of illegal migration'(Hellenic Coastal Guard, 2011)which included among others the construction of the 10.3 kilometres concrete wall along the land borders with Evros, the northeast of Greece[6]and Turkey, for combating 'illegal' entries or as today referred to as the 'invasion'[7]. The program also agreed on increased operational support from Frontex which included joint land and sea operations, as well as the provision of technical and operational support to national authorities, the development of a National Border Surveillance System complying with EU requirements for the development of the European Border Surveillance System (EUROSUR), the operation of First Reception Centers and a new system of reception and identification services. Meanwhile the municipal policies on immigrants' control and apprehension in the urban centers of Greek cities through official "sweep" operations such as Xenios Zeus as outlined also in the Greece Country Report for Border management and migration controls in Greece (Ilias et al., 2019). The Hotspot Approach was also developed by the European Commission as part of an immediate action plan to assist EU member states located at the external EU border (May 2015) which would focus on registration and identification procedures, return operations and on assisting in the implementation of the temporary relocation schemes, the closure of the border with the so-called Western Balkans Corridor, and the Joint EU–Turkey Statement of 7 March 2016, in which

> Turkey furthermore agreed to accept the rapid return of all migrants not in need of international protection crossing from Turkey into Greece and to take back all irregular migrants intercepted in Turkish waters. Turkey and the EU also agreed to continue stepping

5 https://frontex.europa.eu/research/assessment-of-technologies/
6 For more details, see: http://www.hcg.gr/node/1260
7 https://www.france24.com/en/20200305-citizen-patrols-ward-off-invasion-on-greek-turkish-border

up measures against migrant smugglers and welcomed the establishment of the NATO activity on the Aegean Sea (European Council b, 2016).

The EU until now appears determined to avoid the incidents of 2015 and 2016 when more than a million people crossed its external borders through Turkey and Greece pressuring Turkey to honour their joint statement, reminding also that has paid about half of a promised 6 billion euros to help Turkey finance housing, schools and medical centers for the refugees stranded on its territory[8].

Since the last days of February 2020 extreme conditions and developments at the Evros borders and at the East Aegean Islands where thousands of people are stranded at the external borders of Europe after the Turkish government declared that will not stand in the way of anyone who wish to cross the borders to Europe. The EU reacted through diplomatic media management like the visit of the President of the Commission by helicopter to watch the situation at the borders and public statements:

> "While the Council acknowledges the increased migratory burden and risks Turkey is facing on its territory and the substantial efforts it has made in hosting 3,7 million migrants and refugees, it strongly rejects Turkey's use of migratory pressure for political purposes. This situation at EU's external borders is not acceptable. The Council expects Turkey to implement fully the provisions of the 2016 Joint Statement with regard to all Member States. This Statement produces tangible results, including by supporting Turkey's significant efforts in hosting migrants and refugees. Both the EU and Turkey stand to benefit from the continuation of this cooperation and commitment" (European Council c, 2020)

The Greek authorities reacted with propagandising the discourse of 'asymmetric threat' and 'invasion' of refugees and the necessity to employ all possible means to 'hold the gates'. The immediate reactions were extreme deployments of fully equipped military and police forces operating jointly with nationalist civilian groups against refugees at the Evros borders as European Council on Refugees and Exiles (ECRIT) report (2020). Greek state invoked almost immediately an emergency clause of European treaties suspending acceptance of new asylum applications and cutting welfare benefits for those who have granted asylum[9] while the national security council has taken the decision to increase the level of deterrence at the borders to the maximum as the Prime Minister of Greece twitted. There is a broad consensus on behalf of the Greek authorities on the adoption of emergency legal tools justifying the choices of extraordinary and asymmetric threat; the Prime Minister, Kyriakos Mitsotakis was the first to declare that Greece is not facing a refugee/migration problem but an "asymmetric threat," in Evros during a joint press conference with the heads of the EU's top institutions.[10]Suspension of asylum procedures is in violation of the Geneva Convention, the European Convention on Human Rights as well as national Greek law while the Strasbourg-based

8For more about the EU-Turkey conflict see: https://www.reuters.com/article/us-syria-security-turkey-vonderleyen/eu-tells-turkey-to-pull-migrants-back-from-greek-border-idUSKBN20W1AU

9 See: https://greekcitytimes.com/2020/03/08/mitsotakis-government-cuts-allowances-to-illegal-migrants/

10 See: https://orthodoxtimes.com/greek-pm-greece-facing-an-asymmetric-threat-not-a-refugee-migration-problem/

Council of Europe has condemned both Turkey and Greece, calling the current situation an "unprecedented humanitarian crisis."

2.2 Defining smartness in technical assemblages

The ideas related to the concept of smartness in assemblages are to be found in the context and processes of computation and machines that can handle arithmetical processes that only a human computor was able to perform. Going back to the 17th century, the invention of the slide rule in 1620 was a mechanical manifestation of the growing need of complicated calculation and the technical device followed the publications of John Napier on the concept of logarithm; it is based on the logarithmic express to allow for fast division and multiplication of numbers. The idea that a device is capable of performing these tasks followed new generations of physical philosophers and inventors, and later in the electric era, scientists to the desire of building "mechanical brains". Network analyzers of the late 19th century express the needs for computing "the change of the periodical phenomena produced by the use of the mechanical network of a steam engine"(Tympas, 2017:98). In the beginning of the 20th century, the tasks of modelling the expansion of electric power transmission indicated the needs for vast amounts of complicated computations while integrators and differentiators, as analog computers supported military efforts for precision in the mechanization of the calculation of the fire control of external ballistics (Tympas, 2017). In the field of modern engineering, the scientific idea that early electronic computers can be presented as intelligent machines seems to be cultivated from the previous representations of differential and network analysers as intelligent or as "machines that think". A notable example of this trend is the 1914

presentation in Scientific American by C. H. Claudy of a sizeable tide predictor as "A Great Brass Brain" defined by its capacity to do "mathematical calculations (Tympas, 2017), claiming its inspiration by Roger Bacon's alleged "brazen head or android".

Since the decade of 1940 and the interwar research agendas, the notion of digital is constantly used throughout the representation of advanced computing systems. The famous EDVAC would be as von Newmann described "a very high-speed automatic digital computing system" (von Neumann, 1993) possessing human qualities like computational memory that appeared as the equivalent to the "associative neurones on the human nervous system" (i.e:29) and input and output organs that would be resembling the human sensory system. This tendency to inscribe human traits on machines and vice versa revives in the turn of the 20th century under the realm of computing systems; an analog computing machine was presented in analogy to the capabilities of a human computor in the earlier years of computing instruments production. Von Neumann in the mid of 20th century employed the neuron analogy of the McCulloch-Pitts artificial neural net (McCulloch & Pitts, 1943) to justify the use of binary system as the new model in computer design introducing his concept on digital machines. Intelligence and smartness is going digital; the language and the analogies that was used in this report stands as a renewal of anthropomorphism in regard to the machines particularly computers. The human brain can now be considered as a "digital computing machine" as McCulloch and some of his fellows in the cybernetic movement of the 1940s were proclaiming and vice versa; a digital computer may be built mimicking the structure and the functions of the human brain hence claiming the rare gift of smartness that only living creatures could possess with the human cognitive abilities regarded as the most complex.

These technoscientific developments that were taking place during the wartime period continued after the war to form "Cybernetics", a paradigmatically interdisciplinary scientific project that would connect humans and machines under the notions of feedback loops and circuits, information theory, communication and control, governors and servo systems, homeostatic and purposive behaviour and digital computers (McCulloch, 1956) Prediction and control alongside with information came to be considered as central notions and characteristics of a desired system or assemblage that ended to include even the human element as component of the machine. As Peter Galison points out, mechanical devices like the anti-aircraft predictor, an assemblage designed by Norbert Wiener during WWII to anticipate the enemy's aircraft future position and shot it down automatically, created a new vision of the enemy-pilot so merged with the machine that the distinction between human and non human was blurred in the end for the purpose of the desired operation (1994). The mechanised 'Enemy Other" was generated in the laboratory-based science of MIT and many other universities around the United States and in Britain during the war, engaged the sciences of operation research and the flow charts analysis, game theory and cybernetics (Galison, 1994) creating a technoscientific view for the human being that was about to celebrate posthumanism as well as new domains of rationality and new techniques for centrally governing populations.

It goes almost without saying that most of the things and assemblages after the millennium are considered and delivered as "smart" without a clear definition of what smart means. The difficulty of

defining "smartness" in artefacts follows a similar struggle for explaining intelligent behaviour in animals and humans that occupied philosophers and scientists of diverse disciplines for a long time. The concepts and methods obtained during the next post-war decades has transformed into a techno-hype for Artificial Intelligence or machine learnign, big data, Internet of Things, Industry 4.0 and generally speaking 'smart living, working and organising'. Yet the concept of 'smartness', cannot be easily defined due to the diversities across the market products and services. What exactly 'smart' means apart from the relation to IT- enabled devices and systems still remains undefined; and the unwillingness to produce usable definitions and uses comes in some degree from the surprisingly wide range of systems and devices that are described as smart. One simple hit on a search engine informs us about the existence of smart cities, cars, phones, governments, homes, materials, clothes, shoes, weapons, bombs, borders and countless other devices, things and systems. However, some suggested principles have been suggested for guiding a definition of smartness as an attempt to surpass the lack of consensus around the term such as the following by Steven Alter:

> Definition of smartness. Purposefully designed entity X is smart to the extent to which it performs and controls functions that attempt to produce useful results through activities that apply automated capabilities and other physical, informational, technical, and intellectual re- sources for processing information, interpreting informa- tion, and/or learning from information that may or may not be specified by its designers (2020:384).

Automated information processing and some degree of self-control, learning, adaptation, and decision making may work as keywords for defining smartness in objects and systems; although one more broad category is consisted of various smart systems:

> Cyber-physical systems are "smart" networked systems that are engineered to sense and interact with the physical world, and to support real-time performance in safety-critical systems. With CPS, the joint behavior of the "cyber" and "physical" elements of the system is critical. Computing, control, sensing and networking are deeply integrated throughout the system, and the actions of components and systems must be carefully orchestrated (Cyber Physical Systems, 2014).

Some examples of situations that benefit from CPS are: "smart cities", energy, military and national defense, building control, emergency response, manufacturing, global commerce logistics and transportation even sustainability. As Halpern, Mitchell, & Geoghegan argues, smartness takes on an ecological dimension and has to deal with unforeseeable events that emerge from an increasingly complex environment and take the form of a political mandate as the "current instantiation of a new technical logic with equally transformative effects on conceptions and practices of governance, markets, democracy, and even life itself" (2017:111). Although it is presented as politically neutral by its advocates, this special "mandate" couples with governmentality, a key goal of bio politics and with the open ended modulation of discipline as described by Deleuze. They sketch the logic and the

mandate of smartness in four sections: "the territory of smartness is the zone, the (quasi-)agent of smartness is population, the key operation of smartness is optimization and that smartness produces resilience (2017:113)

2.3 Placing the smart concept in EU borders

> "Today we see a transformation of Justice and Home Affairs domain. That transformation leads to a very rapid convergence between internal security, border management and migration management from operational and also from policy point of view. We cannot anymore draw lines between them. And on the same time, the ongoing digital revolution will continue and even accelerate its effects in the coming years; therefore EU should continue to further explore the capabilities of technologies to make border management, internal security and migration management".[11] Krum Garkov, executive director of eu-LISA (2018)

In 2018 the project of 'smart borders' was already counting seven years since its first formal proposal, yet legal as well as feasibility concerns halted the implementation and redirected its focus in technical revisions and test pilots. Krum Garkov, the executive director of eu-LISA opened his speech in the 2018 annual conference of the agency under the topic: 'EU Borders - Getting Smarter Through Technology'. Keywords of the day, even in the form of hashtags in the presentations, were digital borders, interoperability of surveillance systems and Frontex. There are some guiding patterns that lead the ongoing transformation of bordering and these are unmistakably the 'Smartness' of machines for the border assemblage, the intertwining of migration movements with internal security and terrorist threats and last but not least the ongoing digital revolution. Specialised market analysts from the security industry reassures the success stories of digital and smart borders:

> "The global border protection market is expected to grow to $168 billion by 2025 driven by investments in key technologies such as autonomous UAS (UAV and UGV), remote weapon stations, maritime analytics, predictive analytics and integrated C4ISR System" (Garg, 2020:1).

That is part of an investment consultancy report, under the title 'Smart Border Management – Transformation from Analog to Digital Borders'. Among the many interesting aspects in the recent ongoing transformations of borders, is the agency of the border protection industry and the various ways for communicating their investment plans to (inter)national policy makers. The rhetoric that is used for influencing investors and for lobbying their expertise and infrastructures, is structured upon bold distinctions like the analog/digital, as if borders were not partly mediated by Information Technologies before. Nevertheless what is important in this passage, is the investing techno-hype on smart military weapons and information infrastructures. The elements of 'smartness' and 'digital' are enough to communicate the modernisation of infrastructures in these special territories of the

11 https://www.youtube.com/watch?v=71P6NebpBfk&feature=emb_rel_pause

european continent; they are not simply national territories, they are the 'european borders' as all officials stress enough, nor restricted only to national laws, and they are usually operated within a grey zone of transparency and law by invoking for instance emergency clauses. As Halpern et al. note, historians of urban planning have used the term 'zone' to indicate a special instrumentation of space that can be reconfigured according to the dominant discourses and practices, like financial and logistical practices; new forms of territory are produced under that logic that may operate out of reach of normal national even international law (2017). Halpern et al. use the term 'zone' to describe the space of smartness; they make the point that the 'smartness mandate' "aims to globalise the zonal logic, or mode, of space" by a "logic of geographic abstraction, detachment and exemption"(p. 113) colonising space through the management of time (2017). Two key examples are the so-called free trade zones and the projects of smart cities. As networked infrastructures they are linked through algorithms, they lie in a grey zone of legality and attempt to manage all 'crises' by "an operation of self-organization through which earlier discourses about structures and the social are replaced by concerns about infrastructure, a focus on sensor systems, and a fetish for big data and analytics, which purportedly can direct 'development' in the absence of clear-cut ends or goals" (p. 115). They make the point, that the contemporary mutations of zones are linked to the implementation of information technologies for optimising management. The case of smartness for the EU borders fulfils the digitalisation mandate of EU in one hand and the securitisation promise on the other. Big Data accumulation, biometrics, algorithmic governance and interaporability are used as practices that are capable to render the assemblage as smart, while smartness takes place simultaneously at the 'grey zones' of border territories and on the 'cloud' to optimise the management of the migration 'crisis'.

Chapter 3

3.1 The ongoing case of 'Smart Borders Package' in EU

As Baldin-Edwars, Blitz and Crawley (2019) point out, framing migration management as 'crises' is used to justify extraordinary and exceptional measures, that are manifested as rapid, informal and flexible policy instruments at odds with the rule of law and the fundamental rights of refugees, migrants and travellers.

The frontiers of Europe are probably one of the most heavy invested industries in EU and certainly one of the most conflicted and death dealing territories. The political, economical and institutional resources that are invested by EU and the Member States are explicitly evident. In the form of the general "border spectacle" (De Genova 2002, 2013) that is reproduced and banalises deaths in transit, in the form of emergency clauses and 'asymmetric wars' or the militarisation of population management alongside with policing citizens and non-citizens alongside with humanitarian approaches.

The first proposal for a more sophisticated and integrated electronic Entry/Exit system was actually made in 2008; the system was not deemed smart in the first place, but the necessity of optimal utilisation of new technologies was the core purpose of the proposal, alongside with the integrated border management strategy, meaning technically integrated databases and operations (Regulation (EU) 2017/2226).

The Schengen Information System (II), the Eurodac database and the Visa Information System (VIS) are existing IT systems in security and surveillance domain. The Schengen Information System II entered into operation on 9 April 2013 replacing the first generation SIS with a more complex, investigative instrument; SIS II contains data on irregular migrants, lost and false travel documents and wanted or missing persons and stores digital images and biometric data. They consist of large databases, which include the storage of biometric data, aiming, among others, at controlling migration flows and identifying and sorting legal and irregular migrants. On February 2013, the European Commission presented further proposals for an Entry Exit System (EES) and a Registered Traveller Programme (RTP) for the Schengen Area, collectively known as the "Smart Borders Package". The Entry/Exit System proposal proposes a centralised storage system for entry and exit data of third country nationals admitted for short stays to the Schengen area. This includes storage of biometrics subject to a transitional period of three years that can be extended if it is necessary (Regulation 2017/2226). As the regulation states, the new phase in the integrated border management would come with the smart borders under the ' European agenda on migration'. The European Council and the Parliament rejected the first proposal after examination in 2014, as the authors of the technical study report:

> Voicing technical, operational and cost concerns, mainly related to the overall feasibility of the proposed new systems and of some of their features. Concerns related especially to the impact on the actual border control process, the RTP token, the data retention period in the EES, the choice of biometric identifiers, the extent to which national Entry/Exit Systems could be integrated and/or reused, the need for enhanced synergies and/or interoperability with existing border control systems, and the possibility for law enforcement authorities to access the EES (European Commission et al., 2014:11).

The Commission consequently initiated a new technical study to identify and assess more suitable and promising options and solutions for the legislation proposal, followed by a Pilot project based on this Study in selected countries-members of the EU. Aim of the pilot project was to examine the feasibility of the proposed techniques implementing them in specific 'high risk' areas around the EU. The new regulation that was proposed and finally adopted after the test pilot did not include the Registered Traveller Program (RTP) but the European Traveller Information and Authorisation System (ETIAS) has taken its place. What is important, among others in this regulation, is the intertwining of migration and terrorist management, as well as the designated capability for the law enforcement agencies to have access to the central database and all the data should be available to the authorities of the Member States and 'Europol'. According to the European Agency for Fundamental Rights (FRA), even in 2018, the impact of large-scale IT systems on fundamental rights remains largely unexplored territory (EUFRA, 2018, p. 9). FRA also shares the opinion, that these large scale IT systems were initially set up by the European Union (EU) for asylum and migration-management and are increasingly also serving internal security matters, while they increasingly rely on biometric identifiers and data (p.9). However, looking closer at the communication from the Commission to the Council in regard to integrated management of external borders:

> "The European Union's external borders are also a place where a common security identity is asserted. The absence of a clearly stated vision and common policy on external borders would entail major political and strategic risks. Those could ultimately block the expression of a viable Union policy on Justice and Home Affairs". (COM, 2002, 233:5)

That was a clear political statement about the future management of external borders and the subsequent procedures for establishing common techniques of governing the borders and for shaping the European identity through securitisation. The general border assemblage helps translating political reasoning into new techniques or regimes of governing and serves as a manifestation of sovereignty. In this case, it is not that large scale IT systems were only initially set up as a solution to migration management but it was about specific and crucial technical choices that could construct EU's envisaged identity as a sovereign and safe integrated Union on one hand and an area of freedom of movement on the other. In that way, the Schengen provisions were honoured, with open borders and free movement among the Member States and controlled mobilities for third country nationals by filtering the influx of migrants and travellers. The focus in the next chapter will be in the test pilots for the Entry/Exit system that were performed in Greece

3.2 Technical overview of Entry/Exit system, ETIAS and interoperability

The EES consist of a Central System, which operates a computerised central database of biometric and alphanumeric data, a National Uniform Interface in each Member State, a Secure Communication Channel between the EES Central System and the central Visa Information System, and a secure and encrypted Communication Infrastructure between the EES Central System and the National Uniform Interfaces. Each Member State should connect its national border infrastructures to the National Uniform Interface, and in order to enable the generation of statistics and reporting, a data repository should be established at central level. A web service will verify at any moment the remaining authorised stay, as well as whether a TCN has already used the number of entries authorised by her visa (EU 2017/2226). This regulation refers also to the justified necessity of the use of biometrics, "despite its impact on the privacy of travellers, as it is a reliable method of identifying third-country nationals with no possession of travel documents or any other means of identification, a common situation for irregular migrants"(p. and because biometrics allow for a more reliable matching of entry and exit data of bona fide travellers with the same result in terms of accuracy of identification (Regulation 2017/2226).

> "The use of biometrics, despite its impact on the privacy of travellers, is justified according to the regualations for two reasons. First, biometrics is a reliable method of identifying third-

> country nationals who are present on the territory of the Member States but not in possession of travel documents or any other means of identification, a common situation for irregular migrants. Second, biometrics allow for a more reliable matching of entry and exit data of bona fide travellers. The use of facial images in combination with fingerprint data makes it possible to reduce the total number of fingerprints required to be registered, while enabling the same result in terms of accuracy of the identification".(Regulation 2017/2226: 5)

In April 2016, the Commission revised the proposal based on the Smart Borders pilot report. New features were proposed for the Entry/Exit System (EES), while the Regulation for a Registered Traveller Programme (RTP) was withdrawn. There was no consideration on the first proposals for a test pilot and came into consideration only after the EC and the Parliament rejected the project and certain existing legal provisions concerning checks and surveillance at the borders required several amendments.

The European Travel Information and Authorisation System (ETIAS)

> «We need to know who is crossing our borders. By November, we will propose an automated system to determine who will be allowed to travel to Europe. This way we will know who is travelling to Europe before they even get here.»
>
> Jean-Claude Juncker, European Commission President, State of the Union Address, 14 September 2016

The European Travel Information and Authorisation System (ETIAS) 'should contribute to a high level of security, to the prevention of illegal immigration and to the protection of public health by providing an assessment of visitors prior to their arrival at the external border crossing points'. (Regulation 2018/1240:2).
The initiative for a European travel-authorisation system is not new. In a communication from April 2008 on 'preparing the next steps in border management in the EU the EC stated its intention to "examine the possibility of introducing an electronic system of travel authorisation at EU level" (Communication from the Commission to the European Parliament, 2008:9). In the study that was carried out by PricewaterhouseCoopers in 2011, the conclusion considered, that at that time the conditions were not met for establishing such a system. It would not gain the full capabilities envisaged in the first proposal, due to the fact that there was no availability of other databases and systems that could become interconnected except for the SIS database, which was the only with the capacity to connect to and check entry conditions in advance (PwC, 2011). ETIAS is an automated risk assessment tool designed to perform security risk assessment with the use of pre-screenings and the possibility of assessing security and migratory risks prior to arrival at the border with the use of the Common Identity Repository (CIR) . It is designed to provide statistics and generate information on legal migration flows and other items of interest for the policy makers and is of key importance for better implementing an integrated management of external borders (European Commission et al.,

2016). The risks can be evaluated via ETIAS by direct hit, networks analysis and data analytics. The firsts case evolves "direct looking for known entities based on information (specific values) available in databases" whereas network analysis evolves "unknown entities in connection with a known entity based on information/specific values available in databases (connections with known persons of interest through phone numbers, email addresses, etc)" (2016:20). Data analytics is about setting risk-assessment rules and identifying patterns on the basis of risk indicators/risk profiles and looking for aggregations of the risk indicators or matches against risk profiles. Risk assessments related to pubic health as high epidemic risks are part of the services of the system. (Regulation 2018/1240). However, contact scanners for fingerprint capture were proposed as optimal technical choices in the test pilot of the Entry/Exit system as will be discussed in the next chapter.

In April 2019, the Common Identity Repository (CIR) rules for borders and visa checks were finally adopted by the majority of the Parliament. The purpose of the repository is to aggregate both identity records (names, dates of birth, passport numbers, and other identification details) and biometrics (fingerprints and facial scans), and make its data available to all border and law enforcement authorities. The Schengen Information System, Eurodac, the Visa Information System (VIS) and the three components of the new smart border assemblage: the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Records System for Third Country Nationals (Regulation 2018/1240). The repository of screening rules will be a new system in the EU; a similar set-up has been put in place in the US, where all relevant agencies (law enforcement, migration, border management, intelligence) input data into a central system used in the ESTA automatic risk assessment. What makes it a special case for the EU technopolitical environment, is that such an enormous database and the repository of screening rules alongside with the Entry/Exit system and the envisaged interoperability with other databases and systems, is attached primarily to the political momentum, shaping the technologies in ways that fasten the supposed or the actual maturity and feasibility of the systems that are planned to integrate.

3.3 Efficiency and feasibility through rhetorics: A critical assessment of the results on test pilot in Greece

The Greek test pilot of smart borders were conducted in two key places, both considered as 'hot spots'; in Kipoi Evrou, the northeastern land borders with Turkey and in Piraeus, the major port of Greece and were conducted from May to August 2015. The tests in Piraeus focused on the enrolment of fingerprints and the use of automated facial recognition in a moving cruise vessel with the purpose to evaluate the feasibility, user-acceptance, duration and the delivered quality of enrolling 4 fingerprints, enrolling a live facial image , capturing the facial image from an eMRTD and verifying the facial image captured from the eMRTD against the enrolled live facial image (PricewaterhouseCoopers, 2015, test pilot:297). There was no technical integration with the other system and the type of device consisted of optical 4 FPs contact reader, a standard web-camera and a laptop with dedicated application for the pilot. The NFIQ standard was used for assessing fingerprint quality throughout the test pilots with the thresholds either determined by the vendors or after consultation with experts from Member States (p. 11). NFIQ stands for NIST Fingerprint Index Quality, as it was developed and standardised by National Institute of Standards and Technology (NIST). It is a quality metric that has become a de facto standard for assessing fingerprint quality and its computation is mandatory in the ANSI/NIST ITL 1-2007. It worths noting, that NFIQ 2.0 algorithm was already being developed during the implementation of the pilot and is now considered as the updated standardised quality assessment for fingerprint enrolment. The new version 2.0 of the NFIQ algorithm, which is based on artificial intelligence, makes use of machine learning for AFIS Automated Fingerprint Identification System and is now set as the standard for fingerprint quality in the EU Entry/Exit System (Commission, 2019/329). Secunet provided a modular software framework that allowed training the NFIQ 2.0 algorithm based on the concept of machine learning, which resulted into the algorithm now set for the Entry/Exit system.[12] What seems to be at stake in this case, is that the new algorithm has different assessment criteria; for instance it uses a higher resolution quality score, in range of 0-100 according to the international biometric sample quality standard ISO/IEC 29794-1:2016 as opposed to 1-5 (NIST, 2016). A higher resolution biometric sample is useful for properly training the NFIQ algorithm. For the purpose of the technical report, feasibility was defined based on ISO/IEC/IEEE 29148:2011 as being composed of: Being technically achievable, not requiring major technology advances, fitting within system constraints like cost, schedule, and technical, legal, regulatory constrains and with acceptable risk (PricewaterhouseCoopers, 2015, test pilot:12).

The conclusion of the executive summary report on smart borders is that the pilot confirms the feasibility of deploying biometric identifiers at Schengen external borders, in terms of accuracy, effectiveness and impact ((PricewaterhouseCoopers, 2015a). It points out, that the overall project lived up the expectations, managing to deliver evidence-based results proving the high rate of

12 https://www.secunet.com/en/project-news/nfiq-2-0-key-role-to-improve-the-quality-assessment-of-fingerprints-in-the-ees/

travellers' satisfaction and the high rate of positive feedback by the participating border guards. However, looking closer to the reports, many deviations from the feasibility context are observed as well as technical issues considering failures to reach quality thresholds standardised by NIST. In the next chapter, I will focus to the Greek test pilot to discuss some of the issues that have been raised throughout the procedure and their subsequent treatment from the experts as negligible to the overall positive assessment of the test pilot.

The overall system assessment for the test pilot procedures both in Piraeus and Kipoi Evrou is considered successful in the final technical report. However, the results of separated, vital tasks like fingerprint enrolment or image verification are shown to have failed reaching the thresholds given by vendors which should comply with NFIQ. More attempts would be necessary to capture a decent quality fingerprint leading to more time consuming procedures and more workload for the border guards-users of the devices. The results for the assessment of the users' experience with the procedure, show conflicting statements of the travellers' acceptance of the procedure.

According to the technical report, fingerprint enrolment in the operational procedures of Piraeus was considered successful if the NFIQ threshold (values of 1 or 2 for the thumb, index, middle and ring fingers and 1, 2 or 3 for the little finger) was reached at the first attempt (2015:300). The fingerprints of the index, middle, ring and little fingers of the right hand of volunteering TCNs were captured using a standard optical live scan device. The decision threshold was determined either directly from the vendors or after consultation with experts from Member States. Decision threshold refers to the acceptance or rejection of biometric data which depends on the quality or matching score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict ((PricewaterhouseCoopers, 2015a:11). In TC1 for Piraeus, the vendor adjusted the thresholds according to NFIQ and as the graph shows, in most of the cases the machine failed to acquire samples and the quality thresholds were not reached. Only a 31% success rate was reported; which means that medium to poor quality data samples would be used not only for registering in the databases but also for training the algorithm associated with automated matching prediction. The performance of the automated biometric identification system (ABIS) depends on the quality of the

samples and rejection of low quality

as the report itself points out "is

applied in many biometric systems as a means for improving ABIS performance" (15) .

Piraeus - TC1 success and failure rate with contact device at vendor threshold

Piraeus - FI related test cases success and failure rate

Source:(PricewaterhouseCoopers, 2015a)

As the graphs show, the success rate for image verification was 30%, which is the percentage of the test cases that the given threshold was reached, and more attempts would be necessary to achieve successful verification reaching the quality threshold, while “document reading errors were not collected due to modalities of the device”.
Another interesting point in the quality threshold assessments in the report, is that due to operational pressures, border guards felt unable to force re-enrolment attempts in all cases despite the thresholds not being reached. It is not exactly known what kind of operational pressures occur, but all these pressures are highly probable to occur throughout all the future procedures. This was noted to have been the case in approximately 68% of cases in which the first enrolment had at least one finger below threshold.

The other test pilot was undertaken at the border-crossing point of Kipoi Evrou, a road border between the northeastern part of Greece and Turkey, It is considered one of the busiest borders of the eastern frontier of the Schenghen area and certainly one of the most politically charged. The goals were to test the feasibility of both fingerprint and iris enrolment, the time required to enrol different biometrics, the quality obtained and the users’ acceptance of the biometric enrolment process and the device utilised (p. 168). Tests were run in parallel throughout, enrolling 4 fingerprints plus iris, 8 fingerprints and iris and finally 10 fingerprints and iris.The overall fingerprint enrollment procedure was reported as successful, however, a subnote explains that a ‘soft’ NFIQ-based threshold of NFIQ<4 for all fingers was used at Kipoi and the main threshold was based on device auto-capture functionalities (p.169). The report points out that most of the participants expressed satisfaction subsequent to their participation in the pilot, and just 4% of the traveller population expressed themselves as dissatisfied, concluding that even the border guards indicated the participants generally expressed satisfaction.(p.177). What comes as a paradox was that the qualitative feedback received by the border guards-users concludes that 86% of them perceived travellers’ acceptance as “not very enthusiastic," 57% of replies indicated that they did not see any added-value with the process as tested while the remaining 43% indicated that the additional biometric step made no significant difference (p. 178). Even though the quality thresholds were set low and no re-attempts attempted, which would make the procedure more time consuming, border guards considered the procedure lengthy with no added value for them nor for the participants.
One important and quite unprecedented matter that needs to be further explored is that all the test pilots were carried out using contact scanners for fingerprint capturing, thus proposing their usability as successful type of devices for employment in the Entry/Exit system. The smart borders package was approved with these type of scanners just before the outbreak of the Corona virus pandemic, leading to the necessity for contactless scanner in order to avoid further spread of the virus .

3.4 Moving beyond biometrics. The case of iBorderCtrl

"The global maritime and border security market is growing fast in light of the alarming terror threats and increasing terror attacks taking place on European Union soil, and the migration crisis ... iBorderCtrl system will collect data that will move beyond biometrics and on to biomarkers of deceit." (European Commission, 2018)
George Boultadakis of European Dynamics, project coordinator

The news report on the success stories of research and innovation projects of the European Commission concludes that the partner organisations of iBorderCtrl are likely to benefit from this growing European security market – a sector predicted to be worth USD 146 billion (EUR 128 bn) in Europe by 2020. The Intelligent Portable Control System is one of the recent success stories for the research and innovation program of the Commission (Commission, 2015). The 4.5 million EU's Horizon 2020 funded project is aiming to facilitate the work of border guards in spotting illegal immigrants, and so contribute to the prevention of crime and terrorism as well as to facilitate border

procedures for bona fide and law-abiding travellers (The Project | IBorderCtrl, n.d.). It claims to bring together many state of the art technologies, both hardware and software, ranging from biometric verification, automated deception detection, document authentication and risk assessment. It is designed upon the concept of interoperability of EU systems for security, border and migration management as envisaged by the EC, and demonstrates many of the features planned to be included in the Entry/Exit (EES) and the European Travel Information and Authorisation (ETIAS), the main components of Smart Borders. It unifies different interdisciplinary modules into an overall system and consists of a two-stage procedure: a registration before the travel to the Traveller User Application (TUA), an on-line system to gather initial personal (including social media), travel document and vehicle data followed by a short, automated, interview with a humanoid avatar, subject to lie detection powered with artificial intelligence and link the traveller to any pre-existing authority data. A risk-based assessment then is performed, utilising multi-factor analytics and the data that have been registered are processed and correlated with publicly open data or external systems such as the SIS II. Upon completion of all required preregistration steps, the TUA generates a QR code that is sent to the traveller which can be used to the border check point by a border guard to retrieve all the information collected during the preregistration phase (O'Shea et al., 2018).

The second stage of the procedure is taking place at the border crossing point where the collected information is now available to the Border Guard through the Border Guard User Application (BGUA). All analytic results from each technology are merged to identify risks and specific potential issues to the border guard for the final evaluation of the traveller. Biometric checks are then applied, fingerprints, palm vein and face, matching for identity verification and lastly if there is a vehicle crossing the border an additional check may be performed to detect any hidden humans inside the vehicle by Hidden Human Detection Tool, a module which consists of an electromagnetic / radar sensor and an acoustic sensor subsystem. In conclusion, the main modules that compose the overall system are: a Biometrics Module, a Face Matching Tool (FMT), a Document Authenticity Analytics Tool (DAAT), a Hidden Human Detection Tool (HHD), External Legacy and Social interfaces system (ELSI), a Risk Based Assessment Tool (RBAT), the Integrated Border Control Analytics Tool (BCAT) and an Automatic Deception Detection System (ADDS) (O'Shea et al., 2018). The central vision of iBorderCtrl's project was to design, test, trade and implement not only a 'smart deception detection system' but an overall system assemblage capable to monitor travellers and migrants on the 'cloud' before arrival, deterritorialising border controls in a great extent but also to provide novel technologies for the old school, ground border controls.

The iBorderCtrl project was conducted by a consortium of governmental stakeholders, universities and industries. Among the main participants of the project are the Manchester Metropolitan University and the Institute of Communication and Computer Systems (ICCS) of the School of Electrical and Computer Engineering (ECE) of the National Technical University of Athens (NTUA); Kemea, the Greek center for security studies, and the Hungarian national police, as well as a number of security, biotechnology and information industries such as Stremble Ventures LTD, JAS Technologies Ltd, Everis Aerospace and defence, Biosec Group, and European Dynamics (iBorderCtrl, n.d.)

One interesting point of this case from an STS approach, is that the overall project may be described from an innovation policy point of view as what Etzkowitz and Leydesdorff (2001) have described as the triple-helix model of innovation; governmental stakeholders as well as academia and industry forming a consortium to further innovation; in this case the triple helix model is expanded to include a military/police research and innovation helix. The automatic deception detection system has its origins on various forms of lie detection, such as polygraphs, voice stress analysis, behavioral analysis; polygraphs were designed for and used by police and military intelligent services from the Progressive Era to extract convictions by avoiding to a certain degree, torturing the prisoners and as part of the professionalisation of police interrogation attempts for standardising admissibility of scientific evidence (Wilde, 2014). The cardio-pneumo psychogram, ancestor of the polygraph (Larson, 1923) was utilising blood pressure, pulse, and breathing rate to detect deceptive behaviours. Automated face recognition and verification systems and the algorithms they use are already considered by experts as mature technologies for implementation as in the case of the 'smart border' package; the novelty in the case of the iBorderCtrl assemblage is the move beyond biometrics to biomarkers of a human body for security risk assessments. 'Biomarkers of deceit' are used in this case as features that can be transformed into quantifiable data that can be the input of machine learning statistical models to perform a classification task. The features are extracted from raw data, such as the video session with the conversational agent avatar or other forms of sensors and machine learning methods to"fit a model to the training dataset to map the multidimensional feature space to the output label space (deception or no-deception labels)" (Sánchez-Monedero & Dencik, 2020:6). The ADDS system is built on a configuration of artificial neural networks, which are used to detect facial objects and extract non-verbal behaviour in the form of micro gestures over short periods of time (O'Shea et al., 2018). Nonverbal communication "refers to the ways in which beings convey information about their emotions, needs, intentions, attitudes, and thoughts without the use of verbal language" (Hall, 2001:1) , such as facial expressions, gaze, posture, gestures while micro expressions are considered as "unconscious, extremely quick, sometimes full-face expressions of an emotion"(Speaking of Psychology, n.d.). A human being is considered to continually transmit nonverbal behaviour, hence leading to non-verbal leakage and clues to deception (Ekman and Friesen, 1969). In the case of ADDS which utilise the patented Silent Talker artificial intelligence based deception detector, the raw data from each frame of video streaming during the interview are processed in sequence and the information is compiled or accumulated for the purpose of classification (O'Shea et al., 2018). Artificial Neural Networks are trained as object locators to find the position of particular objects (left-right eye, etc.) while pattern detectors spot particular state of objects and the variations in the state of an object determined by a specific pattern detector are referred to as a "channel". The input to the final deception classifier is provided by group channel coders which form a summary vector to a ANN trained to classify input vectors as either truthful or deceptive (2018). An animated avatar developed by Stremble and presented in a uniform to convey an air of authority, poses a set of questions as illustrated below:

Question Number	Question
1	What is your family name?
2	What is in your case?
3	Have you seen any posters of prohibited items?
4	Are there any items from the lists of prohibited items in your case?
5	How many items are in the case?
6	If you open the case and show me what is inside, will it confirm that your answers were true?
7	What is your first name?
8	When were you born?
9	Where were you born?
10	What is your current citizenship?
11	Please tell me the name of a friend or family member who can confirm your identity?
12	What is the relationship of this person to you?
13	Where does this person live?

Experiment Interview Questions (O'Shea et al., 2018)



Male avatar developed by Stremble (O'Shea et al., 2018)

The simulation tests were taken place in three different member states with specific experience in border controls. Greece, Hungary and Latvia were chosen to test the overall system not in real conditions but as simulated scenarios of a border crossing point procedure. The main reason was that the pilot tests would violate many legal constraints of the GDPR and the overall applicable legal framework; the developers of the project claim also that this was only a "proof of concept" research project, during which "the main strategy for its evaluation through the aforementioned scenarios was on researching and promoting technology at a conceptual level, while seeking to evaluate its potential benefit for society and its impact on privacy and fundamental rights of individuals" (iBorderCtrl, n.d). This statement among others comes in contradiction with the relevant patent disclosures, the confidentiality status that was given to the project due to commercial interests[13] and the conflicted interests for some of the main researchers of the program[14]. In the Greek scenario, testing took place at Kemea and Trainose premises, involving only members of the Consortium and the Greek Border Authorities while cases of pedestrians, vehicle and passenger train crossing the borders were examined. The pilot tests were mainly focused on usability testing of software applications and ergonomics testing of the Portable unit with the hardware sensors integrated (Scenarios Results | IBorderCtrl, n.d.). The Hungarian National Police offered a border crossing point having the

13 See the discussion held by the Transparency Unit of the Secretariat-General of the European Commission upon the request for public access of the disclosed documents. The result was to make publicly available three technical documents with almost all the pages on them blackened, making them practically useless.
https://www.asktheeu.org/en/request/iborderctrl_forschungsprojekt_ho

14 Dr. Athos Antoniades is the Head of Research and Development, and C.E.O.of Stremble Ventures Ltd and one of the leading authors of 'Intelligent deception detection through machine based interviewing' alongside with J O'Shea, co-founder and consultant for the Silent Talker Intelligent systems team. Dr. O'Shea helped develop, test, and patent the proprietary Silent Talker software. Dr Keeley A Crockett is the Senior Artificial Intelligence Scientist in the same team as well as one of the principal investigators on the iBorderCtrl. See:https://www.silent-talker.com/about-us/

infrastructure to properly test and validate the capabilities of the system in a pilot deployment and did not include real travelers, but only members of the Hungarian National Police.

The overall system of iBorderCtrl is an assemblage of various software and hardware technologies, ranging from portable biometric readers and scanners, various emerging and novel subsystems for automatic detection controls, wireless networking for mobile controls , etc. It also comprises of heartbeat detectors for detecting hidden humans and objects in vehicles, gas sensors capable of measuring CO2 and/or O2 level. If a person hides in a vehicle, the level of CO2 will raise and the level of O2 will decrease (D3.1 Data Collection Devices - specifications; iBorderCtrl, 2018:102). As the authors of the project point out, these advanced surveillance tools and methods are required as the most trending way of illegal border crossing is to cross the "green border" meaning by crossing land borders while the next most trending way is hiding in vehicles and impersonation. This assemblage of high technologies that constitutes the overall system contributes to the ongoing process of deterritorialising the border surveillance and control, transferring them into virtual reality but also gives emphasis to old school technologies of radars and gas sensors acknowledging the grounded materiality of folded, hidden bodies in vehicles' crypts[15], thus designing an overall sociotechnical solution for the bona-fide traveller and the illegalised migrant both in virtual and the physical realm. The 'move on to biomarkers' signifies the intrusion of biomedical terms and practices for profiling travellers and migrants by measuring their emotional state, hence making not only the features of their bodies readable from a computing machine as van der Ploeg & Sprenkels (2011) has argued on the case of biometrics, but also the supposed truthfulness of their intentions; algorithms and AI then perform risk assessments about the degree of hazard that may carry into EU. This logic is similar to the original use of biomarkers in medicine as "a characteristic that is objectively measured and evaluated as an indicator of normal biological processes or pathogenic processes" (WHO, 2001) and is used in risk assessment procedures to predict the incidence of a disease. Biomarkers are used as objective indications of medical state observed from outside the patient – which can be measured accurately and reproducibly and specific biomarker have been shown to correctly predict relevant clinical outcomes across a variety of treatments and populations (Strimbu and Tavel, 2010). The supposedly 'biomarkers of deceit' are used in this case in analogy with the biomarkers in medicine but with the bold difference that they refer to emotional states and intention rather than to a pathological medical state. The analogies that occur in these two cases are between the distinctions of healthy/ill and truthful/deceptive and the same practices and terms that are used to categorise a body as diseased in the medical case, are used to categorise the bodies as legal or illegal in the security domain.

Conclusion

"The Strategic Agenda recalls that the EU must work on all aspects of the digital revolution and artificial intelligence, in a manner that embodies our societal values, promotes inclusiveness and remains compatible with our way of life" (European Council, 2020:6)

15 For the dis/abling material culture of crypts and migration see: 'Bodies Folded in Migrant Crypts: Dis/Ability and the Material Culture of Border-Crossing', Galis et al., 2016

The complexities of creating supranational border control practices through the deployment of large technical systems and the creation of certain agencies to coordinate and support the research, development and operations are undoubtedly high enough to mobilise a vast amount of political and legal institutions as well as their public discourse, specialised agencies, universities and technoscientific experts, industries and social organisations. The political discourse in the last years has been reshaping in conjunction with the mandated digital transformation of borders and under the notion of 'interoperability'. The executive director of EU-Lisa has stressed in the foreword of the agency's strategic plans for the period of 2018-2022 that:"The area of internal security in EU is going through a major transformation, moving from the physical to the virtual world"(Eu-Lisa, 2017:1). This was also the first time for the European Union to possess a dedicated agency responsible for managing and promoting information and communications technology(ICT); moreover, this institutional move is considered as a key success factor for implementing the Union's policies in the area of justice, security and freedom (2017).

Technological assemblages of bordering, either physical or virtual emerge as necessary components of sociotechnical systems that are envisioned for addressing certain problems that emerged upon their conception. As Scheel has shown, the culture of distrust is inscribed in the Schengen visa regime's risk management approach and it is not created just by instances of fraud, as well as the notion of risk itself creates a culture of institutionalized distrust in Schengen visa regime (2017). In a similar way, the proposed technical systems inscribe political and cultural concerns about migration and the identity of Europe. Examining the test pilots of the Entry/Exit system as well as the technical proposals of the smart borders, provided some insights about the negotiations between technical feasibility and added value and the technopolitical mandate for constructing the envisaged system. What makes biometric recognition systems so attractive for border control purposes is their alleged capacity to verify the claimed identity of a person with unprecedented speed and accuracy. However as the developers of the iBorderCtrl admit: "Comparing biometric technologies is difficult as most solution providers have not been certified by independent laboratories but their figures have been defined by companies themselves or this information are not provided at all" (iBorderCtrl, Data Collection Devices - specifications 2017:34). In addition, it should be noted that automated systems could be programmed to identify individuals using sensitive data, such as race, ethnicity or health.

As Kelly Gates remarks "Understanding the experimental status of the technology is critical, because the prevalent myth of inevitability surrounding this and other new forms of surveillance itself performs an important role in their institutionalization, and in the broader effort to shape the future toward certain ends"(2011:6).

Speaking about illegal migrants or illegality, we are given the impression that the process of illegality is primarily static in time, unquestionable fair and somehow 'naturalised'. In reality, as De Genova points out, the aftermaths of law making are the 'illegal' bodies or the illegal mobilities as well as the constructions of sociopolitical categories and classifications of minoritised citizens or denizens (2019).Processes of illegalisation come along with regimes of borders and 'unauthorised' migration and law practices that render migrants as 'illegal aliens', and must be seen as a tactic that produces

conditions for the production of new categories of minorities vulnerable to the recriminations of the law De Genova has argued on "the legal production of illegality" (2002, 2005). In that way, the condition of illegality can be continually revised so as to ensure the availability of a vulnerable workforce, susceptible to deportation (2002, 2005, 2019). The analysis of these heterogeneous practices of illegalisation has been very productive in explaining regimes of citizenships and labour organisation, 'geographies of death'. Adding the processes of technology design and mediation in these constructions of illegality and sociopolitical categories provide also an explanation of the ways that political and legal reasoning is practically manifested as well as how these technologies co-produce law making and political reasoning. Apparatuses of the 'migration machine' (Dijstelbloem (2011) appear as capable of rendering many sociopolitical concepts into networked practices of surveillance and control. The 'smart borders package' in this sense is not to be seen as a mere linear process of technological progress but as a way of flexible intervention for managing populations and 'crises' by producing 'illegalities', as well as capable of invoking new disciplines that require new legislative proposals and/or the implementation of more state of the art devices and systems in order to tackle emergency situations. The legal and political production of illegality in migration goes along with the technical rearrangements of the ever going project of smart borders; data collection, aggregation and making sense of them is both politically and technically rendered. Computerization or algorithmication of surveillance systems certainly present serious negotiations among experts and policy makers and new future and unpredictable risks. New technological systems usually emerge in a loose regulatory environment, nevertheless they attempt to tackle political promises and cultural needs, as the ability to control the "threats" and "crises" that occur along and within the EU borders. Digital transformation mandates for border surveillance foster many transformations in vital social domains as the freedom to mobility and migration and share many features with the analytical concept of the 'smartness mandate' that takes place alongside.

The ongoing technical transformations of bordering techniques or the technopolitcs of the 'smart borders, as well as the spectacle they produce, evolve alongside with the continuous process of the European integration and sovereignty, migration regimes as controlled circulation of mobility, capitalisation of security and discourses of belonging. This technopolitical regime of managing populations and their movements through biometric and algorithmic risk assessment and control, brings apart from technoscientific expertise and entrepreneurship, military concepts and practices as all the 'old school' technologies of concrete fences remind as well as with novel military techs as unmanned drones, thermal cameras and the C4i concept of command, control, communication, computer applications and intelligent systems.

References

Alter, S. (2020). Making sense of smartness in the context of smart devices and smart systems. Information Systems Frontiers, 22(2), 381–393. https://doi.org/10.1007/s10796-019-09919-9

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Baas, M., & Yeoh, B. S. (2018). Introduction: Migration studies and critical temporalities. Current Sociology, 001139211879292. doi:10.1177/0011392118792924

Baldwin-Edwards, M., Blitz, B. K., & Crawley, H. (2019). The politics of evidence-based policy in Europe's 'migration crisis'. *Journal of Ethnic and Migration Studies*, *45*(12), 2139–2155. https://doi.org/10.1080/1369183X.2018.1468307

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. Alternatives: Global, Local, Political, 27(1_suppl), 63–92. https://doi.org/10.1177/03043754020270S105

Bigo, D. (2011). Freedom and speed in enlarged borderzones. In V. Squire (Ed.), The contested politics of mobility. Borderzones and irregularity (pp. 51–73). London: Routledge.

Brown, W. (2010). Walled States, waning Sovereignty

Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES). http://data.europa.eu/eli/dec_impl/2019/329/oj

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union. https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52008DC0069

Cyber physical systems: A perspective from keith marzullo » ccc blog. (n.d.). Retrieved 29 June 2020, from https://www.cccblog.org/2014/11/06/cyber-physical-systems-a-perspective-from-keith-marzullo/

De Genova, N. P. (2002). Migrant "illegality" and deportability in everyday life. Annual Review of Anthropology, 31(1), 419–447. https://doi.org/10.1146/annurev.anthro.31.040402.085432

Ekman, P., & Friesen, W. V. (1969). Nonverbal leakage and clues to deception †. Psychiatry, 32(1), 88–106. https://doi.org/10.1080/00332747.1969.11023575

European Council, 2020, Strategic guidelines in the field of Justice and Home affairs, 5636/20, JAI 65

European Council b, 2016, Press release, EU-Turkey statement, 18 March 2016. (n.d.). Retrieved 29 May 2020, from http://www.consilium.europa.eu/en/press/press-releases/2016/03/18/eu-turkey-statement/

European Council c, 2020, Press release, Statement of the Foreign Affairs Council, https://www.consilium.europa.eu/en/press/press-releases/2020/03/06/statement-of-the-foreign-affairs-council-on-syria-and-turkey/, accessed 9/5/2020

European Council on Refugees and Exiles, 2020, Joint Statement: "Protect our laws and humanity!" https://www.ecre.org/joint-statement-protect-our-laws-and-humanity/

European Commission, Directorate-General for Home Affairs, & PricewaterhouseCoopers. (2014). Technical study on smart borders: Final report. Publications Office. http://bookshop.europa.eu/uri?target=EUB:NOTICE:DR0114990:EN:HTML

European Commission, Directorate-General for Migration and Home Affairs, & PricewaterhouseCoopers (Firm). (2016). Feasibility study for a european travel information and authorisation system (Etias): Final report. http://dx.publications.europa.eu/10.2837/36503

European Commission, 2018, Research and Innovation Projects, Success Stories, 'Smart lie-detection system to tighten EU's busy borders'. Retrieved 27 May, from https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726

European Union: European Commission, Communication from the Commission to the Council and the European Parliament, "Towards Integrated Management of the External Borders of the Member States of the European Union", COM(2002) 233 final, 7 May 2002, COM(2002) 233 final, available at: https://www.refworld.org/docid/3f4e3cf84.html [accessed 29 June 2020]

Eu-Lisa strategy 2018-2022 (2017). Retrieved 17 April, from https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Strategy%202018-2022.pdf

Foucault, M (2007). Security, Territory, Population. New York: Palgrave Macmillan

Frontex News release, (2020). Retrieved 20 May 2020, from https://frontex.europa.eu/media-centre/news-release/frontex-to-launch-rapid-border-intervention-at-greece-s-external-borders-NL8HaC

Galison, P. (1994). The ontology of the enemy: Norbert wiener and the cybernetic vision. Critical Inquiry, 21(1), 228–266. https://doi.org/10.1086/448747

Garg, H. (2020, January 5). Smart border management -transformation from analog to digital borders. Frost & Sullivan. https://ww2.frost.com/frost-perspectives/smart-border-management-transformation-from-analog-to-digital-borders/

Gates, K. (2011). Our biometric future: Facial recognition technology and the culture of surveillance. New York University Press.

Gilles, R. P. (2010). The cooperative game theory of networks and hierarchies. Springer.

Hall, J. A. (2001). Nonverbal communication, social psychology of. In International Encyclopedia of the Social & Behavioral Sciences (pp. 10702–10706). Elsevier. https://doi.org/10.1016/B0-08-043076-7/01813-1

Halpern, O., Mitchell, R., & Geoghegan, B. D. (2017). The smartness mandate: Notes toward a critique. Grey Room, 68, 106–129. https://doi.org/10.1162/GREY_a_00221

Hecht, G. (2009). The radiance of France: Nuclear power and national identity after World War II. MIT Press.

Hellenic Coastal Guard, 2011. Παρουσίαση στο υπουργικό συμβούλιο (6/9), από τον υπουργό προστασίας του πολίτη, κ. Χρήστο παπουτσή, του ολοκληρωμένου προγράμματος διαχείρισης των συνόρων για την αντιμετώπιση της παράνομης μετανάστευσης. Retrieved 8 March 2020, from http://www.hcg.gr/node/1260

iBorderCtrl. (n.d.). Retrieved 29 June 2020, from https://www.iborderctrl.eu/#Project-Participants

iBorderCtrl. (n.d.)b. Retrieved 29 June 2020, from https://www.iborderctrl.eu/The-project

iBorderCtrl. (n.d.)c. Retrieved 29 June 2020, from https://www.iborderctrl.eu/Scenarios-Results

Ilias, A., Leivaditi, N., Papatzani, E., & Petracou, E. (2019). Border management and migration controls in greece. Zenodo. https://doi.org/10.5281/zenodo.3370199

Jasanoff, S (Ed.) (2004). States of Knowledge The co-production of science and social order. London: Routledge

Larson, J. A. (1923). The cardio-pneumo-psychogram in deception. Journal of Experimental Psychology, 6(6), 420–454. https://doi.org/10.1037/h0074457

Leydesdorff L. (2013) Triple Helix of University-Industry-Government Relations. In: Carayannis E.G. (eds) Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship. Springer, New York, NY

Lyon, D (Ed) (2003). Surveillance as Social Sorting: Privacy, risk, and digital discrimination. London: Routledge

McCulloch, W. S. (1956). Toward some circuitry of ethical robots or an observational science of the genesis of social evaluation in the mind-like behavior of artifacts. Acta Biotheoretica, 11(3–4), 147–156. https://doi.org/10.1007/BF01557008

McCulloch, Warren S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. The Bulletin of Mathematical Biophysics, 5(4), 115–133. https://doi.org/10.1007/BF02478259

Mezzadra, S., & Neilson, B. (2013). Border as method. Or, the multiplication of labor. London: Duke University Press.

Nail, T (2016). Theory of the Border. New York: Oxford University Press

News release. (n.d.). Retrieved 29 June 2020, from https://frontex.europa.eu/media-centre/news-release/frontex-to-launch-rapid-border-intervention-at-greece-s-external-borders-NL8HaC

NIST Fingerprint Image Quality, 2016, https://www.nist.gov/system/files/documents/2018/11/29/nfiq2_report.pdf

O'Shea, J., Crockett, K., Khan, W., Kindynis, P., Antoniades, A., & Boultadakis, G. (2018). Intelligent deception detection through machine based interviewing. 2018 International Joint Conference on Neural Networks (IJCNN), 1–8. https://doi.org/10.1109/IJCNN.2018.8489392

Policy study on an EU Electronic System for travel Authorization (EU ESTA), 2011. Retrieved 5 April, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/esta_main_en.pdf

PricewaterhouseCoopers. (2015a). Smart borders pilot project: Report on the technical conclusions of the pilot. Volume 1. Volume 1. LISA. http://bookshop.europa.eu/uri?target=EUB:NOTICE:EL0415804:EN:HTML

PricewaterhouseCoopers. (2015b). Smart borders pilot project: Technical report annexes. Volume 2. Volume 2. LISA. http://bookshop.europa.eu/uri?target=EUB:NOTICE:EL0415805:EN:HTML

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011. http://data.europa.eu/eli/reg/2017/2226/oj

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226. http://data.europa.eu/eli/reg/2018/1240/oj

Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

Rumford, C. (2014). Cosmopolitan borders. Palgrave Macmillan.

Sánchez-Monedero, J., & Dencik, L. (2020). The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. ArXiv:1911.09156 [Cs]. http://arxiv.org/abs/1911.09156

Scott, J. W. (2012). European politics of borders, border symbolism and cross-border cooperation. In T. M. Wilson & H. Donnan (Eds.), A Companion to Border Studies (pp. 83–99). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118255223.ch5

Sheller M (2011) Cosmopolitanism and mobilities. In: Nowicka M and Rovisco M (eds) The Ashgate Research Companion to Cosmopolitanism. Aldershot: Ashgate

Skeggs B, 2004 Class, Self, Culture (Routledge, London)

Speaking of Psychology: Nonverbal communication speaks volumes. (n.d.). Https://Www.Apa.Org. Retrieved 29 June 2020, from https://www.apa.org/research/action/speaking-of-psychology/nonverbal-communication

Speaking of Psychology: Nonverbal communication speaks volumes. (n.d.). Https://Www.Apa.Org. Retrieved 29 June 2020, from https://www.apa.org/research/action/speaking-of-psychology/nonverbal-communication

Trauttmansdorff, P. (2017). The politics of digital borders. In C. Günay & N. Witjes (Eds.), *Border Politics* (pp. 107–126). Springer International Publishing. https://doi.org/10.1007/978-3-319-46855-6_7

Tympas, A. (2017). Calculation and computation in the pre-electronic era. Springer London. https://doi.org/10.1007/978-1-84882-742-4

van der Ploeg, I., & Sprenkels, I. (2011). Migration and the machine-readable body: Identification and biometrics. In H. Dijstelbloem & A. Meijer (Eds.), Migration and the New Technological Borders of Europe (pp. 68–104). Palgrave Macmillan UK. https://doi.org/10.1057/9780230299382_4

van der Ploeg, I., (2006) 'Borderline identities: the Enrollment of Bodies in the Technological reconstruction of Borders in Monahan, T. (Ed.). (2006). Surveillance and security: Technological politics and power in everyday life. Routledge.

Van Houtum, H., & Van Naerssen, T. (2002). Bordering, ordering and othering. Tijdschrift Voor Economische En Sociale Geografie, 93(2), 125–136. https://doi.org/10.1111/1467-9663.00189