The role of security and defence companies in EU migration and border control and the impact on the protection of the rights of refugees, migrants and asylum seekers[1]

Contemporary border control and migration management policies and practices of the European Union are structured within a framework characterised by an intimate collaboration between public and private interests, with public interests broadly represented by EU agencies and member states, and private interests by security and defence companies, lobbying consultancies, law firms, universities and research institutes. Particularly defining about the public-private collaboration is the increased reliance on advanced and innovative border technologies which are developed and deployed with the dual aim of controlling irregular migration, and simultaneously, sealing off and securing the European borders. These advanced and innovative border technologies range from pre-screening technologies like biometrics comprising of facial features and fingerprints, to land and maritime surveillance by technologically advanced systems like early warning radar systems and unmanned aerial vehicles (UAVs) that can detect suspicious movements or vessels from a certain distance. This has created a market for technologically advanced software, technologies and equipment that is shaped, supported and provided primarily by major security and defence companies such as Airbus (formerly known as EADS and henceforth Airbus/EADS), Finmeccanica (now known as Leonardo), Thales, BAE Systems, and Safran, in collaboration with software companies, universities, research centres and think-tanks making migration control a profitable and viable option.

With the War on Terror having translated into a War on Immigrants there is a conflation of security with migration and border control. Consequentially, there is a plethora of exemplifying instances which marks the involvement and ascent of security and defence companies with public entities. In the aftermath of the terrorist attacks of 9/11 on 11th September 2001, the Madrid Bombings on 11th March 2004, and the London Bombings of 2005, we witness a robust involvement of security and defence companies allegedly providing ‘security’ through a range of technological innovations. The deployment of advanced technologies simultaneously fulfils the role of fortification and securitisation centred on the figure of the migrant. With terrorist attacks leading to increased reliance on advanced and innovative security technologies, the current global military expenditure are at levels close to that of the Cold War period (SIPRI 2016) creating a burgeoning global security market which stands at roughly €100 billion, employing around 2 million people (European Commission 2012). Within this development, the proliferation of border and migration control technologies persists as a subset of the larger

[1] Richa Kumar, currently a practising immigration lawyer in the UK, has obtained her PhD from University of Kent, Brussels School of International Studies, on the public-private in-distinctions in shaping the European migration and security market through migration and border control technologies.

security market capitalising on the persevering of the interlinkage between migration and a range of other threats.

With the fostering of the security-migration interlinkage within which EU migration and border control is framed, we witness its furtherance along the public-private collaboration in the context of European funded research programmes such as the Framework Research Programme (FP6 and FP7) and the current Horizon 2020. Under the aegis of EU funded research programmes, a vast gamut of migration and border technologies have been developed and deployed, both in "number and variety" (Guild and Carrera 2013: 4). The European Research Programmes have been spearheaded by major security and defence companies in Europe with the aim of compensating for a declining defence budget since the end of the Cold War and controlling migration in lieu of abolishing internal borders. Other aims include the establishment of a credible and competitive European brand of EU security products in the global security market and improving employment opportunities within the EU. Tracing the public-private intimacy that characterises the proliferation of migration and border control technologies in the European Union, this paper teases out the nature and the extent of the involvement of major security and defence companies through which they leverage and perpetuate their dominance. Asserting their dominance through the incorporation of technical imperatives corresponding to their technical wherewithal in policies and laws, key reports, calls for proposals and tenders, their power to shape and construct European security is reinforced through furthering military-rooted competencies, cross-sectorality, cross-shareholding, state-shareholding and lobbying. Studying the public-private intimacy is critical to comprehend the power geometry of circumscribing contemporary European migration and border and its larger implications on the perpetuation of an insecurity narrative centred on the figure of the migrant. This power geometry evades the division of 'public' and 'private' – the 'public' referring to the "action and agents of the state" and 'private' referring to market economy (Weintraub 1997: 5). Also, by corollary, it prevaricates the traditional locus of responsibility that emanates from a state/market distinction where the state is seen as the sole locus of the political and the market as non-political (ibid.).

With an aim to probe and map the 'symbiotic' (Chinkin 1999, O'Reilly 2010) public/private collaboration that characterises contemporary European migration control practices, this paper starts with tracing a range of border technologies that have proliferated within the contours of the larger security market. Looking at the key drivers that have spurred the development and deployment of border technologies, we see a recurrence of major security and defence companies that shape the EU security market at large. This recurrence particularly brings fore the obfuscation and futility of divisions such as military/civil, security/defence, software/brute technology (Dijstelbloem 2009, Dijstelbloem et al. 2011), new/old technologies (Guild and Carrera 2013), or functional domains of land/air/maritime/cyber (Broeders and Hampshire 2010, Amicelle et al. 2009, Dijstelbloem 2009, Dijstelbloem et al. 2011, Broeders and Engbersen 2007) that characterise the EU security market at large. In addition to the futility of divisions, the proliferation of EU border technologies is characterised by overlapping market segments, a multiplicity of actors, including companies, European agencies, law firms, lobbying consultancies, research institutes, universities, military academies and trade associations who mobilise and coalesce around the development and deployment of border technologies. Therefore, mindful of the futility of traditional divisions and dualisms, this paper maps the domination of major security and defence companies along military rooted technological competencies, their relations with other companies and state governments, and the support received by bureaucratic institutions and lobbying organisations. By leveraging these competencies and relations, the major security and defence companies have inhabited crucial positions on key advisory boards of organisations and are in constant and regular contact with state authorities, thus playing an important role in shaping the EU security market.

Bolstered by claims of technological neutrality, efficiency, sophistication and progress, these companies configure the security discourse mobilising a specific vocabulary of technical imperatives which is used in policies, directives, project descriptions, conferences and exhibitions. Holding the promise of 'seamless' border control (Broeders and Hampshire 2013) and greater security, advanced and innovative border technologies are framed as an indisputable 'fix' or a 'salvation tool' (Bonditti 2005 in Bigo 2008, Guittet and Jeandesboz 2010, Bronk 1998, European Commission 2004b, ESRAB 2006) and are being continuously deployed in militarised operations dubbed as 'saving lives' (European Commission 2014b). In the process of configuring the security discourse at the interstices of public and private, questions of advancement of border technologies are fused with concerns of global competition, employment, and safety and security benefiting and empowering major security and defence companies at the expense of controlling and disenfranchising migrants at the risk of derogating refugee protection. This raises major concerns of accountability, responsibility and locus of politics that is circumvented and obfuscated to the detriment of migrant and refugee protection creating a technologically advanced labyrinthine of controls and barriers 'punctuating the journey' (Bigo 2013, also see Carrera et al. 2008, Pickering and Weber 2006) which has been variously named as a 'neo-refoulement regime' (Hyndman and Mountz 2008) and 'deportation regime' (Dietrich 2005).

The European Security Market and the Proliferation of Border Technologies

With the "necessity to ease freedom of movement for EU citizens and immigrants within the EU, there is a challenge of controlling the Schengen Borders of 8,000 km of external land borders and nearly 43,000 km of external sea borders of the EU" (Wolff 2010: 24). In addition, concerns of the abolition of internal EU borders were aggravated by the attacks of 9/11 in the USA followed by the Madrid (2004), London (2005) and Paris (2015) attacks: these events have been the key drivers for the proliferation of border technologies in the EU and have provided the necessary impetus to the security market at large in the EU and setting the parameters within which companies operate with the promise to provide technological salvation for migration and border control. The driving impact of these events was not separate and exclusive; each event dovetailed into another, amplifying the momentum at which investments in the development and deployment of security technologies were made.

The abolition of internal EU borders rendered a 'specific flavour to EU borders', with heightened apprehensions of a 'security deficit' (Mathiesen 1999, Boswell 2007). This led to the fortification of EU's external borders and subsequent investments in large-scale information exchange technologies like SIS I and SIS II (Schengen Information System)[2] that has been developed by the French company ATOS, as well as VIS (Visa Information System)[3] developed by Accenture and Sagem Défense Sécurité.

This process of compensating for the so-called security deficit acquired unprecedented momentum in the aftermath of the attacks of 9/11 which was the second key driver. Leading to the instituting of the 'War on Terror' and the creation of Department of Homeland Security in the USA, there were massive investments in the US defence industry. For instance, the US company Lockheed Martin alone received contracts worth $29 billion from the Pentagon in 2008, with other major contractors being Boeing, Northrop Grumman, Raytheon and General Dynamics (Global Research 2011, Hartung 2012.). The Business Insider (2016) reported that Homeland Security companies, which develop security screeners and inspection systems, have had a 'decade of financial bonanza' with OSI Systems, reporting a 10 % increase in the revenues of $595.1–656.1 million. These developments raised serious concerns about the survival of European security and defence companies: with their intense lobbying to support and bolster the competitive element of European industry, various research programmes were created under the aegis of the European Commission and sectors of security, research and technology were transferred from DG Research to DG Enterprise in 2004 thereby moving the security research portfolio closer to a pro-industrialist stance (Hayes 2006: 22; Karampekios et al. 2017: 200).

The events of 9/11 were clearly more beneficial to US security and defence companies; the bombings in Madrid and London, which were closer home, enabled interlinking the general public's anxieties about societal security with its fears about immigration as a threat to physical safety, firmly embedding the securitised view of immigration within the domestic and regional politics of Western Europe (Huysmans 2000, Lahav, Messina and Vasquez 2007: 3). Giving the necessary impetus to Europe's "self-described fight against 'illegal' immigration" (Geddes 2008: 171), the attacks of Madrid and London were vital for ascending the role of European security and defence companies: in the aftermath of the 2004 Madrid bombings, the *Comisaría General de Información*, which is the counterterrorism branch of the National Police force,

[2] Schengen Information System (SIS) is a joint information system that contains information on individuals, particularly migrants and objects that can be accessed by authorities like border guards and police to carry out automated checks for the purposes of issuing visas, residence permits and law enforcement. SIS II is the second generation Schengen Information System launched in April 2013 and includes enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. See more at: European Commission (2020) "Schengen Information System", in https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/schengen-information-system-sis_en, accessed on 24.03.2020.

[3] Visa Information System (VIS) is a largescale IT database system which allows Schengen states to exchange information with consulates in non-EU countries and all external border crossing points of Schengen States on visa nationals (European Commission 2017c).

established new units in the areas of strategic analysis, information systems and technologies, and had funds redirected to them, receiving an 11 % increase in their budget (Reinares 2009). In similar vein, the Madrid Metro Authority awarded a €132.5 million contract to the Spanish civil and engineering construction company ACS Group and advanced security solutions company, Prosegur, to enhance security in the Madrid underground stations by installing surveillance cameras throughout the metro network and deploying private security agents (ACS Group 2005). In response to the London bombings in 2005, a consortium of companies involving Motorola, Thales Group, Fluor, HSBC and Laing Investment was awarded a £2 billion contract to equip the London Underground System with radio communication systems and surveillance cameras (Thales Group 2009). A month after the Paris attacks, defence companies witnessed a rise in their stocks, with state budgets bidding to meet the terror threat; BAE Systems, the £16 billion company, Europe's biggest weapons manufacturer and world's second (SIPRI 2015), saw a rise in their stock by four percentage points in the early trading (The Guardian 2015). In June 2018, EU leaders have agreed to increase the budget for migration and border control to €34.9 billion (European Commission 2018) with the Multiannual Financial Framework (MFF) for 2021-2027, with the aim of making the EU the fourth largest investor in Europe in defence industry research after the UK, France and Germany (Cooper 2017).

The Ascent of the European Security Market

The European Union (EU) security market has a global market share of 25-35 %, ranking second to the US security market which is the market leader (ECORYS 2009). The EU security market is estimated to have an annual turnover of €30 billion, employing around 180,000 persons (European Commission 2016, ECORYS 2009, European Commission 2012: 10). The global security market is dominated notably by Lockheed Martin, Boeing, Raytheon, Northrop Grumman and United Technologies, capturing a 40 % market share (ECORYS 2009, Gloannec et al. 2013, Relyea 2002, SIPRI 2016).

With ambitions of harnessing the "untapped strengths of the 'security' industry and the research community" (European Commission 2004a: Online), the European Commission has actively been supporting security research to broaden its share in the global security market laying the policy framework to support the expansion of European security market. In February 2004, the European Commission launched a 'Preparatory Action on the enhancement of the European industrial potential in the field of Security Research' (PASR 2004) allocating a sum of €65 million for the period 2004–2006. PASR was complemented by a number of projects funded under the Community's Sixth Framework Programme (FP6) under the thematic area of 'Towards a global dependability and security framework' (European Commission 2007). PASR and FP6 prefaced the establishment of the European Security Research Programme (ESRP) under which the Seventh Framework Research Programme for Research and Technological Development (FP7) was established, with an allocation €1.4 billion for the period of 2007–2013 (European Commission 2011b) and the current Horizon 2020 programme has allocated €225 million to security research (European Commission 2019).

The aims and objectives of EU security research was to address security threats ranging from chemical, biological, radiological, nuclear and explosive threats (CBRNE), terrorism, international migration, health, pandemics and environmental change, to concerns of standardisation, i.e. creating an 'EU brand'. Crucially, however, these developments at the EU level generated an EU security market which was prefaced by intense collaboration and intimacy between major security and defence companies – namely Airbus/EADS, BAE Systems, Finmeccanica and Thales group – and EU institutions playing a pivotal role in shaping the EU security market at large and the proliferation of security technologies aimed at migration and border control in the EU.

EU Border Control as a Subset of the EU Security Market

The abolition of internal European borders heightened the need for a 'seamless' mechanism of border control across land, air and sea borders (Broeders and Hampshire 2013) while simultaneously strengthening cyber intelligence. Empowered by the ambition of a seamless border control, in 2002, the Spanish government erected fences, known as SIVE (Sistema Integrado de Vigilancia Exterior or Integrated System of External Vigilance) which are equipped with a technologically advanced early-warning radar system and night vision cameras, deployed with the aim to seal off its maritime borders along the Spanish coastline close to Morocco (De Haas 2008: 1309, BBC 2002, Indra 2010). SIVE has integrated communication systems with the communication networks of Spanish Guardia Civil to facilitate immediate action, which was developed by the Spanish company AMPER, Tecosa of the Siemens Group and Indra costing about €150 million. Since the deployment of SIVE in 2002, an investment of €232 million had been made until 2008 to update it with new technologies (De Haas 2008: 1309, BBC 2002, Indra 2010 and 2011, Articlesbase 2012, Carling 2007). SIVE is a telling example that the development and deployment of border technologies is embedded within the larger security market as technologies operate with multiple functionalities requiring regular upgrades – a wherewithal which are a forte of established security and defence companies.

Further, with the events of 9/11, Madrid and London bombings, migration carries the "spectre of terror" (Feller 2006: 511) and is constructed as a security threat whereby anxieties about societal security intersect with the fears about migration as a threat to physical safety, law and order, planning and fruition of terrorist activity (Koser 2005, Huysmans 2000, Lahav, Messina and Vasquez 2007: 3). After 9/11, over 1,000 mostly Arab and Muslim foreigners were arrested and detained under immigration law violations to uncover the potential terrorists amongst them (Spencer 2008: 3). Similar linkages between terrorism, 'illegal' immigration and organised crime were espoused for in the EU after the incidents of Madrid and London bombings (House of Lords 2005, Baldaccini and Guild 2007) which gave the necessary impetus to Europe's "self-described fight against 'illegal' immigration" (Geddes 2008: 171). With the persisting migration–security linkage, expectedly, there is an overlap between the strategies employed against terrorist activities, organised crime and 'illegal' immigration which in turn is reflected in the range of border technologies that are developed and deployed across the EU and the market segments and key companies which are being mapped in the next two sections.

EU Border Technologies: Market Segments, Technological Domains, Key Companies

The various market segments of aviation, maritime, border security and counter-terror intelligence are used to intersperse and punctuate a migrant's journey with a range of border technologies. These border technologies comprise of information communication technologies (ICTs), smart walls and fences enabled with sensors and cameras, biometrics based on facial features, iris and fingerprints, stationary and mobile surveillance systems equipped with technologically advanced systems like early warning radar systems, unmanned aerial vehicles (UAVs) and drones which are deployed for identification, surveillance, detection and interception.

The key segments that perceptibly caters to migration and border control along the migration-security linkage are primarily aviation, maritime, border security and counter-terror intelligence as they comprise of technologies that install controls and barriers to detect, identify, intercept, track and trace migrants. This reflects a technological labyrinthine that interrupts a migrant's journey at every point with the aim to prevent his/her arrival, to detect, intercept, surveil, track and return (Bigo 2013, Carrera et al. 2008, Pickering and Weber 2006). Based on the description by ECORYS (2009) which has been replicated by the European Commission (2012) in its Security Industrial Policy, below is a brief description of these segments:

- Aviation or air security refers to the "detection, identification, tracking and tracing of goods and persons for secure and safe air transport" (ECORYS 2009: 91). This sector has "grown considerably in the aftermath of 9/11" (ECORYS 2009: 91) owing to the nature of the attacks whereby a scanned and screened airplane was used as a weapon to conduct the attacks;
- Maritime or sea security refers to the "detection, identification, tracking and tracing of goods and persons for secure and safe maritime transport" (ECORYS 2009: 133). The sector includes "sea safety and security, sea environment, fisheries, trade and economic interests of the European Union as well as the general law enforcement and defence" (Sempere 2011: 65). Like the aviation sector, this sector has witnessed growth due to concerns of a "9/11 type of a terrorist attack that can happen at the seas or a port by using a ship as a terrorist weapon" (ECORYS 2009: 52);
- Border security refers to the "controlling of border checkpoints and the surveillance of unregulated frontiers deployed with the aim of restricting 'illegal' immigration, terrorism and organized crime" (Sempere 2011: 64);
- Counter-terror intelligence is one of the "fastest growing market segments along with the aviation sector" (ECORYS 2009: 32). This segment caters to "high level security threats which is high on the political agenda" (ibid.). It involves the "gathering of information, monitoring, detection, maintaining profiles and databases, analysis of databases and communication" (Sempere 2011: 4) and as a market segment, it overlaps with other market segments, particularly due to its concerns to pre-empt the next terrorist attacks.

In the EU, issues of migration and mobility are increasingly being interpreted as problems of security (Faist 2002, 2005) coupled with the complex nature of its borders. The complexity of

EU borders have been variously described as “heterogeneous, delocalized, dispersed, fragmented and transnational” (Bigo 2005: 77, Bigo 2004) or as ‘shifted up, down and out’ (Lavenex 2006, Guiraudon and Lahav 2000, Guild 2002, 2005, 2006, and 2009, Bigo and Guild 2010), “policed at a distance” (Bigo and Guild 2005: 234) and as ‘digital borders’ (Broeders 2007, Brouwer 2008). Owing to the complex nature of European borders, we witness the development and deployment of a range of border technologies across the domains of aviation, maritime, border security and counter terror intelligence to compensate for the abolition of internal borders and migration-security interlinkage.

This vast gamut of advanced and innovative ‘border technologies’ “encompass both war – and crime – fighting” (Bigo et al. 2008: 5) capacities and are developed at the convergence of civil and military technologies, forming a crucial component of contemporary European Union security practices (Guittet and Jeandesboz 2010). These border technologies lie at the technological continuum of defence, security and civil applications and are increasingly developed and deployed to the ‘migration problem’ or the ‘problem of the Mediterranean’. This is particularly clear from the nature of military capability deployments for the recent search-and-rescue missions like the Operation Mare Nostrum by the Italian Navy (Marina Militare 2016, Musarò 2016) and Operation Triton by Frontex (ANSA News 2016, European Commission 2014b, Frontex 2016). Particularly important to note is that even when border technologies are developed and deployed with the aim to abate and control other security threats like human smuggling, trafficking, organised crime or overstaying, they centre on the figure of the migrant as a result of the persisting linkages made between migration and a range of security threats.

Along the migration-security nexus, a range of border technologies have been developed as a part of various technology projects funded by the European Commission, as a part of the European Research Programme, EU agencies like the European Space Agency (ESA) and at member-state level. The Migrants Files (2015) published a report analysing 39 Research and Development (R&D) projects that focused on migration control which were financed by the European Commission and the ESA in the period of 2002 to 2013, with a total cost of €225 million (The Migrants Files 2015) which has benefited the major security and defence companies. Of the said 39 R&D projects, Airbus/EADS participated in 10 of them via 14 subsidiaries, Finmeccanica worked on 16 projects via 13 subsidiaries, and Thales in 18 projects via 13 subsidiaries (The Migrants Files 2015). Cryptically named projects like AMASS – Autonomous Maritime Surveillance System – were financed for amplifying maritime surveillance claiming to help “detect suspicious vessels” and provide authorities with early warning of illegal activities at sea, thus improving overall protection of European shores (AMASS 2011: Online). The AMASS project was led by Carl Zeiss Optronics together with nine other technology specialists and border agencies from across Europe – including Fraunhofer-Institut für Informationsverarbeitung in Technik und Biologie (IITB), Instituto Canario de Ciencias Marinas, and the Armed Forces of Malta. The estimated costs of the project were €4 million. Other examples of projects financed are: Doggies[4], Sniffer[5], Sniffles[6] and Snoopy[7] which focus on the development of 'advanced olfactory sensors' – or smelling capabilities – for detecting hidden humans at border crossings; TALOS[8] – Transportable Autonomous Patrol for Land Border Surveillance – which was developed for amplifying land border surveillance to detect, track and prevent illegal border crossings. Thus, border technologies range from software based technologies to military grade technologies which are provided by major security and defence companies and are deployed for identification, surveillance, detection and interception (Broeders and Hampshire 2010, Amicelle et al. 2009, Dijstelbloem 2009, Dijstelbloem et al. 2011, Broeders and Engbersen 2007).

Prior to profiling the dominance of major European security and defence companies, it is worth appreciating the role of technological domains within larger market segments such as aircrafts/drones, biometrics, command and control systems, Port Access Control, communication systems, perimeter security systems, Radio-Frequency identification systems, as well as surveillance, tracking and tracing to briefly comprehend their role in migration and border control.

Aircrafts/drones refer to military-grade aircrafts, unmanned air vehicles (UAV), Remotely Piloted Aircraft Systems (RPAS) and drones that are primarily developed for military needs but are increasingly used for border protection (Sempere 2011: 64). These aircrafts and drones are different from regular passenger and cargo aircrafts. In the EU, military drones have been used for search and rescue missions in the Mediterranean (Koslowski and Schulzke 2018, Monroy 2020) by Frontex. Aircrafts and drones can be deployed across the domains of land, air and water to conduct border surveillance. The surveillance capacities of aircrafts and drones can be amplified with electro-optical cameras and thermal imaging cameras that independently detect moving targets and keep them in focus and locate mobile and satellite telephones (Monroy 2020).

Biometrics-enabled communication systems are increasingly being seen as the most trusted method of identification and access control and are used for law enforcement, physical access control (including border control), logical access control to information systems and convenience (ECORYS 2009: 204). Biometrics utilise a range of biological information like behaviour, signature, facial features, fingerprint, hand geometry, iris, palm print, voice recognition and vascular details, and is used in EU-wide databases like SIS I and SIS II, VIS and Eurodac[9] (ECORYS 2009: 184). Biometric systems are composed of computer systems,

[4] See at: http://www.fp7-doggies.eu/, accessed on 21.02.2016.

[5] See at: http://www.sniffer-project.eu/, accessed on 21.02.2016.

[6] See at: http://www.sniffles.eu/, accessed on 21.02.2016.

[7] See at: http://cordis.europa.eu/result/rcn/175826_en.html, accessed on 21.02.2016.

[8] See at: http://talos-border.eu/, accessed on 22.01.2016.

[9] Eurodac is an acronym for European Asylum Dactyloscopy Database. Eurodac is an information technology system for comparing fingerprints of asylum seekers was established in 2003. It was brought in force by Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the

secure communication networks, characterisation/comparison software (biometric engine), data encryption algorithms, secure data stores, and biometric data capturing devices. Advancements made in this technology promise to make it more effective than other technologies in combating terror attacks: in the aftermath of the Brussels attacks, the CEO and founder, Neil Norman, of Human Recognition Systems (HRS) said that “biometrics can help combat terrorism by profiling” (Lee 2016: Online). The European biometrics market is estimated at €708.4 million and several European pilot projects have been carried out to use biometrics in border and transport management, for example, Privium Programme at Schiphol Airport (The Netherlands), project PEGASE at Charles de Gaulle Airport (France), and project miSense at Heathrow Airport (UK).

Command and control systems also known as C2 systems refer to military communication systems which support the commander by performing three functions: creating and maintaining the common operational picture (COP); supporting decision making by improving its speed and accuracy and supporting preparation and communication of execution information (Globalsecurity.org 2020). C2 systems have been used in military warfare and in the context of border controls they can be used for border surveillance. It can integrate a range of technologies like radar technologies for the detection of low flying aircrafts for air surveillance, coastal radar, maritime patrol aircraft (MPA), light patrol aircrafts, UAV, patrol vessels for maritime surveillance, satellite technologies, mobile devices and handsets such as tablets and smartphones (Leonardo 2020, European Commission 2017a, Thales Group 2019b).

Port Access Control Systems refer to a combination of devices to prevent access to port areas. These can include intrusion and fire detection, CCTV, video surveillance, card readers, and computer systems (ECORYS 2009, Sempere 2011). Access control of ports is crucial due to their importance as critical infrastructure for freight and passenger transport network as well as important border control from the perspective of maritime security (Andritsos 2013).

Information technology (IT) and secure communication systems comprise of IT-based secure communications and are embedded in several equipments with the aim of transmitting information to central units that collect and process data, and a user interface that presents relevant information to the operator, thereby helping in increasing awareness and ensuring proper and immediate response (Sempere 2011: 49). IT and secure communications are used as components of other systems with the claim to enhance their capabilities; this is often provided by companies with system integration capabilities. Systems like the European databases Eurodac, the Schengen Information System (SIS I/SIS II), and the Visa Information System (VIS) (Bigo and Guild 2005, Broeders 2007, Carrera and Geyer 2007) are examples of IT-based secure systems. These systems have severe implications on migration and border

establishment of ‘Eurodac’ for the comparison of fingerprints for the effective establishment of the Dublin Convention [2000] OJ L 316/1. See more at: European Commission (2020) “Identification of applicants (EURODAC)”, in https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en, accessed on 26.03.2020.

control. For instance, the Schengen Information System (SIS) contains information on millions of individuals, especially third country nationals who have been refused entry to the Schengen territory (Brouwer 2005: Online). Eurodac, the Schengen Information System (SIS I/SIS II), and the Visa Information System (VIS) are data sharing and data collection devices that have been developed for the purposes of controlling immigration and safeguarding security (Brouwer 2005: Online). By Council decision 2004/512/EC, the Visa Information System (VIS) aims at improving the functioning of the common policy in the field of visa; internal security and the fight against terrorism; fight against fraud; the prevention of visa shopping; the improvement of the possibilities to return 'illegal' immigrants; and finally, the improvement of the application of the Dublin Convention (Brouwer 2005: Online, ECRE 2007: 33, Broeders and Hampshire 2010: 10).

Perimeter security systems refer to the deployment of a combination of technologies like smart fences, electric fences, cameras, sensors, underground cables which can be enabled with cameras, sensors, radio signal monitoring system to detect movement, protect unregulated border crossings against 'illegal' migration, organised crime and terrorism (Sempere 2011: 64, European Commission 2012). The 2002 SIVE is an example of such perimeter security system. Perimeter protection involves a wide array of technologies like robots, cars, trucks, guns, communication systems, sensor-enabled fences and walls, and screening and scanning devices. Their deployment involves the integration of technologies and devices which companies with system integration capabilities are able to provide.

RFID systems is an abbreviation for Radio-Frequency Identification systems. RFID systems enable the identification, collection of attributes, and tracking and tracing of persons and goods. Due to the controversial issue of RFID systems being potentially misused for eavesdropping, encryption and false identification, the surveys (Sempere 2011, ECORYS 2009, Want 2006) have referred to its usage only in the area of cargo and goods tracking. RFID systems are widely used for tracking and tracing of goods for both aviation and maritime security which also enable the detection of hidden human bodies which plainly implicate on detecting and controlling migrants.

In addition, technologies are used for the **surveillance, tracking** and **tracing** of goods, vessels, trucks and aircrafts. CCTV systems, for instance, are deployed with the aim of "recognising and tracking objects such as people and vehicles and monitor behaviour such as spot loitering" (Munday et al. 2006: 11, in Sempere 2011: 62). Particularly, tracking and tracing of chemical, biological, radiological, nuclear and explosive (CBRNE) threats have become an urgent concern after the attacks 9/11, owing to fears of nuclear materials being shipped around the world and their potential usage by terrorists. CBRNE detection is followed by responses to neutralise it (ECORYS 2009: 165). Several scholars have expressed the concern that these technologies have a corrosive impact on the rights of people at large, and migrants in particular, who are profiled and 'banned' (Mathiesen 1999, Bigo 2006, Amoore 2009).

Below we utilise existing market surveys of ECORYS (2009) and Sempere (2011) to tabulate the key companies and border technologies involved in the development and deployment of border technologies:

Table
Border technologies and key companies assembled from ECORYS (2009) and Sempere (2011)

Border Technologies	**Key Companies**
Aircrafts/Drones (Civil and military aircrafts)	Airbus, Aérospatiale, BAE Systems, Boeing, Dassault, Diehl, Finmeccanica, Lockheed Martin, Northrop Grumman Corporation, Safran Group, Thales
Biometrics	Accenture, Cogent Systems, Image Ware Systems, Indra, Iris Guard, L-1 Identity Solutions, Motorola, NEC Advanced Security Solutions, Lockheed Martin, Northrop Grumman, Precise Biometrics, SAGEM Morpho, Sagem Sécurité, Unisys
Command and control systems Port Access Control	BAE Systems, Airbus/EADS, Indra, Kongsberg, Thales
Communication systems	Atos Origin, BT Global Services, Cap Gemini, Cisco, Deutsche Telekom (T-Systems) IBM, Airbus/EADS, Motorola, Harris Corporation, Selex, Telefónica, Telecom Italia
Perimeter security systems	Alenia Aeronautica, BAE Systems, Dassault, Airbus/EADS, EMT, Indra, Kongsberg, Meteor, Saab, Sagem, Thales
Radiofrequency identification (RFID)	Avery Dennison, Checkpoint Systems Inc., Datamars SA, HID Global, IBM, Intel, Infineon Technologies, Intermec Technologies Corp., Philips Semiconductors, Savi Networks, Sensormatic –Tyco, Sokymat, ST Microelectronics, Sun Microsystems, Tagmaster/ WaveTrend, Texas Instruments Radio Frequency Identification Systems, UPM Raflatac
Screening and scanning	Bruker Daltonics, General Electric, Gilardoni, L-3 Communications Corporation, Rapiscan Systems, Smiths Detection
Surveillance, tracking and tracing	Axis Communication, Bosch Security Systems, Cassidian, G4S Securitas Group, Gunnebo, Honeywell, Ingersoll -Rand

The foregoing table does not aim to be exhaustive as it is often difficult to gather information on company profiles due to confidentiality as well as the constant mergers and acquisitions which fluctuate their product profile. Crucial to the very nature of these technologies is their usage of a combination of technologies which necessarily affords them the forte of major security and defence companies specialising in military technologies and in system integration capabilities. Further, there is a diverse range of actors that are engaged in this market in various capacities, such as suppliers of technological systems, customers, research, maintenance, logistic support, training and simulation as mapped in the above table. However, it is illustrative on two counts: the utilisation of a combination of technologies to build border control systems, and the recurrence of certain companies in various technological domains indicating their dominance in the market. For instance, automated border crossing systems deployed at Schiphol, Frankfurt, Paris, and Heathrow airports utilize iris-based and fingerprint-based systems biometric systems in combination with electronic passports and identity cards which are enabled with RFID chips (Loeschner et al. 2007). The data from biometrics and electronic passports is read by computer systems and then checked against existing databases; only when approved, electronic gates open for the passenger to exit (ibid.). For border control operations, Frontex deploys a combination of technologies and equipment such as vessels, aircraft, patrol cars and heartbeat detectors (Frontex 2019). Due to the combination of technologies used, consequentially, the systems must be integrated and interoperable thus giving a comparative edge to major security and defence companies.

Secondly, the table crucially exemplifies the recurrence of companies who dominate the security market across technological expertise and products: for instance, Airbus/EADS specialises in civil and military aircrafts and drones, and also offers products in command and control systems as well as perimeter security systems. This recurrence of major security and defence companies involved in the development and deployment of security technologies across technological domains and market segments emerges due to their technological and financial wherewithal to acquire the means to provide border technologies which can be deployed in war as well as for border control. Probing further into the domination of the security market, the next section looks closely at the roles and relationships between the various actors in the security market.

Profiling the Domination of Major European Security and Defence Companies

In this section we unveil the extent and expanse of the relationships and the role of major security and defence companies in asserting domination in the European Union security market. The major companies have the human and technological resources at their disposal which allow them to play a central role in creating the conditions to facilitate the development and deployment of border technologies in the EU.

Military rooted technological competencies

We profile this domination of the major companies by first looking at the military rooted technological competencies that are furthered as imperatives through reports, tenders and calls for proposals. Major security and defence are placed advantageously to develop and deploy border technologies as they have established technical wherewithal to meet requirements that are rooted in military technological competencies like dual-use technologies, system integration and interoperability. Comprehending these technological requirements in everyday language, as done below, provides us with an insight in their military nature of these technical competencies which are considered crucial to the design and development of border technologies.

Dual-use technologies are technologies that can be used for both "military and civil purposes" (Bigo et al. 2008: 5) including technologies like drones and submarines. An example of dual-use technologies in migration control is the usage of military aircrafts and drones in maritime surveillance, or submarines locating and intercepting rubber boats with 'illegal' migrants. Various naval and air-based operations like Ulysses,[10] Triton,[11] Orca,[12] RIO IV,[13] and Project

[10] Ulysses is an operation led by Spain in co-operation with France, Italy, Portugal, and the United Kingdom with the aim of enforcing sea border controls off the coasts of the northern Mediterranean and Canary islands.

[11] Triton is a project led by Greece in co-operation with France, Italy, and Spain. It took place in March 2003 involving joint sea border controls in the south-eastern Mediterranean.

[12] Orca is a project led by Norway with Finland, Germany, Netherlands, Sweden, Estonia, and Poland as observers. The operation's objective is the prevention of 'illegal' immigration/trans-border crime and 'illegal' use of visas and documents issued to seamen by improving co-operation between border control authorities.

[13] RIO IV is led by Spain, the aim of the operation is to improve border control systems and practices in designated ports in EU candidate countries.

Deniz[14] are all aiming at increased interceptions of migrants (Sianni 2003: 31). In 2018, Frontex, the European Maritime Safety Agency (EMSA) and Portuguese authorities launched the first joint Mediterranean drone surveillance operation; this project had a total allocation of €76 million of which €66 million was allocated to the Portuguese company Tekever along with the Italian defence company Leonardo (a Finmeccanica company) and Portuguese company UA Vision (Nowak 2019).

System Integration refers to the capability of building client-tailored computing systems that connect the various sub-systems to make them coordinate and function as a whole, which are often called "system-of-systems solutions" (Mawdsley 2013: 27, Sistemi Informativi Aziendali 2012). Perimeter defence systems is an example of such integrated systems used for migration control. It comprises of fences which are enabled with video cameras, sensors, and barbed wires that can identify a mutant (an 'illegal' migrant or an animal) and can send the data into an alarm system enabling direct intervention. In addition, system integration also enables the traditional roles of army, navy, coastguards, and intelligence to change because of the technology and its capability to link them. For instance, the European Integrated Border Management (EIBM) aims at "national and international coordination and cooperation among all relevant authorities and agencies involved in border security and trade facilitation to establish effective, efficient and coordinated border management at the external EU borders" and this necessarily requires an integration of systems (European Commission 2014b: Online).

Interoperability of systems refers to the "ability of Information Technology (IT) systems and business processes to support the exchange of data and to enable the sharing of information and knowledge" (European Commission 2005: Online, Besters and Brom 2010, Gonzalez-Fuster and Gutwirth 2011). Interoperable systems particularly refer to computer-based data systems which can communicate between themselves as well as utilising "common security and defence facilities that enable connection, interaction and communication for exchange of data and services with other equipment" (NATO 2012). Border crossing systems often marketed as the "perfect single system" (Hoijtink 2014: 470) have the traits of system integration as well as interoperability. Gemalto, a Thales company, provides integrated border management services comprising of automated visa and passport checks, and perimeter surveillance with CCTVs around ports; the received data is connected to a control room (Gemalto 2019). The biometric engines for the biometric processing of visa applicants conduct automated biometric checks against existing systems by reading passports. In the process, these services detect fraud and match data against watch lists, thereby centralising the data in an entry-exit system. In case a visa holder overstays, the system moves the person, i.e. the 'overstayer', from the 'legal' to 'illegal' category.

Rooted in traditional military practices of command and control systems, simulation and modelling (Robkin 2010), these technological requirements are ubiquitous in reports of organisations like Group of Personalities, European Security Research Advisory Board,

[14] Project Deniz involves the secondment of experts to Turkey to combat trafficking of 'illegal' immigrants by sea

European Security Research and Innovation Forum and other advisory boards; they are incorporated as desirable and mandatory requirements in call for tenders, bids, and project specifications. For instance, FP7 projects valorised these requirements for the security projects: PERSEUS (Protection of European seas and borders through the intelligent use of surveillance) was coordinated by the Spanish defence company Indra Sistemas SA along with defence companies like Airbus/EADS and SAAB. The project which ran from 2011-2015 aimed at "monitoring illegal migration and combatting related crime and goods smuggling" (European Commission 2019). PERSEUS was developed along the technological imperatives of system integration (eg. "integration of assets and platforms, integration between systems, integration of maritime related services"), dual use (eg. "dual use procurements of high-technology assets") and interoperability (eg. "an interoperable Perseus Data Model") (European Commission 2019: Online). These traits have been valorised in the Horizon 2020 programme as well thus giving a comparative edge to major European security and defence companies which have the ability to provide them.

Cross-sectoral competencies

Major security and defence companies have established wherewithal to build technologies that interact across technological domains, capabilities, sectoral boundaries and the security/defence divide; this is known as cross-sectoral competencies. Cross-sectorality also implies the utilisation of technological competencies of one sector in another, for example the transfer of military competencies in civil matters and vice versa (ECORYS 2009). Another example of cross-sectorality is utilising air-based technologies like drones and UAVs for maritime surveillance. Cross-sectorality has provided the major security and defence companies with a comparative advantage as they specialise in various areas of the military, such as aerospace, maritime and land. These companies have also been able to expand their expertise in emerging technologies like biometrics or ICT-based technologies. Below we look at the various competencies across sectors of the major security and defence companies.

BAE Systems specialises in defence, security and aerospace and its US subsidiary, BAE Systems Inc., specialises in electronics, intelligence and land armaments which gives BAE Systems expertise across aviation, border security and intelligence (BAE Systems 2012). Mergers and acquisitions have been crucial in expanding their competencies: BAE Systems acquired Tenix Defence and Atlantic Marine to expand its operations in maritime security; Detica, ETI, Norkom, L-1 Intelligence Services group and OASYS Technology have expanded their expertise in the field of cyber intelligence (BAE Systems 2011, Boston Business Journal 2010, Business Wire 2010). In addition, BAE Systems has a joint venture with Loughborough University with the aim to "promote social and economic programmes in the global marketplace"; in this joint venture, BAE Systems owns a 55 % stake and the Loughborough University owns a 45 % stake (Corporate Watch 2002 and 2015).

Airbus/EADS has competencies in aviation, maritime, border security, satellite services, emergency solutions, surveillance, communications, maintenance and logistics (Morrison 2010). Acquisitions of Sofrelog and Atlas Elektronik which had been merged into Sofrelog Atlas Maritime has further consolidated its position in maritime security. Airbus/EADS has a strong support and service division which has been strengthened with the acquisition of Vector Airspace and Satair. In 2005, EADS acquired Nokia's Professional Mobile Radio (PMR) activities which specialise in secure communications.

Finmeccanica specialises in seven sectors: aeronautics, helicopters, space, electronics, defence systems, transportation and construction. It has expertise across various domains of security and across the civil/military distinction. Its subsidiaries specialise in the sectors of transportation and construction, leveraging its expertise in the area of critical infrastructure towards which increasing attention is given to secure the EU projects such as SAWSOC (Situation AWare Security Operations Center) (European Commission 2017a), CockpitCI (Cybersecurity on SCADA: risk prediction, analysis and reaction tools for critical infrastructures) (CockpitCI 2019) and PANOPTESEC (PANOPTESEC 2014) in all of which Finmeccanica companies were participating to fortify the critical infrastructure against natural disasters, terrorist attacks and criminal activities (Sempere 2011: 3).

Thales Group has expertise in aerospace, space, ground transportation, defence and security and it has several subsidiaries and companies world over that enhances its cross-sectoral edge. With its acquisition of Gemalto in 2017, Thales has become a global leader in digital identity and security (Thales Group 2019b). Thales Canada Transportation Solution formerly known as Thales Rail Signalling Solution specialises in communication-based transport control systems for railways (Thales Group 2014d). Thales Defence & Security Inc. is a US based company of Thales Group, involved in US government projects, and supporting strategic partnerships in the development of key technologies for the defence market (Thales Group 2018). Thales Underwater Systems, formerly known as Thomson Marconi Sonar specialises in underwater activities for naval purposes (Thales Group 2019d). Thales Optronics specialises in optronic equipment for air, land and naval usage (Thales Group 2019c). In 2006, Thales Group acquired ADI Limited and renamed it as Thales Australia which specialises in systems, products and services in the defence, security and civil markets (Thales Group 2014a). Arisem was acquired in 2004, specialising in data mining software solutions for media, healthcare, defence, security and finance sectors (Arisem 2011). Thales Training & Simulations Ltd. specialises in training and simulation solutions industry in both civil and military applications (Thales Group 2014c). Thales Group company Alcatel is active in space business and rail signalling solutions business (Thales Group 2019a).

Cross-sectoral competencies enable major security and defence companies to "operate in more than one market" enabling them to utilise "experience in intelligence, surveillance and reconnaissance as well as command and control in the military sector" as well as in the civil sector (Sempere 2011: 157, 164). Advances in electronics, information and communication technologies financed in other sectors of digital security can be leveraged in border security by being utilised as smart cards, RFID tags, or mobile communications (Sempere 2011). Thus, cross-sectorality also allows for the circulation or 'heterogenous use' of technologies (Bigo et al. 2008). By leveraging the cross-sectoral competencies, a whole gamut of technologies ranging from satellite imagery, drones, radar, port management systems, satellite communications, mobile radios and naval ships get deployed for migration control. In addition, the European Commission’s technological requirements of integration, interoperability and dual-use which are incorporated in the research programmes necessarily imply that the companies exploit their advantageous position with the development of systems that can be used across sectors.

The cross-sectoral edge of major security and defence companies is continuously expanded through mergers and acquisitions primarily of small and medium enterprises in the European security market. Acquiring small and medium sized companies (SMEs) plays a crucial role in the expansion of the products and service portfolio of major security and defence companies. In 2008, Airbus/EADS acquired the US Plant CML which specialises in emergency response solutions and services (ECORYS 2009: 223). This acquisition expanded Airbus’ competency to provide “situational awareness, urgent communication, expedite response, promote collaboration and increase response efficiency” (Airbus Defense and Space 2011) which is a key market segment to cater to ‘new threats’ like “terrorist attacks, suicide attacks, bombing of critical infrastructure like train stations or subways” (Sempere 2011: 31). In 2007, Finmeccanica acquired the British VEGA Consulting Services Ltd (VEGA) which specialises in simulation and training (Mawdsley 2013: 28) whereby software is used to artificially recreate incidents. Simulation and training is a sector where “companies involved in military simulation enjoy a competitive advantage due to the similarity of technologies” (Sempere 2011: 59). BAE Systems has made some major acquisitions, expanding its operations in sectors of applied intelligence, maritime security and financial crime. In 2008, it acquired Detica to form BAE Detica, now known as BAE Systems Applied Intelligence (IT News 2012), and in 2010, it acquired the Danish cyber and intelligence company ETI (Washington Technology 2010 and 2011), thereby expanding its operations in applied intelligence. In 2008, the Thales Group acquired the British company n-Cipher and the Dutch company Sdu-Identification, both of which specialise in the area of secure communications. The expertise and competencies of the acquired companies enable the major companies to develop “synergies” (Sempere 2011: 157) with existing capabilities and expand their foothold in the market.

Cross-shareholding

Major security and defence companies have stakes in each other either directly or through their subsidiaries. This formal relationship that ensues between these major companies through shares in each other is called cross-shareholding. Below, we look at the cross-held stakes and shares between the European major security and defence companies as of 2017: Thales, BAE systems, Finmeccanica and Airbus/EADS. The companies have a breadth of specialisations which gives them a strong global and European foothold. Having stakes and shares in each other and establishing joint venture companies expands the cross-sectoral edge of the companies and gives them considerable advantage in dominating the security market at large.

Thales Alenia is a satellite manufacturer and a joint-venture company between Thales which holds 67 % and Finmeccanica which holds 33 % of the company (Thales Group 2014b). In 2017, Thales Alenia has won two contracts worth €180 million with the European Commission to cover the development and operationalisation of Galileo for the period of 2017–2020 (Military Technologies 2017). Interestingly, the involvement of Thales Alenia is indicative of the lock-in effects that characterise such projects: Thales Alenia was involved in the Galileo[15] project in 2008 and in 2010, with the 2010 involvement being of €85 million contract to operationalise Galileo by early 2014 (Thales Alenia Space 2010, 2011).

Eurotorp is a consortium specialising in naval defence and is co-held by the Thales Group for 24 %, Finmeccanica for 50 % through its subsidiary company Whitehead Alenia Sistemi Subacquei, and DCNS, a French defence company holding 26 % (European Commission 2003, DCNS 2017).

Telespazio is a space flight company and is co-held by Thales holding 33 % and Finmeccanica holding 67 % (Telespazio 2017). Interestingly, the Galileo Service Operator (GSOp) worth €1.5 billion has been awarded to Spaceopal which is a joint venture of Telespazio and the German Space Agency (GPS World 2017). This shows the involvement of the same major companies through joint ventures and subsidiaries in different aspects of projects: Thales Alenia as well as Telespazio won contracts in the Galileo project.

Eurofighter, an advanced combat aircraft, is a consortium with Finmeccanica holding 21 %, Airbus/EADS holding 46 %, and BAE Systems holding 33 % (Eurofighter Typhoon: no date). It has been deployed in operations in Libya, Iraq and Syria (ibid.).

MBDA Missile Systems is a developer and manufacturer of missile systems and is co-owned by BAE Systems which holds 37.5 %, Finmeccanica (25 %), and Airbus/EADS (37.5 %), which makes it a truly integrated European defence company. MBDA has a strong global presence and works with over 90 armed forces worldwide (MBDA Systems 2014).

Eurosam, co-held by Thales and Finmeccanica, is a subsidiary of MBDA Missile Systems specialising in naval and ground-launched air-defence missiles (Eurosam 2013). Eurosam is collaborating with "Turkish defense organizations to provide technology transfer to Turkey and bring the opportunity of export to third party markets" (Army recognition 2018: Online).

NHIndustries is a helicopter manufacturing company and is co-held by EADS/Airbus holding 62.5 %, Finmeccanica holding 32 % through its subsidiary AgustaWestland, and Fokker Aerostructures, a Dutch Aerospace company, holding 5.5 % (NHIndustries 2014).

It is important to note that the percentages of shares held are under constant flux due to mergers and acquisitions and selling off of companies. For instance, in 2014 Airbus/EADS announced the "disinvestment of its assets in Fairchild Controls, Rostock System-Technik, AvDef and Atlas Elektronik and stakes in Dassault" (Aviation Week 2014, Industry Week 2014) with the aim to refocus its business strategy towards military and defence in response to the wars in Syria, Libya, Ukraine.

Crucially, having stakes and shares in each other and establishing joint ventures gives companies like Thales, BAE systems, Finmeccanica and EADS/Airbus, a considerable edge in dominating the security market at large. With one of the cross-held companies benefiting, it in

[15] Galileo is Europe's Global Navigation Satellite System (GNSS), providing improved positioning and timing information with significant positive implications for many European services and users. See at: European Global Navigation Satellite Systems Agency (2019) "Galileo is the European global satellite-based navigation system", accessed on 30.03.2020.

turn benefits them all: this has been the case in FP7 projects where for instance Telespazio, a joint company between Thales and Finmeccanica, has participated in eight projects under the Seventh Framework Research Programme (FP7) with an EU contribution of €6.1 million (Jeandesboz and Ragazzi 2010).

Companies also have robust business exchanges between them: Safran Group, which is a French multinational company specialising in aircraft, rocket engine, aerospace components, and security, was formed in 2005 by the merger of Snecma and Sagem SA and acts as a sub-system producer for the major security and defence companies; Aircelle, a Safran Group company, is the nacelle systems integrator for both the engines offered on the Airbus A380 manufactured by EADS; Labinal Power Systems and its subsidiary Technofan, which are Safran Group companies, supply components for Boeing and Airbus/EADS commercial airplanes and for combat aircrafts of Dassault, Boeing and Lockheed Martin (Safran 2014a, 2014b, 2016).

In addition to the foregoing advantage which is based on company product profile as traced across military rooted technological competencies, cross-sectoral competencies and constant mergers and acquisitions of small and medium sized companies, university products, the major security and defence companies also assert their dominance through persisting formal relationships through shareholding with the State authorities as well as with major companies which we explore in the section below.

Relationships beyond public-private dualisms

The role of military and security companies in shaping and profiting from migration and border control ensues along public/private blurring in parallel with formal frameworks of state shareholding and stretching out to informal networks of lobbying and support via bureaucratic novelties created at the interstices of public and private realms. In the next section we look at the state-shareholding patterns in major security and defence companies followed by mapping various agencies and organisations that operate beyond strict public-private distinctions.

State-shareholding

Traditionally, “state ownership is common across all of Europe’s defense sectors” (Avascent 2013: 4) with the aim to “protect information relating to sensitive military equipment” (O’Donnell 2010: 4). This formal relationship has resulted in the persistence of strong and enduring relationships between major security and defence companies and their national governments as well as other states through their national government’s diplomatic ties.

Based on the shareholding information available on the company websites, the table below maps the state shareholding in the major security and defence companies:

Table
(State)-Shareholding in major EU security and defence companies[16]

Company	Shareholders	Percentage
Airbus/EADS [a]	SOGEPA – Societé de Gestion de Participations Aéronautiques is a French holding company owned completely by the government of France.	11.3
	GZBV – Gesellschaft zur Beteiligungsverwaltung mbH & Co. KG operates as a subsidiary of KfW; KfW Bankengruppe is a German-owned development bank.	10.1
	SEPI – Sociedad Estatal de Participaciones Industriales is a public law entity, whose activities follow the private legal system, and which is attached to the Spanish Ministry of Finance and Public Administrations.	3.9
	Free float shares (Institutional Investors & Retail) refer to publicly available shares for trade.	73.6
	Treasury shares	0.4
BAE Systems [b]	In February 1981, the British government sold the 51.57 % share in BAE System in order to return the company to private ownership. The remaining 48.43 % shares were finally sold in April 1985 but the government retained a single £1 'Golden share' that would allow it to veto any possibility of foreign ownership, which was used in order to oppose the BAE Systems and EADS merger.	
	Franklin Resources Inc. is a global investment management organisation known as Franklin Templeton Investment.	6.2
	Brandes Investment Partners, LP is an investment advisory firm, specializing in managing global equity and fixed-income assets for clients worldwide.	4.0
	CGNU plc, known as Aviva plc since 2002, is an insurance company.	3.2
Finmeccanica [c]	Italian Ministry of Economy and Finance	30.2
	Institutional Investors	51.6
	Individual Investors	17.5
	Treasury Shares	0.7
Thales [d]	Through TSA, a holding company wholly owned by the French state.	27
	Dassault Aviation	24.8
	Free float shares (Institutional Investors & Retail) refer to publicly available shares for trade. Employees hold 2.60% of these.	49.3

a: Based on: Airbus Group (2013, February 26) 'Annual Results 2013', by Tom Enders (Chief Executive Officer) and Harald Wilhelm (Chief Financial Officer).

b: Based on: BAE Systems (2016) 'Heritage: British Aerospace UK', in http://www.baesystems.com/en-us/heritage/british-aerospace-uk, accessed on 05.12.2016; Corporate Watch (2016) 'BAE Systems: Who, Where, How much?', in https://corporatewatch.org/company-profiles/bae-systems-who-where-how-much, accessed on 05.12.2016; Franklin Resources Inc. (2016) 'Company Information', in http://www.franklinresources.com, accessed on 05.12.2016; Brandes Investment Partners (2015) 'Homepage', in https://www.brandes.com, accessed on 05.12.2016; Aviva plc (2002) 'CGNU becomes AVIVA', in http://www.aviva.com/media/news/item/cgnu-becomes-aviva-1191/, accessed on 05.12.2016.

c: Based on: Finmeccanica (2012) "Consolidated Financial Statement", in http://www.annualreport2012.finmeccanica.com/documents/13226/38630/140_142_finmeccanica_and_financial_market.pdf/f4cb9e79-e23a-4dc4-ad12-6f72f077762b, accessed on 06.05.2014.

d: Based on: Thales Group (2016), 'Shareholding structure', in https://www.thalesgroup.com/en/investor/retail-investors/share-and-shareholding, accessed on 05.12.2016; Dassault Aviation (2016), 'Homepage', in http://www.dassault-aviation.com/fr/dassault-aviation/finance/actionnariat/, accessed 05.12.2016.

State ownership in the major security and defence companies has played a crucial role in the investments in the company which are often in line with state agenda. Similarly, states in turn shape a budget plan that can strengthen the national defence companies. This has resulted in investments that emboldens the use of military technologies for civil purposes. For example, there is an increased usage of national military resources like naval ships, submarines, and

[16] The above table is based on company shareholding patterns as accessed in 2017. The information was gathered from company websites, organigrams and reports.

drones for the alleged search and rescue missions (Akkerman 2018, Jones and Johnson 2016). The Transnational Institute, the Campaign Against Arms Trade (Stop Wapenhandel 2019) and Delàs Centre found that at least €900 million was spent on land walls and fences between 2006 and 2017, with a further €676.4 million on maritime operations aimed at keeping people away from Europe's shores (Stone 2019).

In addition, state ownership in major security and defence companies shape security and migration control practices in third countries outside of the European Union. A crucial case is Finmeccanica's role in the construction of Libyan border control capacities consists of a "special relationship of a common colonial history, and bounded by important economic ties" (Klepp 2010: 80). In 2006, the Finmeccanica subsidiary AugustaWestland together with Italy and Libya formed the joint venture LIATEC (Libyan Italian Advanced Technology Company) resulting in a contract of 10 AW109 helicopters worth €80 million (Lemberg-Pedersen 2013: 159). In 2009, the Finmeccanica subsidiary Selex Galileo had a deal of selling 50 drones to Libya to patrol the Southern borders (ibid.). The French company Morpho, now known as IDEMIA, provides immigration processing solution with the biometric civil registration system in Mauritania (Frowd 2014). In 2009, Airbus had signed a €3 billion contract with Saudi Arabia to build their border security system "including Radar/Camera Technology and TETRA Communication, covering the totality of 9,000 km along the borders of Saudi Arabia" (HCC 2015, Reuters 2019).

In addition to state ownership, national governments play a complex role in the public/private in-distinction of the EU security market: national governments, particularly ministries, feature as the primary customers for most companies (ECORYS 2009, Sempere 2011). Ministries – particularly the ministry of defence and the ministry of interior, depending on the relevant ministerial authority for police and military in the respective member state – are very often the end-customer for defence and security products (ibid.). The European Commission and various other EU bodies are also an end-customer for many companies, especially for companies providing secure communications and IT solutions (eu-LISA 2017). The collaboration between government and companies pans out in different capacities: governments and government-affiliated institutes like military academies provide support to test the products developed by the companies. State shareholding and the producer/customer relationship particularly that ensues between states and major security defence companies brings fore the public/private blurring that persists in the security market.

Bureaucratic Novelties and Lobbying Organisations

The clout of major security and defence companies is furthered at an institutional level through bureaucratic institutions and lobbying organisations which are structured along the public/private blurring and operate to further the security agenda in alliance with the companies.

Bureaucratic novelties such as the European Defence Agency (EDA) and the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) are structured along the public/private intimacy and operate in close collaboration with major security and defence companies to create and foster a technologically driven security agenda that aligns with the expertise of the security and defence companies.

The European Defence Agency (EDA) is one example of such a bureaucratic novelty and was created in 2004. This EU agency is responsible for strengthening the industrial and technological base of the defence sector and participates in defining a European capabilities and armaments policy. It has taken initiatives towards promoting dual-use technologies, thus "lifting the strict separation between research for civilian and military purposes which is to help the defence industry recuperate in times of austerity and major budget cuts" (Drent et al. 2014: 9). The EDA plays a crucial role in harmonising defence in the EU and its membership comprises of former diplomats, military personnel and politicians as its members, making it comparable to US Pentagon (Barigazzi and Smith-Meyer 2016).

The EDA plays a crucial role in aligning corporate interests of major security and defence companies with the role and ambitions of the European Commission. For instance, EDA holds its annual conference which is a high profile arms lobby event in the Brussels and in 2016 almost 300 arms companies including 22 Airbus employees, and 16 employees of Thales, defence lobby associations and think tanks attended the event (Vranken 2017: 9). In addition, EDA has promoted military rooted technological competencies and military research and technology programme (ibid.: 12) in light of the defence cuts which has shaped the European Security Research Programme. Its insistence of removing the civil-military divide squarely aligns with the technological competencies of the major security and defence companies enabling the companies to leverage military technologies in civil applications at large particularly favouring the use of dual use technologies (Vranken 2017).

The second key bureaucratic novelty is the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) which was created in 2017 (eu-LISA 2015, 2017, 2019). It is based in Tallinn and is responsible for "the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU" (eu-LISA 2017: Online). eu-LISA brings the management of EURODAC, the Visa Information System (VIS) and the second-generation Schengen Information System (SIS II) and Smart Borders under its aegis (eu-LISA 2017, Bigo 2014). eu-LISA operates on the public/private nexus particularly through its management of the databases which are developed, deployed and maintained by security and defence companies and plays a crucial role in awarding projects. Like EDA, eu-LISA holds important meetings: in April 2019, eu-LISA hosted a roundtable on "seamless border crossings" (eu-Lisa 2019) and in May 2019, it awarded a €142.1 million four-year contract to implement and maintain its Entry/Exit System to a consortium of IBM Belgium, Atos Belgium and Finmeccanica (Akkerman 2019: 6). A particular case in point of the public-private nexus is the work experience of the executive director of eu-LISA, Krum Karkov: he has work experience in private sector companies like Experian Group Ltd. (specialising in data and analytics), Hewlett Packard (an American multinational IT company) and the Bulgarian National Revenue Agency and, mindful of the contentious nature of his work experience, the eu-LISA published a 'Declaration of Non-Conflict of Interest' (eu-LISA 2015).

Trade or **professional associations** such as the European Organisation for Security (EOS) and AeroSpace and Defence Industries Association of Europe (ASD) have played a very significant role in shaping the European security research aligned with the interests of major security and defence companies (EOS 2016). ASD and EOS collectively represent the interests of major security and defence companies, sub-system producers and SMEs. Briefly, the AeroSpace and Defence Industries Association of Europe (ASD) is a defence industry lobby group which includes representatives from the defence industry and most importantly public actors like government representatives, and policy makers. They have played a crucial role in shaping security research in the European Union. EOS, is an offshoot of ASD which was formed "with the realization that there is a need to enlarge the dialogue beyond industry" (Schilde 2017) which is reflected in its membership: EOS membership comprises of companies, research institutes and SMEs. With an overlap between the membership of these two associations, unsurprisingly, we see the pervasiveness of military and defence logics in constructing security through key reports and position papers and the larger security research programme in Europe. Organisations like EOS and ASD provide key representation to the security industry as well as a space for public-private collaboration (Lemberg-Pedersen 2013, Schilde 2017). EOS and ASD have several closed-door working groups and regularly organise high-level security roundtables where public and private actors interact and collaborate. EOS also sets up task forces like the EUROSUR task force, to foster interaction between the industry and the Commission.

That apart, ASD and EOS are also involved in policy work and in the drafting of white papers and position papers for the European Commission: both ASD and EOS have actively lobbied and contributed towards policies such as the Security Industrial Policy and the Defence Industrial Policy as well as law-making on a harmonised defence and security market. ASD and EOS play a complex role of simultaneously being a lobbying association, an actor and a forum for collaboration. As a lobbying association, they represent and promote the business interests of the security and defence industry through their white papers, position papers, workshops, meetings, conferences. As an actor, the EOS has participated in several ESRP research projects[17] which is an important source of funding for the association.

[17] E.g., COPRA (Comprehensive European Approach to the Protection of Civil Aviation), EURACOM (European risk assessment and contingency planning methodologies for interconnected networks), SECUR-ED (Secured urban transportation – European Demonstration), CRISYS (Critical Response in Security and Safety Emergencies), ARCHIMEDES, CAPITAL (Cybersecurity research Agenda for PrIvacy and Technology chALlanges), CYSPA (European Cyber Security Protection Alliance), SEMIRAMIS (SEcure Management of Information Across MultIple Stakeholders), STRAW (Security Technology Active Watch), CONTAIN (CONTainer security Advanced Information Networking), COuRAGE (Cybercrime and CyberterrOrism (E)Uropean Research Agenda), CORE (Consistently Optimised REsilient ecosystem), DRIVER (DRIVing Innovation in crisis management for European Resilience), EUROSKY (Single European Secure Air-Cargo Space), POP-ALERT (Emergencies, Resilience and

Lobbying consultancies, also often known as 'government relations' or 'public relations' consultancy, and law firms are crucial in representing the "business interests to the EU institutions" (Bouwen 2002: 366). Working in conjunction with bureaucratic novelties like EDA, eu-LISA, ASD and EOS, these actors actively lobby for the business interests of major security and defence companies. They specialise in establishing relations with the European Commission, advising companies on appropriate legal and regulatory interventions, thus ensuring that companies make successful funding grants by liaising with the right Directorate General (DG) or Member of European Parliament (MEP). Firms such as Welcomeurope, Hill+Knowlton/HK Strategies, and Havas Public Affairs enable companies to find the appropriate access to lobby, locate grants and funding opportunities, keep abreast of upcoming tenders and bids, push for industry-specific policies and regulations, and assist in making grant applications (Welcomeurope 2016, Hill+Knowlton/HK Strategies no date, Havas Public Affairs 2016). Welcomeurope, for example, provides assistance for a "good preparation for European projects, managing EU grants, responding for call for proposals, offer training courses on how to master funding from European Commission" (Welcomeurope 2016: Online). Law firms such as the Alber & Geiger law firm advertises itself as a "leading EU government relations law firm" (Alber & Geiger 2016).

Major security and defence companies have their in-house lobbyist or public relations consultant and in some other cases, they outsource it to third parties like the above and thus continue with external and internal lobbying. Through these lobbying consultancies, the major security and defence companies are able to access new DGs and MEPs, and navigate the European Commission in an advantageous way. These actors are crucial for their services for making successful grant applications and securing grants within the FP7 projects, which had been dominated by the major security and defence companies (Jeandeboz and Ragazzi 2010) and the Horizon 2020. Law firms are crucial for legislative lobbying and often help the companies to lobby for beneficial legislations and policy frameworks.

Notably, these bureaucratic novelties, trade associations and lobbying consultancies create and further the construction of a security threat and, particularly, of the 'migrant threat' in conjunctions with multiple actors by leveraging the technological requirements of dual use, system integration and interoperability which in turn benefits the major security and defence companies. They further the belief that the 'migrant threat' can be managed and controlled through risk analysis, intelligence and information sharing, tracking and tracing of entries and exits of people, thus echoing the promise of seamless border control which representatives of the major security and defence companies market and sell.

The construction of European security

Having obtained an overview of the reasons and methods through which major security and defence companies assert dominance, in the following section we look at how this has shaped

Training), SAFEPOST (Reuse and development of Security Knowledge assets for International Postal supply chains), SOURCE (Societal Security Network) (EOS 2016).

the European security market and migration and border control by fomenting the migration-security nexus, primarily through the European Security Research Programme (ESRP). Central to the perpetuation of the domination of companies in migration and border control is the "continued link between the migration industry and government policies" (Gammeltoft-Hansen and Sørensen 2012, 2013). This continued link allows security and defence companies to frame the regulatory framework, laws and policies on migration and border control through standard-setting, lobbying and lock-in effects by virtue of the knowledge and expertise their representatives possess. Lock-in effects refer to the accumulation of knowledge and expertise by security and defence companies due to their extensive experience in the provisioning of security services and technologies (Lemberg-Pedersen 2013). As these major companies draw personnel with such knowledge and expertise into their organisations, government agencies, other bodies as well as other companies lack such personnel (Lemberg-Pedersen 2013). As a result, it becomes necessary to contract the same company for the development, deployment, as well as maintenance and update of the technology, which as a whole is known as life cycle management.

An example illustrating the lock-in effect is the contract that has been signed for the maintenance of the biometric engine called Visa Information System (VIS). VIS is a system that allows the Schengen States to collect and exchange visa data of third-world country nationals (European Commission 2017c). Developed by the companies Accenture and Sagem Défense Sécurité, it utilises a biometric engine that enables the biometric capture of fingerprints and facial features of third-world country nationals upon arrival in the EU. In 2013, the European Commission selected a consortium of companies, including Accenture, Morpho and HP, to maintain EU Visa Information and Biometric Matching Systems for three years for a contract value of €70 million (Findbiometrics 2011). Notably, Morpho, which is also involved in the maintenance of the system, is the new name for Sagem Défense Sécurité after its merger with Safran Group. HP is the only new entrant in the list of companies hired to manage the system but has robust business links with Accenture as they have an IT outsourcing alliance known as Accenture Hewlett Packard Enterprise (Accenture 2015). Thus, the same companies or their business compatriots or subsidiaries are engaged in different stages of the development and deployment of technology: inception, development, implementation, management, monitoring and evaluation. This implies that the companies not only frame the solution, but also set the standards to measure its efficacy and effectiveness, which if not met, is framed as necessitating further technological interventions or upgrading the technology.

In addition to the persistence of lock-in effects, the influence of major security and defence companies can be traced through various reports and market research produced by ASD and EOS. In 2005, ASD led the 'Stakeholders platform for supply chain mapping, market condition analysis and technologies opportunities' (STACCATO) within the ambit of the 'Preparatory Action on the enhancement of the European industrial potential in the field of Security Research' (PASR), whereby ASD conducted a study on security issues, possible market, missions and goals. Interestingly, STACCATO was overall led by major European security and defence companies which leveraged the military-rooted notions of situational awareness, interoperability, and system integration by information gathering, interpretation, integration and dissemination leading to the sharing of intelligence (European Commission 2004a) in shaping the European Security Research. It comprised of four work packages led by major security and defence companies: Stakeholder Platform (led by EADS/Airbus), Market Condition Analysis (led by Finmeccanica), Integration of Priorities and Recommendations (led by Thales), and Analysis of Competencies of the Supply Chain (led by EU Joint Research Centre) (Hayes 2010: 149). It also produced an (unpublished) report entitled 'How to foster the European Security Market', which mapped existing security research competencies in the 27 member states and proposed "methods and solutions for the creation of a security market and a structured supply chain in Europe" (Hayes 2009: 13). The STACCATO results were crucial in the materialisation of ESRP along the technical requirements of interoperability, dual use and system integration for combating new threats which were cohered in the 2006 ESSTRT consortium (on 'European Security, Threats, Responses and Relevant Technologies') led by Thales (ESSTRT 2006). The ESSTRT, in its final report, the 'New Approaches to Counter-Terrorism', focused on threats along the internal/external in-distinction necessitating a technological approach premised on interoperability, dual-use and system integration, as it argued for greater intelligence, surveillance and border controls (ESSTRT 2006, Hayes 2009: 14).

The materialisation of the European Security Research Program was prefaced by robust interactions between the European Commission and representatives of major security and defence companies through high-level venues in the field of security research which overlapped with the membership of ASD and EOS, namely: Group of Personalities (GoP) (2003-2004), European Security Research and Advisory Board (ESRAB) (2005-2006), and European Security Research and Innovation Forum (ESRIF) (2008-2009). These played a crucial role in setting the process and priorities of the European Security Research Program (ESRP) as shown in the table below:

Table
Company representatives on EU Forums and Boards working towards initiatives, policies and research on EU security

Forum	Company Representatives				
	BAE Systems	Finmeccanica	Airbus/EADS	Safran Group	Thales Group
Group of Personalities on Security Research (2003-2004)	Chief Executive of BAE Systems (Mike Turner)	Chief Technical Officer and Senior Vice President of Product Policy (Giancarlo Grasso)	Chief Executive Officer (Rainer Hertrich)	Not represented	Chief Executive Officer (Denis Ranque)
STACCATO – ASD led study (2005)		Market Condition Analysis	Stakeholder Platform		Integration of Priorities and Recommendations
European Security Research Advisory Board (2005-2006)	Technology Policy & Strategy Consultant (Terry Knibb)	Chairman & Chief Executive Officer (Pier-Francesco Guarguaglini)	Senior Vice President & Chief Executive Officer (Markus Hellenthal)	Chief Executive Officer (Jacques Paccard)	Vice Chairman (John Howe) Senior Vice President & Managing Director (Tim Robinson)
European Security	Not represented	Chief Technical Officer and Senior	Head of Advanced	Chairman & Chief Executive Officer	Managing Director (Greverie Franck)

Research and Innovation Forum (2008-2009)		Vice President of Product Policy (Giancarlo Grasso)	Concepts (Mey Holger)	(Jean-Paul Herteman)	
Security Industrial Policy (2012)		Chairman (Pier Francesco Guarguaglini)	Chief Executive Officer (Domingo Ureña Raso)	Not represented	Chief Executive Officer (Victor Chavez)
	Chief Executive Officer of MBDA* (Antoine Bouvier)				
Defence Industrial Policy (High Level Conference) (2013)	Not represented	Chief Executive Officer of Agusta Westland (Daniele Romiti)	Chief Executive Officer (Bernhard Gerwert)	Not represented	Not represented

* MBDA Missile Systems, a developer and manufacturer of missile systems, is owned between BAE Systems, Finmeccanica and EADS

The above table is based on the public reports of the various fora in which the company representatives participated and through their participation in these fora. Major security and defence companies have been the driving force behind the formulation of ESRP, the Security Industrial Policy (2012), and the Defence Industrial Policy (2013). According to Bigo and Jeandesboz (2010), the 'public-private dialogue' has preceded the inception and shaping of the ESRP (also see Hayes 2006, 2009). The formulation of the Security Industrial Policy was preceded by European Commissions' acknowledgement of ESRIF's recommendations on European Security Research and Innovation Agenda and the need for an industrial policy initiative for the security industry (European Commission 2010) which was supported by high-level targeted consultations organised by the European Organisation for Security (EOS); the High Level Public-Private Security Roundtable held in February 2011 and 2012 (EOS 2016); the High Level Conference on Defence and Security Industries and Markets in 2011[18] (European Commission 2011a), furthering Defence-related Directives (2009/43/EC on transfers[19] and 2009/81/EC on procurement[20]).

Similarly, the formulation of the Defence Industrial Policy was preceded and followed by similar meetings and conferences like the High Level Conference on the Future of the European defence sector, Setting the Agenda for the European Defence Industry which had speakers from

[18] The High Level Conference on Defence and Security Industries and Markets in 2011 was attended by representatives of Finmeccanica, MBDA, Thales, Airbus and ASD (European Commission 2011a).

[19] European Commission (2009) 'Directive 2009/43/EC Of The European Parliament And Of The Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community', L146/1, Brussels.

[20] European Commission (2009) 'Directive 2009/81/EC Of The European Parliament And Of The Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC', L 216/76, Brussels.

AgustaWestland (a Finmeccanica company), Airbus Military and Saab,[21] Halan Buskhe (European Commission 2014a). Thus, major security and defence companies have a significant latitude in their involvement in shaping the EU security market at large due to their access to human technological resources, formal and informal connection with government personnel, staff members of the European Commission and various other agencies. This also explains why the major defence companies Thales and Selex (a subsidiary of Finmeccanica and Sagem) were the major beneficiaries of the funding for the FP7 projects. For the total allotted sum of €443.2 million for 91 FP7 projects, Thales Group participated in projects with the total worth of €253.8 million, more than half of the total allotted budget (Jeandesboz and Ragazzi 2010: 25, Bigo and Jeandesboz 2010: 4).

EOS has participated in several ESRP research projects[22] which constitutes an important source of funding for the association. With their representatives on key boards and high-level meetings and conferences, they have set research priorities of the ESRP and helped institute the Security Industrial Policy and Defence Industrial Policy on the recommendations of the Boards like ESRIF which were initiated to strengthen the 'Public-Private Dialogue in Security Research' (European Commission 2007). These measures prioritise the competencies of major security and defence companies whereby they are in an advantageous position to capitalise on their experience, connections and resources. Organisations like EOS and ASD give a strong strategic voice to the industry and open a space for public-private collaboration.

research institutes where their influence is visible through funding of courses, research and faculty positions, and broadly shaping research and pedagogy along corporate lines. Companies collaborate with universities and research institutes or research and technology organisations (RTOs) where they play a significant role in deciding course content, setting up new course modules and research. The relations between universities and major security and defence companies is crucial in knowledge production, training, and shaping early stages of research that cater to company needs. For instance, BAE Systems collaborated with Loughborough

[21] SAAB is a Swedish multinational aerospace and defence company specializing in aeronautics, combat weapons, surveillance, training and simulations, logistics and maintenance and submarines. See more at http://saabgroup.com/, accessed on 23.11.2016.

[22] E.g., COPRA (Comprehensive European Approach to the Protection of Civil Aviation), EURACOM (European risk assessment and contingency planning methodologies for interconnected networks), SECUR-ED (Secured urban transportation – European Demonstration), CRISYS (Critical Response in Security and Safety Emergencies), ARCHIMEDES, CAPITAL (Cybersecurity research Agenda for PrIvacy and Technology chALlanges), CYSPA (European Cyber Security Protection Alliance), SEMIRAMIS (SEcure Management of Information Across MultIple Stakeholders), STRAW (Security Technology Active Watch), CONTAIN (CONTainer security Advanced Information Networking), COuRAGE (Cybercrime and CyberterrOrism (E)Uropean Research Agenda), CORE (Consistently Op-timised REsilient ecosystem), DRIVER (DRIVing Innovation in crisis management for European Resil-ience), EUROSKY (Single European Secure Air-Cargo Space), POP-ALERT (Emergencies, Resilience and Training), SAFEPOST (Reuse and development of Security Knowledge assets for International Postal supply chains), SOURCE (Societal Security Network) (EOS 2016).

University which resulted in a substantial redevelopment of modules which was funded by BAE Systems, and over 200 Loughborough students consequentially started careers at BAE Systems after completing their courses (BAE Systems 2013, Crawford 2008). As a part of this collaboration, under BAE Systems-sponsored studies at Loughborough University, PhD student Andy Jones designed a system to cool the electronic systems within an aircraft most effectively (BAE Systems 2013).

Airbus/EADS, through its EADS Foundation, collaborates with Cardiff University and the Welsh government to support SMEs and other universities in the region (Cardiff University 2011). In 2016, a new position was created in Sheffield titled ‘Airbus Chair in Advanced Manufacturing’ in the Department of Automatic Control and Systems Engineering (ACSE). In the position description “[t]he Airbus Chair, […] is aimed at establishing a unique, world-leading research collaboration” between, Airbus UK and University of Sheffield and “the focal point of this collaboration will be the 43 million pounds state-of-the-art ‘Factory 2050’, which is hailed as UK’s first fully reconfigurable assembly and component manufacturing research facility” (University of Sheffield 2016: 1).

By participating in crucial boards and outlining the security agenda, representatives of major security and defence companies ensure that such technological requirements are integrated as a part of larger EU policy and regulatory framework along the migration-security nexus. Moreover, these requirements are furthered and integrated in calls for proposal and tenders, such that major security and defence companies are best placed to provide them by developing these systems on a large scale, leveraging their decades of experience and vision to set the security agenda which is based on their capacities to provide complete systems which simultaneously strengthen their strategic positions and further their interests. By routinely mobilizing “imaginations” (De Goede et al. 2014) of fear, a migrant suicide-bomber, or an infected migrant boat, private companies capitalise on the framing of the ‘migrant threat’ fusing it with issues of unemployment, US competition, the end of Cold War, a declining European defence industry and EU’s ambition to be a global player, and technology being perceived as an imperative to achieving security. Questions about how viable it is to have submarines and drones doing maritime surveillance in terms of costs of deployment and death at seas are not raised but framed in terms of better management of the ‘migrant threat’ through risk analysis, intelligence and information sharing, tracking and tracing of entries and exits of people to reduce costs or to avoid deaths on the seas.

Constructing the ‘Migrant Threat’ and Security in the EU

With financial and political stakes circumscribing the development and deployment of border technologies in the EU, major security and defence companies like Airbus/EADS, BAE Systems, Finmeccanica, or Thales work in close collaboration with EU institutions, research institutes, universities, lobbying consultancies, law firms and military academies. The ‘migrant threat’ is often described and alluded to in cryptic, technological terms: the migrant is described and de-politicised into a detectable heartbeat, a traceable movement or body fluids, a “manageable through quantification and risk analysis” (Darling 2014: 81), and through surveillance and tracking which strengthens the space for technological solutions and ‘managerial skills’ (Bigo 2006, Darling 2014, Geiger & Pécoud 2010, Statewatch 2014). Utilising this language, several of the European Security Research Projects within the Seventh

Framework Program (FP7) target to control the migrant through thermal cameras which are used by border guards; through heartbeat and smell detectors known as 'artificial olfactory sensors', 'artificial noses' or CO_2 (carbon dioxide) probes; through advanced optronics which are integrated in the FP7 project AMASS; through advanced body detection dogs which can smell the presence of hidden humans, such as the project Sniffer; through motion detectors and advanced satellite imagery; through drones and intelligent fences.

All these methods frame the migrant as a de-politicised and technologically manageable threat displacing all questions of migrant rights as well as accountability of private actors. A crucial implication of framing the migrant as a technologically manageable threat is that it neutralises and naturalises the deployment of border technologies: any instance of technological failure or inefficiency which manifests in the death of migrants or their entry into the EU reinforces the need for smartening and upgrading the available technologies. The unfettered proliferation of border technologies postured within the logics of smartness, neutrality and effectiveness has a corrosive impact on the protection of refugees and migrants by pushing them to undertake dangerous routes towards seeking asylum and protection (Andersson 2014, 2016, Lutterbeck 2006).

With border technologies deployed to create a technological labyrinthine to smarten the borders, detect migrants and intercept them before they reach the European shores, the refugee protection regime is derogated by creating a 'neo-refoulement regime' (Hyndman and Mountz 2008) which refers to a geo-political strategy of preventing the possibility of asylum through a new form of forced return different from non-refoulement as enshrined in *Article 33* of the Refugee Convention (UN General Assembly 1951). With border technologies, 'neo-refoulement' is effectuated tracing, tracking and intercepting the migrant before they reach the European territory where they could make a claim (Hyndman and Mountz 2008: 250; Levy 2010: 95). Dietrich (2005) and Genova and Peutz (2010) maintain that the usage of border technologies in conjunction with a range of other policies and non-entrée measures creates the preconditions for a new deportation regime where the state power's more despotic proclivities are exercised without inhibition while largely shielded from robust critical scrutiny.

Obfuscating the questions of protections of migrants and refugees, we in fact see a burgeoning security market developing along in-distinctions and blurrings of dualisms such as public/private internal/external, inside/outside, civil/military, security/defence, and old/new technologies. This almost "chameleon-like" (Avant et al. 2010: 361) recasting and re-articulation of the public/private distinction challenges the construction of the 'public' as the domain of political and public authority, and of the 'private' as the domain of profit-making and the economy, and hence, as an apolitical or non-political domain (Leander 2009, Abrahamsen and Williams 2008). These blurrings align with profit motives of companies, competition with US companies, and seek the resurrection of a declining defence industry and EU's ambitions to emerge as a robust, global and international player. In the process, questions of accountability, responsibility and transparency are circumvented, undermined and corroded and it is increasingly difficult to place the locus of legal and political responsibility. There is no constant, objective basis for labelling an activity or an actor as 'private' or 'public' and the collaborations instead serve as mechanisms to obscure political accountability and responsibility (Chinkin 1999, Kennedy 1982).

Built on the tenets of interoperability, integration, seamlessness, efficiency, and neutrality, we witness the emergence of a selective-mobility regime which, on the one hand, smoothly facilitates trade and tourism but simultaneously sorts and filters the illegal and illegitimate and severely shrinks the protection space on the other. This selective-mobility regime stands in contradiction to the protection space afforded by the Refugee Convention read along with other relevant treaties and conventions as it frames a refugee along the migration-security nexus who must be controlled, managed, categorised and sorted as “desirable” or “undesirable” (Bigo and Guild 2005: 234) making migration control a viable and profitable enterprise.

REFERENCES

Abrahamsen, R. and Williams, M.C. (2008) “Public/private, global/local: the changing contours of Africa’s security governance”, *Review of African Political Economy*, 118, pp. 539-553.

Accenture (2015) “Accenture Launches New Innovation Center for HP Technology”, in https://newsroom.accenture.com/industries/systems-integration-technology/accenture-launches-new-innovation-center-for-hp-technology.htm, accessed on 13.9.2016.

ACS Group (2005) “Annual Report”, in http://www.grupoacs.com/ficheros_editor/File/03_accionistas_inversores/03_informe_anual/grupo_acs_2005_annual_report.pdf, accessed on 13.6.2016.

Airbus Defense and Space (2011) “PlantCML® changes name to Cassidian Communications, Inc., an EADS North America Company”, *Critical Matters*, in http://airbus-dscomm.com/news-events/press-releases.php?id=1&PlantCML%26reg+changes+name+to+Cassidian+Communications%2C+Inc.%2C+an+EADS+North+America+Company, accessed on 30.1.2017.

Akkerman M. (2018) “Militarization of European Border Security”, in N. Karampekios, I. Oikonomou, E. Carayannis (eds.) *The Emergence of EU Defense Research Policy. Innovation, Technology, and Knowledge Management,* Innovation, Technology, and Knowledge Management Book Series, Springer, Cham, pp. 337-355.

Akkerman, M. (2019, November) “The business of building walls”, in https://www.tni.org/files/publication-downloads/business_of_building_walls_-_full_report.pdf, accessed on 30.03.2020.

Alber & Geiger (2016) “European Lobbying – Diplomacy – Litigation”, in https://albergeiger.com/, accessed on 27.05.2016.

AMASS (2011) “Autonomous maritime surveillance system”, in http://www.amass-project.eu/amassproject/content/index, accessed on 15.10.2012.

Amicelle, A., Bigo, D., Jeandesboz, J., Ragazzi, F. (2009) “Catalogue of Security and Border Technologies at use in Europe Today”, *INEX Deliverable D.1.2.*, Centre d’études sur les Conflits.

Amoore, L. (2009) “Algorithmic war: Everyday geographies of the War on Terror”, *Antipode*, 41(1), pp. 49-69.

Andersson, R. (2014) *Illegality, Inc.: Clandestine Migration and the Business of Bordering Europe*, University of California Press, Oakland.

Andersson, R. (2016) “Hardwiring the frontier? The politics of security technology in Europe’s ‘fight against illegal migration”, *Security Dialogue*, 47(1), pp. 122-139.

Andritsos, F. (2013) “Port Security & Access Control: a Systemic Approach”, *IISA 2013*, Piraeus, pp. 1-8.

ANSA News (2016) “Frontex Triton operation to ‘support’ Italy’s Mare Nostrum”, in http://www.ansa.it/english/news/2014/10/16/frontex-triton-operation-to-support-italys-mare-nostrum_ad334b2e-70ca-44ce-b037-4d461ec0d560.html, accessed on 13.9.2016.

Arisem (2011), “Actionnaires”, in http://www.arisem.com/?q=fr/actionnaires, accessed on 25.3.2014.

Articlesbase (2012) “Obzerv Technologies Helps Government to Integrate Long Range Night Vision Camera Solutions”, in http://www.articlesbase.com/electronics-articles/obzerv-technologies-helps-government-to-integrate-long-range-night-vision-camera-solutions-5804845.html, accessed on 12.10.2012.

Avant, D., Finnemore, M. and Sell, S. (2010) (eds.), *Who governs the globe?*, Cambridge Studies in International Relations, Cambridge University Press, Cambridge.

Avascent (2013) “State Ownership In The European Defense Industry: Change Or Continuity”, European defense industrial base forumoccasional paper, in https://www.avascent.com/wp-content/uploads/2013/01/Avascent-State-Ownership.pdf, accessed on 29.03.2020.

Aviation Week (2014) “Airbus Group to Focus on Military Aircraft, Space and Missiles” in http://aviationweek.com/defense/airbus-group-focus-military-aircraft-space-and-missiles, accessed on 7.6.2016.

BAE Systems (2011) “BAE Systems announces recommended offer to acquire Norkom”, in http://www.baesystems.com/article/BAES_026877/bae-systems-announces-recommended-offer-to-acquire-norkom?_afrLoop=115066744619000&_afrWindowMode=0&_afrWindowId=null#%40%3F_afrWindowId%3Dnull%26_afrLoop%3D115066744619000%26_afrWindowMode%3D0%26_adf.ctrl-st, accessed on 26.3.2014.

BAE Systems (2012) “BAE Systems Overview – Opportunities 2012”, in http://www.sbtdc.org/events/opportunities/2012/ppt/bae-systems-overview.pdf, accessed on 26.3.2014.

BAE Systems (2013) “Research into Military Jet Aircraft”, in http://www.baesystems.com/article/BAES_162648/research-into-military-jet-aircraft?_afrLoop=101072636033000&_afrWindowMode=0&_afrWindowId=null#%40%3F_afrWindowId%3Dnull%26_afrLoop%3D101072636033000%26_afrWindowMode%3D0%26_adf.ctrl-state%3D1anadg7jt0_4, accessed on 26.3.2014.

Baldaccini, A. and Guild, E. (2007) (eds.) *Terrorism and the Foreigner: A Decade of Tension around the Rule of Law in Europe*. Martinus Nijhoff, Leiden.

Barigazzi. J. and Smith-Meyer, B. (2016) “A European Pentagon”, in http://www.politico.eu/article/the-eus-not-quite-pentagon-european-defense-agency-jorge-domecq-eu-military-cooperation/, accessed on 26.1.2017.

BBC (2002) “Spain unveils coastal spy system”, in http://news.bbc.co.uk/2/hi/europe/2194043.stm, accessed on 12.10.2012.

Besters, M. and Brom, F. (2010) “Greedy’ Information Technology: The Digitalization of the European Migration Policy”, *European Journal of Migration and Law*, 12(4), pp. 455-470.

Bigo, D. (2004) “Criminalisation of ‘Migrants’: The Side Effects of the Will to Control the Frontiers and the Sovereign Illusion”, in B. Bogusz, R. Cholewinski, A. Cygan and E. Szyszczak (eds.), *Irregular Migration and Human Rights: Theoretical, European and International Perspectives*, Martinus Nijhoff Publishers, Leiden, pp. 61-92.

Bigo, D. (2005) “Frontier controls in the European Union: Who is in Control?”, in D. Bigo and E. Guild (eds.), *Controlling Frontiers: Free Movement into and within Europe*, Ashgate, London, pp. 49-99.

Bigo, D. (2006) “Internal and external aspects of security”, *European Security*, 15(4), pp. 385-404.

Bigo, D. (2008) “International Political Sociology”, in Williams, P.D., *Security Studies – An Introduction*, Routledge, Oxon and New York, pp. 116-129.

Bigo, D. (2013) “Border, Mobility and Security”, in Kauppi, N. (ed.), *A Political Sociology of Transnational Europe*, ECPR studies, Rowman & Littlefield International, London, pp. 111-127.

Bigo, D. (2014) “The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts”, *Security Dialogue*, 45(3), pp. 209-225.

Bigo, D. and Guild, E. (2005) *Controlling Frontiers: Free Movement into and within Europe*. Ashgate, London.

Bigo, D. and Guild, E. (2010) “The Transformation of European Border Controls”, in B. Ryan and V. Mitsilegas (eds.), *Extraterritorial Immigration Control. Legal Challenges*, Martinus Nijhoff Publishers, Leiden, pp. 252-273.

Bigo, D., Bonditti, P., Jeandesboz, J. and Ragazzi, F. (2008) “Security technologies and society: A state of the art on security, technology, borders and mobility”, in *Converging and Conflicting Ethical Values in the International Security Continuum in Europe* (INEX), INEX D.1.1., INEX Partner 3 C&C, Work package 1, 7th Framework Program, European Commission.

Bigo, D. and Jeandesboz, J. (2010) “The EU and the European Security Industry – Questioning the ‘Public-Private Dialogue’”, INEX Policy Brief, in http://aei.pitt.edu/14989/1/INEX_PB5_e-version.pdf, accessed on 25.2.2013.

Bonditti, P. (2005) “Biométrie et maîtrise des flux: vers une ‘geo-technopolis du vivant-en-mobilité’?”, *Cultures & Conflicts*, 58, pp. 131-154.

Boston Business Journal (2010, 7 September) “BAE buying Oasys Technology for up to $55M”, by Rodney H. Brown, in http://www.bizjournals.com/boston/blog/mass-high-tech/2010/09/bae-buying-oasys-technology-for-up-to-55m.html, accessed on 27.3.2014.

Boswell, C. (2007) “Migration control in Europe after 9/11: Explaining the absence of securitization”, *Journal of Common Market Studies*, 45(3), pp. 589-610.

Bouwen, P. (2002) “Corporate lobbying in the European Union: the logic of access”, *Journal of European Public Policy*, 9(3), pp. 365-390.

Broeders, D. (2007) “The new digital borders of Europe: EU databases and the surveillance of irregular migrants”, *International Sociology*, 22(1), pp. 71-92.

Broeders, D. and Engbersen, G. (2007) “The Fight Against Illegal Migration Identification Policies and Immigrants’ Counterstrategies”, *American Behavioral Scientist*, 50(12), pp. 1592-1609.

Broeders, D. and Hampshire, J. (2010), “The Digitalization of European Borders and Migration Controls – Migration to Europe in the Digital Age (MEDiA)”, in http://www.mediaresearchproject.eu/reports/Report2_Borders.pdf, accessed on 3.11.2010.

Broeders, D. and Hampshire, J. (2013) “Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe”, *Journal of Ethnic and Migration Studies*, 39(8), pp. 1201-1218.

Bronk, R. (1998) *Progress and the Invisible Hand – The Philosophy and Economics of Human Advance*. Little Brown and Company, London.

Brouwer, Evelien (2005), “Data surveillance and border control in the EU: Balancing efficiency and legal protection of third country nationals”, *Working Paper 14*, in http://www.libertysecurity.org/article289.html, accessed on 20.10.2011.

Brouwer, E. (2008) *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*. Brill, The Netherlands.

Business Insider (2016) “Homeland Security Companies Made A Fortune After 9/11”, in http://www.businessinsider.com/homeland-security-companies-made-a-fortune-after-911-2011-9?IR=T, accessed on 13 June 2016.

Business Wire (2010, 13 July) “BAE Systems Completes Acquisition of Atlantic Marine”, Airlington, in http://www.businesswire.com/news/home/20100713006861/en/BAE-Systems-Completes-Acquisition-Atlantic-Marine#.UzNUk_ldXF0, accessed on 26 March 2014.

Cardiff University (2011) “Cardiff joins EADS and Welsh Government to drive technological innovation”, in http://www.cardiff.ac.uk/news/articles/cardiff-joins-eads-and-welsh-government-to-drive-technological-innovation-6906.html, accessed on 06.05.2014.

Carling, J. (2007) "The Merits and Limitations of Spain's High-Tech Border Control", Migration Policy Institute, in http://www.migrationinformation.org/Feature/display.cfm?ID=605, accessed on 12.10.2012.

Carrera, S. and Geyer, F. (2007) "Terrorism, Borders and Migration: The Commission's 2008 Policy Strategy in the Area of Freedom, Security and Justice", *CEPS Policy Brief*, 131(1), Policy Paper.

Carrera, S., Guild, E., and Bigo, D. (2008) "What Future for the Area of Freedom, Security and Justice? Recommendations on EU Migration and Borders Policies in a Globalising World", *CEPS Policy Brief*, 156, Brussels.

Chinkin, C. (1999) "A critique of the Public/Private Dimension", *European Journal of International Law*, 10(2), pp. 387-395.

CockpitCI (2019) "A European FP7 Project – CockpitCI – THE GRID MUST GO ON", in https://cockpitci.itrust.lu/home/index.htm, accessed on 28.03.2020.

Cooper, H. (2017) "Insecurity is cash cow for Europe's defense firms", in http://www.politico.eu/article/nato-russia-tensions-mean-big-business-for-eu-defense/, accessed on 06.01.2017.

Corporate Watch (2002) "BAE Systems - A Corporate Profile", in http://www.corporatewatch.org/?lid=182, accessed on 26.03.2014.

Crawford, A. (2008) "Experience Led Engineering – Industry Sponsorship of Degree Programs", Loughborough University, in https://www.raeng.org.uk/education/vps/principles/workshop_sept_2008/Dr_Adam_Crawford.pdf, accessed on 26.03.2014.

Darling, J. (2014) "Asylum and the Post-Political: Domopolitics, Depoliticisation and Acts of Citizenship", *Antipode*, 46(1), pp. 72-91.

DCNS (2017) "Governance", in http://en.dcnsgroup.com/group/en-profil/en-gouvernance/, accessed 7.6.2016.

De Goede, M., Simon, S. and Hoijtink, M. (2014) "Performing preemption", *Security Dialogue*, 45(5), pp. 411-422.

De Haas, H. (2008) "The myth of invasion: the inconvenient realities of African migration to Europe", *Third World Quarterly*, 29(7), pp. 1305-1322.

Dietrich, H. (2005), "The desert front: Supported by Libya, the EU starts setting up deportation and refugee camps in North Africa", in http://www.noborder.org/nolager/more/display.php?id=4, accessed 13.02.2011.

Dijstelbloem, H. (2009) "Europe's new technological gatekeepers. Debating the deployment of technology in migration policy", *Amsterdam Law Forum*, 1(4), pp. 11-18.

Dijstelbloem, H., Meijer, A. and Besters, M. (2011) "The Migration Machine", in H. Dijstelbloem and A. Meijer (eds.), *Migration and the new technological borders of Europe*, Migration, Minorities and Citizenship Series, Palgrave Macmillan UK, London, pp. 1-21.

Drent, M., Landman, L., and Zandee, D. (2014) "The EU as a Security Provider", Clingendael report, Netherlands Institute of International Relations, at http://www.clingendael.nl/sites/default/files/Report_EU_as_a_Security_Provider_december_2014.pdf, accessed on 27.5.2016.

ECORYS SCS Group (2009), "Study on the Competitiveness of the EU Security Industry", Within the Framework Contract for Sectoral Competitiveness Studies - ENTR/06/054, Enterprise and Industry, Brussels, in http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=5579, accessed on 12.3.2013.

EOS (2016) "EOS: The European Voice of Security – The European high-level security roundtable", in http://www.eos-eu.com/Middle.aspx?page=voice, accessed on 13.6.2016.

ESSTRT Consortium (2006) "European Security: High Level Study on Threats, Responses and Relevant Technologies, study financed by the European Commission under the Preparatory Action for Security Research (PASR)", in http://www.statewatch.org/Targeted-issues/ESRP/documents/pasr_en.pdf, accessed on 16.12.2016.

eu-LISA (2015) "Annual Public Statement Of Commitment", in http://www.eulisa.europa.eu/Organisation/Documents/Declaration%20of%20non-Conflict%20of%20Interest%20-%20ED.pdf, accessed on 02.02.2017.

eu-LISA (2017), "About us", in http://www.eulisa.europa.eu/AboutUs/Pages/default.aspx, accessed on 26.01.2017.

eu-LISA (2019) "eu-LISA Industry Roundtable Focuses on Seamless Border Crossings", in https://www.eulisa.europa.eu/Newsroom/PressRelease/Pages/eu-LISA-Industry-Roundtable-Focuses-on-Seamless-Border-Crossings.aspx, accessed on 30.03.2020.

Eurofighter (no date) "About us – Ownership of Eurofighter Consortium", in https://www.eurofighter.com/about-us, accessed 25.3.2014.

European Commission (2003) "Case No COMP/M.3217 - CARLYLE /FINMECCANICA / AVIO", SG (2003) D/231328, in http://ec.europa.eu/competition/mergers/cases/decisions/m3217_en.pdf, accessed on 27.01.2017.

European Commission (2004a) "Communication on the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, towards a programme to advance European security through Research and Technology", COM(2004) 72 final, Brussels, Belgium.

European Commission (2004b) "Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research", European Communities, Luxembourg, in https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/gop_en.pdf, accessed 27.05.2015.

European Commission (2005) “Improving efficiency and interoperability of large-scale data bases in the field of Justice, Freedom and Security - A short glossary”, MEMO/05/440, Brussels, Belgium.

European Commission (2007) “The European Security Research and Innovation Forum (ESRIF) - Public-Private Dialogue in Security Research”, MEMO/07/346, Brussels, Belgium.

European Commission (2010) “An Integrated Industrial Policy for the Globalisation Era - Putting Competitiveness and Sustainability at Centre Stage”, COM(2010) 614, Brussels, Belgium.

European Commission (2011a) “High Level Conference Defence and Security Industries and Markets”, in http://ec.europa.eu/internal_market/publicprocurement/docs/defence/conference20110523/programme_en.pdf, accessed on 9.6.2016.

European Commission (2011b) “Investing into Security Research for the Benefits of European Citizen”, Enterprise and Industry, Security research Projects under the 7th Framework Programme for Research, in ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/securityresearch_catalogue2010_2_en.pdf, accessed on 15.10.2012.

European Commission (2012) “Security Industrial Policy – Action Plan for an innovative and competitive Security Industry”, COM(2012) 417 final, Brussels, Belgium.

European Commission (2014a) “High Level Conference on the Future of the European defence sector: Setting the Agenda for the European Defence Industry”, in http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=7206, accessed on 13.06.2016.

European Commission (2014b) “How does Frontex Joint Operation Triton support search and rescue operations?”, in http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/background-information/docs/frontex_triton_factsheet_en.pdf, accessed 13.09.2016.

European Commission (2016) “European integrated border management”, in https://ec.europa.eu/home-affairs/content/european-integrated-border-management_en, accessed on 28.03.2020.

European Commission (2017a) “SAWSOC - Situation AWare Security Operations Center”, Record number: 110931, in https://cordis.europa.eu/project/id/313034, accessed on 29.03.2020.

European Commission (2017b) “SEC-20-BES-2016 - Border Security: autonomous systems and control systems”, in https://cordis.europa.eu/programme/id/H2020_SEC-20-BES-2016, accessed on 27.03.2020.

European Commission (2017c) “Visa Information System”, in http://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en, accessed on 31.01.2017.

European Commission (2018) “EU budget: Commission proposes major funding increase for stronger borders and migration”, in https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4106, accessed on 25.03.2020.

European Commission (2019) “Protection of European seas and borders through the intelligent use of surveillance”, Record number: 97515, in https://cordis.europa.eu/project/id/261748, accessed on 28.03.2020.

European Security Research Advisory Board - ESRAB (2006) “Meeting the challenge: the European Security Research Agenda - A report from the European Security Research Advisory Board”, Office for Official Publications of the European Communities, Luxembourg.

Eurosam (2013) “Eurosam”, in http://www.eurosam.com/, accessed on 22.04.2014.

Faist, T. (2002), “Extension du domaine de la lutte’: International Migration and Security before and after September 11, 2001”, *International Migration Review*, 36, pp. 7-14.

Faist, T. (2005) “The migration-security nexus: International migration and security before and after 9/11”, COMCAD Arbeitspapiere – working papers, 9, COMCAD - Center on Migration, Citizenship and Development, Bielefeld.

Feller, E. (2006), “Asylum, Migration and Refugee Protection: Realities, Myths and the Promise of Things to Come”, *International Journal of Refugee Law*, 18(3-4), p. 509-536.

Findbiometrics (2011) “European Commission Selects Consortium Of Accenture, Morpho And HP To Maintain EU Visa Information And Biometric Matching Systems”, in http://findbiometrics.com/european-commission-selects-consortium-of-accenture-morpho-and-hp-to-maintain-eu-visa-information-and-biometric-matching-systems/, accessed on 06.05.2014.

Frontex (2016) “Roles and Responsibilities”, in http://frontex.europa.eu/operations/roles-and-responsibilities/, accessed on 14.04.2016.

Frontex (2019) “Frontex Operations”, in https://frontex.europa.eu/faq/frontex-operations/, accessed on 28.03.2020.

Frowd, P. (2014) “The field of border control in Mauritania”, *Security Dialogue*, 45(3), pp. 226-241.

Gammeltoft-Hansen, T. and Sørensen, N. (2012) “The Migration Industry and Future Directions for Migration”, *DIIS Policy Brief*, in https://www.ciaonet.org/attachments/20347/uploads, accessed on 18.05.2016.

Gammeltoft-Hansen, T. and Sørensen, N. (2013) (eds.) *The Migration Industry and the Commercialization of International Migration*. Routledge, London and New York.

Geddes, A. (2008), *Immigration and European Integration: Beyond Fortress Europe*. Manchester University Press, Manchester.

Geiger, M. and Pécoud, A. (2010) (eds.), *The politics of international migration management*, Migration, Minorities and Citizenship Book Series, Palgrave Macmillan UK, London.

Genova, N. and Peutz, N. (eds.) (2010), *The Deportation Regime: Sovereignty, Space, and the Freedom of Movement*, Durham: Duke University Press.

Gloannec, A., Irondelle, B. and Cadier, D. (2013) “New and Evolving Trends in International Security”, Working Paper 13, Transworld, in http://www.transworld-fp7.eu/wp-content/uploads/2013/04/TW_WP_13.pdf, accessed on 22.04.2014.

Army Recognition (2018) “SAMP-T air defense system to be manufactured by Turkey and Eurosam”, in https://www.armyrecognition.com/june_2018_global_defense_security_army_news_industry/samp-t_air_defense_system_to_be_manufactured_by_turkey_and_eurosam.html, accessed on 30.03.2020.

Global Research (2011) “9/11: Who Really Benefited? - Fact and Not Fiction.”, in http://www.globalresearch.ca/9-11-who-really-benefited/25762, accessed on 20.5.2016.

Globalsecurity.org (2020) “The Command and Control System”, Chapter 5, in https://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap5.htm, accessed on 27.03.2020.

Gonzalez-Fuster, G. and Gutwirth, S. (2011) “When ‘digital borders’ meet ‘surveilled geographical borders’. Why the future of EU border management is a problem”, in http://works.bepress.com/serge_gutwirth/56/, accessed on 15.01.2016.

GPS World (2017) “Galileo declares: Open for business!”, in http://gpsworld.com/galileo-declares-open-for-business/, accessed on 27.01.2017.

Guild, E. (2002), “The Border Abroad – Visas and Border Controls “, in K. Groenendijk et al. (eds.), *In Search of Europe’s Borders*, Kluwer Law International, Den Haag, pp. 86-104.

Guild, E. (2005) “The Legal Framework: Who is Entitled to Move?”, in D. Bigo and E. Guild (eds.), *Controlling Frontiers: Free Movement Into and Within Europe*, Ashgate, Hants, pp. 14-48.

Guild, E. (2006) "The Europeanisation of Europe's Asylum Policy", *International Journal of Refugee Law*, 18(3-4), pp. 630-651.

Guild, E. (2009) *Security and Migration in the 21st Century*. Polity, Cambridge.

Guild, E. and Carrera, S. (2013) "EU Borders and Their Controls: Preventing unwanted movement of people in Europe?", CEPS Essay No. 6/ 14, CEPS, Brussels.

Guiraudon, V. and Lahav, G. (2000) "A Reappraisal of the State Sovereignty Debate", *Comparative Political Studies*, 33(2), pp. 163-195.

Guittet, E. and Jeandesboz, J. (2010) "Security Technologies", in J.P. Burgess (ed.) *The Routledge Handbook of New Security Studies*, Routledge, London, pp. 229-239.

Hartung, W. (2012) "The Military – Industrial Complex Revisited: Shifting Patterns of Military Contracting in the Post-9/11 Period", in http://watson.brown.edu/costsofwar/files/cow/imce/papers/2011/The%20Military-Industrial%20Complex%20Revisited.pdf, accessed on 11.06.2016.

Havas Public Affairs (2016) "Havas Public Affairs Brussels", in http://havaspr.com/?page_id=262, accessed on 26.01.2017.

Hayes, B. (2006) "Arming Big Brother: The EUs Security Research Programme", TNI Briefing Series, (06/1), The Netherlands.

Hayes, B. (2009) *Neoconopticon: The EU security – industrial complex*. Transnational Institute and Statewatch, in https://www.statewatch.org/analyses/neoconopticon-report.pdf, accessed 14.02.2013.

Hayes, B. (2010) "'Full spectrum dominance' as European Union security policy. On the trail of the 'NeoConOpticon'", in K.D. Haggerty and M. Samatas (eds.), *Surveillance and Democracy*, Routledge, London, pp. 148-169.

HCC (2015) "Border Security Services", in https://www.htcc.com.sa/border.html, accessed on 30.03.2020.

Hill+Knowlton Strategies (no date) "Our Expertise" in, http://www.hkstrategies.com/, accessed on 26.01.2017.

Hoijtink, M. (2014) "Capitalizing on emergence: The 'new' civil security market in Europe", *Security Dialogue*, 45(5), pp. 458-475.

House of Lords (2005) After Madrid: the EU's response to terrorism – Report with Evidence", 5th Report of Session 2004-05, HL Paper 53, in https://www.publications.parliament.uk/pa/ld200405/ldselect/ldeucom/53/53.pdf, accessed on 24.03.2014.

Huysmans, J. (2000) "The European Union and the securitization of migration", *Journal of Common Market Studies*, 38(5), pp. 751-777.

Hyndman, J. and Mountz, A. (2008) “Another Brick in the Wall? Neo-Refoulement and the Externalization of Asylum by Australia and Europe”, *Government and Opposition*, 43(2), pp. 249-269.

Indra (2010) “Indra to Deploy Surveillance System for Spanish Coast”, in http://www.defencetalk.com/indra-to-deploy-surveillance-system-for-spanish-coast-24161/, accessed on 12.10.2012.

Indra (2011) “Indra to Implement The External Surveillance Integrated System (Sive) on Tarragona’s Coast for € 2.9 M”, in http://www.indracompany.com/en/noticia/indra-to-implement-the-external-surveillance-integrated-system-sive-on-tarragona-s-coast-for, accessed on 12.10.2012.

Industry Week (2014) “Airbus to Sell off Units in Plan to Refocus Business Strategy”, in http://www.industryweek.com/companies-executives/airbus-sell-units-plan-refocus-business-strategy, accessed on 07.06.2016.

IT News (2012) “Stratsec rebrands as BAE Detica”, by Darren Pauli, in http://www.itnews.com.au/News/325779,stratsec-rebrands-as-bae-detica.aspx, accessed on 26.03.2014.

Jeandesboz, J. and Ragazzi, F. (2010) “Review of security measures in the Research Framework Programme - Study”, Reference No.PE 432.740, Directorate General for Internal Policies Policy Department Citizens’ Rights and Constitutional affairs Civil liberties, Justice and Home Affairs, European Parliament, Brussels, Belgium.

Jones, R. and Johnson, C. (2016) “Border militarisation and the re-articulation of sovereignty”, *Transactions of the Institute of British Geographers*, 41, pp. 187-200.

Karampekios, N., Oikonomou, I. and Carayannis, E.G. (2017) *The Emergence of EU Defense Research Policy*. Springer, New York.

Kennedy, D. (1982) “Stages of the Decline of the Public/Private Distinction”, *University Of Pennsylvania Law Review*, 130, pp. 1349-1357.

Klepp, S. (2010) “Italy and its Libyan Cooperation Program: Pioneer of the European Union’s Refugee Policy?”, in J.-P. Cassarino (ed.), *Unbalanced Reciprocities: Cooperation on Readmission in the Euro-Mediterranean Area*, Special Edition, Middle East Institute, Viewpoints, Washington, pp. 77-93.

Koser, K. (2005), “Irregular migration, state security and human security”, Paper prepared for the Policy Analysis and Research Programme of the Global Commission on International Migration, in http://iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/policy_and_research/gcim/tp/TP5.pdf, accessed on 08.09.2011.

Lahav, G., Messina, A. and Vasquez, J. (2007), "The Immigration-Security Nexus: A View from the European Parliament", Paper presented at the EUSA Tenth Biennial International Conference, in http://aei.pitt.edu/7945/, accessed on 29.11.2011.

Lavenex, S. (2006) "Shifting up and out: The foreign policy of European immigration control", *West European Politics,* 29(2), pp. 329-350.

Leander, A. (2009) "Habitus and Field", Working Paper, 9, Copenhagen Business School, Denmark, in http://openarchive.cbs.dk/bitstream/handle/10398/7966/Habitus_and_Field_Working_Paper.pdf?sequence=1, accessed on 19.04.2016.

Lee, J. (2016) "HRS CEO discusses role of biometric technologies in combating terror attacks", in http://www.biometricupdate.com/201604/hrs-ceo-discusses-role-of-biometric-technologies-in-combating-terror-attacks, accessed on 10.01.2017.

Lemberg-Pedersen, M. (2013) "Private security companies and the European borderscapes", in T. Gammeltoft-Hansen and N. Nyberg Sørensen (eds.), *The Migration Industry and the Commercialization of International Migration*, Routledge, London and New York, pp. 152-172.

Leonardo Company (2020) "Military Systems for Border, Territory & Maritime Control", in https://www.leonardocompany.com/en/land/force-protection-and-border-control/border-control-systems, accessed on 27.03.2020.

Levy, C. (2010) "Refugees, Europe, Camps/State of Exception: 'Into The Zone', the European Union and Extraterritorial Processing of Migrants, Refugees, and Asylum-seekers (Theories and Practice)", *Refugee Survey Quarterly*, 29(1), pp. 92-119.

Loeschner, J., Riha, Z. and Martin, V. (2007) "BIOPASS Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports", Report number: JRC40718, Frontex.

Lutterbeck, D. (2006) "Policing Migration in the Mediterranean: ESSAY", *Mediterranean Politics*, 11(1), pp. 59-82.

Marina Militare (2016) "Mare Nostrum Operation", in http://www.marina.difesa.it/EN/operations/Pagine/MareNostrum.aspx, accessed on 13.09.2016.

Mathiesen, T. (1999) *On globalization of control: Towards an integrated surveillance system in Europe*. Statewatch, London.

MBDA Systems (2014) "Who we are", in http://www.mbda-systems.com/, accessed on 19.03.2014.

Military Technologies (2017) "Thales Alenia Space wins European Commission contracts to support ESA and GSA for Galileo system engineering and operational support services", in http://military-technologies.net/2017/01/13/thales-alenia-space-wins-european-commission-contracts-to-support-esa-and-gsa-for-galileo-system-engineering-and-operational-support-services/ , accessed on 27.01.2017.

Monroy, M. (2020) "Drones for Frontex: unmanned migration control at Europe's borders", Analysis in Statewatch, in http://www.statewatch.org/analyses/no-354-frontex-drones.pdf, accessed on 27.03.2020.

Morrison, M. (2010) "EADS's disparate group of subsidiaries", in FlightGlobal, in http://www.flightglobal.com/news/articles/eads39s-disparate-group-of-subsidiaries-344474/, accessed on 19.03.2014.

Munday, P., Pakenham, M., Nicoll, A., Haine, J., Rinkineva, K., Jaarva, M., Johnson, J. and Waller, A. (2006) "New European approaches to Counter Terrorism", in ESSTRT Deliverable D6-1. Final Report.

Musarò, P. (2016) "Mare Nostrum: the visual politics of a military-humanitarian operation in the Mediterranean Sea", *Media, Culture & Society*, 39(1), pp.1-18.

NATO (2012) "Interoperability: Connecting NATO Forces", in http://www.nato.int/cps/en/natohq/topics_84112.htm, accessed on 24.11.2016.

NHIndustries (2014) "The Partnership", in http://www.nhindustries.com/site/en/ref/Partnership_22.html, accessed on 26.03.2014.

Nowak, J. (2019) "Drone Surveillance Operations in the Mediterranean: The Central Role of the Portuguese Economy and State in EU Border Control", Border Criminologies Blog, in https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2019/02/drone, accessed on 28.03.2020.

O'Donnell, C. (2010) "How should Europe respond to sovereign investors in its defence sector?", Centre for European Reform, Policy Brief, in https://www.cer.eu/sites/default/files/publications/attachments/pdf/2011/pb_swf_defence_sept10-203.pdf, accessed on 29.03.2020.

O'Reilly, C. (2010) "The transnational security consultancy industry: A case of state corporate symbiosis", *Theoretical Criminology,* 14(2), pp. 183-210.

PANOPTESEC (2014) "Welcome to the Official Website of the PANOPTESEC Project", in http://www.panoptesec.eu/about_panoptesec/#, accessed on 28.03.2020.

Pickering, S. and Weber, L. (2006) (eds.) *Borders, mobility and technologies of control.* Springer, Amsterdam.

Reinares, F. (2009) "After the Madrid bombings: Internal security reforms and prevention of global terrorism in Spain", *Conflict and Terrorism*, 32(5), pp. 367-388.

Relyea, H. (2002) "Homeland Security and Information", *Government Information Quarterly,* 19, pp. 213-223.

Corporate Watch (2015) “BAE Systems Company Profile”, in https://corporatewatch.org/bae-systems-company-profile/, accessed 30.03.2020.

Reuters (2019, 5 May) “Airbus considers legal action against Germany over Saudi ban: sources”, in https://www.reuters.com/article/us-germany-saudi-arms-airbus-idUSKCN1SB0JA, accessed on 30.03.2020.

Robkin, M. (2010) “A Short History of Interoperability”, FDA-Continua-CIMIT Workshop, in http://www.mdpnp.org/uploads/1_Robkin_26Jan.pdf, accessed on 24.11.2016.

Safran (2014a) “Group Organization”, in http://www.safran-na.com/spip.php?rubrique71, accessed on 27.03.2014.

Safran (2014b) “History”, in http://www.safran-group.com/site-safran-en/group/safran-a-dynamic-group/, accessed on 27.03.2014.

Safran (2016) “Capital shareholding structure”, in http://www.safran-group.com/finance/safran-share/capital-structure-and-voting-rights/Capital%20shareholding%20structure%20and%20voting%20rights, accessed on 02.02.2017.

Schilde, K. (2017) *The political economy of European security*, Cambridge University Press, Cambridge.

Sempere, C.M. (2011) “A survey of the European security market”, Economics of Security Working Paper, 43, Deutsches Institut für Wirtschaftsforschung (DIW), Berlin.

Sianni, A. (2003), “Interception practices in Europe and their implications”, *Refuge: Canada's periodical on refugees,* 21(4), pp. 25-34.

SIPRI (2015) “The SIPRI Top 100 Arms-Producing And Military Services Companies, 2014”, SIPRI Fact Sheet, in http://books.sipri.org/files/FS/SIPRIFS1512.pdf, accessed on 06.01.2017.

SIPRI (2016) “World Military Expenditure – Military Spending Graphics”, in https://www.sipri.org/research/armament-and-disarmament/arms-transfers-and-military-spending/military-expenditure, accessed on 06.12.2016.

Sistemi Informativi Aziendali (2012) “Integration – a necessary evil”, in http://elite.polito.it/files/courses/02CIX/SystemIntegration.pdf, accessed on 01.05.2014.

Spencer, A. (2008) “Linking Immigrants and Terrorists: The Use of Immigration as an Anti-Terror Policy”, *The Online Journal of Peace and Conflict Resolution*, 8(1), pp.1-24.

Statewatch (2014) “Viewpoint: ‘Border security’ exports: dividing lands across the globe”, in http://www.statewatch.org/analyses/no-246-border-security-analysis.pdf, accessed 13.06.2016.

Stone, J. (2019, 11 November) “Powerful military and security industry’ profiting from dividing Europe 30 years after Berlin Wall fell”, *The Independent*, in https://www.independent.co.uk/news/world/europe/berlin-wall-anniversary-30-years-military-security-thales-airbus-leonardo-a9198531.html, accessed on 30.03.2020.

Stop Wapenhandel (2019, 14 April) "Border security, military industry and EU militarisation", Presentation at the seminar on Euromilitarism, Oorlog is geen Oplossing / VD AMOK / Network No to War – No to NATO, Amsterdam, in http://www.stopwapenhandel.org/node/2271, accessed on 30.03.2020.

Telespazio (2017) "Profile", in http://www.telespazio.com/about-us-chi-siamo/our-company, accessed on 27.01.2017.

Gemalto (2019) "Gemalto Border Management", in https://www.gemalto.com/brochures-site/download-site/Documents/gov-border-management.pdf, accessed on 28.03.2020.

Thales Alenia Space (2010) "Thales Alenia Space: contract signed for the Galileo system Support Services", in https://www.thalesgroup.com/sites/default/files/asset/document/Galileo_services_signature_26012010.pdf, accessed on 27.01.2017.

Thales Alenia Space (2011) "First two Galileo satellites successfully launched", in https://www.thalesgroup.com/sites/default/files/asset/document/Galileo%20IOV%20succesful%20launch.pdf, accessed on 27.01.2017.

Thales Group (2009) "Emergency Radio goes live", On the move#6, Spring 09, in https:// www.thalesgroup.com/sites/default/files/asset/document/Emergency%20radio%20goes%20live.pdf, accessed on 22.04.2014.

Thales Group (2014a) "Australia", in https://www.thalesgroup.com/en/australia, accessed on 25.03.2014.

Thales Group (2014b) "Thales Alenia Space – Innovative space solutions to enhance people's lives and extend our reach beyond Earth", in https://www.thalesgroup.com/en/thales-alenia-space, accessed on 25.03.2014.

Thales Group (2014c) "Training & Simulation Solutions", in https://www.thalesgroup.com/en/training-simulation, accessed on 25.03.2014.

Thales Group (2014d) "Transportation – Canada", in https://www.thalesgroup.com/en/canada/transportation, accessed on 25.03.2014.

Thales Group (2018) "Thales Defence & Security Inc.", in https://www.thalesdsi.com/, accessed on 29.03.2020.

Thales Group (2019a) "History – New Chapter", in https://www.thalesgroup.com/en/global/group/history, accessed on 29.03.2020.

Thales Group (2019b) "Thales completes acquisition of Gemalto to become a global leader in digital identity and security", in https://www.thalesgroup.com/en/austria/news/thales-completes-acquisition-gemalto-become-global-leader-digital-identity-and, accessed on 29.03.2020.

Thales Group (2019c) "Thales Optronics", in https://www.thalesgroup.com/en/optronics, accessed on 29.03.2020.

Thales Group (2019d) "Underwater Warfare", in https://www.thalesgroup.com/en/activities/defence/naval-forces/underwater-warfare, accessed on 29.03.2020.

The Guardian (2015) "Defence industry's stock rises as state budgets bid to meet terror threat", in https://www.theguardian.com/business/2015/dec/07/defence-industry-stock-rockets-budgets-rise-terror-threat, accessed on 21.05.2016.

The Migrants Files (2015) "The Money Trails – Follow the money – some of it – into the sub-economy spawned by migration", in http://www.themigrantsfiles.com/, accessed on 08.05.2016.

UN General Assembly (1951, 28 July) "Convention Relating to the Status of Refugees", United Nations, Treaty Series, vol. 189, in , accessed on 31.03. 2019.

University of Sheffield (2016) "Airbus Chair in Advanced Manufacturing", Job reference Number: UOS014583, in https://jobs.shef.ac.uk/sap(bD1lbiZjPTQwMA==)/bc/bsp/sap/hrrcf_wd_dovru/application.do?PARAM=cmNmdHlwZT1waW5zdCZwaW5zdD01NzlBNjY1MTE0MTU2Q0E3RTEwMDAwMDBBQzFFODg3OA%3d%3d, accessed on 13.11.2016.

Vranken, B. (2017) "Securing Profits: How the arms lobby is hijacking Europe's defence policy", Verdes Actie, in http://www.istopthearmstrade.eu/sites/default/files/Securing_profits_web.pdf, accessed on 30.03.2020.

Want, R. (2006) "An introduction to RFID technology", *Pervasive Computing*, IEEE, 5(1), pp. 25-33.

Washington Technology (2010) "Purchase of Danish company expands BAE's cyber, intell capabilities – British defense giant adds another security services company", by David Hubler, in http://washingtontechnology.com/articles/2010/12/22/danish-purchase-bae-global-cyber-and-intell.aspx, accessed on 26.03.2014.

Washington Technology (2011) "BAE wraps up purchase of L-1 intelligence trio", by David Hubbler, in http://washingtontechnology.com/articles/2011/02/16/bae-purchase-of-l1-intelligence-trio.aspx, accessed on 27.03.2014.

Weintraub, J. (1997) "The theory and politics of the public/private distinction", in J. Weintraub and K. Kumar (eds.), *Public and private in thought and practice: Perspectives on a grand dichotomy*, The University of Chicago Press, Chicago, pp. 1-42.

Welcomeurope (2016) “EU funding grants and funds from Europe such as European Community Grant 2014-2020”, in http://www.welcomeurope.com/, accessed on 13.06.2016.

Wolff, S. (2010), “EU Integrated Border Management Beyond Lisbon: Contrasting Policies and Practice”, in R. Zapata-Barrero (ed.), *Shaping the normative contours of the European Union: a Migration-Border Framework*, CIDOB, Barcelona, in http://www.cidob.org/en/publications/monographs/monographs/shaping_the_normative_contours_of_the_european_union_a_migration_border_framework, accessed on 04.07.2011.