

MARKET FORCES

THE DEVELOPMENT OF THE EU SECURITY-INDUSTRIAL COMPLEX



CONTENTS

EXECUTIVE SUMMARY	1
1 INTRODUCTION: SECURITY FOR WHOM, FROM WHAT?	7
2 THE EMERGENCE OF A EUROPEAN SECURITY-INDUSTRIAL COMPLEX	11
2.1 Pursuing the “ultimate goal”	13
2.2 Security research: a €1.4 billion networking exercise	15
2.3 Reinforcing the fortress	19
2.4 The long arm of the law	23
2.5 Freedom, security and justice?	28
3 PUBLIC INTEREST, PRIVATE DIALOGUE	31
3.1 Visions of the future	33
3.2 The “end-to-end approach”: a state-corporate merger	34
3.3 Friends on the inside: shaping legislation	36
3.4 Joining the dots: public-private partnership	38
4 BUILDING THE ‘SECURITY UNION’	43
4.1 The price of security	45
4.2 All-seeing eyes: fighting crime and terrorism	46
4.3 The walls around us all: border security	51
4.4 The devil is in the digital: cybersecurity	56
4.5 Disaster resilience: unknown unknowns need all-purpose surveillance	60
5 CONCLUSIONS: THE ROAD TO HELL?	63
Annex 1: Top 50 recipients of ESRP funds to December 2016	66
Annex 2: National distribution of the Internal Security Fund	67
List of acronyms used in this report	68



EXECUTIVE SUMMARY

While the European Union project has faltered in recent years, afflicted by the fall-out of the economic crisis, the rise of anti-EU parties and the Brexit vote, there is one area where it has not only continued apace but made significant advances: Europe's security policies have not only gained political support from across its Member States but growing budgets and resources too.

The increased securitisation of the European Union has relevance not only for its Member States but for the world which will be affected by the measures, technologies and strategies being developed, sold and deployed. The emergence of 'security' as the EU's increasingly default response to complex social and ecological crises is also significant given the current political context of rising authoritarian parties and governments all-too-willing to use the latest security tools to maintain and extend power.

This report digs deep into the EU's funding of its security strategy. It shows that between 2014 and 2020, a total of at least €8 billion has been allocated to budgets directed towards security measures - €3.8 billion to the Internal Security Fund (ISF), €1.7 billion to the European Security Research Programme, €3.1 billion to the Asylum, Migration and Integration Fund (which has numerous uses in the context of security policy) and some €2.4 billion for EU home affairs agencies such as Europol and Frontex. While still a small amount in comparison to the EU's total budget of €1 trillion between 2014 and 2020, it is a significant development given that a decade ago the bloc had no dedicated budgets for security, justice or home affairs.

The report's investigation of the different budgets also draws out the big picture of where the funding is going and what it is helping to construct: an all-encompassing vision of security that seeks to combat a seemingly limitless number of "threats" ranging from terrorism to petty crime, and which displays a marked tendency of treating the entire population (European and especially non-European) as potential objects of suspicion that must be surveyed and if necessary detained, obstructed or even killed. This vision has been propelled by military and security corporations whose profits depend on a world of suspicions, fears and threats – and who have not only been major beneficiaries of EU security spending, but have also been given an unprecedented role in designing the security research programme.

In a 2009 report by Statewatch and TNI, we warned that EU's security, research and development policies were "coalescing around a high-tech blueprint for a new kind of security". We summed up the vision in the title of the report, *NeoConOpticon*, to capture the metaphor of an all-seeing prison combined with the increasingly neoconservative, corporate-led vision of the EU's security and defence policies. It warned that we were "turning a blind eye to the start of a new kind of arms race, one in which all the weapons are pointing inwards". That report examined the early years of EU security strategies,



from 2003 to 2008, and focused on the beginnings of the European Security Research Programme (ESRP) and the 85 projects it had funded up to that point.

Market Forces focuses on the development of EU security policies and budgets through the 2007-13 period and their successors, which were launched in 2014 and will run until 2020. These include the ESRP, which funds research to develop new technologies for law enforcement, border control, cybersecurity and critical infrastructure protection and leans heavily towards technologies and techniques initially deployed or favoured by military forces: drones, data-mining tools, large-scale surveillance systems, biometric recognition and automated behaviour analysis tools. It also explicitly seeks to develop “dual-use” technologies for both civil and military use.

The report also analyses the Internal Security Fund (ISF), distributed to EU Member States to enhance the powers of law enforcement and border control agencies (including through numerous new surveillance and analysis systems). The aim – albeit not yet realised – is that EU funds pay for both the development of new technologies and their subsequent purchase at EU or national level, creating a self-fulfilling loop of supply and demand. Despite warnings and public concerns over the direction of the EU’s security strategy, the journey towards a world of ubiquitous public-private surveillance and control systems continues, for the time being, largely unabated.

The report is divided into three sections: the first provides a summary of the early development of the European Security Research Programme, its incorporation into the EU’s formal research agenda, and the concurrent development and implementation of EU policies and budgets in the area of justice and home affairs from 2007 to 2013. The second section looks at the institutions, corporations and organisations involved in the development and ongoing implementation of the EU’s security research agenda and security policies, and the ways in which private interests have long-managed to successfully shape the public policy and research agenda. The third section looks at current EU security policies and budgets. It seeks to provide a general overview of aims and objectives of current policies, the funds available for implementing them, and which organisations have so far been the chief beneficiaries.

The EU’s security agenda is now so sprawling and complex that no one report can cover every aspect of it, but there are a few key themes that are worth drawing out here.

SECURITY-INDUSTRIAL COMPLEX: STATE-CORPORATE MERGER

A European security-industrial complex began to emerge in 2003 when the EU endorsed the establishment of a ‘Group of Personalities’ (GoP) to draw up plans for a research programme on new “homeland security” technologies. The GoP’s proposals became the ESRP, which was formally incorporated into the EU budget in 2007, and processes by which corporate representatives are able to influence the EU’s security research agenda have been continued and consolidated in the years since.

The current chair of the European Commission’s official advisory group on the ESRP, the Protection and Security Advisory Group (PASAG), is Alberto de Benedictis, a former long-term senior employee at arms firm Finmeccanica (now Leonardo) and a former chairman at private defence and security industry lobby group AeroSpace and Defence Industries Association of Europe, (ASD). He is joined in the PASAG by former and current employers of Isdefe (Spain’s state-owned arms company), Airbus and Morpho, alongside officials from major research institutes and state agencies such as the European Defence Agency, Europol and the Dutch National Police.

Public-private contacts are also maintained elsewhere. EU officials and corporate executives have continued to come together in a series of high-level events in February 2011, March 2012, March 2013 and April 2014 to look at how to better promote Europe’s security industry. Meanwhile, the groups such as the European Organisation for Security (EOS, with a declared lobbying budget of €200,000-299,999 in 2016 alone) and ASD (a €298,000 lobbying budget in 2015) ensure that industry is well-represented in the corridors of power in Brussels. Indeed, an EOS-led organisation, the European Cybersecurity Organisation, has now been awarded significant influence over the ESRP’s cybersecurity research agenda as part of a multi-million euro “public-private partnership”.

The level of corporate influence is no accident: one of the core objectives of the EU’s security policy is ensuring profits for the European security industry. As the Commission once put it: “A competitive EU security industry is the *conditio sine qua non* of any viable European security policy and for economic growth in general.” While the Commission sometimes rejects industry proposals, it has nevertheless granted unprecedented industry involvement in security research and Europe’s broader security strategies.

CORPORATIONS AND RESEARCH INSTITUTES REAP THE BENEFITS

It hardly comes as a surprise, therefore, that some of the biggest winners so far of the 2014-20 EU security research budget have been major corporations. As of December 2016, Atos was involved in 15 projects, (€6.5 million), Thales (nine projects, €4.6 million), Engineering (an Italian company, six projects, €4 million) and Airbus (two projects, €3.6 million). In the previous six-year period (2007-2013), the main corporate players were Thales (€28.5 million, 63 projects), Selex (€23.2 million, 54 projects), BAE Systems (€14.2 million, 32 projects) and Indra (€12.3 million, 16 projects). In total, private companies took almost €552 million from the FP7 ESRP (2007-2013) budget, some 40% of the €1.4 billion total. Per project, private companies took almost 25% more money on average from the 2007-13 ESRP than they did from counterpart research programmes such as health, ICT, energy, environment and transport.

Private companies are not the only significant recipients of ESRP funding, however. Major research institutes have also benefitted massively, such as Germany's Fraunhofer Institute, France's *Commissariat à l'énergie atomique et aux énergies alternatives* (CEAS), Greece's Centre for Research and Technology Hellas and TNO in the Netherlands. Many of these organisations' agendas are well-aligned with the EU's own: boosting industry profits whilst promising public security through the introduction of new technologies. Many of them have also held seats on the PASAG and its predecessors. In the 2007-13 ESRP, the Fraunhofer Institute was the single largest overall recipient of funding, garnering €51.5 million for its role in 85 projects. It was followed by TNO (€30 million, 54 projects), the Swedish Defence Research Institute (€31.8 million, 53 projects) and the CEAS (€15 million, 39 projects). Research institutes continue to be major beneficiaries of funding in the 2014-20 period.

It is likely that the security industry would not survive without the considerable public funding supplied by the EU and its member states. As even the European Organisation for Security (EOS), the sector's chief lobbying group has highlighted: "security is often in a position of market failure," where "the allocation of goods and services by a free market is not efficient". Yet the "market forces" represented by the industry are nevertheless seen as a crucial element in EU security policy, giving rise to novel governance structures. As a 2014 study for the European Parliament noted with regard to certain funding schemes in the ESRP: "In sharp contrast with the idea of shaping a security market... the underlying idea here seems to be the promotion of a non-market commercial relation between the 'security industry' and public sector customers." These processes raise serious questions over agenda-setting and accountability.

MILITARISED PANOPTICON

Hundreds of EU-funded research projects were examined for this report. Taken together, a picture emerges of an attempt to build an integrated, EU-wide interoperable, high-tech, surveillance system directed at combating a multiplicity of threats. The projects range from plans for border surveillance drones and multi-biometric identification and authentication systems, to the automated detection and analysis of "terrorist-related content" online and the development of new covert surveillance devices.

The ESRP also deliberately blurs the line between civilian and military technologies. While the legislation governing the research programme says that "activities carried out under Horizon 2020 shall have an exclusive focus on civil applications," the Commission has stated its intention to "evaluate how the results [of research projects] could benefit also defence and security industrial capabilities." The EU is also moving towards a new research budget for military research. As if in a sequel to the process that established the ESRP, a high-level 'Group of Personalities' dominated by state officials and industry representatives (including familiar names such as Indra, Airbus, BAE Systems and Finmeccanica) were invited to map the way ahead. This currently involves proposals for a €1 billion annual budget for military research from 2020 onwards.

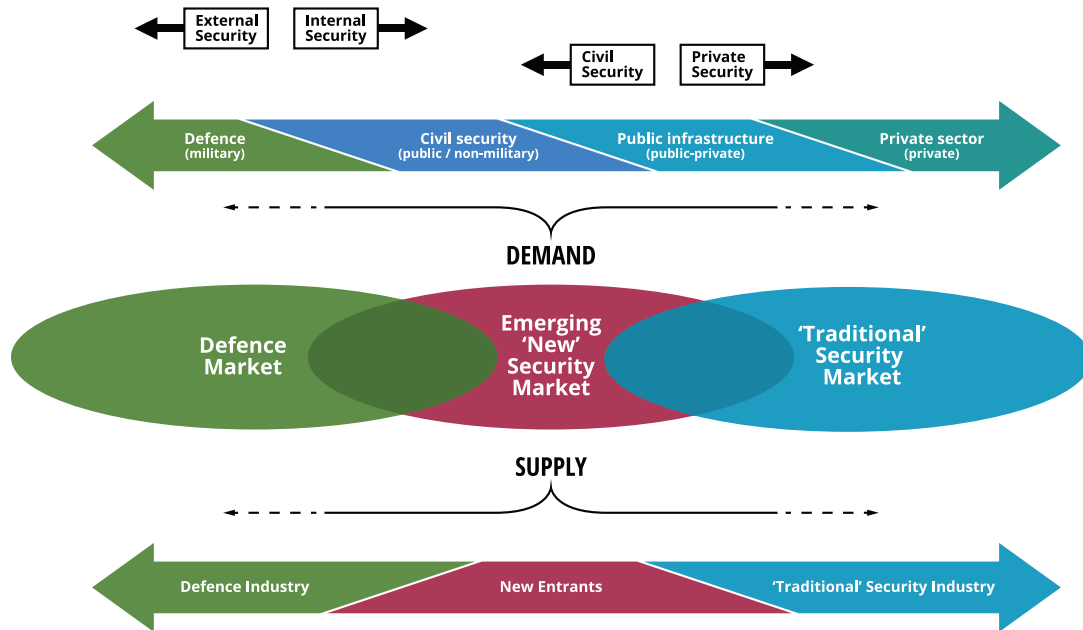
Some of the long-term goals evident in the research funding, policies and security legislation approved in recent years include:

- **Nurturing transnational policing networks.** The EU is helping police forces to access and process information on a scale traditionally reserved for security and intelligence agencies, whilst providing financial and institutional backing for the development of secretive, unaccountable networks. For example, the Passenger Name Record (PNR) Directive, approved in April 2016, places all air travellers entering, leaving or flying within the EU under suspicion: they are automatically profiled against police watchlists and databases. One ESRP project, COMPOSITE, investigating "change management" in the

police, reveals the growing interest from police in the integration of information systems, the use of mobile technology, surveillance systems, digital biometrics and use of social media for publicity and investigation purposes. The Dutch police for example are cited approvingly for their “mobile weapons scanners” and research into the use of smells, bright lights and noises “to exploit physical reactions to create ‘less-lethal technologies’ with a mass effect” for use on crowds. Such technologies have been one topic of interest to the Dutch-led European Network of Law Enforcement Technology Services (ENLETS).

- **Europe-wide networked DNA databases and exchange of personal data.** The EU is moving towards ensuring national law enforcement agencies can seamlessly exchange DNA, fingerprint and vehicle data, at the same time as national DNA databases are growing steadily – an average of 10% over the course of 2015, with over 5.7 million individuals’ DNA samples held across the EU at the end of that year. Through the Prevention of and Fight Against Crime Fund (ISEC), the EU spent at least €12.2 million on projects aimed at completing the network of national DNA databases. Research projects such as INGRESS (€3.2 million in EU funding and led by French security giant Safran), ARIES (€2.2 million), FLYSEC (€4.1 million), PROTECT (€5 million) and others aim to further spread the use of biometric authentication checks throughout society.
- **Increased investment in surveillance systems.** Many ESRP projects seek to extend an already-elaborate system of state and inter-state surveillance. The €4.9 million FORENSOR project, for example, seeks to develop and validate “a novel, ultra-low-power, intelligent, miniaturised, low-cost, wireless, autonomous sensor (‘FORENSOR’) for evidence-gathering” which will store audio and video and operate for up to two months with no additional infrastructure. ROBIN hopes to develop “a mobile robot platform able to perform autonomous protection of critical infrastructures”; INVEST, a smart CCTV for automated detection and tracking of “suspects”; and Starlight, systems for enabling video surveillance in the dark. Even the sewage system is to be used for surveillance: the microMole project proposes installing sensors to “track waste associated to ATS [amphetamine-type stimulants] production,” and the 2016-17 ESRP work programme foresees other utility networks, for example water, electricity or telecommunications, being deployed for law enforcement purposes.
- **Pre-crime identification.** The idea of pre-crime - that you could be convicted based on your potential or likelihood of committing a crime – began as a science-fiction concept made popular by the film *Minority Report*, but the massive expansion of automated systems of surveillance and tracking are moving us rapidly in that direction. One EU project, INDECT, was awarded €11 million from the EU and sought intelligent “automatic detection of threats and recognition of abnormal behaviour or violence, to develop the prototype of an integrated, network-centric system supporting the operational activities of police officers.” Numerous other projects in this vein have been funded by the ESRP, while Member States have their own programmes in place. Malta and Greece have committed themselves to using the Internal Security Fund budget to develop “intelligence-led policing models” that will help predict “crimes that have already been committed or will be committed in the future.”
- **Militarising the EU’s borders.** Through both its research projects and security budgets (notably the External Borders Fund and Internal Security Fund-Borders), the EU is actively supporting the ongoing militarisation of European borders. For example, from 2007-10, EU funds contributed to the deployment of 545 border surveillance systems covering 8,279 kilometres of the EU’s external borders and 22,347 items of border surveillance equipment. It also included funding for detention centres, including in Greece, despite public reports on the appalling conditions for migrants. A long series of projects that currently includes SafeShore (€5.1 million), RANGER (€8 million) and ALFA (€4.6 million) seek to expand border surveillance, particularly through the use of drones. One previous project, TALOS (€13 million in EU funding and including Israel Aerospace Industries, the Hellenic Aerospace Industry and PIAP, a Polish robot manufacturer) even tried to develop an automated border control robot. Although the review of the project admitted that the robot “may be too complex” for border agencies to put into use, its vision of semi-autonomous border security remains a key plank of EU policy.
- **Disaster resilience preparedness.** The effects of climate change and extreme weather are also seen as key drivers for the development of security products and approaches. As one project, I-REACT (€5.4 million), has stated rather crudely, climate change will “enable new business development opportunities around natural disasters triggered by extreme weather conditions, which will reduce the number of affected people and loss of life.”

OVERVIEW OF THE SECURITY MARKET: SUPPLY AND DEMAND CHARACTERISATION



Source: Ecorys, 'Study on the competitiveness of the EU security industry', 15 November 2009

DEMOCRATIC DEFICIT AND THE DEMAND FOR NEW VISIONS OF SECURITY

Throughout the development of Europe's security agenda, there has been a consistent pattern of democracy playing catch-up to money, corporate influence and a belief that we can never have too much high-tech "security". The EU-wide border surveillance system Eurosur, for example, has been supported with millions of euros from the Commission since 2007, even though legislation establishing the system was not approved until 2013. A similar process of funding and rolling out programmes well ahead of legislation can be seen with the Passenger Name Record (PNR) air travel surveillance programme (€50 million in EU funding came in 2012, four years before EU legislation) and the EU's "smart borders" project (in development for almost a decade but only just coming up for approval by the European Parliament and Council of the EU). Given the far-reaching nature of these projects and the need for a robust discussion on how to prevent human rights being superseded by security objectives, this lack of democratic accountability is deeply disturbing.

This is not to say that "societal considerations" have not been an issue in the ESRP. The need for compliance with fundamental rights, democratic values and ethical standards has been noted repeatedly in the multitude of EU documents on security research. As criticisms of the security research agenda emerged in the early years of the ESRP, the Commission moved to ensure that security research projects complied with more stringent ethical checks, and broadened the agenda somewhat to fund less technologically-determined, more socially-focused research.

The Commission's 2011 legislative proposal for Horizon 2020 suggested it hoped to move away from the hard-edged, high-tech research that characterised the ESRP. It proposed that security research be merged into a broader theme on 'Inclusive, innovative and secure societies' that called for "rediscovering or reinventing successful forms of solidarity, coordination and creativity." However, national officials in the Council and MEPs in the Parliament (including some with close connections to the security industry) rejected these ideas and others that would have developed a broader "human security" research agenda and ensured more stringent oversight of projects. The result is a research agenda that remains largely focused on finding problems at which to direct commercialised industry "solutions".

A rigorous process of ethical approval remains in place – and is undoubtedly essential – but it will not overcome the political environment and objectives in which it is framed. As argued in a report for the ESRP-funded SURPRISE project: "Security policies... have increasingly adopted a conceptual approach to security problems that is strongly solution-driven and tends to neglect the variety and complexity of social, economic, technical and political factors that may have caused those security problems in the first place." Similar sentiments were expressed in a European Parliament report in 2010. It noted that while future research proposals "indicate a growing awareness for questions of fundamental rights and freedoms", they "remain overly framed by the concerns of the defence and security industry and national and European security agencies and services." In this respect, it seems little has changed.

INEFFICIENCY AND POOR RESULTS: A SAVING GRACE?

It is a sad reflection that perhaps the greatest constraint on the development of the sweeping security visions endorsed by the EU and its Member States has been bureaucratic inefficiency or the impractical nature of projects. In the case of the External Borders Fund, for example, the European Court of Auditors (ECA) in 2014 reported that EU funds had been ineffective, seriously deficient and misspent by national governments. Similarly, the formal evaluation of the 2007-2013 ESRP found that very few of the projects looked likely to result in concrete products (only 11% reported registration of intellectual property), and they performed badly too in terms of other key performance indicators such as academic publications.

The main success the evaluation could point to was that the ESRP had “improved the connections between the providers [corporations and research institutes] and users [state agencies] of novel civil security solutions,” allowing them to “to develop common concepts, terminology, open interfaces, middleware, etc. that will in turn facilitate improved multilateral and cross-border cooperation.” Seen from this perspective, the ESRP in FP7 has the appearance of a €1.4 billion networking exercise, and a cash cow for corporations and research institutes.

SECURITY: A ONE-WAY STREET?

Nevertheless, despite its failings and inefficiencies, this building of a security community that binds corporate interests and government policy cannot be discounted: it continues firmly on the path towards an internally and externally militarised Europe. As a European Parliament report noted in 2014, the Commission’s dedication to supporting the security industry and developing technologies of surveillance “overrules all other societal considerations, which are relegated to preoccupations with societal acceptance of security technologies.”



Officials from the public and private sector get together to thrash out a “security industrial strategy” for the EU.


Moreover, this is not simply a case of “bureaucrats in Brussels” implementing measures against the wishes of the Member States. While the European Commission retains significant room for manoeuvre in its initiatives, EU security policy is strongly driven by national state interests, and it is EU Member States that are leading the charge towards authoritarian and security-focused government. Following terrorist attacks and the growing numbers of refugees created by wars in Syria and elsewhere, governments across Europe have moved to reinforce security measures to the detriment of individual rights. Executive power has been bolstered at the expense of oversight by parliaments and independent agencies; standards of proof in court proceedings have been diminished; and security and law enforcement agencies have been given significant new powers for surveillance, amongst other issues.

The EU has done little to prevent these developments at national level, in part for fear of disturbing the fragile “unity” that exists between the EU’s Member States, but also because they complement the EU’s own measures towards total border surveillance, pro-active and “intelligence-led” law enforcement, the surveillance and profiling of migrants and EU nationals, and the expansion and interconnection of biometric databases.

NEED FOR A NEW APPROACH

It is clear that Europe faces major challenges, from the increase in terrorist attacks to the growing impact of climate change, that require collective responses. The question is whether they require the responses offered so far: extraordinary legal and policy measures combined with the development and deployment of new surveillance and control technologies often based on ideas of hierarchical command-and-control. The presumption that underpins many of the policies and technologies emerging from EU initiatives is one of countless, dispersed, almost-invisible threats, serving to propel new “public security” initiatives and corporate profit – although it is far from clear that these two goals are easy bedfellows. More fundamentally, these processes are, as the academics Eliav Lieblich and Adam Shinar have put it, undermining “a foundational principle of the liberal order” – that “the state does not act upon the presumption that its citizens are threatening.”

It is noticeable that these new forms of security have been advancing at the same time as more traditional forms of social security have been deliberately eroded in the context of austerity. Yet research shows that issues relating to income, employment and financial security are what make most people feel secure, to a far greater degree than traditional security measures such as police presence or militarised borders. The reinforcement of pervasive, high-tech security measures has long been the primary consideration for the EU’s security strategists, with the private interests that stand to gain from this process always ready to offer their guidance and reap the rewards. It is time for a new direction before it is too late.

A young woman with dark hair, wearing a green hijab with gold floral patterns and a bright yellow jacket, stands outdoors. She is holding a white rectangular sign with both hands. The sign has handwritten text in black ink. The background is a blurred outdoor setting with trees and a paved area.

Stopped and searched
because I fitted the
profile of a person
who could be "violent
at a protest"

One of a series of photographs by Darren Johnson exploring young people's "stop and search" encounters with the police.

SECTION 1: INTRODUCTION

SECURITY FOR WHOM, FROM WHAT?

We live in dangerous times for democracy. Over the last decade, governments in Europe and elsewhere have adopted increasingly nationalist, authoritarian and xenophobic rhetoric, laws and policies at the expense of the individual rights that are supposedly fundamental to European life.

Amnesty International has described these developments as the fruit of “a new bargain... which promises security and economic betterment in exchange for surrendering participatory rights and civil freedoms.”¹ The results can be seen in the rise of authoritarian parties (in the Netherlands, UK, France and elsewhere) and governments (for example in Hungary and Poland²) across Europe and further afield, as in the USA, India or the Philippines.³

The EU, “founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights,”⁴ has done little to prevent these developments. Its own laws, policies and budgets serve to enhance state power, regardless of the government in control. In conjunction with transnational corporations, research institutes and others, the EU is pouring billions of euros into the development of a new arsenal of militarised security technologies and transnational bodies that sit beyond traditional forms of democratic oversight and control, still firmly rooted in the nation-state.

The EU’s budgets for law enforcement, counter-terrorism, border control and security research amounted to €3.8 billion in the period between 2007 and 2013. In the current period, which runs from 2014 to 2020, they have grown to a total of some €11 billion – small fry in comparison to the EU’s total budget of almost €2 trillion between 2007 and 2020, but it is a significant development given that a decade ago the bloc had no dedicated budgets for security, justice or home affairs. Relevant budgets include the Internal Security Fund (ISF, €3.8 billion), the European Security Research Programme (ESRP, €1.7 billion), some €2.4 billion in funds for EU home affairs agencies such as Europol and Frontex (who have a key role in the EU’s security agenda), and the Asylum, Migration and Integration Fund (AMIF, €3.1 billion), which is increasingly playing a role in security measures.

The type of security currently on offer is not that offered by the social democratic welfare states of previous decades – themselves now a rose-tinted memory following years of cutbacks, privatisations, limitations and stringent austerity measures.⁵ Rather, it is security from a series of unceasing “threats” – terrorism; organised crime; mass migrations; people, drug and nuclear trafficking; weapons of mass destruction; climate change; and natural disasters, to name but a few.

All these problems clearly require responses. The question is whether they require the responses offered so far: extraordinary legal and policy measures combined with the development and deployment of new surveillance and control technologies often based on hierarchical command-and-control practices.

In January 2017 an *Amnesty International* report examined 14 European countries that have, both on their own steam and in order to implement EU law, introduced “new legislation and policies intended to address the threat of terrorism” and in doing so “have steamrolled rights protections.” This includes, amongst other things: derogations from human rights standards; limitations on procedural rights and the lowering of standards of proof in court; the use of administrative measures in place of criminal sanctions; fast-tracked legislation; the

gifting of new powers to the executive, state agencies and security bodies with little oversight; and the use of secret evidence in trials and other limitations on the ability to challenge state actions.

The report warned that the continent is on a path towards “a deep and dangerous state of permanent securitisation,” noting that:

*“Ultimately... the threat to the life of a nation... does not come from the isolated acts of a violent criminal fringe... but from governments and societies that are prepared to abandon their own values in confronting them.”*⁶

Indeed, while governments are keen to highlight that these actions are aimed at ‘fighting’ terrorism, their application has gone much further. Many of the states examined by Amnesty had invoked national security concerns to “arbitrarily target migrants and refugees, human rights defenders, activists, political opponents, journalists, minority groups, and people lawfully exercising their rights.”

These legal and policy developments have come about in an environment in which security is understood as best delivered through the importation, knowingly or not, of militaristic models of command-and-control and the widespread deployment of new surveillance technologies. The staggering advances in computing power, data storage, analytical systems and networked devices in the last two decades offer massive potential to liberate and empower individuals and to democratise societies. At the same time, the possibilities they offer for enhancing the repressive powers of states against those deemed unwanted or undesirable – through biometric identification, predictive policing systems, “less-lethal” weaponry, or the use of drones and other remote technologies – are truly frightening.

The 2003 European Security Strategy noted the world’s “increasingly open borders in which the internal and external aspects of security are indissolubly linked,”⁷ while its 2016 update referred to the “internal and external threats and challenges” that require new investments in “the monitoring and control of flows which have security implications”.

This is to be done through the deployment of “Intelligence, Surveillance and Reconnaissance, including [drones], satellite communicates, and... permanent earth observation,” along with “digital capabilities to secure data, networks and critical infrastructure.” Military power must also be enhanced: “Member States need all major equipment to respond to external crises and keep Europe safe... full-spectrum land, air, space and maritime capabilities, including strategic enablers.”⁸

These pronouncements favour what the academic Stephen Graham has described as “a radical ratcheting up of techniques of tracking, surveillance and targeting,” in which public and private spaces are transformed into “key battlespaces... requiring permanent and profitable lockdown and targeting within worlds of boundless, ambient and mobile threat.”⁹ This presumption of countless dispersed threats undermines, in the words of Eliav Liebllich and Adam Shinar, “a foundational principle of the liberal order, “that:

“[T]he state does not act upon the presumption that its citizens are threatening. When threat is presumed, there is a strong push towards preventive action... this is precisely military logic. Moreover, since there is no knowledge of a concrete threat, [police] actions will mostly be collective. They will almost certainly be based on circumstantial evidence at best or discriminatory profiling at worst.”¹⁰

The European Commission chose to launch the current iteration of the European Security Research Programme (ESRP) at the 2013 edition of Milipol, a major “worldwide exhibition of internal state security,” which claims it can provide “the know-how and innovations of every theme related to internal State security,” from fencing to night vision goggles, and communications systems to “less-lethal” weapons.¹¹ Thales, a major beneficiary of the programme, promises its government customers “the systems they need to identify, to assess and to neutralise threats” that “threaten order and sovereignty”.¹² The biggest overall recipient of ESRP funding, the Fraunhofer Group for Defence and Security, notes that due to “social and political turbulence, security is a future market with enormous growth potential.”¹³

Meanwhile, one market research firm has been even more candid, arguing that homeland security equipment and services should provide governments with “credible security” from “internal dissent”.¹⁴ What this amounts to is a militarised defence of the increasingly unequal and unsustainable social and political *status quo*, undertaken through “a new public-private partnership for homeland security... based on a simple *quid pro quo*: profit for companies and power for states.”¹⁵ As the UK’s 2010 National Security Strategy puts it: “The security of our nation is the first duty of government. It is the foundation of our freedom and our prosperity.”¹⁶ But the security of a *nation*, or a state, and the security of its people can, of course, mean very different things: prioritising the former may simply serve to buttress social inequalities that would be reduced or minimised by prioritising the latter.

The possibility of “a deep and dangerous state of permanent securitisation”; the development and implementation of militarised security technologies and doctrines; emerging forms of public-private governance that meld the narrow interests of corporations with the authoritarian tendencies of interior ministries and law enforcement agencies; and the ongoing construction of control systems and infrastructure that can be put to use by liberal and illiberal governments alike – it all makes for a toxic mix.

In this context, calls to “take back control” emanating from groups on the conservative and authoritarian end of the political spectrum – segments of the UK’s Conservative Party and UK Independence Party, Hungary’s *Fidesz* or France’s *Front National* – might appear a counter-trend. But rather than encouraging popular democratic participation and involvement based on principles of inclusion, tolerance and equality, their politics are more geared towards consolidating elite power through exclusionary laws and policies. Unfortunately, the EU does not currently offer an alternative path. While calls to embrace the EU might offer a less narrowly nationalist viewpoint, the bloc’s security policy remains driven by national governments and powerful corporate interests, underpinned by a ‘democratic deficit’ and a firm attachment to austerity economics and increasingly securitised internal and external policies.

Thus, the now-established political dichotomy between being ‘pro-Europe’ or ‘anti-Europe’ is largely irrelevant on security policy, given the embrace of the politics of fear and exclusion at both national and European levels. In some respects, it is simply a question of at what scale you would like your public-private security state to operate. For those who would rather see respect for fundamental rights, individual liberties and democratic standards take precedence over politics and policies beholden to panicked security demands and the wishes of big business, there is an urgent need to reframe debates about security and to mobilise effectively to challenge current narratives and practices at both national and transnational levels.



UK-French border fence in Calais

THE EMERGENCE OF A EUROPEAN SECURITY-INDUSTRIAL COMPLEX

“New threats have emerged that ignore state borders and target European interests outside and within EU territory... These threats call for European responses and a comprehensive security approach that addresses internal as well as external security and can combine civil and military means.” (Group of Personalities in the field of Security Research, ‘Research for a Secure Europe’, 2004)¹⁷

“Technology that protects soldiers... inevitably becomes more affordable as deployment spreads from the military to airports and then on down to commercial industries and buildings. A pleasant side effect of all the spending on anti-terror technology will be a reduction in crime.” (Mark P. Mills, ‘The Security-Industrial Complex’, Forbes, 29 November 2004)¹⁸

This section explores the EU budgets and policies developed in the early 21st century and subsequently brought into the formal EU policy-making arena. In 2007, the European Security Research Programme (ESRP) was established under the heavy influence of security, defence and technology corporations and research institutes. This came at the same time as the EU acquired more legislative and financial powers in matters related to the 'Area of Freedom, Security and Justice', leading to the acquisition of significant amounts of infrastructure for border control and law enforcement and the development of new, unaccountable, transnational bodies and networks. The projects and policies put in place during the 2007-13 period have helped to prepare the ground for their current extension and expansion – at the same time as increasingly dangerous powers are adopted by governments across Europe.

2.1 PURSUING THE “ULTIMATE GOAL”

As the EU expanded eastwards, so did the bloc’s ambitions, and it acquired new powers and budgets on security policy. €3.9 billion was available between 2007 and 2013 to implement security research projects, to implement the EU’s model of “integrated border management”, and to develop new law enforcement and critical infrastructure protection networks and procedures.



Official celebrations in Brussels for the EU's 2004 enlargement.

In 2003, the EU's fifth enlargement was agreed, through which ten new states¹⁹ would join the bloc in 2004. Bulgaria and Romania would subsequently join in 2007. In a 2004 document, the European Commission noted that while EU policies were “traditionally... centred on the agriculture sector, on cohesion, on the creation of an integrated internal market and on the achievement of macroeconomic stability,” there were some new priorities for the enlarged EU. Alongside the completion of the internal market, key aims were for the EU to assume “a coherent role as a global partner,” including by “contributing to civilian and strategic security”, and “the completion of an area of freedom, security and justice [AFSJ] and access to basic public goods.”

The AFSJ and European citizenship itself were “associated with the European and economic social model,” requiring clean air, water and soil, high-quality and safe goods and food, and the provision of “health and education, energy supplies, transport, telecommunications or postal services.” Yet just as the EU acquired a greater role and increased funding in the realm of security, the onset of the financial crisis saw the European Commission also take on a key role in enforcing austerity measures. In countries across Europe, the Commission has helped enforce programmes to dismantle welfare states and cut social services. As social security in the traditional social-democratic sense was under attack, homeland security was on the ascent.

Crucial to the EU's new role in security was the adoption in 2003 of the European Security Strategy. This argued that “Europe faces new threats which are more diverse, less visible and less predictable,” particularly terrorism, the proliferation of weapons of mass destruction, failed states and organised crime.”²⁰ There followed a two-track process: one was the establishment of the €1.4 billion European Security Research Programme (ESRP), a process dominated by big business and state officials; the other was the introduction of new EU security budgets dealing with border control (€1.8 billion), the “fight against crime” (€600 million) and “terrorism and other security-related risks (€140 million). This was a significant step towards the “ultimate goal” outlined by the European Commission in 2004: having “budgetary means at the service of a political/economic objective”.²¹

The ESRP began with a European Commission decision to establish a ‘Group of Personalities’ (GoP) to offer “guidance”. The Commission cited the need “to have the most technologically advanced instruments for anticipating new security threats and dealing with them in a way that serves [the EU's] interests and respects its values.”²² The GoP was made up of representatives from the EU, national defence ministries and research institutes, and Europe's largest arms and IT companies. Four MEPs also took part in the group, which first met on 6 October 2003.

Four days later, the Commission announced that the GoP's recommendations would "be included in a Communication to be presented by the Commission by the end of 2003." It appeared in February 2004, essentially reproduced the recommendations of the GoP (whose report would be published a month later) and announced that the Commission "had already established a 65 million euro budget line for a 'Preparatory Action for Security Research' [PASR]," which would act as a foundation for a formal European Security Research Programme from 2007 onwards.²³

From 2004 to 2006 the PASR funded 39 projects dealing with five priority areas:

- "Improving situation awareness", i.e. surveillance and intelligence-gathering;
- "Optimising security and protection of networked systems";
- "Protecting against terrorism";
- "Enhancing crisis management"; and
- "Achieving interoperability and integrated systems for information and communication" (linking national and international law enforcement and security databases and communications systems).

23 of the 39 projects were led by companies whose primary interests lay in selling arms and other military equipment. PASR also financed projects aimed at the long-term development of EU security policy and research.²⁴ Between 2002 and 2006 the EU's 6th Framework Programme on research and development (the predecessor to the 2007-13 FP7) and the PASR funded over 200 projects concerned with the GoP's priorities.²⁵

In September 2004 another Commission communication promised to establish a 'European Security Research Advisory Board' to advise on the content and implementation of the ESRP, "paying due attention to the proposals of the Group of Personalities"; to establish the European Security Research Programme from 2007 onwards; and to ensure that the ESRP was closely linked with other EU policy areas, such as foreign affairs, internal security and defence.²⁶

The Commission's informal decision to establish the GoP was taken without a clear legal basis, but it was not the only questionable part of the whole process. The decision to award €65 million to the PASR was taken without any consultation of the EU's Member States or the European Parliament, and the legal basis cited by the Commission was "competitiveness of the Community's industry (Article 157 of the EC Treaty), when arguably it should have been "research and technological development" (Article 163(3)). Despite these irregularities, the security research programme steamed ahead. An interim evaluation of

the PASR found that the programme "strengthened the Commission's institutional capacity to implement EU security research," as well as providing "a useful testing ground to establish what types of projects and research topics would be effective in contributing to the strategic aims of the future ESRP."²⁷

Further contributions to this end came from the European Security Research Advisory Board (ESRAB), established by a Commission Decision in 2005. As with the setting up of the GoP, European and national parliaments were not consulted. Nominations for membership of the group came from Member State officials, the European Defence Agency and "other unspecified 'stakeholder groups'."²⁸ ESRAB's mandate was to advise the Commission on, among other things, "strategic missions and priority areas for future security research", but it "appears to have had less to do with research than the needs of commerce and the objective of better integrating the supply chain (corporations) with the demand chain (governments)."²⁹ 14 out of the 50 seats went to the defence and security industries, with the rest taken up by Member States (18 seats), academics and research institutes (14 seats) the European Defence Agency and Europol (one seat each), and two groups described as "civil liberty groups and think tanks." A closer analysis suggested that whatever they were, civil liberty groups they definitely were not.³⁰

The final ESRAB report was published in September 2006 and set the priorities for the €1.4 billion security theme within the EU's 7th Framework Programme for Research and Technology Development's (FP7), which ran from 2007 until 2013 with a total budget of over €50 billion. The 2009 Statewatch/Transnational Institute report *NeoConOpticon*, highlighted ESRAB's priorities for security research:



*"[I]mpose total surveillance (so-called 'situation awareness and assessment')... introduce identity checks and authentication protocols based on biometric ID systems; deploy a range of detection technologies and techniques at all ID control points; use high-tech communications systems to ensure that law enforcement agents have total information awareness; use profiling, data mining and behavioural analysis to identify suspicious people; use risk assessment and modelling to predict (and mitigate) human behaviour; ensure rapid 'incident response'; then intervene to neutralise the threat, automatically where possible. Finally, ensure that all systems are interoperable so that technological applications being used for one mission can easily be used for all the others."*³¹

And thus the scene was set for security research under FP7, which funded a vast number of projects investigating a bewildering array of high-tech, intrusive and repressive technologies and systems (see section 2.2).

At the same time, the EU's first dedicated budgets for security policy were on the verge of coming into being. In May 2007 the European Parliament and the Council of the EU reached agreement on the €1.8 billion External Borders Fund (EBF) as part of the 'Solidarity and Management of Migration Flows' programme, which also included the European Return Fund (€676 million), the European Refugee Fund (€630 million) and the European Fund for the Integration of third-country nationals (€825 million). The EBF was dedicated to managing the EU's external borders "in an integrated way, to welcome legal immigration... and protect from illegal entrants," with a key objective being the creation of "the European Border Agency [Frontex] to pave the way for the creation of a European Border Guard Corps" (see section 2.3).

The EBF was accompanied by the Prevention of and Fight against Crime (ISEC) and Terrorism and other Security-related Risks (CIPS) programmes, worth €600 million and €140 million respectively. The EU's law-making setup at the time meant their respective legal bases were adopted by the Council alone – the European Parliament did not obtain "co-decision" on justice and home affairs legislation (other than that dealing with migration) until the Lisbon Treaty came into force in December 2009.

The ISEC budget sought to:

"contribute to a high level of security for citizens by preventing and combating crime, organised or otherwise, in particular terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud."

While CIPS aimed to:

"stimulate, promote and develop measures on prevention, preparedness and consequence management based, inter alia, on comprehensive threat and risk assessments... and aiming to preventing [sic] or reducing risks linked with terrorism and other security related risks."

The funds and legislation agreed during this period developed and reinforced a whole host of novel systems and bodies: financial intelligence units for the analysis of banking data; DNA, fingerprint, vehicle registration, criminal records and air passenger data collection and exchange systems; networks to "counter" drug trafficking, violence against and sexual exploitation of children, and human trafficking; new tools to deal with cybercrime; transnational counter-radicalisation networks; and critical infrastructure protection methodologies

and tools. The funds have also paid for the work of "monopoly networks" such as ATLAS (a network of national specialist counter-terrorism units), RAILPOL (rail policing), AQUAPOL (waterways), AIRPOL (airports) and TISPOL (road policing). In 2009 these informal networks were recognised by the European Commission as "de facto monopolies" at a European level in their respective areas of expertise.³²

The coming into force of the Lisbon Treaty at this time also led to significant institutional changes in the EU. The European Parliament obtained full negotiating powers over new legislation in justice and home affairs (previously it could only co-legislate on migration-related legislation), and the EU adopted an Internal Security Strategy (ISS) to complement the 2003 European Security Strategy. Responsibility for overseeing the implementation of the ISS went to the Standing Committee on Operational Cooperation on Internal Security (COSI), a secretive working group within the Council that continues to expand its strategic remit, yet suffers from a significant transparency and accountability deficit (see section 2.4).

The €3.9 billion total of the security research, borders and crime and terrorism budgets between 2007 and 2013 may not be much in comparison with the total EU budget of almost €1 trillion during the same period, but it is a vast amount of money in its own right and highly significant given that the EU previously had no such dedicated budgets. Equally, while the available information suggests that the budgets and accompanying laws, policies and projects did not achieve all they set out to, they have led to significant developments in the construction of new security institutions, agencies and networks operating at European level.

2.2 SECURITY RESEARCH: A €1.4 BILLION NETWORKING EXERCISE

The demands of the industry lobby came through loud and clear in the projects funded by the €1.4 billion for security research between 2007 and 2013, and corporate participants were one of the biggest financial beneficiaries. Nevertheless, funding appears to have been more useful for network-building than developing new security technologies.

The '7th Framework Programme for Research and Technology Development', known more simply as FP7, was launched in 2007 and ran until 2013. Its total budget of €51 billion represented a 63% increase on FP6³³ and €1.4 billion was made available to the ESRP, which was formally integrated into the programme under the "security" theme and eventually funded over 300 separate research projects.

The formal objectives of the programme were laid out in legislation adopted in 2006:

“To develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security, to stimulate the cooperation of providers and users for civil security solutions, improving the competitiveness of the European security industry and delivering mission-oriented research results to reduce security gaps.”³⁴

The resulting projects covered everything from border control robots to the development of new “innovation management” strategies for law enforcement authorities. The content of some of the projects suggests that the requirement to “respect fundamental human rights including privacy” was little more than window-dressing.

The scope of the “threats” that projects sought to address extended from transnational organised crime and large, complex natural and man-made disasters to “petty crime”, misuse of the international postal system³⁵ and even railway graffiti.³⁶ From surveillance drones to automatic tracking and tracing systems, “intelligent decision support” software for crisis management situations and automated data-mining software for investigating money laundering and terrorist financing, to “innovation management” techniques and open and closed source data-gathering and processing systems, the overall picture is a high-tech, public-private system of monitoring and control in the name of the “security of the citizen”.

The structure of the ESRP in FP7 essentially matched that proposed by the ESRAB, and was based on four “mission areas” and three “cross-cutting areas”. The table below shows the topics accompanied by figures from the final evaluation of the FP7 ESRP, showing the percentage of total projects and funding in each.³⁷

TABLE 1: DISTRIBUTION OF FUNDING BY RESEARCH THEME IN THE FP7 EUROPEAN SECURITY RESEARCH PROGRAMME

FP7 topic	ESRAB proposal	No. of projects	% of all projects	% of all funding
Security of citizens	Protection against terrorism and organised crime	55	18%	19%
Security of infrastructure and utilities	Critical infrastructure protection	52	17%	20%
Intelligent surveillance and border security	Border security	31	10%	17%
Restoring security and safety in case of crisis	Restoring security in case of crisis	55	18%	23%
Security and society	No proposal	46	15%	9%
Systems integration, interconnectivity and interoperability	Systems integration, interconnectivity and interoperability	31	10%	8%
Security research coordination and structuring	No proposal	34	11%	6%
Other	N/A	3	1%	0%

Projects were undertaken by consortiums primarily made up of corporations and other companies, research organisations, higher education institutes, state agencies and ministries. However, corporations and major research institutes took the majority of funding. The top corporate recipients were:

- Thales (€28.5 million, 63 projects);
- Selex (€23.2 million, 54 projects);
- Airbus (€14.2 million, 32 projects);
- Indra (€12.3 million, 16 projects);
- Isdefe (€10.5 million, 16 projects);
- BMT Group (€9.5 million, eight projects);
- Morpho (€8.8 million, 19 projects);
- Atos (€7.6 million, 16 projects);
- BAE Systems (€6 million, 10 projects) and
- Vitrociset (€5.7 million, 10 projects).

In total, private companies took almost €552 million from the FP7 ESRP budget, some 40% of the €1.4 billion total.

The single largest overall recipient of funding was the German research institute Fraunhofer, which received €51.5 million for its role in 85 projects. It was followed by:

- the Dutch organisation TNO (€30 million, 54 projects);
- the Swedish Defence Research Institute (€31.8 million, 53 projects);
- France’s *Commissariat à l’énergie atomique et aux énergies alternatives* (€15 million, 39 projects);
- Finland’s VTT Research Centre (€12.4 million, 29 projects);
- the European Commission’s Joint Research Centre (€6.1 million, 27 projects);

- Greece's Center for Security Studies (€5.8 million, 27 projects);
- the Austrian Institute of Technology (€12.8 million, 22 projects);
- Greece's Demokritos research centre (€7 million, 19 projects); and
- Italy's National Research Council (€3.7 million, 16 projects).

Research institutes overall took 25% of the budget, some €348 million.

Aside from winning large chunks of the ESRP budget, corporations and research institutes were also able to obtain greater funding per project compared to their counterparts from other types of organisation. According to the formal, final evaluation of the FP7 ESRP produced by Technopolis group and published in September 2015, each time private companies participated in a project, they took almost 25% more money on average from the ESRP than they did from counterpart research programmes such as health, ICT, energy, environment and transport, amongst others. Research institutes took 10% more, while public bodies received somewhat less, just 86% of the average rate across all research programmes.³⁸

Many of the top beneficiaries of ESRP funding were represented in the Group of Personalities and ESRAB, which had helped design the overall security research programme, and many of them also held seats from 2007 to 2013 on the Security Advisory Group (SAG), which sets the agenda for the annual ESRP work programmes. In 2007, "five out of 20 SAG experts were working for organisations affiliated to EOS" (the European Organisation for Security, Europe's main security industry lobby group) and when the group's membership was renewed in 2010 that number climbed to seven out of 22.³⁹ TNO, the Swedish Defence Research Institute and Fraunhofer were also members, along with the Polish Border Guard, the German Federal Criminal Police, the General Inspectorate of the Romanian Police, the Estonian, Italian, Spanish and UK interior ministries, and the European Defence Agency, amongst others.⁴⁰ The dominance of corporate, state and research institute representatives has not altered significantly in the SAG's successor, the Protection and Security Advisory Group (see section 3.7).

The work programmes are ultimately approved by state officials sitting in the Programme Committee, but the SAG's agenda-setting role means that individuals are able to push for the prioritisation of research topics of interest to their organisations.⁴¹ *NeoConOpticon* highlighted this issue, noting that:

"[T]he failure to clearly separate the design of the programme (and setting of its priorities), on the one hand, from the would-be applicants (and their clamour for funding), on the other, has engendered a structural conflict of interests."

This chimes with the findings of a study undertaken for the European Parliament (EP) in 2010, which concluded that security research is addressed "through the concerns of security agencies and services and the industry, without taking into account the requirements flowing from the EU's internal area of freedom." Furthermore, the study found, a "large proportion" of FP7-funded projects are "dedicated to developing technologies of surveillance, to the detriment of a broader reflection on the impact of such technologies for citizens and persons concerned with the EU's security policies," and while future research proposals "indicate a growing awareness for questions of fundamental rights and freedoms", they "remain overly framed by the concerns of the defence and security industry and national and European security agencies and services."

There have been changes in the overall make-up of the advisory group over the years, shifting the balance between industrial and other interests to varying degrees. Nevertheless, ensuring greater industry involvement in its strategic direction and in the resulting projects is now an explicit aim of the European Commission. A former chairman at military and security lobby group ASD is now chair of Protection and Security Advisory Group (the latest name for the SAG) for precisely this reason (see section 3.4). It seems that, for the time being at least, the conclusions reached by a 2014 report for the European Parliament will continue to be relevant:

*"Security research puts research at the service of industry rather than society. This move is grounded in the assumption that support to industry will lead to job creation and growth across all sectors, including the security sector. This assumption overrules all other societal considerations, which are relegated to preoccupations with societal acceptance of security technologies."*⁴²

This is not to say that "societal considerations" have not been an issue in the ESRP. The need for compliance with fundamental rights, democratic values and ethical standards has been noted repeatedly in the multitude of documents on security research emanating from EU institutions and high-level advisory groups since the early years of the 21st century, and over time attempts to ensure that security research projects meet ethical requirements have become more thorough, detailed and consistent.



The Technopolis report contains a case study highlighting some of the issues surrounding ethics in security research. It notes that: “the Security Research programme had among the highest number of ethical reviews” in the FP7 cooperation theme (only ICT and health research had more), and that the available data suggests that there were at least 90 ethical reviews of FP7 projects that were eventually funded (of over 300), “which is much higher than the 10% rate seen in FP7 overall.”

In FP7 all projects proposals considered eligible for funding were subject to an ethics screening by independent experts contracted by the European Commission. If significant concerns were highlighted the proposal would be subject to an ethics review by independent experts specialising in ethics, the recommendations of which would be “taken into account in subsequent grant negotiations and can lead to obligatory provisions in the conduct of the research,” and projects can also be subjected to a further ethics audit designed to ensure issues raised are taken into account.⁴³ The process is broadly similar in Horizon 2020.⁴⁴

Criticism directed at the ESRP – regarding, for example, conflicts of interest in the design of the programme and a lack of concern over the development of intrusive technologies⁴⁵ – led to a greater focus on ethical issues and “societal considerations” in the annual FP7 work programmes. Potential participants were encouraged to give greater consideration to potential ethical issues, with some including parallel ethical research in their work or setting up an ethical advisory board as part of the consortium.⁴⁶ An increasing number of individual projects focusing on ethical issues were also funded,⁴⁷ and the ESRP work programmes in Horizon 2020 continue to emphasise the need for projects to meet ethical requirements and comply with privacy and data protection standards.

All this is undoubtedly welcome. But the question that remains is whether the approach in place, which seeks to ensure compliance with ethical standards both in the research process itself and (albeit with less emphasis) in any technologies or products that are the result of that process, will ever be able to take into account concerns over the dominant conception and implementation of security technologies and policies.

This is, at heart, a far broader political question that requires rethinking current approaches to security based on the identification and neutralisation of “threats” isolated from their broader socio-economic environment. A rigorous ethical approval process is necessary in any research programme, but it is unlikely to overcome the political environment by which it is framed. As argued in a report produced for the ESRP-funded SURPRISE project:

“Security policies... have increasingly adopted a conceptual approach to security problems that is strongly solution-driven and tends to neglect the variety and complexity of social, economic, technical and political factors that may have caused those security problems in the first place.”⁴⁸

Funding these technological “solutions” was of course one of the key goals of the ESRP from its inception. Yet despite the significant amount of money on offer, the programme largely failed to achieve its aim of developing new security technologies. A survey undertaken for the Technopolis report found that the programme had:

“[A] positive impact on each of its specific objectives. The great majority of participants (75%+) hold this opinion. There is very little difference in the feedback, objective by objective. However, on balance, a greater share of participants believes the programme has made a substantial contribution to the ‘developing technology to build capability’ objective (85%).”

This might have been the opinion of those asked by the evaluators, but the numbers suggest a different picture. Of the 61 fully completed and assessed projects examined:

“There are seven projects (11%) – spread across five mission areas – that have reported at least one IPR [intellectual property registrations]. Between them, these projects reported a total of 19 intellectual property rights, including 10 reported as a patent application. This is the equivalent of one IPR reported for every €7.7 m of EC contribution (for the full set of 61 projects), and one patent application for every €16.3m of EC contribution...”

The study does not offer comparative figures, but this certainly seems like an expensive investment in economic activity. A 2010 study undertaken for the Commission seemed to offer a forewarning of this problem: “The EC security research programme certainly represents a considerable effort which has attracted many companies, but has not led so far to important procurement programmes.”⁴⁹ Indeed, the Technopolis report noted that of all the research themes sitting under the FP7 ‘Cooperation’ heading (which also covers health, transport, space and the environment, amongst other things), security research was “in the lower quartile” for all key performance indicators such as academic publications and IPR registrations. A case study on intellectual property resulting from security research noted that there are a host of potential reasons behind this, but that nevertheless: “given the largely applied, near-term nature of much of the Security Research programme, it is perhaps surprising that more projects are not reporting IPR.”⁵⁰

Whatever might be said about IPR, academic publications and other key performance indicators, however, the Technopolis report argued that “none of these really capture the focus of the Security Research Actions.” The benefits instead may have been less tangible: “the programme has improved the connections between the providers [corporations and research institutes] and users [state agencies] of novel civil security solutions,” allowing them to “to develop common concepts, terminology, open interfaces, middleware, etc. that will in turn facilitate improved multilateral and cross-border cooperation.” As an EU official at the 2013 Milipol “internal state security” exhibition put it, the FP7 ESRP has led to the development of a “true European security research community.”⁵¹

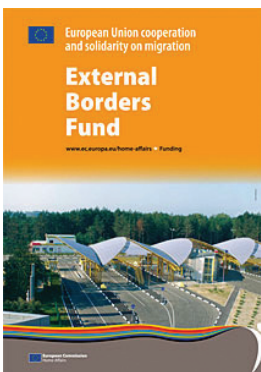
Seen from this perspective, the ESRP in FP7 has the appearance of a €1.4 billion networking exercise, and a cash cow for corporations and research institutes. As the next sections explore further, the development of new networks and communities aimed at helping the EU and its Member States deal with “new threats which are more diverse, less visible and less predictable” was also a key feature of other EU security budgets during the 2007-13 period.

2.3 REINFORCING THE FORTRESS

Formal evaluations of the EU’s 2007–13 External Borders Fund have provided scarce information on what the money has achieved, but the information that is available shows a significant emphasis on implementing policies detrimental to the rights of migrants and refugees.

While critics of the EU’s migration policies had long-used the phrase ‘Fortress Europe’ to condemn the way in which the bloc and its Member States sought to deter refugees and “irregular” migrants, it was during the 2007-13 period that the EU began providing regular funding to the Member States to help procure the surveillance systems, technical equipment and information networks deemed necessary for implementing the EU’s model of “integrated border management”. The €1.8 billion External Borders Fund (EBF) aimed to ensure the management of the EU’s borders “in an integrated way, to welcome legal immigration... and protect from illegal entrants,” with objectives including further operational

cooperation amongst Member States, the development and improvement of border surveillance systems, and increasing the exchange of information between national authorities.⁵²



Countries participating in the EBF



A formal evaluation of the External Borders Fund is due towards the end of 2017, but it is not clear if it will be of much use. A Commission planning document notes that the fund was adopted without common statistical requirements. Different “indicators” for the assessment of projects are used in each Member State, making it “impossible to aggregate them at the EU level.” There is “considerable risk” that national authorities will not comply with the “common indicators” drawn up after the programmes were agreed.⁵³

Gathering comparable data on the use of the EBF by Member States is not the only problem with the programme. In 2014 the European Court of Auditors (ECA), responsible for examining the lawfulness of spending, raising and accounting for EU funds, issued a damning report on the implementation of the EBF based upon investigations in five Member States: Greece, Italy, Malta, Poland and Spain. The ECA concluded that:

“The... EBF has contributed to external border management and fostered financial solidarity. However its further EU added value was limited, overall results could not be measured due to weaknesses in the responsible authorities’ monitoring and there were serious deficiencies in the ex post evaluations by the Commission and the Member States. Crucially, the audit found serious weaknesses in the management of the fund in key Member States, i.e. in Greece, Spain, Italy and, for the early funding years, Malta... The Court found that it was not able to assess the extent to which the EBF has supported the

*fund's priorities... Despite the low quality of the objectives and indicators, the Commission approved the Member States' programmes in view of the need to implement the fund.*⁵⁴

Amongst other things, the Commission approved – whether knowingly or not – the purchase and rental of hundreds of vehicles that, on paper, were to be used by the Italian authorities in border surveillance and identification operations at the country's southern sea borders. They were ultimately used for other purposes. In one case, new vehicles were deployed in and around detention centres “as far north as Turin, Milan and Bologna and were not involved in the surveillance of the external border”. In another case, increased numbers of vehicles were bought “primarily due to extra funds being available” and “are also used for ‘regular’ police work.”⁵⁵

More disturbingly, funding was provided for a detention centre in Mytilene, on the Greek island of Lesbos, where the conditions were described as “abominable” by the European Committee for the Prevention of Torture and which the UNHCR said should be shut down. As the ECA report notes: “At the time of the decision to fund the project, the unacceptable conditions were widely known,” although the Commission was apparently given a “misleading project description” by the Greek authorities. It will claw back the money used to fund the centre, which was “deactivated” between October 2009 and June 2010.

Unfortunately, it would seem that lessons have not been learnt from this sorry episode. EU funding (this time from the Internal Security Fund) is once again paying for detention centres on Greek islands. An April 2016 report by *Amnesty International* found that thousands of people were being detained on Lesbos and Chios following the conversion of the EU's “hotspots” – set up to register and process refugees and migrants – into closed detention centres. Conditions remain appalling. An Amnesty press release said:

*“No asylum seeker should be automatically detained, and these detention centres on Lesbos and Chios are not in any way fit for purpose for the many young children, people with disabilities, or people with urgent medical needs we've met. They must be released immediately.”*⁵⁶

The EBF has also co-financed offices at the Spanish-Moroccan borders in Ceuta and Melilla in which people can – in theory – apply for asylum. In practice, the offices are located behind multiple, three-metre high, razor-wire topped fences that have been erected by the Spanish authorities and which serve to prevent people from exercising their right to apply for international protection.

While the Commission officially refuses to fund border fences, it has had no qualms about supporting the Spanish system of “border management” through financing “CCTV camera-equipment” in Ceuta and “a watchtower in Melilla,” (€164,000 in 2010),⁵⁷ the establishment in both enclaves of “police offices to manage procedures related to the irregular influx of migrants” (€448,000 in 2012) and “reinforcement of resources of the State security forces in Ceuta and Melilla” (almost €4 million in 2012).⁵⁸ Reports by civil society organisations and journalists have repeatedly condemned the situation in the two enclaves, but the European Commission has apparently satisfied itself that Spanish policy and practice is, on paper at least, in conformity with EU and international norms.⁵⁹



A demonstration against Spanish and EU border policies in Ceuta, one of Spain's enclaves in North Africa.

The Commission's own mid-term evaluation of the EBF (which was not published until 2014) was rather more upbeat than the ECA's report:

*“[T]he EBF is fulfilling its purpose as an EU tool for co-financing investment in the external borders and in the consulates of participating countries. In so doing it serves the interests of the Schengen area as a whole and is achieving visible, lasting results.”*⁶⁰

The report noted that: “According to most Member States, many actions would have been impossible or less effective without the EBF,” and the improved inspection and surveillance abilities funded by the EU “resulted in fewer illegal crossings, more visa applications, and fewer apprehensions.” Indeed, some Member States reported that the EBF financed a significant proportion of their spending on border management, visas and IT equipment for border control between 2007 and 2010⁶¹ – but given a lack of common statistical indicators and recording methods, making use of the figures is rather difficult.

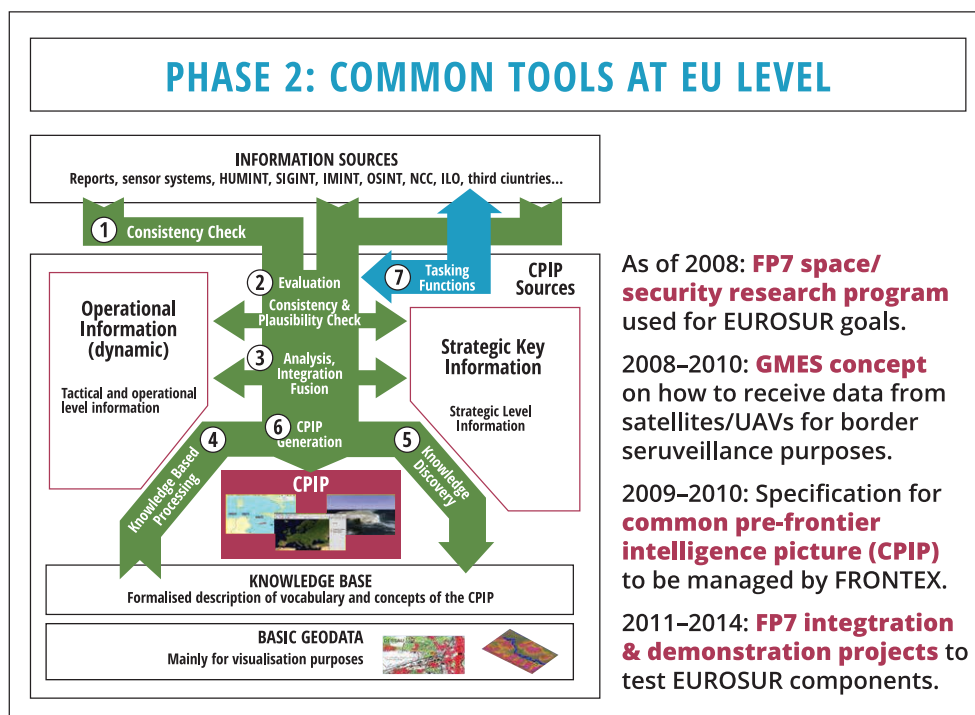
Nevertheless, it is worth highlighting some of the “visible, lasting results” mentioned in the Commission's report. Across the EU, a vast amount of infrastructure and new technology was acquired by national authorities, including:

- 3,153 vehicles (boats, helicopters, motorbikes, and more);
- 545 border surveillance systems covering 8,279 kilometres of the EU's external borders;
- 22,347 items of "operating equipment for border surveillance" (for example thermal imaging systems, video surveillance equipment, night vision goggles, "camouflage and protection equipment") and 212,881 items of "operating equipment for border checks" (such as document verification equipment and fibre-optic networks);
- 710 new places in detention facilities;
- upgrades to consulates ("210 visa sections newly built or renovated, 257 pieces of equipment purchased to upgrade security");
- the development of national systems connected to the EU's Visa Information System, Schengen Information System II and Eurosur;
- the training of 32,594 staff in EU border and visa legislation.

With regard to border surveillance equipment, the report notes that Spain acquired more than any other Member State, adding 386 items to its *Sistema Integrado de Vigilancia Exterior* ('Integrated Exterior Surveillance System', SIVE): "This enabled Spain to intercept 5,239 irregular migrants and improve the security of its maritime border, reducing irregular migration to the Canary Islands by 17.5%." The experience of SIVE has been useful in the development of the EU-wide Eurosur border surveillance system, and Spanish companies and state institutions have played a prominent role in many of the FP7-funded projects geared towards this end.

A major effort was PERSEUS (Protection of European seas and borders through the intelligent use of surveillance), which aimed to "build and demonstrate an EU maritime surveillance system integrating existing national and communitarian technologies and enhancing them with innovative technologies." Partners included Indra, NATO, Airbus, EADS, the Spanish Guardia Civil, Saab and Boeing. The EU contributed almost €28 million from a total cost of over €43 million.⁶² The report's final summary was keen to highlight its role in developing the Eurosur surveillance system through the testing and integrating of technologies to "collect, process, fuse and exploit data coming from a variety of heterogeneous sensors [different kinds of sensors, in plain English], while 'closing the operational loop' through tasking and efficient control of our border surveillance assets."⁶³

Alongside PERSEUS, other projects that supported the development of maritime surveillance and control systems included AMASS (€3.5 million contributed by the EU),⁶⁴ CLOSEYE (€9.2),⁶⁵ I2C (€9.9 million),⁶⁶ OPARUS (€1.2 million),⁶⁷ OPERAMAR (€670,000),⁶⁸ SEABILLA (€9.8 million),⁶⁹ SUNNY (€9.6 million),⁷⁰ TRITON (€1.5 million),⁷¹ WIMAAS (€2.7 million),⁷² SAGRES (€3.4 million),⁷³ LOBOS (€2 million)⁷⁴ and DOLPHIN (€4 million).⁷⁵ The latter three were funded by the FP7 space budget, rather than security, and sought to make use of satellite surveillance and monitoring to help develop the "concept of operations" for Eurosur. The prior five were concerned with the development and testing of surveillance technologies (for example drones and sensor networks), the improvement of on-board ship identification systems and the integration of existing systems.



A slide from a European Commission presentation outlining the process foreseen for developing Eurosur.

A small number of organisations were prominent within these projects. 148 organisations participated overall, with 211 participations in total (different divisions or subsidiaries of the same organisation may participate multiple times in one project). However, 14 organisations⁷⁶ took part in three or more projects each, participating 54 times overall (26% of the total), receiving collectively almost €26 million (30%) of the €85.3 million granted.

Similar observations can be made with regard to the development of “smart borders” – the automation of border control processes such as security screening and identity checks in order to facilitate a great number of travellers, at the cost of extensive data collection and processing. In 2008 the European Commission formally pronounced its interest in the idea,⁷⁷ and in 2013 it proposed legislation which was knocked back by the Council of the EU and the Parliament. Further proposals (now under discussion, see section 4.3) appeared in April 2016, but in another example of the conjunction between the democratic deficit and technological research and development, the ESRP had by this time been funding the relevant technologies and procedures for years.⁷⁸

Projects aimed at supporting the smart borders project include ABC4EU (EU contribution of €12 million),⁷⁹ FASTPASS (€11.3 million),⁸⁰ FIDELITY (€12 million),⁸¹ INGRESS (€3.2 million),⁸² MOBILEPASS (€3.1 million),⁸³ TERASCREEN (€3.5 million)⁸⁴ and XP-DITE (€10 million).⁸⁵ These looked at technologies and procedures for automated border control gates, enhanced passports, improved security checkpoints and screening technologies. As with Eurosur-related projects, a relatively small number of organisations dominated the projects mentioned above – 16 of the 99 participating organisations featured in 36 of the 110 projects, obtaining 39% of the funding (€20.7 million of €31.7 million).

The foreseen introduction of smart borders is heavily reliant on the use of biometric technology. INGRESS (Innovative Technology for Fingerprint Live Scanners), led by Safran and with a total of €3.2 million funding from the EU (total cost, €4.2 million), focused on “border control and law enforcement applications” and aimed to develop new types of:

“high-quality fingerprint images that will still be compliant with programs and applications currently using digital fingerprints as a mean of authentication or identification (EU-Passport, EURODAC, VIS, Entry/Exit, Registered Traveller Program or other European and national applications).”

The benefits? “Thanks to INGRESS, more efficient and accurate fingerprint live scanners will have an impact on the quality of life for the citizen who will be able to spend less time in identity checking.” Except, that is, when there are more identity checks:

“Biometrics sub-surface sensors will enable to use eID documents more often and will democratise their use... this will make possible to use fingerprints more easily in many areas: electronic identity documents[,] credit cards, loyalty cards or future e-documents including fingerprints. The majority of users already see biometrics as convenient. With these innovative sensors, it is to be available everywhere for everyone.”⁸⁶

That such a development would be positive is a widely-shared view amongst state officials and industry representatives, who do not seem to be concerned by the possibilities for pervasive control and monitoring of individuals, nor the fact that many people would consider repeated demands for their fingerprints as an unwarranted and intrusive request for constant submission to authority. Joerg Sauerbrey, head of public security at Siemens, put it like this in 2008: “Based on current developments, a global identity management system and electronic documents with biometric functions may also become an everyday reality.”⁸⁷



The border control robot developed by the TALOS project: “may be too complex” to be put into use, according to the project consortium.

Demands for more stringent border security also led to one of the most visibly-controversial projects to come out of the ESRP in FP7: TALOS (Transportable Autonomous Land Order Surveillance). This sought “to develop and field test the innovative concept of a mobile, modular, scalable, autonomous and adaptive system for protecting European borders” – in simpler terms, robots for the surveillance and control of land borders, and the associated communication infrastructure. The project partners claimed it would have the ability to “undertake the proper measures to stop the illegal action almost autonomously with supervision of border guard officers.”⁸⁸

Partners in the TALOS project included Israel Aerospace Industries, Hellenic Aerospace Industry and *Przemysłowy Instytut Automatyki i Pomiarów* (PIAP, a Polish robot and automation equipment manufacturer). The EU provided nearly €13 million of a total cost of €19.5 million.

The resulting product was a clunky, bulky mini-tank rather than a sleek science fiction fantasy,⁸⁹ that the project consortium admits “may be too complex” for border agencies to put into use. Nevertheless, the policies and ideas that led to its development remain firmly in place. The project’s final report noted that “it is possible to envisage the transition of assistance vehicle drivers into operators and high-level controllers of fleets of unmanned vehicles”.⁹⁰ This vision of semi-autonomous border security remains a key theme of the ESRP in Horizon 2020, the follow-up to FP7 that runs from 2014 until 2020.

One of the key outcomes of the EU’s border security efforts, then, has been to distribute funding to companies that have a vested interest in the further securitisation

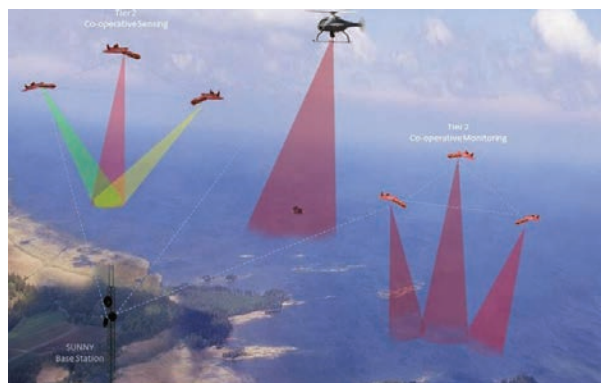
of Europe’s borders through the deployment of various surveillance and control technologies. While in many cases technology development through the ESRP may not have been entirely successful, the provision of funding for such projects is a clear indication of the aims of European “integrated border management” policy, with all its accompanying inconsistencies. It has been observed by Dutch researcher Mark Akkerman that amongst the

companies hoping to “secure” Europe’s borders “are some of the biggest arms sellers to the Middle-East and North-African region, fuelling the conflicts that are the cause of many of the refugees.” For example, “Finmeccanica, Thales and Airbus, prominent players in the EU security business are also three of the top four European arms traders, all active selling to countries in the Middle East and North Africa.”⁹¹

Meanwhile the ESRP has no doubt helped to develop and integrate networks of state officials, corporate representatives and others with a vested interest in the high-tech model of border control favoured by the EU. EU funding through the EBF has also contributed to the development of networks based less on technology and more on people, for example by financing the work of Immigration Liaison Officers (ILOs). These officials are posted abroad by national authorities and Frontex to “gather information from certain third countries of origin or transit of international migration with a view to contributing to sufficient management of this phenomena.”⁹² EBF funding paid for postings to Kenya, Iraq, Angola, Cape Verde, Algeria, Ukraine, Moldova, Georgia and Belarus, amongst other places.

These ideas remain in vogue and are being taken up with gusto across the continent. The successor to the EBF, the Internal Security Fund – Borders, is continuing the practice of equipping national authorities with more resources to implement and extend these policies. The

ESRP remains on hand to develop the technologies and practices needed to do so.



Maritime surveillance as foreseen by the SUNNY project.

2.4 THE LONG ARM OF THE LAW

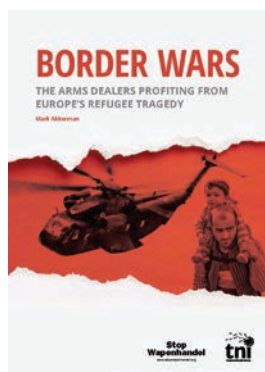
Budgets introduced to support national law enforcement agencies have contributed to the development of little-known transnational policing networks, the spread of interconnected DNA databases, the introduction of travel surveillance and profiling systems and the establishment of bodies for financial surveillance and analysis.

As money from the EBF was flowing to Europe’s border control authorities, the ISEC (€600 million) and CIPS (€140 million) funds were helping to enhance national and transnational policing powers and the protection of “critical infrastructure”.⁹³ As with the EBF, final evaluations of the ISEC and CIPS budgets are yet to be published, although a mid-term evaluation was carried out. A subsequent Commission Communication noted that:

“During the 2007 – 2009 period, the Programs cumulatively supported nearly 400 projects and financed approximately 150 procurement contracts, worth a total of €213 million. ISEC allocations amounted to €167 million for CIPS to €46 million.”⁹⁴

The Commission, and the external evaluation on which it based its mid-term report, argued for the importance of the projects:

“[T]he achievement of permanent changes in operational procedures/practices emerges as the most common impact, but many projects are also expected to achieve a permanent capacity building effect and to contribute to shape the policy debate. Of particular importance, is the contribution of many projects to the implementation of specific EU policies or pieces of legislation, such as the Prüm Decision, the Council

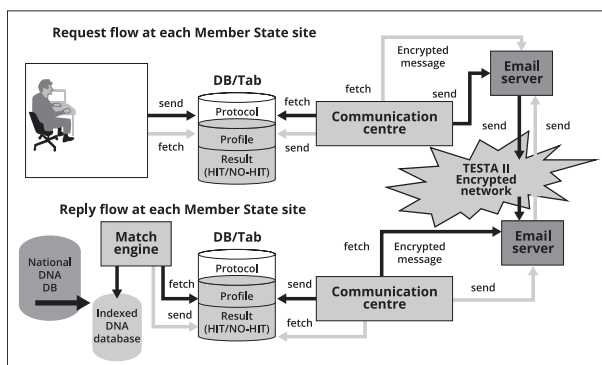


Framework Decision on the violence against children, the Decision on financial intelligence, and – as concerns CIPS – the European Program for Critical Infrastructure Protection.”



Co-funded by the Prevention of and Fight against Crime Programme of the European Union

The Prüm information exchange network was set up to ease the exchange of DNA, fingerprint and vehicle registration data amongst national law enforcement authorities. The legislation behind it was incorporated into the EU *acquis* after beginning life as an inter-governmental treaty⁹⁵ and it established the world's first system for “the automated cross-border matching of biometric data.” Touted as a way to fight serious transnational crime and terrorism, an early report on DNA data-matching between Spain, Luxembourg and Spain showed that the vast majority of exchanges were related to “property crime, such as theft or fraud”.⁹⁶ As of May 2017, 25 Member States can exchange DNA data, 21 can exchange fingerprint data, and 20 vehicle registration data.⁹⁷ The EU has been making increasing efforts in recent years to ensure the completion of the network, which was supposed to be in place by August 2011.⁹⁸



An EU diagram outlining the data exchange process through the Prüm network.

Some Member States (for example, Luxembourg and Ireland) had to establish national DNA databases to meet the requirements of the Prüm legislation, and the most recent statistics show that Europe's national DNA databases are growing steadily – an average of 10% over the course of 2015, with over 5.7 million individuals' DNA samples held by national authorities at the end of that year.⁹⁹ A further 800,000 “stains” (DNA found at crime scenes belonging to persons unknown) are held across the same databases.¹⁰⁰

Through the ISEC fund, the EU has spent at least €12.2 million on projects aimed at completing or enhancing the Prüm network, although given that one aim of EU security policy is to boost the profits of European companies, it is ironic that the backbone of the system is the FBI-developed CODIS (COmbined DNA Index System).¹⁰¹ The global integration of such systems is foreseen. The “future vision” for “DNA data sharing” is to: “Make the world flat for the international exchange of forensic DNA so that limitations are due to law, regulation and policy,” according to a presentation by an FBI official.¹⁰²

After 2010 the ISEC programme was adapted somewhat to the demands of the newly-adopted Internal Security Strategy (ISS). This declared that:

“The time has come to harness and develop common tools and policies to tackle common threats and risks using a more integrated approach: that is the main aim of the Internal Security Strategy. To achieve that aim we have chosen a security model which integrates action on law enforcement and judicial cooperation, border management and civil protection.”

The ISS called for “a wide and comprehensive approach to internal security” based on “a proactive, intelligence-led approach”; “a comprehensive model for information exchange”; judicial and operational cooperation; integrated border management; “innovation and training”; cooperation with non-EU states on the “external dimension of security”; and “flexibility to adapt to future challenges”. The “effective democratic and judicial supervision of security activities” was also promised.¹⁰³

Thus, 2011, 2012 and 2013 saw ISEC “targeted calls”, published by the Commission, on the topics of:

- trafficking in human beings (between 2007 and 2013 the budget funded at least 63 projects worth €18.4 million on this topic);
- financial and economic crime, such as corruption (€26.4 million, 81 projects);
- “illegal use of the internet” and cybercrime (€28.5 million, 81 projects);
- chemical, biological, radiological and nuclear (CBRN) issues (€6 million, 15 projects); radicalisation (€8.1 million, 25 projects);
- joint investigation teams (€9.9 million, 24 projects); Prüm (€12.2 million, 23 projects); and
- Passenger Name Records (PNR, €50 million, 14 projects, an issue examined further in section 4.3).

ISEC also regularly provided funding for the “monopoly networks” noted in section 2.1. An evaluation of three of these networks (AQUAPOL, RAILPOL and TISPOL) noted that: “For the European Commission, these networks can represent powerful tools of governance in a field that remains driven by EU member states.”¹⁰⁴

The far smaller CIPS budget, meanwhile, focused heavily on the development of new guidelines, rulebooks and “toolkits” for owners and operators of critical infrastructure such as electricity, water, transport and

telecommunications systems; as well as exercises for emergency services and special forces to simulate responses to terrorist attacks, systems for “intelligent” video surveillance and numerous workshops and courses to try to enhance cooperation between national authorities and public and private institutions. The mid-term evaluation carried out for the Commission noted that “compared to ISEC, CIPS projects tend to have a more modest operational content,” and significant portions of the funding went to commercial entities and research institutes, rather than predominantly state institutions as in ISEC.¹⁰⁵

The ongoing development and interconnection of national Financial Intelligence Units (FIU) through the FIU.NET system was another target of the ISEC budget. FIUs exist to address financial crime such as money laundering and terrorist financing – two issues that few would dispute the need to address. At the same time, the possibility of national authorities being afforded greater surveillance powers over the financial transactions of ordinary individuals is something that deserves careful scrutiny.¹⁰⁶ Under the EU-US Terrorist Finance Tracking Programme (TFTP), the details of thousands of bank transactions passing through Europe are handed to the US authorities every year.¹⁰⁷ The Commission is soon to consider (not for the first time) the introduction of a similar system for the EU,¹⁰⁸ and financial data-mining has been a focus of various ESRP projects in FP7.

The HEMOLIA project, led by Israel's Verint Systems and with a €3 million EU contribution, sought to develop:

“a new generation Anti-Money Laundering (AML) intelligent multi-agent alert and investigation system which in addition to the traditional financial data makes extensive use of modern society's huge telecom data source, thereby opening up a new dimension of capabilities to all Money Laundering fighters... and Financial Institutes...”¹⁰⁹

Data-mining, data-processing and data fusion systems for various other purposes were the subject of investigation in ADVISE (€3 million, led by Italian company Engineering);¹¹⁰ CAPER (€5.6 million, involving the Italian interior ministry, Portuguese justice ministry, Spain's *Guardia Civil* and the Israeli ministry of public security);¹¹¹ LASIE (€8.3 million, also led by Engineering);¹¹² and ePOOLICE (€3.5 million, with Spanish state-owned Isdefe, Thales, Fraunhofer, Europol and the Spanish interior ministry all on board).¹¹³ The VIRTUOSO project received €8 million from the EU and sought to provide “European Security stakeholders” with “a set of advanced information processing tools” for “end-user oriented applications” such as “open source collection” and “decision support”. Airbus, Atos, Thales, Isdefe and the *Commissariat à l'énergie atomique et aux énergies alternatives* were some of the partners of the project.

The development of systems for the automated collection and processing of information, and even automated decision-making, was a common theme in FP7 projects aimed at law enforcement applications. One project that received some public attention¹¹⁴ was INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment),¹¹⁵ led by Poland's AGH University of Science and Technology, that promised:

“[I]ntelligent processing of all information and automatic detection of threats and recognition of abnormal behaviour or violence, to develop the prototype of an integrated, network-centric system supporting the operational activities of police officers.”

The EU paid nearly €11 million of the project's €14.8 million total cost. The project's final report lists numerous awards received for its work and states that “INDECT research teams published over 400 scientific papers” – a staggering figure given that the 61 ESRP projects analysed by the Technopolis report (see section 2.2) produced just 214 publications in total, of which just 34 appeared in “high-impact peer-reviewed journals.”¹¹⁶

Other projects with similar aims were:

- MOSAIC (“decision support at various levels to enhance situation awareness, surveillance targeting and camera handover”, €2.7 million from the EU and led by the University of Reading with support from BAE Systems, two UK police forces and others);¹¹⁷
- ADABTS (“automatic detection of abnormal human behaviour”, €3.2 million, partners included the Swedish Defence Research Institute, TNO, the Bulgarian interior ministry, BAE Systems and the UK Home Office);¹¹⁸
- P-REACT (“a sensor data (video and motion) capturing and archiving network/platform that allows the protection of small businesses from petty crimes”, €1.5 million, led by Spain's Vicomtech);¹¹⁹
- TACTICS (a “decision making framework” based on “behaviour analysis, characteristics of the possible urban-based targets and situational awareness”, €3.5 million, involving TNO, the RAND Corporation, Fraunhofer, Safran, the Dutch defence ministry and the International Security and Counter-terrorism Academy from Israel);¹²⁰
- iDetect 4ALL (“alerting technology for surveillance and intruders detection”, €2.3 million, led by the UK's Instro Precision and with a strong contingent of Israeli companies as partners);¹²¹

- SMARTPREVENT (“enhance detection and prevention of petty crimes in local urban areas by exploiting the full potential of video-surveillance systems”, €1.5 million, led by Spanish company Treelogic);¹²²
- SAMURAI (“a real-time adaptive behaviour profiling and abnormality detection system”, €2.5 million with Queen Mary University of London (the coordinator) and Selex the two highest-paid participants);¹²³ and
- ZONESEC (“large scale surveillance with high performance detection of localized abnormal activities and alerts”, €9.3 million, led by Greek company Exodus and with Airbus and Thales amongst the numerous project partners).¹²⁴



A SAMURAI project brochure highlighting the need for automated “abnormal behaviour” detection to meet the “European Security Challenge”.

It has long been argued by civil liberties advocates that public surveillance systems (such as CCTV) do not only infringe upon civil liberties, but also have a limited effect on in dealing with crime. Available research suggests that this is indeed the case,¹²⁵ but the response seems to have been to make surveillance systems even more intrusive and ‘intelligent’ in the hope of achieving results. While ethnic discrimination and racial profiling by police forces across Europe has long been a problem¹²⁶ that recently seems to have intensified in the wake of terrorist attacks and large-scale refugee movements,¹²⁷ few of these projects appear to demonstrate any awareness of the risks of potentially building such biases into automated system. This is a danger that has also been highlighted in relation to the numerous “predictive policing” systems that have come into vogue in recent years.¹²⁸

Further attempts to develop new technologies for law enforcement authorities came from all angles: electromagnetic weapons and drones to stop “non-cooperative vehicles” (SAVELEC¹²⁹ and AEROCEPTOR¹³⁰); biometric capture, recognition and testing systems (INGRESS,¹³¹ FIDELITY,¹³² BEAT¹³³); inflatable, portable “air bags” for protection against bullets and explosives

(RAPTOR¹³⁴) and all manner of detection, screening and sensing systems to “secure” the water supply against deliberate contamination or to detect hints of chemical, biological, radiological, nuclear and other bomb-making materials; or to locate drugs, concealed people and goods (for example SecurEau,¹³⁵ SAFEWATER,¹³⁶ ISIS,¹³⁷ TAWARA-RTM,¹³⁸ SNIFFER,¹³⁹ SNOOPY,¹⁴⁰ HANDHOLD¹⁴¹ and DOGGIES¹⁴²). Yet while the initial aim may have been policing or critical infrastructure protection, projects sometimes went in other directions: the SUBCOP project (with an EU contribution of €3.5 million and led by the Swedish Defence Research Institute)¹⁴³ investigated “less-than-lethal” methods to stop suicide bombers, and helped fund the development of a “sound blaster” that is now apparently being marketed as useful in “addressing the migrant crisis”.¹⁴⁴

Other EU interventions, while complex, were not always so technologically fanciful. The European Criminal Records Information System (ECRIS) was established in 2012 to ease the exchange of criminal record data between EU Member States. It is soon due to be expanded to encompass non-EU (“third country”) nationals. In 2013, the second-generation Schengen Information System (the world’s largest law enforcement database) was finally launched after years of delays, and is currently being enhanced to allow fingerprint searches and the storage of DNA profiles. The Visa Information System, which gathers biometric data from all short-stay visa applicants to the Schengen area, was also gradually established at all Member States’ consulates and visa processing centres around the world.

It was also in this era that the EU’s notorious 2006 Data Retention Directive came into force, requiring telecommunications providers to retain data on all customer phone and internet usage. The Directive was annulled in April 2014 by the European Court of Justice, which noted that it required “an interference with the fundamental rights of practically the entire European population... without any differentiation, limitation or exception being made”.¹⁴⁵ The Directive effectively transformed all users of telecoms devices into potential suspects, in a clear example of the “presumption of threat” thesis examined in the first section of this report. Despite the repeal of the Directive, many national retention schemes remain in place and Member States remain committed to finding ways to implement EU-wide data retention rules.¹⁴⁶

Other developments included EU policing agency Europol receiving a new legal basis in 2009 (which was further renewed in 2016) allowing it to further expand its databases and analysis efforts. The European Investigation Order, proposed in 2010 and finally agreed in 2014, aims to “make cross-border investigations faster and more efficient,” covering:

“[A]lmost all investigative measures such as interviewing witnesses, obtaining of information or evidence already in the possession of the executing authority, and (with additional safeguards) interception of telecommunications, and information on and monitoring of bank accounts.”

Here, the European Parliament’s interventions in the legislative process were able to ensure the inclusion of human rights protections in an instrument based on a proposal that EU law expert Steve Peers initially described as prescribing a “reduction in human rights protection” and “an attack on the national sovereignty of Member States.”¹⁴⁷ Other laws on interpretation, translation and information rights for criminal suspects, the right to lawyer and the right to legal aid have also sought to improve individuals’ procedural rights across the EU,¹⁴⁸ although their practical effect remains to be seen.

The ability for police operations to be coordinated at EU level has also increased significantly since the creation of the EU’s Standing Committee on Operational Cooperation on Internal Security (COSI) following the entry into force of the 2009 Lisbon Treaty. Through this forum and others in the Council of the EU (for example, the Working Party on Frontiers or the Law Enforcement Working Party), EU-wide police operations are regularly organised and assessed, as through the EU’s “policy cycle on serious and organised crime.” This was first called for by the 2009 Stockholm Programme and the subsequent Internal Security Strategy, and began in 2011.¹⁴⁹ European Parliament oversight of the work of COSI, the policy cycle and other EU-coordinated operational activities is minimal, amounting to nothing more than an annual report on the committee’s activities, despite the fact that operations sometimes have concerning implications on the ground.

The ‘Mos Maiorum’ operation in October 2014, for example, encouraged police forces to target those who “facilitate[d] illegal immigration” – in theory, organised people smugglers, but also potentially those individuals who help people cross borders for humanitarian reasons.¹⁵⁰ One clear result of the operation was to give the green light to numerous incidents of racial profiling. Submissions from volunteers across the EU during the operation included one from Bulgaria that reported police entering a hostel and saying they were “looking for refugees”, and one from Germany saying that police were looking for “illegal refugees” with “dark skincolor [sic].”¹⁵¹

As noted at the start of this section, the “achievement of permanent changes in operational procedures/practices” was cited by the Commission’s external mid-term evaluation as “the most common impact” of ISEC and CIPS-funded projects. Yet these two budgets were

introduced through decisions taken by the Council alone – their democratic legitimacy is questionable, to say the least. Elsewhere, new laws, policies and projects have given rise to new transnational bodies and networks subject to little democratic oversight, while ESRP projects have helped to draw public and private officials closer together. The EU may be beset by all manner of crises, yet despite this – or perhaps in part because of it – the threads connecting national law enforcement authorities and EU institutions and agencies to one another have become intertwined to an unprecedented extent in the last decade.



One of several posters distributed by campaigners and activists in the run-up to and during the Mos Maiorum operation.

2.5 FREEDOM, SECURITY AND JUSTICE?

The EU’s budgets for security research and for justice and home affairs policies have become detached from earlier proposals that linked them to basic social rights.

Examining the EU’s response to the economic crisis, Brussels-based citizen watchdog organisation, Corporate Europe Observatory observed that:

“[H]arsh austerity measures were imposed, and policies were adopted to attack social rights, including pensions and labour laws across Europe... The net result of all these new European

laws and measures is that economic decision-making is steadily being taken out of the hands of nationally elected parliaments, not in order to be handled democratically at the European level, but to push neoliberal policies through via unaccountable bureaucratic mechanisms, [emphasis added] and with the threat of sanctions as the ultimate weapon.”¹⁵²

National governments retain tremendous powers in the field of justice, home affairs and security. Nevertheless, the security laws, policies and budgets implemented by the EU between 2007 and 2013 shows slow progress towards a largely unaccountable transnational apparatus exercising traditional forms of coercive power through novel technological means. Transnational cooperation is undoubtedly a necessity to deal with crime, terrorism, migration and a whole host of other issues, but it is essential that its form (for example, whether it has been subject to democratic approval or not) and what it seeks to achieve (for example, an intensification of deadly border control policies or law enforcement surveillance capabilities) are the subject of public discussion and debate.

This is especially so given the increasing emphasis on this type of “hard” security. In 2004 the European Commission noted the key role that basic social rights played in the ‘Area of Freedom, Security and Justice’ (AFSJ), but these issues are no longer formally associated with security policy. It seems that as traditional forms of social security have been deliberately eroded, enthusiasm for the doctrine of homeland security – sometimes referred to in Europe as “civil security” or “societal security” has continued almost unabated. Yet research carried out in the UK suggests has shown that “issues relating to... income and immediate experiences of employment were consistently the most important” in what made people feel secure in their lives, to a far greater degree than traditional security measures such as “police presence on the streets”.¹⁵³ The reinforcement of “traditional” (and not-so-traditional) security measures now seems to be the primary consideration for the AFSJ, and the private interests that stand to gain from this process have long been on hand to try to shape it.



EUROPE'S SECURITY-INDUSTRIAL COMPLEX



Research shows that issues relating to income, employment and financial security are what make most people feel secure, to a far greater degree than traditional security measures such as police presence or militarised borders. Yet the reinforcement of pervasive, high-tech security measures has long been the primary consideration for the EU's security strategists, with the private interests that stand to gain from this process always ready to offer their guidance and reap the rewards.

INSTITUTIONS



European Commission

DIRECTORATE-GENERALS:

- Directorate-General for Migration and Home Affairs (DG HOME)
- Directorate-General for Communications Networks, Content and Technology (DG CONNECT)

ADVISORY GROUPS:

- Protection and Security Advisory Group (PASAG) (2007-13, 23% of participants from security and defence companies; Commission currently working on a "slight overall increase of industry representation")
- Programme Committee for 'Secure societies Protecting Freedom and security of Europe and its citizens'



Council of the European Union

WORKING PARTIES:

- Law Enforcement Working Party (LEWP)
- Standing Committee on Operational Cooperation on Internal Security (COSI)
- Working Party on Information Exchange and Data Protection (DAPIX)
- Working Party on Frontiers
- High-Level Working Group on Asylum and Migration
- Strategic Committee on Immigration, Frontiers and Asylum (SCIFA)

EU AGENCIES

- European Border and Coast Guard Agency / Frontex (borders)
- Europol (police cooperation)
- Eurojust (judicial cooperation)
- eu-LISA (large-scale IT systems)



European Parliament

- Committee on Industry, Research and Energy (ITRE)
- Committee on Civil Liberties, Justice and Home Affairs (LIBE)

POLICIES

FOREIGN POLICY AND EXTERNAL SECURITY:

European Security Strategy (2003) and Global Strategy for Foreign and Security Policy (2016)

CYBERSECURITY: Cybersecurity Strategy (2013)

INTERNAL SECURITY: Internal Security Strategy (2009), Renewed Internal Security Strategy (2015) and European Agenda on Security (2015)

CRIME: Policy cycle on serious and organised international crime (2011-13, 2014-17, 2018-21)

MIGRATION: European Agenda on Migration (2015)

SECURITY INDUSTRY: Security Industrial Policy (2012)

CRITICAL INFRASTRUCTURE: European Programme for Critical Infrastructure Protection (2006) and New approach to the European Programme for Critical Infrastructure Protection (2013)



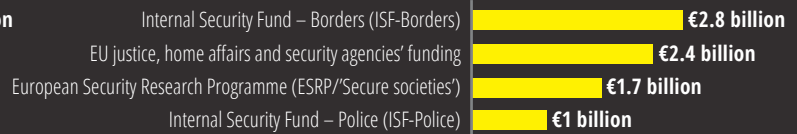
FUNDING PROGRAMMES



2007–13



2014–20



2007–13 TOTAL: €3.94 billion

2014–20 TOTAL: €7.9 billion

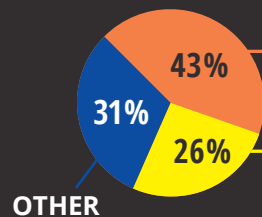
(over 2x increase)

"A competitive EU security industry is the conditio sine qua non of any viable European security policy and for economic growth in general."

(European Commission, 2012)

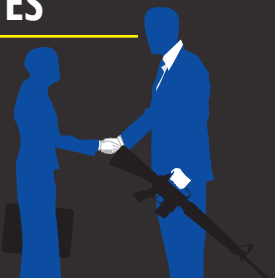
INDUSTRIAL COMPLEX: CORPORATIONS & RESEARCH INSTITUTES

SECURITY RESEARCH BUDGET BENEFICIARIES (2007-2016)



PRIVATE COMPANIES
€745.5 MILLION

RESEARCH INSTITUTES
€456.5 MILLION



LOBBY GROUPS

- **European Organisation for Security (EOS)**: 2016 lobbying budget €200,000–299,999; has so far received over €2.5 million from the ESRP for 15 projects
- **AeroSpace and Defence Industries Association of Europe (ASD)**: lobbying budget €298,000 2015

CORPORATE BENEFICIARIES

- THALES** (€33.1 million, 72 projects)
- SELEX** (€23.2 million, 54 projects)
- AIRBUS** (€14.2 million, 34 projects)
- AtoS** (€14.1 million, 31 projects)
- indra** (€12.3 million, 16 projects)
- BMT Group** (€10.6 million, 9 projects)
- Isdefe** (€10.5 million, 16 projects)
- MORPHO** (€8.7 million, 19 projects)

- Engineering** (€8.1 million, 10 projects)
- ITTI** (€6.5 million, 25 projects)
- ARTIC** (€7.2 million, 13 projects)
- BAE SYSTEMS** (€6.2 million, 11 projects)
- VITROCISSET** (€5.7 million, 10 projects)
- SAAB** (€5.6 million, 8 projects)
- CASSIDIAN** (€5.3 million, 7 projects)

RESEARCH INSTITUTE BENEFICIARIES

- Fraunhofer Institute
- TNO
- Swedish Defence Research Institute
- Commissariat à l'énergie atomique et aux énergies alternatives
- Austrian Institute of Technology
- VTT Technical Research Centre
- Demokritos
- Stiftelsen
- Italian Space Agency
- Institute of Communication and Computer Systems
- European Commission Joint Research Centre
- National Research Council
- Center for Security Studies
- Inov Inesc
- Norwegian Defence Research Establishment

PUBLIC-PRIVATE FORUMS



Seats held by private sector



GROUP OF PERSONALITIES in the field of security research (2003–04)

8 of 29 seats



EUROPEAN SECURITY RESEARCH ADVISORY BOARD (ESRAB, 2005–06)

14 of 50 seats



EUROPEAN SECURITY RESEARCH AND INNOVATION FORUM (ESRIF, 2007–09)

16 of 65 seats

Plus 280 "main contributors" whose affiliation is not listed in the final report



PARTICIPANTS

28 of 52 seats

OBSERVERS

25 of 31 seats

HIGH-LEVEL SECURITY ROUNDTABLE (2011)

At the 2012 Roundtable 72 of 117 participants were from the private sector



Former EU commissioners Antonio Tajani alongside Lorenzo Mariani (Finmeccanica/Selex) and Luigi Rebuffi (EOS) following a 'High-Level Security Roundtable'

PUBLIC INTEREST, PRIVATE DIALOGUE

“[W]e need to achieve a European Model for Security based on a holistic, comprehensive approach, and industry should have a role to play from the very beginning of the definition process.” (Santiago Roura, then-chairman of the European Organisation for Security, April 2014)¹⁵⁴

“A competitive EU security industry is the *conditio sine qua non* of any viable European security policy and for economic growth in general.” (European Commission, 2012)¹⁵⁵

The security industry has continuously lobbied for the EU's security project to be brought further into line with its interests. Following on from ESRAB (see section 2.1), another high-level advisory group, the European Security Research and Innovation and Forum (ESRIF), set out a swathe of demands for the future, the majority of which have been taken up by the EU. An examination (section 3.2) of the FP7 research project, ARCHIMEDES, led by the European Organisation for Security makes clear the dangerous aims of the industry, which has been helped along by MEPs moulding legislation for the period 2014-20 into a more corporate-friendly shape. Further efforts are being made to advance private interests through ongoing lobbying efforts, at high-level "roundtable" events, in private meetings, and through the advisory group set up to outline priorities for the EU's security research agenda. New public-private "governance models" are one result, for example through multi-million euro contracts offered to corporations for the rental of maritime surveillance drone services by EU agencies.

3.1 VISIONS OF THE FUTURE

Another high-level advisory group dominated by state and industry officials produced a report on the future direction of security research that was accepted and approved by the Commission without critical comment.



The "public-private dialogue" that shaped the ESRP's early years and the research priorities in FP7 did not end when ESRAB completed its work (see section 2.2). In March 2007 yet another "informal" group – the European Security Research & Innovation Forum (ESRIF) – was convened in order to "go beyond FP7 security research" and work out how to meet "long term security research

and technological development needs throughout the EU to be covered by national, EU and private investments." It was made up of "a 65-member plenary and some 660 security consultants divided into 11 working groups."

The European Commission said that it was an "informal group, set up jointly and co-owned by its stakeholders from the demand and supply side of security technologies/solutions," and that it is "neither a Commission body nor a Commission driven exercise." As *NeoConOpticon* put it:

*"This is an astonishing statement insofar as it suggests that the Commission has effectively outsourced the strategic development of a €1.4 billion EU research programme to a wholly unaccountable, informal group. If the claim is false, and it is clear that ESRIF is, if not 'driven' then at least 'steered' by the European Commission, then the Commission has failed spectacularly to ensure adequate accountability mechanisms and reported the discharge of its responsibilities quite dishonestly. Both propositions are wholly unacceptable."*¹⁵⁶

ESRIF's sprawling final report – the 'European Security Research and Innovation Agenda' (ESRIA)¹⁵⁷ – made numerous recommendations.

One call was for "common European capabilities": the development of systems, tools and procedures that can be used by some or all Member States and EU institutions and agencies, or "interoperability" to use a phrase favoured in Brussels policy-making circles. Such an approach is favoured by Europe's larger industrial interests because, as remarked in a 2010 study: "The development of a European public security market," in which it is possible to make sales to some or all Member States and EU agencies at once, "is perceived by these companies as a necessary condition for the achievement of profitable business."¹⁵⁸

The ESRIF report noted this would require the "organisational realignment" of government agencies in order "to both shape and respond to security innovation" a topic that has been the focus of a number of FP7 projects and remains on the agenda during Horizon 2020 (see further in section 3.2). ESRIF revived the call for a €1 billion annual budget, and the use of "pre-commercial procurement... to bring research results closer to market." The €1 billion a year has not been forthcoming, but "pre-commercial procurement" – in which public institutions are invited to guide research and development efforts by the private sector, and to commit themselves to the purchase of new technologies – has been introduced into the ESRP in Horizon 2020.

ESRIF also demanded the establishment of "knowledge centres such as CBRN expert groups to guide research" and "pan-European network-enabled capabilities and complex systems in early warning and response readiness." As section 2 highlighted, the formal evaluation of the ESRP in FP7 saw the development of new transnational networks as one of its key benefits, with regard to both the

development of a general security research “community” and more specific interests. Emerging security research networks include the European Customs Detection Technology Expert Group (CDTEG), the Community of Users (CoU) on Disaster Risk and Crisis Management and the European Network of Law Enforcement Technology Services (ENLETS).¹⁵⁹

The expansion of the EU’s Critical Infrastructure Protection programme, setting up an Internal Security Fund and the development of “standards to stimulate private sector investments in security research” were also demanded. All of these themes have been taken up by the EU either through FP7 and H2020 projects, budgets such as CIPS, the development of new legislation (for example the Internal Security Fund), initiatives such as the Security Industrial Policy and attempts to ensure “a more practical implementation” of the European Programme for Critical Infrastructure Protection”.¹⁶⁰ In short: everything ESRI demanded, except for the €1 billion annual budget.

A position of power for the EU in global politics did not escape the notice of ESRI, which called for a “strong and independent technological and scientific base for the EU to safeguard the interests of its citizens” – an aim of both the Security Industrial Policy and the EU’s defence industry policy, with a military research programme also on the way¹⁶¹ – and the closer integration of internal and external security policy. The attempt to find “synergies” in EU’s “internal-external interface” has also developed in recent years¹⁶² and may be further propelled by using Horizon 2020 funding for “dual-use” projects which aim to develop technologies for both civilian and military use (see further in section 4.1).

A fortnight after the publication of ESRI’s final report, the European Commission produced a Communication outlining its “initial position on ESRI’s key findings and recommendations.”¹⁶³ This remains the only formal reaction to ESRI’s report and the “initial position” was, broadly speaking, to reproduce its recommendations. The group’s work was done, but it maintained that its final report “should be seen as a living document,” to be implemented through a “transparent mechanism involving all stakeholders and “revisited and evaluated on a regular basis”. The “public-private dialogue” has continued in recent years. However, judging by results, transparency and including “all stakeholders” do not seem to be its main priorities.

3.2 THE “END-TO-END APPROACH”: A STATE-CORPORATE MERGER

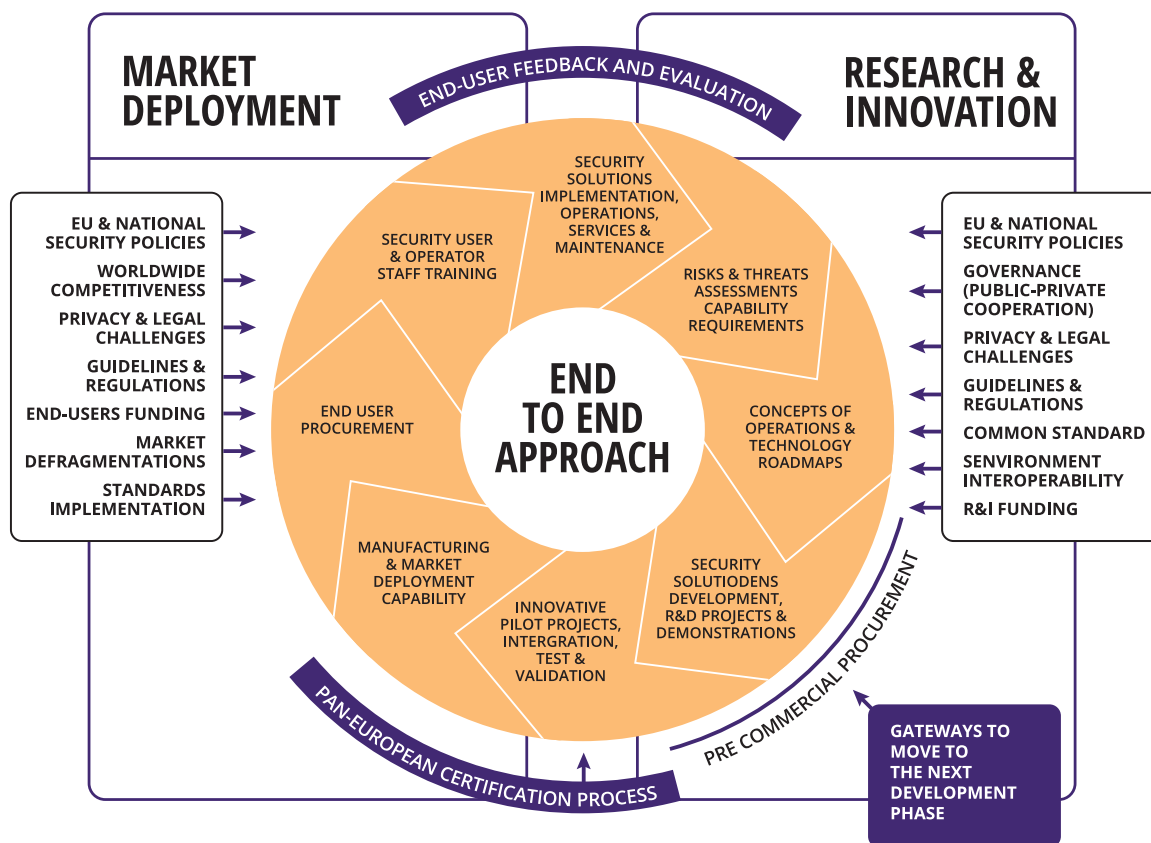
The chief lobby group for the European security industry, which argues that fundamental rights are “not a competitive advantage”, was awarded EU funding to develop its own vision for the drafting and implementation of EU security policy, offering a clear vision of the preferences of major corporations.

The European Organisation for Security (EOS) is the primary lobby group for Europe’s security industry. Based – of course – in Brussels, the group is led on a day-to-day basis by its CEO, Luigi Rebuffi, a former Thales employee who in 2003 proposed the idea for a security industry lobby group and in 2007 founded EOS.¹⁶⁴ The group’s extensive membership list includes a number of Europe’s major military and security companies (Airbus Defence & Space, Indra, Selex, Thales and even another lobby group, ASD) and technology companies (Altran, Atos, Siemens).

It claims to represent “the interest of the European security suppliers including large companies, SMEs, research centres, universities, clusters and associations.”¹⁶⁵ According to the Commission’s Transparency Register, during 2015 EOS received almost €560,000 in funds from the EU through its participation in various FP7 projects, and at the same time spent somewhere between €200,000 and €299,999 on lobbying activities. In 2016, the income it received from grants dropped to €310,902 while the amount it spent on lobbying remained within the same bracket.¹⁶⁶

The group’s “main objective is the development of a harmonised European security market in line with political, societal and economic need,”¹⁶⁷ involving the adoption of what EOS calls an “end-to-end approach for security research and innovation” which foresees the formal integration of public authorities and private companies in a new type of “governance” structure. Through the three year, FP7-funded ARCHIMEDES project (EU contribution: €1.4 million),¹⁶⁸ EOS was given the opportunity to flesh out its vision in considerable detail. It explored ways to develop a European security market and to make public institutions more readily-accepting of innovations cooked up by the private sector.¹⁶⁹ The project’s final report said:

“Coordination between the different DGs, agencies, institutions, policies and funds can be achieved through an EU umbrella programme coordinated politically and operationally by the European Commission and optimising the use of budgets into a smooth flow from research to the market.”¹⁷⁰



Daunting, baffling, and publicly-funded: EOS' proposed "end-to-end approach for security research and innovation". Note that privacy and the law are characterised as "challenges".

The "smooth flow from research to the market" foreseen by the project begins with the drafting of an "EU harmonised" analysis of risks and requirements for new security technologies and services. This will inform "Technology and Implementation Roadmaps for coordinated use of EU, MS and private funding." The acquisition of new products would be accelerated through "faster definition of EU standards and EU validated/certified solutions (EU security label)."

A "public-private dialogue platform" would be involved in governing the process. Reading the EOS proposal, it seems this would be made up of pretty much anyone with an interest in security, except for citizens and their elected representatives.¹⁷¹ In this vision, corporate interests, state policies and the wisdom of various experts are harmoniously aligned – but democracy seems to have left the stage. The report does say: "Democratically, it would be good to have as wide as possible representatives from all countries, sectors, kind of actors," but such an approach has to be tempered by the need for the dialogue to take place "in a closed and trusted environment that allows (when needed) sharing of confidential information."¹⁷²

Such an environment was established in a number of roundtables organised by EOS as part of the project. These covered the whole spectrum of security policy areas¹⁷³ and fostered a "sustained dialogue and exchange

of information among all relevant security stakeholders." The resulting recommendations were distributed to bodies "including DG ENTR [Enterprise & Industry], FRONTEX, the European Council, ENISA [European Network and Information Security Agency], DG ECHO [Humanitarian Aid and Civil Protection], and national EU&Os [end-users and operators]."

The project also proposed the creation of a new public-private 'Alliance for European Growth and Innovation on Security':

*"AEGIS would create a structured link between national organisations of different European countries dealing with security issues and representing different sectors, in order to defend the needs of national and local, public and private, users, operators and suppliers, not only on R&D issues but for all the steps of the life of security solutions and services, as well as facilitating the creation and growth of such national organisations in countries where they are not existing or sufficiently organised."*¹⁷⁴

A conference was held by EOS on 16 May 2014 "in partnership with the Greek Presidency of the EU," with "about a hundred participants with high-level speakers, representing fifteen European countries." They reportedly had a "very fruitful" discussion,¹⁷⁵ although EOS representatives have been reluctant to

answer further questions about the network and the body has not so far received any formal endorsement from EU institutions.

For those concerned about fundamental rights, civil liberties and the basic tenets of democracy, the fact that EOS has not managed to extend its influence as far as it would like should be welcomed. The final ARCHIMEDES report states that concerns over fundamental rights are “politically correct but not necessarily a competitive advantage at MS and international level.” This statement – both worrying and entirely predictable at the same time – coincides with findings from the formal evaluation of FP7 discussed in section 2.2. Only 33% respondents to the evaluators’ survey felt the security industry as a whole has a role to play in “respecting fundamental human rights including privacy,” and just 26% of respondents felt it was relevant for small and medium-sized businesses in the sector.

3.3 FRIENDS ON THE INSIDE: SHAPING LEGISLATION

Legislation on security budgets for the 2014-20 period could have turned out quite differently if the Commission’s original proposal had not been transformed into a more industry-friendly text by the European Parliament and the Council.



Laszlo Felkai (Hungarian Interior Minister), Cecilia Malmström (Home Affairs Commissioner) and Luigi Rebuffi (EOS) present the public-private partnership to the press, March 2011

As noted in *NeoConOpticon*: “It would be over-simplistic... to suggest that the EU is simply an empty shell for the furthering of corporate interests” – although this is certainly the end point of many policies.¹⁷⁶ The legislative procedure that led to the establishment of the €1.7 billion security research programme within Horizon 2020, the EU’s 2014-20 research and technological development programme (with a total budget of some €77 billion) provides a good example of how different

interests engage in the design and implementation of the EU security policy.

In November 2011 the Commission published its legislative proposal for Horizon 2020, and the security industry was likely rather displeased. The proposal seems to suggest that perhaps the pendulum was swinging away from the hard-edged, high-tech research that largely characterised the 2007-13 ESRP. The Commission intended to merge the security research programme into a broader theme: ‘Inclusive, innovative and secure societies’, which would have received a budget of some €3.8 billion.

No specific explanation was offered for the proposal to abandon FP7’s stand-alone security research programme, but the Commission highlighted the issues of economic and gender inequality; “political apathy and polarisation”; Europe’s declining “productivity and growth rates” in comparison to “key emerging economies such as Brazil and China”; and the fact that “many forms of insecurity, whether crime, violence, terrorism, cyber-attacks, privacy abuses and other forms of social and economic disorders increasingly affect citizens.” The proposal argued that:

“These challenges must be tackled together and in innovative ways because they interact in complex and often unexpected ways... it is necessary to think and respond to these issues across their dimensions of inclusiveness, innovation and security at the same time... enhancing the societal dimension of security research will be an important aspect of this challenge.”

The Commission called for:

“[U]nderstanding the underlying trends and impacts at play in these challenges and rediscovering or reinventing successful forms of solidarity, coordination and creativity that make Europe a distinctive model of inclusive, innovative and secure societies compared to other world regions.”

Whether its proposed programme would have allowed the development of “successful forms of solidarity, coordination and creativity” is impossible to say. Amendments to the text by the Council and the Parliament saw security research removed from the ‘Inclusive, innovative and secure societies’ programme and placed into a separate “challenge”, entitled ‘Secure societies – protecting freedom and security of Europe and its citizens’.

In the Parliament, the Committee on Industry, Research and Energy (ITRE) was responsible for dealing with the proposal, and over 1,800 amendments were tabled. Spanish MEP Teresa Riera Madurell, from the Socialists & Democrats (S&D) Group, issued a draft report explaining that:

“Inclusive, innovative and secure societies’... has been divided in two to reflect the specific nature of security challenges: ‘Understanding European societies and societal change’ and ‘Protecting freedom and security in Europe’. Under the first of these new challenges, social sciences and humanities will come to play a decisive role in moving towards more inclusive and innovative societies...

“...the importance of protecting freedom and security in Europe is such that it justifies being included as a challenge in its own right. This new challenge will focus specifically on the pursuit and development of responses to internal and external threats to European security.”¹⁷⁷

This approach was subsequently backed by a majority of other MEPs, in particular those from the conservative European People’s Party, whose members also tabled amendments to the Commission proposal that reflected the approach of Madurell’s report. Thus the Socialists & Democrats and the EPP, the two main groupings in the European Parliament in the 2009-14 legislature, came together (as they have done frequently on other issues)¹⁷⁸ to reverse the Commission’s proposed new approach to security research.

Particularly active for the EPP was Christian Ehler, a German MEP who has significant connections with the security industry. As well as being chief executive of biotechnology company *co:bios Technologiezentrum*s (a post which earns him over €10,000 per month), he is a member of the German European Security Association (the German lobby group for the security industry) and the German Cyber Security Council.¹⁷⁹ He was a member of both ESRAB and ESRIF, the only MEP present at the EOS’ 2011 High Level Security Roundtable, and one of five MEPs at the 2012 event.¹⁸⁰

Ehler submitted dozens of amendments to the Commission’s proposed text, including one suggesting the deletion of the statement: “as security policies should interact with different social policies, enhancing the societal dimension of security research will be an important aspect of this challenge.”¹⁸¹ It was not adopted. Others sought to insert references to security into the texts on research into health, advanced materials, and transport. The German MEP also had the role of rapporteur for Horizon 2020’s rules on participation and dissemination of research findings¹⁸² and he has remained busy beyond his role in drafting the legislation. Amongst other things, MEP Ehler registered complaints along with industry representatives during a spat between

the Commission and industry over the treatment of intellectual property rights stemming from research projects.¹⁸³

Other proposed amendments that would have required more stringent oversight and a more considered approach to security research projects failed. Philippe Lamberts, a Green MEP, sought to amend the proposal to ensure a “broader ‘human security’ research agenda” that would have taken “steps to address the root causes of insecurity” and examined “measures to restore civil liberties, preserve fundamental rights and enhance accountability.” He also tabled amendments that would have required security research projects to consult “the European Data Protection Supervisor, the EU Fundamental Rights Agency, the European Group on Ethics in Science and New Technologies, civil society organisations and academia.” None of his specific amendments were accepted.

The text agreed by the ITRE committee did state that “it is necessary to understand and address the root causes of insecurity,” and that “activities will include a focus on understanding the causes of insecurity and conflict,” but these provisions were successfully removed by the member states within the Council. The Council also successfully watered down references in the ITRE text regarding “the transformation of conflicts within third countries through conflict prevention, peacebuilding, dialogue, mediation and reconciliation and civilian security sector reform.”¹⁸⁴

The Commission’s proposal for a research programme on ‘Innovative, inclusive and secure societies’ thus became ‘Innovative, inclusive and reflective societies’, and a separate budget of nearly €1.7 billion was established for ‘Secure societies – protecting freedom and security of Europe and its citizens’. In addition, significant budgets were allocated to space and other research themes with a security component, such as transport and ICT.

The security-industrial complex has also taken an interest in the development of the Internal Security Fund, which provides financial backing to the Renewed Internal Security Strategy and, potentially, the deployment of ESRP-produced technologies. Marian-Jean Marinescu MEP, vice-chair of the European People’s Party and *rapporteur* within European Parliament’s civil liberties committee for the Internal Security Fund – Borders, was invited to the 2012 High-Level Security Roundtable. A key topic was border control, and the report from the event records Marinescu as saying that: “A clear legislation is needed to implement the proper technology and allow the industry to have predictability for its investments.”¹⁸⁵

TABLE 2: FROM ESRAB, TO FP7, TO H2020

ESRAB proposal	FP7 topic	H2020 topic
Protection against terrorism and organised crime	Security of citizens	Fight against crime and terrorism
Critical infrastructure protection	Security of infrastructure and utilities	Covered by both disaster resilience and digital security
Border security	Intelligent surveillance and border security	Border security and external security
Restoring security and safety in case of crisis	Restoring security and safety in case of crisis	Disaster resilience: safeguarding and security society
No proposal	Security and society	"Security as a societal value is a guiding principle" through each topic
Systems integration, interconnectivity and interoperability	Systems integration, interconnectivity and interoperability	N/A
No proposal	Security research coordination and structuring	N/A
No proposal	No proposal	Digital security

In the subsequent EP report on the ISF-Borders legislation, Marinescu explained that changes introduced to the Commission’s proposal sought to ensure “a uniform and high-quality external border control... achieved through common measures, common security standards able to guarantee the Union added value, and convergent systems which would allow interoperability.”¹⁸⁶ While these may be rote phrases with regard to EU border policy, they are also some of the key requirements for ensuring that profits flow to Europe’s biggest security companies. The final legislation on the Internal Security Fund contains provisions highlighting the possibility of using the funding to acquire technologies developed by the ESRP, a neat attempt to close the loop that starts with research and ends with deployment. In this respect, it seems that an “end-to-end approach” on security is slowly emerging, and the EU is attempting to ensure clear corporate influence on its development.

3.4 JOINING THE DOTS: PUBLIC-PRIVATE PARTNERSHIP

High-level events have long served as venues for discussion on EU security policy to the detriment of more democratic fora, while the

“public-private dialogue” has been advanced behind closed doors and through the deliberate ratcheting-up of corporate influence on the ESRP’s formal advisory group, leading to the emergence of new “governance models” in the security field.



Cream of the crop: mingling and networking after a high-level ASD event

High-level events, typically held at conferencing venues with a “who’s-who” list of attendees from public and private institutions, have long-served as venues for “public-private dialogue” on EU security policy.¹⁸⁷ Following up from ESRIF’s work (see section 3.1), corporate representatives, EU and national officials came together to discuss how the EU could better support the security industry in February 2011, March 2012, March 2013 and April 2014. Participants primarily came from the industry, with a sprinkling of public officials: from the European Commission, EU agencies, national governments and the occasional MEP. Data protection authorities, civil society organisations and more critical parliamentarians were nowhere to be seen.

The 2011 and 2012 events were ‘High-Level Security Roundtables’ organised by EOS under the “patronage” of Cecilia Malmström, at that time EU Home Affairs Commissioner, and then-Commission Vice-President Antonio Tajani. The 2011 event, heralded by Robert Havas of EADS and EOS as “the cradle of a new approach on EU security,”¹⁸⁸ called for the “public/private dialogue on security” to “establish a common roadmap including yearly meetings and the creation of an Internal Security Fund (ISF).” The former, if it has ever been drawn up, has never been made public; the ISF was however set up in December 2013 having been long-called for by industry (in the ESRIF report), the EU and its Member States (for example, in the Stockholm Programme).

The 2012 event, “a major step in deepening the public-private dialogue on security,” placed the emphasis on themes that were “carefully prepared with unprecedented cooperation among four Directorate-Generals of the European Commission and with EOS Members.” A joint “concept paper” making clear industry’s priorities

was drawn up, calling for the adoption of a Security Industrial Policy (it appeared the same year); the further development of the EU's 'Integrated Border Management' system (an ongoing boom for the industry and disaster for migrants and refugees¹⁸⁹); transport security (tentatively being advanced at EU level); and cybersecurity (see section 4.5).¹⁹⁰ The list was extended in 2013 with recommendations on priorities for security research in Horizon 2020, further emphasising cybersecurity as well as standardisation, interoperability, disaster resilience, border control, crime, terrorism and a host of other familiar demands such as for "synergies" between civil and military technology. EU and industry officials met again at the April 2014 annual convention of lobby group ASD.¹⁹¹

Cecilia Malmström told the 2012 Roundtable that the "discussion between public and private stakeholders will be continued, even though in a more informal way, with regular contacts at operational level to exchange information." There has been no shortage of "regular contacts", although they have almost exclusively been with vested corporate interests. Documents released under the EU's access to documents legislation show a steady stream of meetings between EOS and the Commission held between 2012 and 2015, as legislation on Horizon 2020 and the Internal Security Fund (amongst other issues) was under discussion.

In April 2012, following the High-Level Security Roundtable, Luigi Rebuffi and Robert Havas of EOS wrote to Slim Kallas, then-Transport Commissioner, to demand the adoption of "the foreseen Transport Security Communication without any delay". The following month, the Commission published a Staff Working Document on the issue¹⁹² and Kallas invited Rebuffi and Havas to continue discussions.¹⁹³ In July 2013, Graham Wilmott of DG HOME held a meeting with Rebuffi, and in September 2013 Wilmott attended a meeting of the EOS board. On 15 April 2014 Michel Bosco of DG HOME played host to Rebuffi and Haras Caracostas of EOS to discuss the ARCHIMEDES project, and a week later Wilmott and Rebuffi had another private meeting. In May 2014, Wilmott was present at a meeting of the EOS "strategy board" to give a presentation on "the state of play of the Security Industry Policy and of the security research programme."

At a June 2014 meeting, six EOS and five DG HOME representatives met to discuss the EU's "post-Stockholm" programme on justice and home affairs policy,¹⁹⁴ "ways to improve cooperation between industry and DG HOME," and "how to better link DG HOME policies to EU industry competitiveness, Security Industrial Policy, etc." In March 2015 representatives of DG CONNECT joined EOS and DG HOME staff for a meeting, and in April 2015 EOS and HOME met yet again to discuss the "status of the security flagships," the "profile of possible main participants/speakers" at a High-Level Security Roundtable, and "what is the status on the

new EU Security Agenda," which was published by the Commission at the end of May 2015.¹⁹⁵

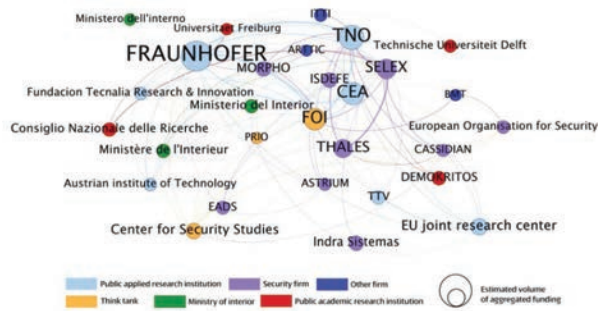
In September 2014, EOS was invited to an EU conference to set the priorities for the EU's Renewed Internal Security Strategy.¹⁹⁶ Santiago Roura – former chairman of EOS and vice-president of Spanish company Indra, who left both jobs after being caught up in a high-level corruption case in Spain¹⁹⁷ – argued that the security industry "would deserve a whole chapter in the next EU Internal Security Strategy." Reiterating the need for an "end-to-end approach" (as discussed in section 3.2), he called for the establishment of "Flagship Initiatives" on border management and cybersecurity, and argued that security is "not only about research but about the effective deployment of innovative solutions at a European Union scale." Thus:

*"[W]e need to achieve a European Model for Security based on a holistic, comprehensive approach, and industry should have a role to play from the very beginning of the definition process."*¹⁹⁸

EU officials were not entirely convinced. Preparatory notes for a 2015 meeting between DG HOME Director-General Matthias Ruete and representatives of lobby group ASD asserted the EU's reluctance to take up the "end-to-end approach" directly, noting that "the development of security research policy remains a competence of the EU institutions,"¹⁹⁹ although this has not stopped them effectively outsourcing the cybersecurity research agenda to an industry lobby (see section 4.4).

This note and others obtained by journalist Dimitri Tokmetzis²⁰⁰ show while the EU has rejected the industry taking over the design of EU security policy wholesale, it has nevertheless consistently sought to ensure greater industry involvement in security research.²⁰¹ The Protection and Security Advisory Group (PASAG) is the successor to the Security Advisory Group discussed in section 2.2 and is the body responsible for giving strategic advice to the Commission on topics for the ESRP work programmes. Research carried out for the European Parliament in 2014 found that during FP7:

"[P]articipants... come mainly from three types of institutions, besides DG Enterprise and Industry of the European Commission (31%). Defence and security firms (SELEX, MORPHO, THALES) represent 23% of individual participations, with other firms accounting for only 3%. The term "end-user" employed in the [Security Advisory Group] report actually encompasses security institutions (18%) and civil protection agencies (10%), both public and private. Finally, the 'research community' can be subdivided in centres for applied research (TNO, FRAUNHOFER – 6%) and Universities, the latter representing 6% of individual participations."



Network chart of major recipients of FP7 ESRP funding and their interconnections through research projects, from the 2014 report "Review of security measures in the 7th Research Framework Programme FP7 2007-2013".

The balance of representatives has changed to varying degrees over the years, but even so its overall contribution has not always lived up to the Commission's expectations. An extensive paper offering "strategic input" for the 2016-17 ESRP work programme was drawn up by the group in July 2014,²⁰² but in 2015 the Commission was lamenting that: "The current SAG has not lived up to our expectations regarding their contribution to the strategic orientation of our Work Programme." Thus it planned to target "new members of the highest stature, invited on a personal basis... Representatives from industry, or with a strong industrial background, will be more numerous than in the past."²⁰³

Alberto de Benedictis, a former senior employee at Finmeccanica and former chairman at defence and security lobby group ASD, was thus brought in to lead the newly-renamed Protection and Security Advisory Group (PASAG).²⁰⁴ This was part of a *rapprochement* between the Commission and ASD after a dispute over the treatment of Intellectual Property Rights in Horizon 2020 research projects.²⁰⁵ In 2015, a Commission background note to a meeting between DG HOME officials and ASD employees (including former Commission employee Burkhard Schmitt) described de Benedictis as fitting "very well with our expectation for senior, well-respected, wise-people in SAG/PASAG." The note said there were "6 more names from industry on the list for 2016, 2017 or 2018 replacements," which would lead to "a slight overall increase of industry representation"²⁰⁶ – just as ASD was publicly bemoaning the fact that the SAG (by this time known as the Secure Societies Advisory Group, SSAG) had "too little industry representation."²⁰⁷

When the Horizon 2020 ESRP began and the group was known as the Secure Societies Advisory Group (SSAG), it had 30 members. 18 were appointed in an "individual capacity" (amongst whom were employees and former employees of Isdefe, TNO and PIAP, as well as the chairman of EU police technology network ENLETS); one was a representative of an interest (although which particular interest is unknown); and 11 represented organisations. These included ASD, EOS, the *Commissariat à l'énergie atomique et aux énergies alternatives*, the Eurotech Security Research Group, the Fraunhofer Institute, the European Defence Agency (EDA), Europol and Frontex.

In January 2016 the advisory group was rebranded again as the PASAG (having been the SAG from 2007-13 and the SSAG from 2014-15). The membership was rejigged, with 26 individual members and four organisations' representatives taking part. Chairing was Alberto de Benedictis, in an "individual capacity" alongside former and current employees of Isdefe, Finmeccanica, Airbus, Morpho, TNO, Fraunhofer, the EDA, Europol, ENLETS, and a wide range of academics (as well as the UN's Special Rapporteur on the right to privacy). EOS, the German Federal Agency for Technical Relief, Fraunhofer and the Swedish Civil Contingencies Agency took up the seats given to organisations.

The group was slimmed down further in January 2017, although de Benedictis still holds the chair and current and former employees of Isdefe, Fraunhofer, the German Federal Office for Information Security, ENLETS, the Italian National Research Council and the Spanish National Institute for Cybersecurity, amongst others, retain their individual seats. The Fraunhofer Institute in fact now has two employees sitting in the PASAG, one of whom, Merle Missoweit, is currently responsible for applying for and executing EU research projects and who also took part in "defining [the] strategic direction of research" at Fraunhofer between January 2013 and July 2014.²⁰⁸ Claudia Gärtner, who has sat on the group since 2016, is presumably well-versed in the ESRP: her company, microfluidic ChipShop,²⁰⁹ has received grants worth a total of almost €3 million from the FP7 and H2020 budgets for the projects Multisense Chip,²¹⁰ EDEN,²¹¹ and ROCSAFE.²¹²

Besides the individuals involved, it is clear the industry is heavily involved – in October 2015 ASD reported that it had:

"[A]lready started to work on input for the preparation of the next bi-annual work programme 2018/2019, trying in particular to identify and promote research themes that could generate large scale funding projects."

The organisation is also "actively promoting better industry representation in the Commission's pool of evaluators" – improving the chances that industry bids will be reviewed by evaluators drawn from industry.²¹³

The position of the European Network of Law Enforcement Technology Services (ENLETS) on the group illustrates well the attempt to build links between public and private institutions. The network, made of Member States' law enforcement technology bodies and in the past financed by the Commission (€500,000 in 2015),²¹⁴ seeks to develop new technology for police forces and has previously shown an interest in automatic number plate recognition, open source and signals intelligence, video surveillance and technology to remotely stop

vehicles.²¹⁵ It has been endorsed by the Council of the EU as a platform for “strengthening the internal security authorities’ involvement in security-related research and industrial policy.”²¹⁶ Patrick Padding (a Dutch police official) was for a time chair of both the PASAG and ENLETS, a ‘double-hatted’ role described in an ENLETS report as “unabatedly important... The connection to industry and research results in mutual understanding and increased flow of end-user demands.”²¹⁷

The search for closer connections between the supply and demand sides of the security “market” has led to other changes. When the ESRP was integrated into FP7, responsibility for it was given not to the Commission Directorate-General for Research & Innovation – which oversaw the majority of the EU’s research programme – but instead to the Directorate-General for Enterprise & Industry (DG ENTR), thus cementing the key role of the “public-private dialogue”. As security scholar Peter J. Burgess has explained, the programme was based on:

“[A] political principle that effective security management in Europe will henceforth depend on the establishment and advancement of a robust security defence procurement market... this one institutional decision has had considerable consequences for the way that security is conceptualised, researched and implemented... the notion of public-private dialogue quickly became the central tenet of security research in Europe.”²¹⁸

As a Commission paper once put it: “A competitive EU security industry is the *conditio sine qua non* of any viable European security policy and for economic growth in general.”²¹⁹ In 2014, DG HOME was given responsibility for the ESRP,²²⁰ a move warmly welcomed by EOS²²¹ and of which a Commission spokesperson said:

“The aim is to create a synergy between research on security and those actually dealing with security policy on a daily basis in the EU: police forces, first responders, fire fighters, and border guards for example. This will improve the added value and effectiveness of the EU’s investment in security research...”

In July 2016, PASAG produced a paper setting out its “visions” for 2030 and its advice to the European Commission for the remaining years of the Horizon 2020 research programme. As well as reasserting the need to continue the four current research priorities (borders and external security; fighting crime and terrorism; disaster resilience; cybersecurity) the group added a

fifth – “Competitive European Security Industry” – and made clear demands for the type of public-private merger advocated by EOS in its “end-to-end approach”. According to PASAG (emphasis added):

*“...we need to expand collaboration between the public and private sectors in the field of civil security. The public private partnership (PPP) instruments, notably the new PPP on cybersecurity, are creating interest in **new governance models with varied stakeholders**. This should help develop security capabilities that would otherwise be unaffordable or impractical... **Other models should also be tested** to alleviate the acquisition burdens of the operators, **by transferring the responsibility to acquire and operate capability to the private sector.**”²²²*

The “new governance models” in question explicitly involve the intertwining of public authorities and private interests, leaving a multitude of questions about accountability, influence and democratic control unanswered. These issues, however, were not mentioned in the PASAG report – instead the concern was with ensuring that governments can afford to deploy the technologies industry offers them – lightening the “acquisition burden” (i.e. cost) by renting technology from private firms, who would retain ownership and be responsible for its operation.

The point was emphasised by PASAG with regard to border control, calling for: “Innovative business models to enable new private sector services to augment border management capability including airborne and land-based surveillance,”²²³ and a 2015 internal note prepared for Commission officials meeting with ASD representatives referred to “exploring the scope for private sector services, through R&D, to undertake public sector protection and security missions for authorities across Europe.”²²⁴ In fact, moves towards such “innovative business models” have been afoot for some time at EU level.



In 2013, EU border agency Frontex attempted to purchase a plane for aerial surveillance of the Greek-Turkish border, but received no bids from potential suppliers. Undeterred, in 2014 the agency tried again – but this time by contracting services from a company, rather than purchasing a plane and the associated surveillance technology outright. The contracted service provided for this pilot project, which involved surveillance of the Bulgarian-Turkish border, was described by the agency as “accessible, qualitative, effective and cost efficient, which stipulates new approaches in Frontex policy for future acquisition of operational assets and services.”

This model has recently developed significantly. In early 2017 the European Maritime Safety Agency signed contracts worth tens of millions of euros for maritime surveillance drone services. However: “EMSA decided not [to] buy the drones... but to rent their availability,” from Portuguese company Tekver, the Portuguese Air Force and Leonardo (formerly Finmeccanica).²²⁵ Imagery and information obtained will be used by EMSA, the European Fisheries Control Agency, and Frontex in its mission for total surveillance of Europe’s borders and beyond.²²⁶ At Europe’s borders, largely away from public scrutiny or knowledge, a new public-private apparatus of surveillance and control is being constructed.

Another victory for the industry has come from the development of schemes aimed at encouraging the purchase of new technologies. Pre-Commercial Procurement (PCP) and Public Procurement of Innovative Solutions (PPI) were introduced into Horizon 2020 to promote better “uptake” of the results of security research projects.²²⁷ They differ in their details, but ultimately revolve around securing commitments from public authorities for the purchase of privately-supplied goods before they are put on the market, as well as greater “end-user” involvement in the design and testing phases of new technologies.

For all the talk of the need to create a “true internal market for security”, the existence of these schemes and the ongoing “public-private dialogue” simply seems to back up the admission made by none other than the EOS itself: that “security is often in a position of market failure,” where “the allocation of goods and services by a free market is not efficient.”²²⁸ As the 2014 study for the European Parliament noted with regard to a scheme that preceded PCP and PPI:

“In sharp contrast with the idea of shaping a security market... the underlying idea here seems to be the promotion of a non-market commercial relation between the ‘security industry’ and public sector customers.”²²⁹

While this might be fruitful for the producers of the latest security technologies and processes, it is far from apparent that the security issues Europe faces will be best addressed by offering corporations yet more influence over public policy. Yet it seems bringing together public and private institutions into novel “governance structures” is a key plank of the ‘Security Union’ that is under construction (see Section 4). The fact that these structures and the unchecked continuation of the “public-private dialogue” poses clear risks for the basic principles of democratic, accountability and transparency is rarely mentioned.

This section examines the development of the EU’s security policy and budgets in the 2014-20 period, which has built on the structures put in place by the 2007-13 budgets and developed within the context of a political environment increasingly characterised by authoritarian security measures implemented by governments of varying political stripes. The security research projects being pursued are increasingly aligned with EU’s own laws and policies, and continue to bear the hallmarks of militaristic ideals for the management and control of society.



Current EU migration and home affairs commissioner, Dimitris Avramopoulos.

BUILDING THE 'SECURITY UNION'

"Increasingly, we're going to be in a society, where we have to be ready to sacrifice certain freedoms in the interest of fighting terrorism" (Charles Michel, Belgian prime minister, August 2015)²³⁰

"You don't need a full-blown war... This is where the market is today." (Gilad Alper, June 2016)²³¹

4.1 THE PRICE OF SECURITY

The EU's multi-billion-euro security budgets provide ample backing for the further development of both national security states and the development of the security-industrial complex at European level, with plans decided and implemented in secret and research funds continuing to heavily benefit major research institutes and transnational corporations.

In April 2014, the EU's €3.8 billion Internal Security Fund was approved. It is split into two areas, one dealing with borders and visas (worth almost €2.8 billion) and the other law enforcement (just over €1 billion, amounts distributed to Member States are outlined in an annex to this report). Combined with the €1.7 billion of the ESRP, these budgets represent a €5.5 billion contribution towards the development of what is now referred to as the 'Security Union'. This moniker emerged in 2016 as a way to encompass the aims of the EU's security policy efforts, which involves doing "everything necessary to support Member States in ensuring internal security and fighting terrorism... in today's world the internal security of one Member State is the internal security of all."²³²

The EU's home affairs funding, which the Commission says "ensures adequate support for building a more open and secure Europe," also includes the €3.1 billion Asylum, Migration and Integration Fund (playing an increasing role in funding security-focused projects) and the almost €2.4 billion reserved for EU home affairs agencies such as Europol and Frontex, adding up to over €11 billion in total. This represents only a small part of the EU's total available funds of over €1 trillion from 2014-20 and pales in comparison to the almost €248 billion apparently spent on "public order and safety" by EU governments in 2014 alone. Nevertheless, as Cecilia Malmström, at the time Commissioner for Home Affairs, noted following the approval of the budget: "despite the financial crisis, the overall resources of the Home Affairs Funds have been increased... This reflects the growing importance of this policy area at EU level."²³⁵

All Member States and the four Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland) are participating in both ISF budgets with the exception of Ireland and the UK in ISF-Borders, and Denmark and the UK in ISF-Police. The Commission has significant strategic influence over how the money is spent – Member States must submit work programmes covering the six years of the budget to the Commission for approval, whereas in the past the money was distributed based on annual work programmes and ad hoc projects. The programmes currently in place were drafted by the Commission and the Member States before the legislation was even approved.²³⁶

The funds are intended to ensure the implementation of the EU's Renewed Internal Security Strategy (ISS), agreed in 2015 and chiefly concerned with terrorism and radicalisation, border security, serious and organised crime and cybercrime.²³⁷ The strategy has spawned a whole host of initiatives²³⁸ and is also accompanied by a specific agenda on cybersecurity, a 'European Agenda on Migration' and a new Global Strategy and Foreign and Security Policy. This latter document calls for new investments in "the monitoring and control of flows which have security implications" through "Intelligence, Surveillance and Reconnaissance, including [drones], satellite communicates, and... permanent earth observation," along with "full-spectrum land, air, space and maritime capabilities, including strategic enablers."²³⁹

The development of such technologies is where the ESRP comes in. The legislation establishing the Internal Security Fund makes a clear link to the security research programme, stating that the funds can be used to pay for "projects aimed at testing or validating Union funded security research projects". If implemented successfully this would complete the process that begins with research and ends with deployment. The Internal Security Strategy was also keen on this point, calling for "enhancing the training, funding, research and innovation possibilities, especially further developing an autonomous industrial security policy." Security is both a political and an economic priority – growth is expected to be significant in the "public security market" in the coming years.²⁴⁰

As of December 2016, €492 million of the ESRP's €1.7 billion budget had been committed. National research institutes have been some of the chief recipients so far, continuing a trend from the FP7 period (see section 2.2). The top 10 organisations to receive funding up to December 2016 feature some familiar names: the Fraunhofer Institute (Germany, 24 projects, €14.2 million in EU funding), France's *Commissariat à l'énergie atomique et aux énergies alternatives* (seven projects, €7.1 million), Greece's Centre for Research and Technology Hellas (eight projects, €4.6 million), TNO (the Netherlands, seven projects, €3.6 million) and the Italian National Research Council (*Consiglio Nazionale della Ricerche*, eight projects, €3.3 million). They are joined by multinational corporations such as Atos (15 projects, €6.5 million), Thales (nine projects, €4.6 million), Engineering (an Italian company, six projects, €4 million) and Airbus (two projects, €3.6 million).

This is par for the course, but there are some changes. An increasing number of higher education institutions and SMEs (small-and-medium-sized enterprises) are participating in the ESRP than previously, which suggests that, to some extent, the ideology and vision underlying the programme – the development of militaristic command-and-control models for "civil security" purposes – has spread from research institutes and corporations to

other bodies as well. This hypothesis is backed up by the numerous grants that have been made to SMEs as part of the ESRP budget. Under the heading of “engaging SMEs in security research”, dozens of funded projects tread remarkably similar ground to many of the bigger research projects during the FP7 period (see section 4.5).

These and other organisations are working on projects for border surveillance systems, big data retrieval and analysis software for law enforcement, counter-radicalisation programmes, critical infrastructure protection methodologies and technologies, and voice and gait biometrics, amongst other things. While their development is no doubt well-intentioned, and while new technologies can undoubtedly play a part in ensuring people’s safety and security, the successful development and deployment of such technologies would offer unprecedented powers to state agencies to monitor and control individual activity, and in this respect it is crucial to critically examine both the technologies themselves and context in which they are supposed to be deployed.

As was argued in section 1, many of these technology development projects, and EU policies themselves, reflect a “presumption of threat” with regard to the population at large that undermines “a foundational principle of the liberal order”²⁴¹ – that individuals are not inherently threatening. These projects and policies are promoted and approved at EU level, where they are significantly shaped by both corporate interests and national government preferences. When they come to be implemented at national level, it will be in an environment shaped by European governments passing “a deluge of laws and amendments passed with break-neck speed, ... undermining fundamental freedoms and dismantling hard-won human rights protections.”²⁴²

This includes fast-track legislative processes for “emergency” legislation, derogation from human rights commitments, lack of independent oversight mechanisms on counter-terrorism powers, the use of administrative control measures and fines to restrict

movement and free expression; and increased possibilities for states to use secret evidence in court.²⁴³ The EU’s security policies risk legitimising and empowering the authoritarian tendencies in some governments that have come to power across the continent over the last decade. It is unsurprising that this is not a point of interest for national governments in the EU who are adopting such powers; but neither does it appear to

have raised the concern (at least publicly) of the European Commission, responsible for proposing legislation and monitoring its implementation.



DANGEROUSLY DISPROPORTIONATE
THE EVER-EXPANDING NATIONAL SECURITY STATE IN EUROPE
SECURITY

Indeed, plans are ongoing to further extend the EU’s security initiatives by propelling greater “synergies” between the development of civil and military technologies and the initiation of an EU military research programme. While the ESRP legislation says that “activities carried out under Horizon 2020 shall have an exclusive focus on civil applications,” the Commission has announced its intention to “evaluate how the results [of research projects] could benefit also defence and security industrial capabilities” and “intends to explore synergies in the development of dual-use applications,” such as drones.²⁴⁴ The ESRP’s “external security” research theme explicitly “requires promoting interoperability between civilian and military capabilities,” and “will include technological development in the sensitive area of dual-use technologies.”²⁴⁵ The legal obligation for “an exclusive focus on civil applications” is apparently meaningless.

The proposed military research programmes is being established through a process remarkably similar to that which established the ESRP (and a recent Public-Private Partnership on Cybersecurity, see section 4.4). A high-level ‘Group of Personalities’ dominated by state officials and industry representatives (including familiar names such as Indra, Airbus, BAE Systems, TNO and Finmeccanica) was invited by the Commission to map the way ahead.²⁴⁶ They called for at least €3.5 billion to be devoted to a European Defence Research Programme (EDRP) between 2021 and 2022,²⁴⁷ a figure the Commission subsequently endorsed.²⁴⁸ ASD has noted that “one of the main challenges” in this will be “to avoid that currently envisaged funding for defence research will come along with a reduction of funding for security research.” The Protection and Security Advisory Group (PASAG, see section 3.4) has established a working group dedicated to ‘Optimising access to dual-use R&D&I for civilian security applications’, while the ground for the EDRP is currently being prepared with a €90 million ‘Preparatory Action’ between 2017 and 2019.²⁴⁹

4.2 ALL-SEEING EYES: FIGHTING CRIME AND TERRORISM

EU law and policy regarding law enforcement is heavily reliant on the nurturing of often-unaccountable transnational policing networks and policy forums; and the collection, processing and transnational exchange of large amounts of personal data, something reflected in the research agenda for the ESRP which is developing a vast array of new tools for surveillance, profiling, and automated crime detection.

The EU's role in law enforcement has long centred on a mixture of legislative interventions (for example, the European Arrest Warrant, the European Investigation Order or the Data Retention Directive) and the establishment of transnational databases, computer networks and training programmes intended to ease the gathering and exchange of information and to encourage the development of a European policing model. Databases – for example on short-stay Schengen visa applicants and asylum-seekers' fingerprints – have been opened up to police access in recent years, while the Schengen Information System is being revamped to make possible fingerprint searches and to include DNA samples. A significant drive for the “interoperability” of EU security databases has recently been launched – seemingly a step towards their eventual interconnection – while the Internal Security Fund and the ESRP are paying for the implementation of EU policy (for example, on air travel surveillance system based on Passenger Name Record data) and the development of further novel technologies.

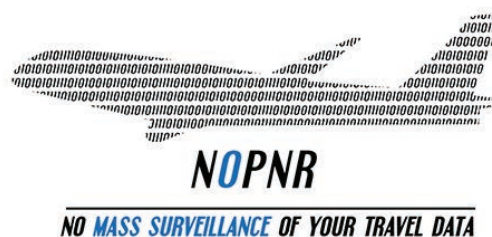
These EU-level developments are accompanied by significant changes at national and local level. Aside from the introduction of numerous repressive legal measures across the EU – increased length of detention without charge, expanded surveillance powers for security agencies and police forces, limits to freedom of expression – law enforcement agencies are increasingly being equipped with new technologies. The COMPOSITE project, funded by the FP7 security budget to investigate “change management” in the police, highlighted the growing interest in the integration of information systems, the use of mobile technology, surveillance systems (including automated systems), digital biometrics (which “will become a ubiquitous piece of digital personal information”) and an increased use of social media for publicity and investigation purposes. Some disturbing technologies are mentioned in the report. For example, the Dutch police are apparently well ahead in “special equipment deployment, such as “mobile weapons scanners” being developed “for patrol officers on the street,” and research into the use of smells, bright lights and noises “to exploit physical reactions to create ‘less-lethal technologies’ with a mass effect” for use on crowds.²⁵⁰

Police forces are, it seems, slowly coming closer to being able to access and process information on a scale traditionally reserved for security and intelligence agencies, and the EU is helping the process along. In terms of crime and counter-terrorism legislation, the high-profile Passenger Name Record (PNR) Directive, approved in April 2016, continues the longstanding theme of mass, pre-emptive surveillance and a “presumption of threat”. The legislation’s stated aim is:

“to prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, to gather evidence and, where relevant, to find associates of criminals and unravel criminal networks.”²⁴⁹

The effect of the Directive is to place all air travellers entering, leaving or flying within the EU under suspicion: they are automatically subjected to checks against police watchlists, databases and profiles. Given the tendency of police forces towards racial profiling, this is far more likely to negatively affect some travellers than others. At the same time, it kills off, at least for air travel, the principle of free movement within the Schengen area, which is based on the requirement that systematic checks at internal frontiers do not exist.

The Commission began providing millions of euros for the development of national PNR analysis units in 2012, long before the legislation was adopted, in an anti-democratic process with echoes of the development of border surveillance system Eurosur and, to some extent, “smart borders” (see section 2.3 and 4.3). This dovetailed neatly with subsequent decisions taken by a select group of Member States in July 2014 (those “most concerned by the issue of foreign fighters in Syria”), who sought “the interconnectivity of national PNR systems while we await completion of the negotiations on the EU PNR Directive.”²⁵² Cecilia Malmström, then EU home affairs commissioner, denied that the EU funding was linked to negotiations on the Directive, but there were certainly a neat convergence of interests.²⁵³



An image produced by the European Digital Rights Initiative (EDRI) as part of the campaign against the PNR Directive.

Member States are currently in the process of implementing the Directive, although seemingly without the urgency they cited when they wanted to get it through the Parliament.²⁵⁴ Former French prime minister Manuel Valls – who was one of those keenest on the legislation “is a cheerleader both for the PNR directive and for a company called Safran, which sells PNR surveillance technology.”²⁵⁵ Safran is one of the many security firms that stand to benefit from the PNR Directive, and the EU is on hand to help: Member States that have not previously received EU funding for the establishment of

national Passenger Information Units can make use of the Internal Security Fund. The Belgian plan for the ISF-Police budget, for example, suggests that “a significant share of the national programme could be devoted to the setting up of a Passenger Information Unit,”²⁵⁶ and further EU assistance is coming from a dedicated informal working group.²⁵⁷

Giving law enforcement authorities the ability to collect and analyse vast amounts of data for the purposes of automated crime prevention and investigation is also a major theme in the ESRP,²⁵⁸ with four major projects currently being funded. ASGARD (‘Analysis System for Gathered Raw Data’) will focus on “Forensics, Intelligence and Foresight (Intelligence led prevention and anticipation),” and aims to “drive progress in the processing of seized data, availability of massive amounts of data and big data solutions in an ever more connected world.” The project “has a singular goal, contribute to Law Enforcement Agencies Technological Autonomy and effective use of technology,” and the project has over 30 participants from across the EU (including IBM, the Italian defence ministry, and the interior ministries of Belgium, Germany, Italy and the UK), with the ESRP budget providing 100% of the €12 million cost.²⁵⁹

The RAMSES project (‘Internet Forensic platform for tracking the money flow of financially-motivated malware’), meanwhile, aims to develop a system able to “extract, analyse, link and interpret information extracted from Internet related with financially-motivated malware,” using “disruptive Big Data technologies” to store and examine “enormous amounts of unstructured and structured data.” The EU is providing €3.5 million to the project, with the Belgian and Italian interior ministries amongst the project participants.

Two further projects will examine automated “detection and analysis of terrorist-related content on the Internet” through data-mining and big data analytics.” TENSOR (‘Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition’)²⁶⁰ and DANTE (‘Detecting and Analysing Terrorist-related online contents and financing activities’).²⁶¹ Both will receive €5 million from the EU, with TENSOR counting Finmeccanica, Thales and EOS amongst the project partners; DANTE has (once again) the Italian interior and defence ministries on board alongside the UK Home Office, the Austrian Institute of Technology and Greece’s CERTH.

MEDI@4SEC, which has a rather smaller budget (€1.9 million), is also concerned with open-source data gathering – it will “seek a better understanding of how social media can, and how social media cannot be used for public security purposes.”²⁶² Amongst the participants are the

Fraunhofer Institute, TNO, lobby group EOS, the Police Service of Northern Ireland and the European Forum for Urban Security, “the only European network of local and regional authorities dedicated to urban security.”²⁶³

The introduction of such tools into day-to-day policing practices would of course merely represent the next generation of what are increasingly normalised practices. The EU’s Data Retention Directive, as mentioned earlier (Section 2.4) was struck down by the European Court of Justice in April but as of November 2015, 15 domestic data retention regimes were still in place (11 had been invalidated, 9 of those by a national constitutional court),²⁶⁴ and a majority of Member States were arguing that “an EU-wide approach has to be considered.”²⁶⁵

New data-gathering tools – and the integration of existing ones – are being financed by the ISF-Police budget, for example in Greece, which plans:

“The implementation of a contemporary intelligence-led policing model which is based on the information process and analysis, so as to encourage not only the suppression of criminality but also the predictive attitude towards crimes that have already been committed or will be committed in the future.”²⁶⁶

The programme agreed between Hungary and the Commission includes “data analysis and phishing of web content and social network sites”;²⁶⁷ Belgium is planning the “development or purchase of software for internet monitoring (e.g. websites of radical groups) and data analysis capacity”;²⁶⁸ Croatia has promised to purchase IMSI catchers and establish an internet monitoring capability (amongst other things);²⁶⁹ while Malta’s options include “the procurement of systems facilitating the detection of patterns of crime, threats and risks.”²⁷⁰

Romania’s national programme proposes “gathering information using new IT capabilities”;²⁷¹ an area in which the country’s intelligence agency also has aspirations. The agency, the SRI, was awarded more than €26 million from the European Regional Development Fund for an “anti-fraud” system that involved acquiring “hardware and software for Internet traffic interception from instant messaging apps or other similar electronic communications programmes,” as well as “a database of approximately 50-60 million images (passport or identity card photos) to which SRI will have unlimited access.”²⁷⁰ The project, which was the only bid submitted and was made just seven hours after the funding was announced, is currently the subject of a complaint to the EU’s anti-fraud office.²⁷³

Digital data is not the only way the EU hopes to enhance the powers of police forces and the myriad other bodies increasingly involved in law enforcement. The ESRP is backing a number of projects that hope to encourage people to voluntarily share more information with the police.²⁷⁴ This is also being promoted by the EU's Radicalisation Awareness Network (RAN), which calls for the surveillance of young people and groups deemed "at risk" by teachers, social workers, doctors and other "first line practitioners". The 2016-17 work programme for the ESRP is seeking projects that will provide:

*"[A] full set of policy recommendations and tools aimed at improving their ability to prevent and detect radicalisation by national and local security practitioners in a timely manner, i.e. before individuals turn towards violent, criminal or terrorists acts."*²⁷⁵

In the UK, which has played a key role in the construction of the EU's radicalisation programme, this process is no longer voluntary: teachers and other registered childcare and education providers are now under a legal obligation to participate in the 'Prevent' programme. The policy has been heavily criticised, including by the country's former Independent Reviewer of Terrorism Legislation:

"The programme, particularly its duty on schools to spot and report signs of radicalisation in pupils, has become a 'significant source of grievance' among British Muslims, encouraging 'mistrust to spread and to fester', said David Anderson QC."²⁷⁶

A delegate speaking at the National Union of Teachers' annual conference said the obligation turns teachers into the "secret service of the public sector".²⁷⁷ Dozens of academics have called for the 'Extremism Risk Guidance 22+' framework, which makes up the "science" behind the programme, to be made public, noting that it "has not been subjected to proper scientific scrutiny or public critique."²⁷⁸ The UK's counter-extremism policy has even led to the development of state-funded propaganda campaigns disguised as independent civil society initiatives.²⁷⁹ Parliament's Joint Human Rights Committee has called for "an independent review of the Prevent Strategy to provide evidence as to what works and what simply drives wedges between the authorities and communities."²⁸⁰

A United Nations report looking at counter-radicalisation programmes across the globe concluded that:

"Preventing or countering violent extremism is often presented as a softer approach to countering terrorism. Yet the elasticity of the term 'violent extremism', and the lack of clarity on what leads individuals to embrace violent extremism, means that a wide array of legislative,

*administrative and policy measures are pursued, which can have a serious negative impact on manifold human rights."*²⁸¹

Furthermore, the report warned that "legislation against extremism has in some instances been used against journalists, religious groups or critics of state policy". EU enthusiasm for countering radicalisation and extremism nevertheless remains undimmed, regardless of concerns over dodgy science and potential political repression.

In total, €314 million from the Internal Security Fund will go towards national projects related to radicalisation between 2014 and 2020,²⁸² and radicalisation policies are explicitly mentioned in the Belgian, Bulgarian, Greek, Swedish and Slovenian national programmes. This area is not new for the EU: numerous counter-radicalisation projects others were funded through the FP7 and ISEC budgets (see section 2.4).²⁸³ The most successful FP7 project, at least in the eyes of the Commission, appears to have been SAFIRE (Scientific Approach to Finding Indicators of and REsponses to Radicalisation, led by TNO and with a €2.9 million EU contribution), which aimed to "develop a process model of radicalisation, describing the process from moderation to extremism,"²⁸⁴ and was subsequently marketed to Member States by the Council and Commission.²⁸⁵

Meanwhile, through the "policy cycle on serious and organised international crime" – one of the key pillars of the Internal Security Strategy – EU structures are becoming increasingly involved in operational policing activity. The Council approved nine priorities that will provide the focus for operations between 2013 and 2017:

- Illegal immigration
- Trafficking in human beings
- Counterfeit goods
- Excise fraud and missing trader intra-community fraud
- Synthetic drugs
- Cocaine and heroin
- Cybercrime: card fraud, child sexual exploitation and cyberattacks
- Firearms
- Organised property crime

After a slow start, the initiative has attracted more support from Member States. Since 2011 (when it developed from the Belgium-led 'Project Harmony'²⁸⁶) it has grown considerably. As a Europol report from June 2016 put it:

"The scale of the OAPs [Operational Action Plans] is larger than ever before. There are 260 actions currently running, 56 from 2015 OAPs and 204 from 2016 OAPs; 130 have an operational focus

and 133 are funded by EMPACT [European Multidisciplinary Platform Against Criminal Threats] Delegation Agreement grants. This is large-scale work.”²⁸⁷

Programmes for the ISF-Police budget affirm national support for the EU approach: Belgium will “adopt a strategic approach, based on our national strategies and the EU policy cycle,”²⁸⁸ Croatia promises an alignment of national priorities in a variety of areas with those of the EU,²⁸⁹ Hungary assures “greater involvement in the implementation of the policy cycle,”²⁹⁰ Latvia notes “the necessity to integrate the EU Policy Cycle on the national level,”²⁹¹ while Romania “is entirely dedicated to implementing the EMPACT priorities and is actively participating in all the priorities of the present EU policy cycle.”²⁹²

Yet despite the scale and scope of the policy cycle, the whole process operates without any significant democratic accountability or transparency. In 2014, an MEP from the conservative European People’s Party asked the Council “how it intends to involve Parliament” in determining the policy cycle priorities,²⁹³ which would introduce at least some degree of democratic involvement. In response, the Council simply said it would “continue to report regularly to the European Parliament on the activities of COSI [the Standing Committee on Operational Cooperation on Internal Security],”²⁹⁴ the Council body that retains overall responsibility for planning and oversight.

As EU Member States’ police forces increasingly work together, they are also supposed to be equipped with all manner of new gadgets, as demonstrated by the current roster of ESRP projects. NOSY (New Operational Sensing sYstem) will cost the EU almost €4.2 million (of a total of €5.37 million) and will be coordinated by Italian company Aero Sekur, a “global provider of advanced survival equipment and systems for mission critical Aerospace & Defence applications”.²⁹⁵ Other participants include the French, Portuguese and Italian interior ministries. The project aims at:

“[T]he development of a miniaturized yet highly sensitive platform, for the detection of illicit or suspicious substances... As deemed necessary by LEAs, the project will develop prototype products to help tackle illegal drug trafficking and development of homemade bombs.”²⁹⁶

The €4.9 million FORENSOR project (FOREnsic evidence gathering autonomous seNSOR), coordinated by Greece’s CERTH research institute, argues that “covert evidence gathering has not seen major changes in decades” (a bold claim given the rise of spyware, IMSI catchers and other law enforcement gadgets). The EU is contributing €4 million of the costs of the project, which aims to develop and validate “a novel, ultra-low-power, intelligent,

miniaturised, low-cost, wireless, autonomous sensor (FORENSOR) for evidence-gathering,” which will:

“[O]perate at remote locations, automatically identify pre-defined criminal events, and alert LEAs in real time while providing and storing the relevant video, location and timing evidence. FORENSOR will be able to operate for up to two months with no additional infrastructure.”²⁹⁷

Meanwhile, if you ever thought that the sewage system wasn’t doing enough to fight crime, then the microMole project (‘Sewage monitoring system for tracking synthetic laboratories’) is here to reassure you, with the development of sensors that “will be installed within the sewage system and will track waste associated to ATS [amphetamine-type stimulants] production.”²⁹⁸ This continues a popular theme from FP7 era – equipping utility networks (for example, water, electricity or telecommunications) with surveillance equipment. The microMole project is complemented by BIWAS, funded under the ‘disaster resilience’ theme, which is concerned that “potential terrorists might threaten water infrastructure in European cities,” and thus an “early warning system against CBRN threats in drinking water” is required.²⁹⁹ Should early warnings fail, the €4.7 million ROCSAFE project, coordinated by the National University of Ireland in Galway, will provide “cost-effective modern remotely-controlled robotic air and ground vehicles” in order “to fundamentally change how CBRNe events are assessed.”³⁰⁰

This kind of work is set to continue. The 2016-17 ESRP work programme contains the theme “integration of detection capabilities and data fusion with utility providers’ networks” and notes that these networks “can constitute networked (mobile) platforms for sensors, but this potential remains largely untapped.”³⁰¹ It seems that the very fabric of towns and cities is set to spy on the population.

The ESRP has also been seeking to enhance the training of law enforcement agents,³⁰² with a number of projects to develop virtual and “mixed-reality” environments aimed at creating a “pan-European platform for serious gaming and training.” Israeli institutions seem to have some expertise in this area: LAW-TRAIN (‘Mixed-reality environment for training teams in joint investigative interrogation-Intelligent interrogation training simulator’)³⁰³ is led by Bar Ilan University and also involves the Israeli public security ministry, along with the Italian interior ministry, the Belgian justice service and the Portuguese ministry of justice, amongst others.³⁰⁴ One of the partners in the AUGGMED (‘Automated Serious Game Scenario Generator for Mixed Reality Training’)³⁰⁵ is the Israeli company Isra-Team 98, which unsurprisingly claims to have “vast and unique ‘hands-on’ experience in all kinds of crisis, especially in War and CBRNE terror events.”³⁰⁶ LAW-TRAIN is to receive €5.1 million and AUGGMED €5.5 million.

These two projects are complemented by TARGET (Training Augmented Reality Generalised Environment Toolkit)³⁰⁷, awarded €6 million to develop:

“Mixed-reality experiences [which] will immerse trainees at task, tactical and strategic command levels with scenarios such as tactical firearms events, asset protection, mass demonstrations, cyber-attacks and CBRN incidents”.

Participants include the Spanish interior ministry, the German and French police schools, and the Fraunhofer Institute. The target audience is “Security Critical Agents – counterterrorism units, border guards, first responders (police, firefighters, ambulance services, civil security agencies, critical infrastructure operators.” The use of games also underpins the GAP project, albeit focused for a change on conflict prevention and peace building.³⁰⁸

Biometrics were a key feature of FP7-funded projects and continue in the Horizon 2020 crime and terrorism research agenda. ARIES (‘Reliable European Identity Ecosystem’)³⁰⁹ has received €2.2 million, with one aim being to “provide a global approach for ID Ecosystem in Europe.” It will investigate “virtual and mobile IDs... derived from strong eID documents in order to prevent identity theft and related crimes.” The project focuses on “secure eCommerce and identity virtualization for secure travel” but has wider ambitions:

“Both, the derivation process, and the derived IDs will be univocally linked to citizens’ biometric features... the project will provide a global approach for ID Ecosystem in Europe to address European-specific concerns to improve identity, trust and security, and better support the law enforcement.”

The FLYSEC project (€4.1 million from the EU), funded under the ‘disaster resilience’ theme, is also keen on making use of biometrics, this time in a model of airport security seemingly based on total surveillance:

“FLYSEC achieves its ambitious goals by integrating new technologies on video surveillance, intelligent remote image processing and biometrics combined with big data analysis, open-source intelligence and crowdsourcing... as well as RFID for carry-on luggage tracking and quick unattended luggage handling. Besides more efficient background checks and passenger profiling, FLYSEC aims to implement a seamless risk-based security process within FLYSEC combining the aforementioned technologies with behavioural analysis and innovative cognitive algorithms.”³¹⁰

Elsewhere in the research agenda, the development of speech recognition systems has received significant

attention as a way to implement various forms of automated access control: the granting or denying individuals permission to access a building or area (see section 4.5).

The general enthusiasm for a “no stone unturned” approach to “fighting crime and terrorism” shows no sign of letting up. That the acquisition of the technologies under development could place vast numbers of people under generalised suspicion, significantly enhance the powers of police forces and magnify current inequities and biases in policing is something that should be of significant concern.

4.3 THE WALLS AROUND US ALL: BORDER SECURITY

The EU’s model of “border security” is converging around a principle of total surveillance and tracking of all non-citizens entering the bloc, whether for tourism, business or to seek refuge, while EU citizens themselves are increasingly the subject of suspicion when they cross the EU’s external borders.

The EU’s migration policies are based on the idea of ‘Integrated Border Management’. This revolves around a “four-tier” model: measures in non-EU states (for example through common EU visa policies, projects aimed at encouraging people to stay put, or by funding border control actions);³¹¹ border control measures at the external borders of the EU; control measures within the Schengen area (for example, through national actions or coordinated operations); and return.

The model revolves around the idea we need to let the “right” people in and keep the “wrong” people out. Just who belongs in each of these categories is a rather contentious subject: refugees, for example, have long been considered the “wrong” kind of person in EU migration policy, as demonstrated by the fact that vast numbers of them must risk their lives on perilous journeys. EU laws prevent them from arriving “regularly”, for example with a simple plane, boat, train or coach journey. Thus, in theory at least, everyone arriving on EU territory is to be subjected to data-gathering and surveillance practices.

The future foreseen in the EU’s border policies and research projects is one of ever-more intensive surveillance and automated decision-making, with the interior and borders of Europe (and beyond) patrolled permanently by integrated robot and sensor networks

that will provide instant information to state officials, or – even better – act “autonomously” to “neutralise” perceived “threats” to Europe’s border security. As one border surveillance project funded by the FP7 budget put it: “You cannot control what you do not patrol.”³¹²



Commission officials present the European Agenda on Migration, May 2015.

Since the beginning of 2015, the increasing number of people arriving in Europe seeking refuge has put the issue of migration to the top of the EU’s policy agenda. The Commission’s ‘Agenda on Migration’, adopted in May 2015, set out the EU’s proposed short- and medium-term response to the humanitarian crisis, and proposals for future EU migration policy more generally. The immediate concerns set out in the paper were saving lives at sea, “targeting criminal smuggling networks”, relocation and resettlement of refugees, increased cooperation with third countries “to tackle migration upstream”, and offering more support to “frontline Member States” (i.e. Italy and Greece).³¹³

As a December 2015 assessment by one group of experts on EU home affairs policy put it, this response has:

“given priority to security-driven (home affairs) and military concerns and interests of the EU and its member states, where the focus on border controls, return and readmission and fighting against smuggling have by and large prevailed, instead of first ensuring full compliance with fundamental human rights standards and principles.”³¹⁴

Rather than taking the opportunity to break with the past and forge a new migration policy that prioritises human rights, “institutional path dependency”³¹⁵ has meant the EU has continued to encourage the militarisation, ‘securitisation’ and externalisation of border control.³¹⁶ Despite the involvement of warships and other military gear (in Operation Sophia) and ongoing attempts to further outsource the EU’s borders to sub-Saharan Africa, the current approach has not (and cannot) stop the deaths inflicted by EU migration and border policies. 2016 was the deadliest year on record for migrants attempting to cross the Mediterranean, with over 5,000 people dying at sea.³¹⁷

One system under development for some time that is oft-cited as a way to prevent deaths at sea is the European Border Surveillance System, or Eurosur. This is made up of a network of national maritime surveillance systems, along with information from agencies such as the European Satellite Centre and the European Maritime Safety Agency that is used to create a “European situational picture,” covering the EU’s borders and a “common pre-frontier intelligence picture (focused on areas beyond the Schengen area and EU borders).”³¹⁸ The EMSA, as noted in section 3.4, has acquired maritime drone surveillance services by renting them from corporations as part of a multi-million euro contract, with the intention to better feed Frontex’s information-gathering.



The foreseen structure of the Eurosur surveillance network, in a presentation produced for the EU-funded GLOBE project

In a wholly undemocratic process (but rather familiar pattern), the system was decided upon and developed some years before it was finally agreed by the EU legislature in 2013. As explained in section 2.3, it has also been helped along significantly by the ESRP, through which millions of euros have been provided for development and implementation.³¹⁹ By December 2014, all 30 participating states were connected to the system,³²⁰ and its further development is being propelled by the ISF-Borders budget. This is supporting Bulgaria in its development of an “automated surveillance system” for its border with Serbia,³²¹ Estonia wants to integrate drones into the system,³²² and all Member States are beefing up their surveillance equipment to better control their borders and feed the Eurosur network, for example with thermal and night vision cameras and various types of sensor systems.

The system is defended politically on the basis that it can help save lives, but this is questionable, and Frontex officials have admitted as much. Gil Aria Fernandez, the agency’s Deputy Executive Director, said in May 2014 that “for the time being, [Eurosur] does not fulfil this service,” that the addition of satellite imagery to the system would not help due to delays in receipt and

processing, and that ultimately: “Improving the situation to prevent casualties, to prevent people from sinking and drowning in the sea, will not be possible by border control, this is obvious.”³²³

Eurosur is supposed to provide national authorities and Frontex with intensive surveillance of the “pre-frontier area,” such as the ports of states in North Africa. The system is in fact geared towards preventing people travelling to Europe in the first place, and it has had some very clear benefits but not for refugees. For example, since 2010 Portuguese firm GMV has been responsible for maintaining the system’s infrastructure. As the company’s press release put it following the signing of the contract to take Eurosur from “pilot project” to full “operational status”, Eurosur “fits in perfectly with GMV’s ongoing strategy of internationalizing its defense and security activities and consolidates its leadership within European border surveillance activities.”³²⁴ More recently, the firm announced that it is contracts with EU agencies that have boosted its international sales to record levels.³²⁵

The support given to Eurosur by the ESRP continues in Horizon 2020. The €5.1 million SafeShore project (‘System for detection of Threat Agents in Maritime Border Environment’) will:

“[C]over existing gaps in coastal border surveillance, increasing internal security by preventing cross-border crime such as trafficking in human beings and the smuggling of drugs. It is designed to be integrated with existing systems and create a continuous detection line along the border. One of the threats to the maritime coast are small Remotely Piloted Aircraft Systems (RPAS) which can carry explosives or which can be used for smuggling drugs, boats and human intruders on the sea shore.”³²⁶

Partners include Belgian police forces, universities from London and Salento (Italy), and Bulgarian, Romanian and Czech companies. The Belgian Royal Military School is leading the project. Its “core solution for detecting small targets that are flying at low altitude is to use a 3D LIDAR that scans the sky and creates above the protected area a virtual dome shield,” which will be developed with partners including the Israeli Ministry of Public Security.³²⁷

The RANGER project (‘RADars for loNG distance maritime surveillancE and SaR opeRations’), led by Exus Software with NATO, the Greek defence ministry and Leonardo (formerly known as Finmeccanica), has been awarded almost €8 million by the EU. It hopes to develop a “surveillance platform offering detection, recognition, identification and tracking of suspicious vessels, capabilities exceeding current radar systems.”³²⁸

ALFA, involving TNO, Thales, Engineering, Atos and the Portuguese interior ministry – amongst others – has received €4.6 million to develop a drone detection system for use initially at the borders, but which will be “suitable for a range of other missions and scenarios such as homeland and event protection and the protection of critical infrastructure.” A common aim of all three projects is the further development of Eurosur and its eventual integration of the CISE system.



Life jackets discarded by migrants and refugees arriving on the Greek island of Lesbos.

The CISE – or ‘Common Information Sharing Environment’ – aims to provide “better and cheaper maritime surveillance” through “integrated maritime surveillance”. Work on this issue has been ongoing since at least 2002:

“The aim of integrated maritime surveillance is to generate a situational awareness of activities at sea, impacting on maritime safety and security, border control, maritime pollution and marine environment, fisheries control, general law enforcement, defence as well as the economic interests of the EU, so as to facilitate sound decision making.”³²⁹

The EU has produced some remarkable figures to try to justify the system: if “all relevant information” was available to various authorities, according to a July 2014 Commission paper, it “could potentially lead to the reduction of such threats and risks by 30% on average.”³³⁰ Plans are rolling ahead: the EU CISE 2020 project was awarded €13 million in the last year of the FP7 ESRP (its total cost is €17 million). It aims to help implement the CISE roadmap by drawing up an “action plan for the operational validation of new elements of R&D,” the “development of an open European test bed for incremental advancement of CISE,” and also by assessing the “organizational instruments necessary to sustain the appropriate governance structure and to stimulate public-private cooperation.”³³¹ Whether there will be any greater democratic oversight of the project, led by the Italian Space Agency and with numerous defence and interior ministries as partners, has not yet been mentioned.³³²

Non-refugee travellers may not have to put themselves at risk of death, injury and post-traumatic stress disorder to enter the EU, but they are becoming increasingly subjected to invasive screening and surveillance methods.³³³ All visa applicants have to submit their fingerprints to national authorities, which are then held in the Visa Information System for five years. A European Travel Information and Authorisation System – essentially an EU version of the US Electronic System for Travel Authorisation – is also under discussion. If introduced:

“visa-exempt travelers [sic] would register relevant information regarding their intended journey via the internet. This would facilitate the border crossing of these third country nationals and increase the effectiveness of the work for the border guards. As a secondary objective, a system could help Law Enforcement Agencies combatting serious crime and terrorism. The automatic processing of this information could help border guards in their assessment of third-country visitors arriving for a short stay.”³³⁴

The European Data Protection Supervisor (EDPS) – an independent EU body with no legislative powers – has warned:

“The proposal provides for the establishment of screening rules, a profiling tool that would enable the ETIAS system to single out individuals suspected of posing [security, irregular migration and public health] risks. In his Opinion, the EDPS stresses that profiling techniques, as with any other form of computerised data analysis, raise serious technical, legal and ethical questions, related to their transparency and accuracy, and calls on the Commission to produce convincing evidence establishing the need for their inclusion and use in the ETIAS system.”³³⁵

Proposals for “smart borders”³³⁶ (see also Section 2.3) are another fundamental plank of the EU’s border plans, and initially consisted of plans for an Entry/Exit System (EES), a Registered Traveller Programme (RTP) and related amendments to the Schengen Borders Code. The EES would take facial and fingerprint biometrics and “record the time and place of entry and exit of third country nationals travelling to the EU,” in order to help detect “overstayers” and assist in law enforcement investigations, while the RTP would allow swifter border crossings for pre-registered and pre-vetted travellers. The RTP plans were subsequently dropped, but the European Parliament and the Council are close to reaching agreement on the EES, despite the fact that the reasoning and financial estimates underpinning the Commission’s proposal were soundly demolished in a report for the European Parliament.³³⁷ France and other Member States have shown an interest in extending it to cover “all travellers” – EU citizens and non-citizens alike.³³⁸

The business interest in the smart borders project is considerable, and it is easy to see why:

“[T]hese new borders would necessitate the erection of special kiosks equipped with biometric tools (e-gates), which all the states included in the free circulation area would have to purchase. In France, 133 Schengen border points could be involved, including 86 airports, 37 ports and 10 train stations. Considering that the cost of each e-gate is estimated to be between 40,000 and 150,000 euros, the investment is not negligible!”³³⁹

This, in fact, may only be the beginning of the new technology required to fully implement the EES. With its aim of detecting “overstayers”, there will presumably be a need for all officials responsible for conducting checks on individuals’ migration status – those working at border crossings and those within national territories – to have access to the system. As the Commission put it in an impact assessment document:

“Overstayers can be apprehended by means of inland controls. In 2014, the number of overstayers detected within the Schengen area amounted to 441,780, according to the regular collection by Frontex of data from Member State [sic]... For the control of third country nationals present in the Schengen area, if the individuals do not present their travel documents (for example, because they claim to have lost them), it is impossible to determine accurately their entry date as well as their citizenship.”³⁴⁰

In this scenario, the mass purchase by national authorities of fixed and/or mobile fingerprint scanners connected to the central system would also be required. Thus, the FP7 security research programme began backing projects not just of automated border control (ABC) gates,³⁴¹ but also a whole host of biometric capture and recognition systems, and the wider deployment of biometrics systems.³⁴²



Frank Smith of the European Network of Law Enforcement Technology Services (ENLETS) explains “mobile solutions for police and borders” at an eu-LISA conference in 2016.

In Horizon 2020, €5 million has been given to the University of Reading-led PROTECT (Pervasive and User Focused BiomeTrics BordEr ProjeCT) consortium to continue these efforts. The project proposes:

“a multi-biometric enrollment [sic] and verification system... taking into account current and next-generation e-Passport chips, mobile equipment and person identification ‘on the move’. Research will be undertaken into optimization of currently deployed biometric modalities, application of emerging biometrics (including contactless finger vein, speaker recognition and anthropometrics), multi-modal biometrics and counter-spoofing, for border control scenarios.”³⁴³

All angles are being covered: the BODEGA project (‘BOrdDERGuArd - Proactive Enhancement of Human Performance in Border Control’) will provide “a holistic view of the Human Factors with regard to the Smart Borders”. What exactly the “human factors” in question are is not explained.³⁴⁴ The project is led by Finland’s VTT Technical Research Centre (*Teknologian tutkimuskeskus*) with Thales, the Austrian Institute of Technology, Atos and the Greek Ministry of Citizens Protection.

The €5 million MESMERISE project, led by Spanish company *San Jorge Tecnológicas* with the Spanish interior ministry, UK Home Office and France’s CEAS, hopes to develop and test a body scanner “able to automatically detect and identify both internal and external concealed commodities being entirely independent of human operator interpretation and training.” Beyond the ESRP, there is even an EU-sponsored network of national representatives that seeks to “bring together good practice and advice to member states in relation to developing and using mobile ID devices for police and immigration services.”³⁴⁵



Former Spanish interior minister Jorge Fernández Díaz offers his fingerprint to a “smart border” gate

The EU’s border security and migration model thus aims to have everyone entering the bloc – from the refugee to the respectable businessman, from the tourist to the travelling salesman, not to mention any goods or produce imported – screened, registered and monitored before, during and after crossing Europe’s borders.³⁴⁶ Aside from the purported benefits for enforcing migration policy, these vast new databanks are also seen as handy sources of information for Europe’s law enforcement agencies, as shown by the access granted to Eurodac and the Visa Information System for police forces, and the demands being made for police access to the Entry/Exit System.³⁴⁷

However, it is not all about the construction of new systems. In a clear example of the logic of suspicion that pervades EU security policy, new rules were recently adopted requiring that all those crossing EU borders (whether EU citizens or not) have their details cross-referenced with EU and international criminal databases. As noted above, there is also some appetite amongst national governments to extend to EU citizens biometric registration schemes currently targeted at “third-country nationals”. In a world of suspicion, few are more suspect than the traveller (who is, of course, also an easy target for new surveillance and control systems).

On the one hand, as security companies and consultants are keen to emphasise, “smart” technologies for intensive data-gathering and processing will – in theory – make it easier to deal with the predicted increases in people entering Europe for work and leisure in the coming decades. On the other hand, it negates the possibility that people might prefer to wait slightly longer in a queue than be subject to intrusive surveillance practices for the sake of their convenience. Either way, they will not have any say in the decisions to introduce such systems. EU citizens – who can have a say on the systems under construction – should know that they may be next in line for the surveillance and data analysis practices that are currently being tested out.

Meanwhile, when it comes to “saving lives at sea,” a simpler (and far cheaper) solution to the problem of the thousands of needless deaths in the Mediterranean would be to make it legally feasible for refugees to enter the EU. A citizens’ initiative on the issue appears to have come to nothing,³⁴⁸ but across the EU the response by ordinary people – in Greece, Serbia, Germany, Austria, France, the UK, Spain, Sweden and beyond – shows that there are hundreds of thousands, if not millions, of people opposed to the divisive and inflammatory rhetoric and policies of their governments and willing and ready to offer sanctuary and hospitality to refugees.

The need for such grassroots initiatives has never been clearer, nor has the need for a significant shift away from the EU’s deadly border model. However, it will require a shift towards new transnational networks able to mobilise on a wider social and political level. As things stand, the only transnational plans afoot – with honourable exceptions³⁴⁹ – are those led by the European Commission that seek pervasive, automated monitoring and intervention in order to enforce current rules. The Protection and Security Advisory Group’s “vision” for 2030 is that:

“EU citizens of good standing should be able to cross all land, sea and air, internal and external EU borders, with no physical barriers... Controls will be exercised by exception and be triggered by alerts activated throughout the EU and not exclusively at border crossings.”³⁵⁰

4.4 THE DEVIL IS IN THE DIGITAL: CYBERSECURITY

The EU's wide-ranging aims in the realm of cybersecurity have seen it largely outsource the design of its research programme to a security industry lobby group, in order to help develop the technologies and procedures perceived as necessary to secure European digital infrastructures and to foster sales overseas.

The increasing use of digital networks and devices in the networks and systems that form the basis of modern societies – for example communications, logistics, and utilities such as electricity and water – has led to an increasing awareness of the need for “cybersecurity”. As an article in Wired magazine put it:

*The growth of cybersecurity into a global industry is the result of the weaponisation of code. From 1994 to 2014, we could all enjoy online communication, commerce and convenience without having to think about security. With the evolution of more of our life into zeros and ones and the rise of the internet of things, cybersecurity needs to be accounted for as a central feature in all products being developed and commercialised.*³⁵¹

This has generated significant interest from public and private organisations alike, and it seems that every week brings a new example of the vulnerability of many “critical infrastructures” that rely on digital networks³⁵² – not to mention the now well-established mass state surveillance revealed most recently by Edward Snowden. Moreover, with the opening up of new areas in which the state and other actors can exercise coercive power, there is ample scope for activities with detrimental effects to individual rights and public well-being.³⁵³



MEPs with Edward Snowden masks during a vote tabled by the Greens/European Free Alliance group in the European Parliament calling for the ex-NSA employee to be given protection in the EU for his whistleblowing efforts.

In the USA, ongoing attempts to introduce cybersecurity legislation have been condemned by the Electronic Frontier Foundation for their “broad immunity clauses for companies, vague definitions, and aggressive spying powers [that] make them secret surveillance bills.”³⁵⁴

Following the publication of the UK's first cybersecurity strategy in 2009, one Member of Parliament warned that: “The cybersecurity strategy uses broad, undefined terms that risk creating panic among the public and a demand for further government powers. We must not retreat into a Cold War mentality.”³⁵⁵ Further afield, laws adopted in the name of cybersecurity have been condemned for promoting “censorship, surveillance and other controls over the internet” (in China),³⁵⁶ and “indiscriminately [limiting] freedom of political and social expression” (the United Arab Emirates).³⁵⁷

At the same time, “cyber” has become another arena from which Europe's security industry is hoping to profit, with the market in Europe (and worldwide) expected to increase by billions of dollars in the coming years.³⁵⁸ As the European Commission notes: it is “one of the fastest growing markets in the ICT sector” and “yields huge economic opportunities.”³⁵⁹ Not surprisingly, it has led to constant lobbying for the EU to adopt policies to “secure European societies with European technology whilst boosting the European demand and competitiveness in cybersecurity and supporting the digital economy.”³⁶⁰ The EU has responded by giving industry a key role in designing a €450 million cybersecurity research policy for the next four years.

According to the EU Agency for Network and Information Security (ENISA), set up in 2004, 23 of the EU's 28 Member States now have national cybersecurity strategies,³⁶¹ with several others being prepared. Under the EU's forthcoming Network and Information Security Directive, all Member States will also be obliged to adopt “a national strategy on the security of network and information systems”.³⁶² The ISF-Police budget is also providing funding for cybercrime and cybersecurity efforts, supporting Member States to establish new systems for coordination between the public and private sectors, acquire new tools and analysis systems, and to “harden” the digital networks related to critical infrastructure.

The EU's own cybersecurity strategy was published in July 2013 and covers a whole host of different policy areas – assisted by the fact there is no single, clear definition for “cybersecurity”. Entitled ‘An Open, Safe and Secure Cyberspace’, it has led to a sprawling web of initiatives³⁶³ based on five priorities:

- “achieving cyber resilience”, described as mitigating and countering “cyber risks and threats having a cross border dimension”;
- a drastic reduction in cybercrime;
- “developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)”;
- developing “the industrial and technological resources for cybersecurity”;
- promoting “a coherent international cyberspace policy for the European Union” and “EU core values”.

It is ironic that many of the large companies operating in the cybersecurity market also promote the increased interconnection of information systems and networks, the use of “cloud” storage and other systems vulnerable to the cybersecurity “threats” for which they sell “solutions”. And while some of those threats are no doubt real, there is also a significant amount of hype surrounding debates on cybersecurity,³⁶⁴ driven in no small part by an industry that is keen to capitalise on an area awash with potential profit.

EOS – which has played a key role in setting up Europe’s newest cybersecurity lobby group, the European Cybersecurity Organisation – has for some time been pushing for the EU to adopt industry-friendly policies. In a July 2010 paper, the group warned that:

“Today, conservative estimates put European cost of the impact of cyber threats at over €350 billion, while the parallel underground economy built around the creation and deployment of cyber threats is evaluated at over €100 billion...”

There is today a clear political awareness, based on facts, that cyber threats are becoming a major issue and can impede operations, economic growth and competitiveness. Cyber Security is recognised as strategic for Europe and its Member States, and the need for European stakeholders to master the key tools to fight cyber threats is clearly recognised.³⁶⁵

Over the following years, EOS fleshed out its vision and now calls for the adoption of an “end-to-end approach” on cybersecurity (on the “end-to-end approach”, see section 3).

Public funding has helped develop EOS’ cybersecurity agenda. The CYSPA (European CYber Security Protection Alliance) project was headed by the lobby group and received €1.7 million from the FP7 ICT research budget. It aimed to promote a “top-down approach” for “trustworthy ICT through a European strategy to protect cyberspace.”³⁶⁶ The CAPITAL project (“Cyber security research Agenda for Privacy and Technology chAllenges”) was also coordinated by EOS and funded by the FP7 ICT budget. It sought to “coordinate European R&D efforts in the cyber security domain and jointly address research and innovation within an Integrated Research & Innovation Agenda.”³⁶⁷

Spurred along by the efforts of EOS and numerous others,³⁶⁸ the Commission has now gone some way towards meeting industry demands. In July 2016, along with the publication of a Communication on ‘Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’, a “contractual Public Private Partnership on cybersecurity” (PPP) was signed between the Commission and a group set up for the purposes of signing the contract, the European Cybersecurity Organisation (ECS). Its overarching aim is to “help to align the demand and supply sectors for cybersecurity products.”³⁶⁹

The ECS’ secretariat function is provided by EOS. Although its membership includes industry associations, transnational corporations, public and regional administrations, universities and small businesses, it is perhaps telling that the group’s plans for the PPP were entitled the “industry proposal”. Indeed, large parts of the document appear to have been taken from EOS cybersecurity working papers. Luigi Rebuffi, head of the EOS, said in a 2015 interview:

“Since 2009, EOS has advocated drafting a European Cyber Security Strategy (adopted in 2013) as well as an EU Cyber Security Industrial Policy to support the development of a genuine European cyber security industry and of increased digital autonomy for Europe... EOS is strongly supporting the creation of the envisaged cyber security PPP announced by the Commission, as it is the first step foreseen in our proposed flagship initiative.”³⁷⁰

The EU will provide €450 million to activities stemming from the partnership, whilst the members of the ECS are supposed to collectively invest three times this amount. The principal aim is:

“To foster cybersecurity market development, job and wealth creation in Europe through a long term investment commitment by cybersecurity industry, research and technology organisations (RTOs), academia, the European Commission, Member States’ public administrations participating in the partnership as well as cybersecurity solution users.”³⁷¹

In an uncanny parallel with the formative years of the European Security Research Programme, this is to be done through giving the members of the ECS significant influence over a “multi-annual research and innovation agenda.” In the words of the contract:

“The Commission commits itself to giving due consideration to inputs and advice from the Association in order to identify research and innovation activities to be proposed for financial support under the Horizon 2020 Framework Programme.”

It further says that the “industry proposal for a partnership and the multi-annual research and innovation roadmap” drawn up by the ECS are the formal “basis for the cooperation” in the PPP.³⁷²

The contract between the Commission and the ECS also sets out “societal objectives”, which include the need to “develop and implement European approaches for cybersecurity, trust, privacy and data protection by design.” This is supposed to help “foster trust in the data-driven economy.” How this will work out in practice remains to be seen. The EU’s General Data Protection Regulation and accompanying legislation,³⁷³ coming into

force in May 2018, will “strictly control how enterprises use [personally identifiable information],” but at the same time the EU and its Member States are “introducing new surveillance legislation that will greatly increase the government’s ability to monitor its citizens.”³⁷⁴ The EU has called for the development of “privacy-by-design” standards for new technologies, although these are to be voluntary.³⁷⁵ It has also funded numerous projects related to privacy and data protection through the Horizon 2020 ESRP budget. However so far they have taken a limited approach to the issue, focusing on individual consumer protection rather than the need to review, rein in or better regulate digital surveillance practices.

For example, PRIVACY FLAG (€3.1 million in Horizon 2020 ESRP funding) and OPERANDO (‘Online Privacy Enforcement, Rights Assurance and Optimization’, €3.7 million) promise to develop tools for individuals to ensure their privacy online. The former “will enable citizens to monitor and control their privacy with a user friendly solution provided as a smart phone application, a web browser and a public website,”³⁷⁶ while the latter will create a platform to be used by “independent Privacy Service Providers... to provide comprehensive user privacy enforcement in the form of a dedicated online service”.³⁷⁷

TYPES (‘Towards transparencY and Privacy in the online advertising business’), meanwhile, will receive nearly €4 million to develop tools that allow individuals to choose which information they give to online advertising firms; to understand where their data is going and how it is being used; and “to know the value of their data”. The overall aim, however, seems to be to examine how to prevent potential loss of revenue for the advertising industry from the use of such tools. According to the project consortium:

“Online advertising generated in 2013 \$42bn worth of revenue and more than 3.4 million direct or indirect jobs in Europe in 2012 alone... the lack of transparency regarding tracking techniques and the type of information companies collect about users is creating increasing concerns in society. Software tools for implementing total mitigation (e.g., ad blocker or cookies blocker) have been released... A massive adoption of these tools by end users may cause disruption in the digital economy...”³⁷⁸

The VisiOn project (‘Visual Privacy Management in User Centric Open Environments’) has similar aims, seeking to develop a “platform” that will “provide clear visualisation of privacy preferences, relevant threats and trust issues along with an insight into the economic value of user data.”³⁷⁹ It is being coordinated by Business-e, an Italian cyber security company and also involves Fraunhofer, Atos, the Belgian Military Medical Academy and others.

The ESRP is providing €2.75 million.

€3.8 million has been awarded to the PANORAMIX project (‘Privacy and Accountability in Networks via Optimized Randomized Mix-nets’), led by the University of Edinburgh, which will develop “mix-nets” to “protect not only the content of communications from third parties, but also obscure the exact identity of the senders or receivers of messages”³⁸⁰ A counterpart can be found in SafeCloud (‘Secure and Resilient Cloud Architecture’, €2.2 million), which aims to “re-architect cloud infrastructure” so that data stored in the “cloud” will be subjected to “partitioning and entanglement”:

“This will make users less reluctant to manage their personal data online due to privacy concerns and will generate positive business for privacy-sensitive online applications such as the distributed cloud infrastructure and medical record storage platform that we address.”³⁸¹

The accessibility of medical records is also under examination in the €3.9 million SHIELD project, led by Spain’s Fundacion Tecnalia and funded under the 2016-17 work programme, which will:

“unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it. This will make it possible to provide better health care to mobile citizens across European borders, and facilitate legitimate commercial uses of health data.”³⁸²

The Exus Software-led KONFIDO project (€5 million) was funded at the same time and is concerned with “state of the art eHealth technology.”³⁸³

No one would dispute the obvious benefits in individuals having greater control over the personal data gathered from them. However, these projects are for the most part concerned less with privacy as an end in itself, and more with data protection as a means to further profit-making – the “digital economy” is, of course, seen by the EU as key to Europe’s future prosperity. More fundamental, or radical, notions of privacy (for example, the right to anonymity) do not get a look-in.³⁸⁴

Elsewhere, the research agenda for cybersecurity (or “digital security” as it is called in the ESRP) is concerned with issues such as “identity, access and trust management”; protecting ICT infrastructure; and “security services (auditing, compliance and certification, risk management, cybersecurity operation, security training services).”

Automated access control – the granting of access (or not) to buildings, areas or services – is one area where there is a thirst for the development of novel identification and surveillance techniques. The OCTAVE project (‘Objective

Control for TAlker VERification', €4.4 million), coordinated by Italian research institute *Fondazione Ugo Bordon*, will investigate "automatic speaker verification" for "unsupervised authentication at a distance". Tests of the consortium's technology will take place in "banking services and physical access within a critical airport infrastructure," and there is the possibility for "wider exploitation in future application in, for example, customer care, telephone banking, e-commerce, logical and physical access control."³⁸⁵ SpeechXRays has similar aims, focusing on "voice acoustics analysis and audio-visual identity verification."³⁸⁶

ReCRED ('From Real-world Identities to Privacy-preserving and Attribute-based CREDENTIALs for Device-centric Access Control', €5 million) hopes to let people use their smartphones (or other "personal mobile device") as a "unified authentication and authorization proxy towards the digital world." If all goes to plan, it will also allow individuals to use their devices for "local access control" as well. CREDENTIAL ('Secure Cloud Identity Wallet') seeks to "develop, test and showcase innovative cloud based services for storing, managing, and sharing digital identity information and other critical personal data." The view here seems to be that the safety and security of digitalised identities is best served by commodifying the means to ensure it.



EU and industry officials launch the Public-Private Partnership on Cybersecurity.

Two projects have been funded under the heading "risk management and assurance models". DOGANA ('aDvanced sOCial enGineering And vulNERability Assesment Framework') will develop a framework for companies and other organisations at risk from being "exposed to the so-called Social Engineering 2.0, and thus prone to targeted cyber-attacks." Two subsidiaries of defence and security multinational Thales are, receiving over €200,000 each, are participating in the project led by Belgian company Engineering International (which will receive over €400,000).³⁸⁷ WISER ('Wide-Impact cyber Scurity Risk framework', €2.5 million) will develop "a cyber-risk management framework able to assess, monitor and mitigate the risks in real-time, in multiple industries."³⁸⁸ Other projects are being funded to look into "information driven cyber security management" (DiSIEM, C3ISP, PROTECTIVE, SHIELD and SISSDEN);³⁸⁹ "trust e-services" (FutureTrust, LIGHTest);³⁹⁰ and "assurance and Certification for Trustworthy and secure ICT systems" (certMILS, ANASTACIA and VESSEDIA).³⁹¹

Cybersecurity also pops up in relation to critical infrastructure protection under the ESRP's 'disaster resilience theme'. CIPSEC, CITADEL, ATENA and SUCCESS are all looking at ways to secure digital networks and information systems, with the latter project planning to "develop an overarching approach to threat and countermeasure analysis with special focus on the vulnerabilities introduced by Smart Meters." As a presentation by an official from the Commission's DG CONNECT put it: "Where else to find cybersecurity and privacy R&D&I in H2020? Almost...everywhere!"

One digital security project funded by the ESRP and being undertaken by a consortium primarily made up of universities is explicitly focused on creating "an alliance for value-driven cybersecurity" – presumably in opposition to profit-driven cybersecurity, although this is not explicitly stated. The €1.5 million CANVAS project states that:

*"The growing complexity of the digital ecosystem in combination with increasing global risks entail the danger that enforcing cybersecurity may bypass other fundamental values like equality, fairness or privacy, whereas downplaying cybersecurity would undermine citizens' trust and confidence in the digital infrastructure... technology development in cybersecurity should incorporate European values and fundamental rights."*³⁹²

The outcome of the project remains to be seen. There will also be a focus on 'Privacy, Data Protection and Digital Identities' in a forthcoming call for proposals, alongside another 'Addressing Advanced Cyber Security Threats and Threat Actors'. Both come under the auspices of the Public-Private Partnership on cybersecurity.

Under the PPP contract, the Commission is bound to ensure that "the inputs and advice received from the Association are developed with the involvement of all relevant stakeholders as appropriate." The development of "inputs and advice" by the members of ECS is of course highly dependent on the resources each of them has to contribute. The disparity between its members – which range from companies such as Ericsson, Indra and Thales to universities, public administrations and small businesses – suggests that some are far more likely to have time and money available than others.

At the same time, the involvement of private interests in cybersecurity issues seems unavoidable. As the Swedish national programme for the ISF remarks: "Private operators account for an increasing share of publicly funded services and own key parts of the infrastructure." The immediate question that arises is how to deal with the conflicting issues of profit maximisation – the *raison d'être* of all corporations – and social well-being and the protection of fundamental rights. As highlighted

elsewhere in this report, EOS has previously stated that fundamental rights are “not a competitive advantage” in the hard-edged world of the security industry.

While EU’s Cybersecurity Strategy emphasises heavily the need to protect and promote fundamental rights in cyberspace, there are no guarantees that this will simply happen by itself: a concerted, critical effort by civil society (in the broadest possible meaning of the term) will be required. And this is no easy challenge; as digital activists Andrew Puddephatt and Lea Kaspar argue:

“Among civil society and public interest groups however, there has, as yet, been little engagement or even research on this issue [cybersecurity]... That is why rather than simply decrying current attacks on data protection and privacy, we need to proactively advocate for a new definition of cybersecurity, centred on the security and rights of the end user, rather than on systems.”³⁹³

Similar conclusions have been reached by Alex Comminos and Gareth Seneque:

“Civil society needs to articulate an agenda for cyber security that puts the security of human beings at the centre of the debate.

“Making cyber security a national security issue can be counterproductive due to its potential for abuse. Cyber security also may be better dealt with by the technical community, the private sector and civil society. The state and military may not always be best suited to dealing with cyber security, and intelligence agencies may have a conflict of interest in ensuring cyber security.”³⁹⁴

4.5 DISASTER RESILIENCE: UNKNOWN UNKNOWNNS NEED ALL-PURPOSE SURVEILLANCE

While the EU’s policies in the field of disaster resilience and related fields such as critical infrastructure protection are relatively modest, the research programme covers topics ranging from climate change to drone detection systems; an underpinning ideal is the need to address perceived threats through increased surveillance, foresight and control of all manner of sites, spaces and phenomena.

‘Disaster resilience’ is the ESRP’s fourth main topic. The overarching concerns of the theme are summed up in the work programme:

“There is barely any societal sector which is not to some extent concerned by disasters and related resilience and security issues. The objective of

this call is to reduce the loss of human life, environmental, economic and material damage from natural and man-made disasters, including extreme weather events, crime and terrorism threats.”³⁹⁵

This is not an exhaustive list – Slovenia, in its draft programme for the ISF budget, noted that “all possible aspects of potential crisis should be considered,” including “social and political unrests as a consequence of deep economic and financial crisis.”³⁹⁶ It could be said that, in essence, underlying the idea of “disaster resilience” is a concern with the “unknown unknowns”.³⁹⁷ The broad scope of this theme has made possible the funding of a whole host of surveillance, tracking and detection technologies.

Critical infrastructure is a key topic under the disaster resilience theme and the topic featured heavily in FP7, with projects funded through the budgets for security as well as space, transport, health and ICT, amongst others. In 2012, a review of the legislation that forms the basis for the EU’s Programme for Critical Infrastructure Protection (EPCIP) found that amongst Member States’ authorities:

“There is a strong perception that implementation of the Directive has not resulted in sufficiently clear and tangible improvements to ECI [European Critical Infrastructure] security levels. A number of facts support this viewpoint, most importantly the fact that relatively few ECIs have been identified... Most MS express great concern that the primary objective of the Directive – improved security – seems to be the area with the lowest level of perceived improvement...”³⁹⁸

The EPCIP was subsequently rebooted with a new, “more hands-on approach” with “four selected critical infrastructures of a European dimension – Eurocontrol [air traffic management], Galileo [the EU’s satellite network], the electricity transmission grid and the gas transmission network.”³⁹⁹

As for the ESRP, one current concern is the development of pan-European coordination, control and management methods, for example through the development of guidelines and “concepts”. The University of Firenze is leading the RESOLUTE project (RESilience management guidelines and Operationalization appLied to Urban Transport Environment, €3.8 million from the EU), alongside CERTH, Fraunhofer, Thales and others, which will:

“[C]onduct a systematic review and assessment of the state of the art of the resilience assessment and management concepts, as a basis for the deployment of an European Resilience Management Guide (ERMG)... The final goal of RESOLUTE is to adapt and adopt the

identified concepts and methods... through the implementation of the RESOLUTE Collaborative Resilience Assessment and Management Support System (CRAMSS).⁴⁰⁰

Fraunhofer is also participating in RESILENS, which will receive €4.1 million from the ESRP and has similar aims to RESOLUTE. The project is led by Irish company Future Analytics Consulting and “will develop a European Resilience Management Guideline (ERMG) to support the practical application of resilience to all CI sectors.”

The guidelines produced by SMR (Smart Mature Resilience, €4.6 million) will “provide a robust shield against man-made and natural hazards”. Those developed by the DARWIN project (‘Expecting the unexpected and know how to respond’, €5 million) will “improve the ability of stakeholders to anticipate, monitor, respond, adapt, learn and evolve, to operate efficiently in the face of crises.” IMPROVER (Improved risk evaluation and implementation of resilience concepts to critical infrastructure, €4.3 million) will seek:

“implementation of combinations of societal, organisational and technological resilience concepts to real life examples of pan-European significance, including cross-border examples.”

According to the project: “The methodology... will provide much needed input to standardisation of security of infrastructure.”⁴⁰¹ This issue also comes up in ResiStand (Increasing disaster Resilience by establishing a sustainable process to support Standardisation of technologies and services, €1.9 million), which aims “to find new ways to improve the crisis management and disaster resilience capabilities of the European Union and individual Member States through standardisation.”⁴⁰²

Projects focused specifically on the effects of climate change have also become more prominent on the ESRP agenda. PLACARD (PLATform for Climate Adaptation and Risk reduction, €2.8 million) is working on the development of a “research and innovation agenda” alongside EU-CIRCLE (A pan-European framework for strengthening Critical Infrastructure resilience to climate change, €7.3 million); and RESIN (Climate Resilient Cities and Infrastructures, €7.5 million). The CLISEL project (Climate Security With Local Authorities) has been awarded almost €900,000 (of a €1.7 million total) under the theme ‘Impact of climate change in third countries on Europe’s security’. It is “based on the presumption that many indirect impacts on Europe’s security emerge and are felt at the local scale, within Europe itself,” something the project consortium argues is “overlooked by most existing initiatives on the so called climate-security nexus.”⁴⁰³

Elsewhere, projects are investigating the “potential of current and new measures and technologies to respond to extreme weather and climate events”, such as ANYWHERE (EnhANCing emergencY management and response to extreme WeatHER and climate Events.)⁴⁰⁴

and the I-REACT project, which proposes integrating information from various systems and technologies “to provide increased resilience to natural disasters though better analysis and anticipation, effective and fast emergency response, increased awareness and citizen engagement.”⁴⁰⁵

The hope of predicting the future runs across projects funded under this theme. The massive ANYWHERE project (€14.5 million in total with a €12 million EU contribution) proposes the development of a “multi-hazard platform providing a better identification of the expected weather-induced impacts and their location in time and space before they occur.”⁴⁰⁶ The largest project funded so far under the scheme, ‘Reaching out’ (€21 million total cost with an €18.8 million EU contribution) is examining how to ensure “effective EU support” to various types of crises outside the EU.⁴⁰⁷ Meanwhile, the beAWARE project highlights how militaristic decision-making structures have entered the civilian realm: the “overall context” for the project “lies in the domain of situational awareness and command and control.” The project proposes harnessing information-gathering and decision support tools “to provide support in all the phases of an emergency incident,” before, during and after it takes place.⁴⁰⁸

As much as the research programme recognises the reality of climate change and extreme weather, the fact that unfettered money-making helped lead to this situation seems to have escaped the notice of the ESRP’s designers. Underlying many of these efforts is the goal of developing products that can be sold to public and private bodies alike. As the I-REACT consortium state rather crudely, the resulting products will:

“enable new business development opportunities around natural disasters triggered by extreme weather conditions, which will reduce the number of affected people and loss of life.”

The project is to receive €5.4 million from the ESRP budget and is led by Italy’s *Istituto Superiore Mario Boella*, alongside 19 other participants. Their efforts will be complemented by BRIGAID (BRIdges the GAP for Innovations in Disaster resilience, €7.7 million) which aims to create ““Communities of Innovation” that bring together “innovators and end-users”, set up methods and facilities for the swift testing and marketing of new products, and “strengthen[s] the competitiveness and growth of companies with the support of a dedicated business team.”⁴⁰⁹

Other projects are looking at pandemics and “toxic emergencies” (PANDEM,⁴¹⁰ TOXI-TRIAGE⁴¹¹); the cultural aspects of disaster response and management (IMPACT,⁴¹² CUIDAR,⁴¹³ EDUCEN⁴¹⁴); and yet more technologies to detect illicit or dangerous substances (ChemSniff,⁴¹⁵ ACES,⁴¹⁶ SPIDERS,⁴¹⁷ Bio-Ax,⁴¹⁸ ART,⁴¹⁹ AIRS,⁴²⁰ INNOPROCITI⁴²¹). The theme of disaster resilience also provides the backdrop for SEREN 3.⁴²² This is the third project funded by the

ESRP to establish and maintain a network of “national contact points” dealing with security research as a whole – officials whose job it is to encourage organisations in their member state to apply for grants, in order to try to claw back the money national governments have paid into the budget in the first place.

Dozens of small grants (€50,000 per project) have been made to small businesses through the ‘disaster resilience’ theme. Drones have been a popular topic here, with projects including systems for detecting drones intruding on critical infrastructure or individuals’ “personal sphere” (SafeSky,⁴²³ DAPS⁴²⁴) and for “aerial/sensing solutions focused on the protection of heavily populated areas, and critical/soft infrastructures” (EXTREMDRON). The SURVEIRON project has been rather more generously-funded than these three, with the EU providing €1.7 million of its €2.5 million total to the Spanish company AEORUM:

“The project is based in a set of AEORUMs intelligent robots embedded inside a fleet of unmanned aerial vehicles (UAVs). This fleet is deployed in fixed and mobile locations and supervised from an emergency command center. When an alarm is notified, the system sends one or more UAVs to the emergency area avoiding any obstacle in their way. Once there, SURVEIRON starts scanning and analyzing automatically the environment with different AEORUM detection technologies. All identified risks are sent to the control center and represented in a 3D environment for an easy evaluation of human operators in real time. The system will also recommend action plans with AEORUM’s decision making technologies based on artificial intelligence.”⁴²⁵



Components of the SafeSky “drone protection” system.

Other grants to small and medium-sized enterprises have looked at everything from “a mobile robot platform able to perform autonomous protection of critical infrastructures” (ROBIN⁴²⁶) to preventing contamination of water supplies (AquaSHIELD,⁴²⁷ WATERGUARD⁴²⁸); examining inks to determine where and by what something may have been printed (Andrupos⁴²⁹); access control through biometrics-at-a-distance (AIRIMGO⁴³⁰); smart CCTV

for automated detection and tracking of “suspects” (Invest⁴³¹); and systems enabling video surveillance in the dark (Starlight⁴³²).

The vast number of projects – whether immediately concerned with ‘disaster resilience’ or not – demonstrates the concern within EU institutions to kick-start a more extensive EU ‘security industry’⁴³³ through all manner of surveillance, monitoring and tracking devices. It also makes clear that the ideas underpinning the ESRP since its inception – “a high-tech blueprint for a new kind of security,” as *NeoConOpticon* put it – have spread from the offices of transnational corporations and research institutes to a multitude of small business, higher education institutes and other organisations across Europe.

While few would doubt the need for “critical infrastructure” to be kept safe and for organisations and institutions to be prepared for potential disasters, the argument made in *NeoConOpticon* remains valid:

“Critical infrastructure may be publicly or privately owned (often in accordance with the EU’s internal market rules) and protected by private security, but it inevitably impacts on public space. From surveillance cameras to security checkpoints, the protection of critical infrastructure is having an increasing impact on the way in which the surrounding public spaces are accessed and controlled.”⁴³⁴

A more theoretical, but equally important, point is that both critical infrastructure protection and disaster resilience are predicated on what Marieke de Goede has called “premeditation” – the attempt to foresee or predict unknown security risks and threats. While the need to keep society safe from potential disasters is of undoubted importance, state policies and projects in this field should not be accepted uncritically. As de Goede has argued:

“Not only does security premeditation offer a fantasy of control and rational management of the uncertain future... more worrying still is the fact that premeditation is performative. This does not mean that disastrous imagined futures will inevitably play out, but it does mean that the imagination of some scenarios over others, the visualization of some futures and not others, entails profoundly political work that enables and constrains political decision making in the present.”⁴³⁵

Furthermore, the framework in which this “premeditation” takes place is often predicated on assessing various sites and spaces deemed vulnerable as if they were military installations open to attack. While nobody could discount the need for individuals and the technologies and systems they rely upon to be kept safe, the ways in which this is done are of crucial importance for fundamental rights and democratic standards.



Riot police block entrance to parliament block entrance to parliament in Kyiv, Ukraine

CONCLUSIONS

THE ROAD TO HELL?

A decade since the EU first obtained significant formal powers in the field of security its powers, plans and proposals continue to expand into new areas and in predictably anti-democratic forms. The majority of these endeavours may be well-intended. But the vision of security that dominates policy-making circles (top-down, technologically-driven and centrally-controlled) and the methods chosen for developing and implementing them (unaccountable and secretive networks, working groups, committees and public-private partnerships motivated, in significant part, by profit) suggest that good intentions are not sufficient to produce forms of security based on inclusivity, participation and the fulfilment of individual rights. This is particularly so when the EU's financial and policy interventions are taking place in a political and social environment increasingly shaped by authoritarianism, discrimination and the removal of rights protections in the name of fighting terrorism and deterring migration.

Indeed, the legal and policy framework established by the EU and its Member States is precisely based on restricting individual rights in the name of achieving security, albeit with far more pronounced effects on certain social groups – for example, ethnic and religious minorities – than others. The pace with which new laws, measures and policies emerge from the security bureaucracies of EU and national administrations suggests that there is a panic at the heart of policy-making circles; a desire to be seen to be doing something, even when it seems clear that such measures will either achieve nothing, infringe upon rights, or both. In other cases, of course, the motivations are more clear – Hungary's Viktor Orban has openly declared that “the new state that we are building is an illiberal state, a non-liberal state.”

The original development of the European Security Research Programme was heavily-influenced by transnational security and defence companies, major research institutes and technology firms, and it is their vision of security that remains dominant in a programme from which they continue to benefit. While the agenda has developed to include new themes, the number of organisations involved has diversified and grown and ethical checks on projects have been stepped up, this appears to have had only a minor effect on the core content of the programme. At its heart it remains concerned with the development of technological security “solutions” that will produce profit for companies and power for states, and a society of suspicion, monitoring and control for the rest of us.

This is not to say that no good has come or can come from the ESRP. It is clear that we live in turbulent times, and research projects that enable individuals and societies to cope with unexpected events or disasters are, in principle, to be welcomed. The same can be said for transnational

systems of governance and policy coordination. Public and private officials see new “threats” as globalised ones for good reason – society faces many problems that may best be dealt with at a transnational or international level. It is the solutions proposed and practiced by those in power – the merging of public and private power, technocratic decision-making, compounded by an utter lack of meaningful democratic institutions – which are so questionable.

Ultimately the problems underlying the policies, proposals and projects examined throughout this report cannot solely be addressed through the reform of legal frameworks or changes to policy priorities – although these would certainly be welcome. For example, ensuring meaningful democratic oversight of the EU's security research programme and other EU security projects and policies would be a significant step.

Nevertheless, these initiatives raise all manner of more fundamental questions: should we continue to give more power to states and corporations in a world that has been made deeply troubled and unequal by those very institutions, and in which new forms of authoritarianism, exclusion, discrimination and social sorting are on the rise? Can processes and institutions that have, by and large, been established by and for small, elite benefit groups be refashioned to provide a wider beneficial purpose? What might genuinely democratically designed, supervised and controlled security policies and technologies look like?

At the same time, it is necessary to consider what the immediate future holds in store. Discussions, decision-making and no doubt heavy lobbying by the industry will soon restart as the EU moves towards deciding its policy priorities and budgets for the 2021-27 period. As authoritarian movements and parties try to assert themselves across Europe, there is a need for new ideas and renewed demands for democratic participation, meaningful systems of accountability, and an end to the overwhelming priority given to corporate interests in research programmes. Yet this will not happen by itself, and on this note it seems appropriate to quote *Amnesty International* again:

“We cannot rely on governments to protect our freedoms, and so we have to stand up ourselves. We have to come together and resist the roll back of long-established human rights. We must fight against the deceitful narrative that we have to trade of our rights in exchange for prosperity and security.”

ANNEX 1: TOP 50 RECIPIENTS OF ESRP FUNDS TO DECEMBER 2016

Organisation	H2020 projects	H2020 funding	Average € p/prj.	ESRP total (2007-Dec 2016)	Country	Type
Fraunhofer Institute	24	€ 14,230,894.25	€ 592,953.93	€ 65,729,868.64	DE	REC
Commissariat à l'énergie atomique et aux énergies alternatives	7	€ 7,116,487.50	€ 1,016,641.07	€ 22,067,036.95	FR	REC
Atos	15	€ 6,527,301.88	€ 435,153.46	€ 14,125,323.53	ES	PRC
Thales	9	€ 4,612,836.26	€ 512,537.36	€ 33,068,767.18	FR	PRC
Centre for Research and Technology Hellas (Εθνικό Κέντρο Έρευνας & Τεχνολογικής Ανάπτυξης, CERTH)	8	€ 4,557,090.25	€ 569,636.28	€ 4,557,090.25	EL	REC
Engineering - Ingegneria Informatica	6	€ 3,966,237.50	€ 661,039.58	€ 8,064,256.50	IT	PRC
Airbus	2	€ 3,592,597.75	€ 1,796,298.88	€ 17,782,805.02	FR	PRC
TNO	7	€ 3,586,620.00	€ 512,374.29	€ 33,517,080.82	NL	REC
Italian National Research Council	8	€ 3,269,560.00	€ 408,695.00	€ 6,948,520.35	IT	REC
Institute of Communication and Computer Systems	5	€ 3,209,626.00	€ 641,925.20	€ 7,243,589.18	EL	REC
Leonardo (Finmeccanica)	5	€ 3,199,575.00	€ 639,915.00	€ 3,202,575.00	IT	PRC
Austrian Institute of Technology	5	€ 3,175,483.75	€ 635,096.75	€ 15,963,840.04	AT	REC
Universitat Politecnica de Catalunya	2	€ 3,158,400.00	€ 1,579,200.00	€ 3,782,538.29	ES	HES
Inov Inesc Inovacao - Instituto de Novas Tecnologias	7	€ 3,090,437.50	€ 441,491.07	€ 5,458,959.00	PT	REC
Department of Health	1	€ 2,835,655.00	€ 2,835,655.00	€ 4,463,656.82	UK	REC
Katholieke Universiteit Leuven	7	€ 2,804,875.00	€ 400,696.43	€ 8,257,611.24	BE	HES
IBM	6	€ 2,690,042.50	€ 448,340.42	€ 2,810,417.50	NL	PRC
Loughborough University	1	€ 2,667,700.50	€ 2,667,700.50	€ 3,225,166.82	UK	HES
Universita Cattolica del Sacro Cuore	2	€ 2,643,693.75	€ 1,321,846.88	€ 4,548,965.55	IT	HES
Stiftelsen Sintef	4	€ 2,640,390.00	€ 660,097.50	€ 8,297,490.78	NO	REC
Universite Catholique de Louvain	4	€ 2,361,983.75	€ 590,495.94	€ 5,031,552.24	BE	HES
EQS - Servicos de Engenharia Qualidade e Seguranca LDA	2	€ 2,316,312.83	€ 1,158,156.42	€ 2,316,312.83	PT	PRC
Aeorum	4	€ 2,262,963.50	€ 565,740.88	€ 2,262,963.50	ES	PRC
Norges Miljo-og Biovitenskaplige Universitet	1	€ 2,156,419.00	€ 2,156,419.00	€ 2,446,326.00	NO	HES
Universite de Nice Sophia Antipolis	2	€ 2,152,987.50	€ 1,076,493.75	€ 2,152,987.50	FR	HES
Exus Software	4	€ 2,098,125.00	€ 524,531.25	€ 2,098,125.00	UK	PRC
National Center for Scientific Research Demokritos	5	€ 2,090,462.50	€ 418,092.50	€ 9,075,434.13	EL	REC
Arttic	3	€ 2,056,827.50	€ 685,609.17	€ 7,202,277.50	IL	PRC
Technische Universiteit Delft	3	€ 2,000,147.50	€ 666,715.83	€ 6,492,939.49	NL	HES
Foundation for Research and Technology Hellas	5	€ 1,988,625.00	€ 397,725.00	€ 2,537,342.37	EL	REC

Type: HES: higher education institute; REC: research institute; PRC: private company; PUB: public institution.

Source: EU Open Data Portal, <https://data.europa.eu/euodp/en/data/>

ANNEX 2: NATIONAL DISTRIBUTION OF THE INTERNAL SECURITY FUND

Member State	ISF-Police (€)	ISF-Borders (€)	ISF total (€)
Austria	12,162,906	14,162,727	26,325,633
Belgium	17,903,720	17,519,321	35,423,041
Bulgaria	32,002,293	40,366,130	72,368,423
Switzerland		18,920,284	18,920,284
Cyprus	8,117,257	34,507,030	42,624,287
Czech Republic	17,029,270	14,381,484	31,410,754
Germany	79,504,401	51,753,437	131,257,838
Denmark		10,322,133	10,322,133
Estonia	13,480,269	21,781,752	35,262,021
Spain	54,227,207	195,366,875	249,594,082
Finland	15,682,348	36,934,528	52,616,876
France	70,114,640	84,999,342	155,113,982
Greece	20,489,650	166,814,388	187,304,038
Croatia	19,095,426	35,609,771	54,705,197
Hungary	20,663,922	40,829,197	61,493,119
Iceland		5,326,980	5,326,980
Ireland	9,243,080		9,243,080
Italy	56,631,761	156,306,897	212,938,658
Liechtenstein		5,000,000	5,000,000
Lithuania	16,120,656	24,704,873	40,825,529
Luxembourg	2,102,689	5,400,129	7,502,818
Latvia	16,941,431	15,521,704	32,463,135
Malta	8,979,107	53,098,597	62,077,704
Netherlands	31,540,510	30,609,543	62,150,053
Poland	39,294,220	49,113,133	88,407,353
Portugal	18,693,124	18,900,023	37,593,147
Romania	37,150,105	61,151,568	98,301,673
Sweden	21,057,201	11,518,706	32,575,907
Slovenia	9,882,037	30,669,103	40,551,140
Slovakia	13,891,478	10,092,525	23,984,003

Sources: ISF-Police: Annex III of Regulation (EU) No 513/2014, ISF-Borders: Annex I of Regulation (EU) No 515/2014. Due to the distribution of emergency funding since the beginning of 2015 to certain Member States (notably Italy and Greece), these baseline numbers have since altered somewhat.

LIST OF ACRONYMS USED IN THIS REPORT

ABC	Automated Border Control	ETIAS	European Travel Information and Authorisation System
AEGIS	Alliance for European Growth and Innovation on Security	EU	European Union
AFSJ	Area of Freedom, Security and Justice	Eurodac	European Dactyloscopy
AMIF	Asylum, Migration and Integration Fund	Eurosur	European Border Surveillance System
ASD	AeroSpace and Defence Industries Association of Europe	FIU	Financial Intelligence Unit
CBRN	Chemical, Biological, Radiological, Nuclear	FP7	Seventh Framework Programme for Research and Development
CCTV	Closed Circuit Television	GoP	Group of Personalities
CEAS	Commissariat à l'énergie atomique et aux énergies alternatives	H2020	Horizon 2020
CERTH	Centre for Research and Technology Hellas	ICT	Information and Communication Technologies
CIPS	Terrorism and other security-related risks	ID	Identity document
CISE	Common Information Sharing Environment	ILO	Immigration Liaison Officer
COSI	Standing Committee on Operational Cooperation on Internal Security	IPR	Intellectual Property Rights
DG CONNECT	European Commission Directorate-General for Communications Networks, Content and Technology	ISEC	Prevention of and fight against crime fund
DG ENTR	European Commission Directorate-General for Industry and Enterprise	ISF	Internal Security Fund
DG HOME	European Commission Directorate-General for Home Affairs and Migration	ISS	Internal Security Strategy
DNA	Deoxyribonucleic acid	ITRE	European Parliament Committee on Industry, Research and Energy
EBF	External Borders Fund	MEP	Member of the European Parliament
ECA	European Court of Auditors	OAP	Operational Action Plan
ECRIS	European Criminal Records Information System	PASAG	Protection and Security Advisory Group
ECS	European Cybersecurity Organisation	PASR	Preparatory Action on Security Research
EDA	European Defence Agency	PCP	Pre-Commercial Procurement
EDPS	European Data Protection Supervisor	PNR	Passenger Name Record
EES	Entry/Exit System	PPI	Public Procurement of Innovative Solutions
EMSA	European Maritime Safety Agency	PPP	Public-Private Partnership
ENISA	European Network and Information Security Agency	R&D	Research & Development
ENLETS	European Network of Law Enforcement Technology Services	R&D&I	Research & Development & Innovation
EOS	European Organisation for Security	RAN	Radicalisation Awareness Network
EP	European Parliament	RTP	Registered Traveller Programme
EPP	European People's Party	S&D	Socialists & Democrats
ESRAB	European Security Research Advisory Board	SAG	Security Advisory Group
ESRIF	European Security Research and Innovation Forum	SME	Small-and-medium size enterprise
ESRP	European Security Research Programme	SRI	Serviciul Român de Informații [Romanian Intelligence Service]
		SSAG	Secure Societies Advisory Group
		TFTP	Terrorist Finance Tracking Programme
		UAV	Unmanned Aerial Vehicle
		VIS	Visa Information System

NOTES

1. *Amnesty International*, 'Report 2016/17: The state of the world's human rights', <https://www.amnesty.org/download/Documents/POL1048002017ENGLISH.PDF>
2. FIDH, 'Hungary: Democracy under Threat: Six Years of Attacks against the Rule of Law', November 2016, https://www.fidh.org/IMG/pdf/hungary_democracy_under_threat.pdf; Laurent Pech and Kim Lane Scheppele, 'Poland and the European Commission, Part I: A Dialogue of the Deaf?', *Verfassungsblog*, 3 January 2017, <http://verfassungsblog.de/poland-and-the-european-commission-part-i-a-dialogue-of-the-deaf/>; Marijn Nieuwenhuis and Sara Salem, 'Dutch elections: little to celebrate', *openDemocracy*, 18 March 2017, <https://www.opendemocracy.net/can-europe-make-it/marijn-nieuwenhuis-sara-salem/dutch-elections-little-to-celebrate>; Nadim Houry, 'Breaking France's Addiction to its State of Emergency', *Human Rights Watch*, 13 March 2017, <https://www.hrw.org/news/2017/03/13/breaking-frances-addiction-its-state-emergency>
3. Tim Dickinson, 'ACLU Head on Bracing for Trump and America's 'Enormous Civil Liberties Crisis'', *Rolling Stone*, 9 January 2017, <http://www.rollingstone.com/politics/features/aclu-head-bracing-for-trump-enormous-civil-liberties-crisis-w460101>; 'India', *Human Rights Watch World Report 2017*, <https://www.hrw.org/world-report/2017/country-chapters/india>; Adrian Chen, 'When a Populist Demagogue Takes Power', *The New Yorker*, 21 November 2016, <http://www.newyorker.com/magazine/2016/11/21/when-a-populist-demagogue-takes-power>
4. Treaty on European Union, Article 2
5. 'Punishing the victims - a beginner's guide to the EU and the crisis', *Corporate Europe Observatory*, 17 February 2014, <https://corporateeurope.org/eu-crisis/2014/02/punishing-victims-beginners-guide-eu-and-crisis>
6. 'Orwellian counter-terrorism laws stripping rights under guise of defending them', *Amnesty International*, 17 January 2017, <https://www.amnesty.org/en/latest/news/2017/01/eu-orwellian-counter-terrorism-laws-stripping-rights-under-guise-of-defending-them/>; 'Dangerously disproportionate: The ever-expanding national security state in Europe', *Amnesty International*, 17 January 2017, <https://www.amnesty.org/en/documents/eur01/5342/2017/en/>
7. 'European Security Strategy, drafted by Javier Solana and approved today (12.12.03) by the European Council', *Statewatch News Online*, December 2003, <http://database.statewatch.org/article.asp?aid=7088>
8. 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy', June 2016, p.45, <http://statewatch.org/news/2016/jul/eu-global-security-strategy.pdf>
9. Stephen Graham, 'When Life Itself is War: On the Urbanization of Military and Security Doctrine', *International Journal of Urban and Regional Research*, 36(1), January 2012, p.138, <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2427.2011.01026.x/abstract>
10. Eliav Lieblich and Adam Shinar, 'The Case Against Police Militarization', 10 January 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2840715
11. Milipol, <http://en.milipol.com/>
12. Thales, 'State', <https://www.thalesgroup.com/en/worldwide/security/state>
13. Fraunhofer VVS, 'Fraunhofer Group for Defence and Security', <http://www.vvs.fraunhofer.de/servlet/is/100261/>
14. 'Homeland Security Market worth \$544.02 Billion – 2018', Markets and Markets, press release, undated, <http://www.marketsandmarkets.com/PressReleases/homeland-security-emergency-management.asp>
15. Ben Hayes, 'NeoConOpticon', *Statewatch/Transnational Institute*, 2009, p.80, <http://www.statewatch.org/analyses/neoconopticon-report.pdf>
16. 'UK: Coalition government presents National Security Strategy: A Strong Britain in an Age of Uncertainty', *Statewatch News Online*, October 2010, <http://database.statewatch.org/article.asp?aid=30054>
17. Group of Personalities in the field of Security Research, 'Research for a Secure Europe', 2004, p.6, http://www.statewatch.org/observatories_files/drones/eu/gop-2004-research-for-a-secure-europe.pdf
18. Mark P. Mills, 'The Security-Industrial Complex', *Forbes*, 29 November 2004, <https://www.forbes.com/forbes/2004/1129/044.html>
19. Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia, Slovakia.
20. 'A secure Europe in a better world', 20 June 2003, <http://www.statewatch.org/news/2003/sep/solanasec.pdf>
21. European Commission, 'Building our common future', COM(2004) 101 final, 26 February 2004, p.34, <http://statewatch.org/docbin/eu-com-2004-building-common-future.pdf>
22. European Commission, 'Towards a programme to advance European security through Research and Technology', COM(2004) 72 final, 3 February 2004, http://www.statewatch.org/Targeted-issues/ESRP/documents/com2004_0072en01.pdf
23. Ben Hayes, 'Arming Big Brother', *Statewatch/Transnational Institute*, 2006, p.20, <http://www.statewatch.org/analyses/bigbrother.pdf>
24. 'Arming Big Brother', p.28. For more detail see 'NeoConOpticon', pp.12-13
25. Ben Hayes, 'NeoConOpticon', *Statewatch/Transnational Institute*, 2009, p.12
26. European Commission, 'Security Research: The Next Steps', September 2004, <http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52004DC0590>
27. Centre for Strategy & Evaluation Services, 'Ex-post evaluation of the Preparatory Action on Security Research (PASR) – Interim Evaluation of FP7 Security Research – Final report', January 2011, p.102, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/interim_evaluation_of_fp7_security_ex_post_pasr_final_report_en.pdf
28. 'NeoConOpticon', p.15
29. Ibid.
30. As recounted in NeoConOpticon, pp.15-16: "The European Commission made much of the inclusion of two "civil society organisations and thinktanks"... it apparently considers the Crisis Management Initiative.. to be a 'civil liberties' organisation." As to the 'thinktank' to which the Commission referred, it was either the EU-funded Institute for Security Studies (rapporteur for the GoP) or the Italian Istituto Affari Internazionali (Institute of International Affairs)".

31. 'NeoConOpticon', p.16
32. Ernst & Young, 'Evaluation of Aquapol, Railpol and Tispol', 15 January 2013, p.14, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/police-cooperation/general/docs/eandy_evaluation_of_aquapol_railpol_tispol_final_report_20130115.pdf
33. European Commission, 'What is FP7? The basics', http://ec.europa.eu/research/fp7/understanding/fp7inbrief/what-is_en.html
34. 'Security', Official Journal of the European Union L 412/26, p.26, 30 December 2006, <http://cordis.europa.eu/documents/documentlibrary/90798681EN6.pdf>
35. SAFEPOST, http://cordis.europa.eu/project/rcn/102916_en.html
36. Graffolution, http://cordis.europa.eu/project/rcn/185512_en.html
37. The final evaluation counted 307 projects, although data made available through the EU's Open Data Portal shows 320 projects. The table here represents the figure of 307 and the number of projects funded under each theme has been worked out on the basis of those figures – the evaluation report does not provide these statistics, and the data made available by the EU does not make it feasible to work it out.
38. Technopolis Group et al., 'Final Evaluation of Security Research under the Seventh Framework Programme – Final Report', September 2015, p.34, <http://www.statewatch.org/docbin/eu-technopolis-assessment-fp7-esrp-2015.pdf>
39. Crina Boros, 'How the EU cosied up to the defence lobby', *EUobserver*, 20 December 2016, <https://euobserver.com/investigations/136310>
40. Full membership lists from 2007 can be seen here: FP7 Security Advisory Group Membership (November 2007), <https://ec.europa.eu/research/fp7/pdf/old-advisory-groups/security-members.pdf>; and from 2010 here: FP7 Security Advisory Group Membership (November 2010), <http://ec.europa.eu/research/fp7/pdf/advisory-groups/security-members.pdf#view=fit&pagemode=none>
41. For further on the issue during this era, see: 'Who's driving the agenda at DG Enterprise and Industry?', *ALTER-EU*, July 2012, https://www.alter-eu.org/sites/default/files/documents/DGENTR-driving_0.pdf
42. *Ibid.*, p.35
43. Technopolis Group et al., p.111
44. See: Louiza Kalokairinou, 'Research Ethics in Horizon 2020', December 2016, <http://www2.vinnova.se/PageFiles/751334543/NCP%20SwedenLouiza%20Kalokairinou.pdf>; and 'Interview with Isidoros Karatzas, Head of the "Ethics and Research Integrity" sector at the European Commission', *eanpages*, 1 May 2015, <https://www.eanpages.org/2015/05/01/interview-with/>
45. As highlighted in NeoConOpticon and research undertaken for the European Parliament: 'Review of security measures in the 7th Research Framework Programme', in 2010, <http://www.statewatch.org/news/2010/nov/ep-review-security-research-programme.pdf> and 2014, <http://statewatch.org/news/2015/jan/ep-2014-04-fp7-security-research.pdf>
46. Technopolis Group et al., p.114
47. *Statewatch* was a partner in one of these – SECILE: Securing Europe through Counter-terrorism: Impact, Legitimacy and Effectiveness, which assessed the scale and scope of EU counter-terrorism measures. See: SECILE, <http://statewatch.org/projects/secile/>
48. Vincenzo Pavone, Sara Degli Esposti, Elvira Santiago, 'Draft Report on Key Factors', *SURPRISE* deliverable 2.2, p.7, <http://surprise-project.eu/wp-content/uploads/2013/10/SurPRISE-D2.2-Draft-Report-on-Key-Factors.pdf>
49. *Istituto Affari Internazionali*, Manchester Institute of Innovation Research, *Institut des Relations Internationales et Stratégiques*, 'Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence', June 2010, p.143, http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf
50. Technopolis Group et al., p.150. The case study is in the same report, pp.146-152.
51. Draft speech prepared for Philippe Brunet, 20 November 2013, <http://www.statewatch.org/docbin/eu-com-2013-11-milipol-speeches-drafts.pdf>
52. Newer Member States had previously been able to benefit from a host of other funds in order to bring their border management capabilities into line with those of older EU states, and the EU also funds "integrated border management" programmes in numerous non-EU states, as explained elsewhere. See: Mark Akkerman, 'Border Wars', *Transnational Institute*, July 2016, pp.25-33, <https://www.tni.org/en/publication/border-wars>
53. European Commission, 'Evaluation and fitness check (FC) roadmap - Ex-post evaluation of the External Borders Fund 2011-2013', October 2015, http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_home_055_evaluation_external_borders_fund_2011-2013_en.pdf
54. European Court of Auditors, 'The External Borders Fund has fostered financial solidarity but requires better measurement of results and needs to provide further EU added value', October 2014, p.38, http://www.eca.europa.eu/Lists/ECADocuments/SR14_15/QJAB14015ENC.pdf
55. European Court of Auditors, 'The External Borders Fund has fostered financial solidarity but requires better measurement of results and needs to provide further EU added value', October 2014, p.26, 28, http://www.eca.europa.eu/Lists/ECADocuments/SR14_15/QJAB14015ENC.pdf
56. 'Greece: Refugees detained in dire conditions amid rush to implement EU-Turkey deal', *Amnesty International*, 7 April 2016, <https://www.amnesty.org/en/latest/news/2016/04/greece-refugees-detained-in-dire-conditions-amid-rush-to-implement-eu-turkey-deal/>
57. European Court of Auditors, 'The External Borders Fund has fostered financial solidarity but requires better measurement of results and needs to provide further EU added value', October 2014, p.43, http://www.eca.europa.eu/Lists/ECADocuments/SR14_15/QJAB14015ENC.pdf
58. European Commission, 'External Borders Fund – Community Actions 2012', undated, http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/external-borders-fund/transnational-actions/docs/community_actions_and_emergency_actions_grants_awarded_2012_en.pdf

59. Parliamentary question E-012287/2015, 'Answer given by Mr Avramopoulos on behalf of the Commission', 27 November 2015, <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2015-012287&language=EN>
60. European Commission, 'Report from the Commission on the ex-post evaluation of the External Border Fund for the period 2007-2010', COM(2014) 235 final, p.17, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/schengen/docs/com_2014_235_f1_report_from_commission_en.pdf
61. For example, for border management, Hungary and Italy reported that the Commission provided over 34% of total funding, Spain 45% and Portugal 53%. Poland, meanwhile, said that 0.64% of its total expenditure on border management came from EU funds, while Germany said: "It isn't possible to indicate an estimate of the share of the contribution in relationship to the total national expenditure for each area of intervention." The national reports for each EU Member State are available on the Commission's website: see 'Ex-post evaluation report (2007-10)' under 'External Borders Fund – National actions', http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/external-borders-fund/national-actions/index_en.htm
62. PERSEUS, http://cordis.europa.eu/project/rcn/97515_en.html
63. 'PERSEUS Report Summary', http://cordis.europa.eu/result/rcn/177064_en.html
64. AMASS, http://cordis.europa.eu/project/rcn/86259_en.html
65. CLOSEYE, http://cordis.europa.eu/project/rcn/108227_en.html
66. I2C, http://cordis.europa.eu/project/rcn/96259_en.html
67. OPARUS, http://cordis.europa.eu/project/rcn/95504_en.html
68. OPERAMAR, http://cordis.europa.eu/project/rcn/86254_en.html
69. SEABILLA, http://cordis.europa.eu/project/rcn/94732_en.html
70. SUNNY, http://cordis.europa.eu/project/rcn/111498_en.html
71. TRITON, http://cordis.europa.eu/project/rcn/111021_en.html
72. WIMAAS, http://cordis.europa.eu/project/rcn/88640_en.html
73. SAGRES, http://cordis.europa.eu/project/rcn/106574_en.html
74. LOBOS, http://cordis.europa.eu/project/rcn/106598_en.html
75. DOLPHIN, http://cordis.europa.eu/result/rcn/159422_en.html
76. Thales, Selex, the European Union Satellite Centre, the EU Joint Research Centre, the Greek Center for Security Studies, GMV, the Spanish interior ministry, Isdefe, and Portuguese interior ministry, Edisoft, Indra, the German Aerospace Center and Infoterra (a subsidiary of Airbus).
77. European Commission, 'A comprehensive vision for an integrated European border management system for the 21st Century', 13 February 2008, <http://www.statewatch.org/news/2008/feb/eu-com-prel-border-man.pdf>
78. Legal proposals adopted by the Commission in 2013 for a "smart borders" system were rejected and replaced in 2016 in a more limited form, with a proposal for an Entry/Exit System (EES) no longer accompanied by one for a Registered Traveller Programme (RTP).
79. ABC4EU, http://cordis.europa.eu/project/rcn/111518_en.html
80. FASTPASS, http://cordis.europa.eu/project/rcn/106743_en.html
81. FIDELITY, http://cordis.europa.eu/project/rcn/102324_en.html
82. INGRESS, http://cordis.europa.eu/project/rcn/110929_en.html
83. MOBILEPASS, http://cordis.europa.eu/project/rcn/185506_en.html
84. TERASCREEN, http://cordis.europa.eu/project/rcn/108442_en.html
85. XP-DITE, http://cordis.europa.eu/project/rcn/104801_en.html
86. INGRESS, http://cordis.europa.eu/project/rcn/110929_en.html
87. Joerg Sauerbrey, 'Developing a European security identity', *Focus*, Summer 2008, p.13, http://www.asd-europe.org/fileadmin/user_upload/Client_documents/ASD_Contents/2_COMMUNICATION/2.5_Publications/2.5.4_FOCUS_magazine/ASD_FOCUS_-Issue_2.pdf, accessed 21 August 2015
88. TALOS, http://cordis.europa.eu/project/rcn/86712_en.html
89. It can be seen in action in a video produced by the project – TALOS, 'Final Project Review', 27 November 2012, <https://www.youtube.com/watch?v=RIV2GtjqzDU#t=150> – and a euronews report on the topic of border control robots, 'Des robots garde-frontières', 20 June 2012, https://www.youtube.com/watch?v=_XTVLKsnjRg
90. 'Final report summary', http://cordis.europa.eu/result/rcn/140453_en.html
91. Mark Akkerman, 'Border Wars', Transnational Institute, 4 July 2016, <https://www.tni.org/en/publication/border-wars>; see also its update, 'Border Wars II', 19 December 2016, <https://www.tni.org/en/publication/border-wars-ii>
92. General Secretariat, 'Common Manual for Immigration Liaison Officers (ILO) posted abroad by Member States of the European Union', 8418/06, 25 April 2006, <http://www.statewatch.org/news/2006/apr/eu-draft-ILO-manual-8418-06.pdf>
93. It is interesting to note that EU heads of state and government are considered to fit the definition of "critical infrastructure": a Belgian project named 'OPLON' received €538,000 from the CIPS budget in 2011. The project is described in one Belgian document as relating to "protecting of the EU institutions during EU summits," and in a Commission document detailing the grant award as concerning

- “resolving a mass hostage-taking situation, involving the Union’s Heads of state sitting on the Council.” See: Belgium, ‘National programme ISF’, 19 March 2015, URL; European Commission, ‘CIPS 2011 Awarded Grants’, undated, http://ec.europa.eu/dgs/home-affairs/financing/fundings/pdf/cips/cips-grants-awarded-2011_en.pdf
94. European Commission, ‘Communication on the mid-term evaluation of the Framework Programme “Security and Safeguarding Liberties” (2007-13)’, COM(2011) 318 final, 16 June 2011, p.3, <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1499355963791&uri=CELEX:52011DC0318>
 95. It was subsequently incorporated into EU law through the ‘consultation’ procedure, in which the Council draws up a text that the Parliament can either accept or reject, but cannot amend.
 96. Eric Töpfer, Searching for needles in an ever expanding haystack: Cross-border DNA exchange in the wake of the Prüm Treaty, *Statewatch Bulletin*, vol 18 no 3, July-September 2008, <http://database.statewatch.org/article.asp?aid=28346>
 97. General Secretariat of the Council, ‘Implementation of the provisions on information exchange of the “Prüm Decisions”’, 5081/2/17 REV 2, 22 May 2017, <http://data.consilium.europa.eu/doc/document/ST-5081-2017-REV-2/en/pdf>
 98. See for example: Chris Jones, “Complex, technologically fraught and expensive” - the problematic implementation of the Prüm Decision’, *Statewatch Analysis*, September 2012, <http://www.statewatch.org/analyses/no-197-prum-implementation.pdf>
 99. General Secretariat of the Council, ‘Statistics and reports on automated data exchange for 2015’, 5129/1/16 REV 1, 22 September 2016, <http://www.statewatch.org/docbin/eu-council-prum-stats-5129-rev-1-16.pdf>
 100. Council of the European Union, ‘Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border-crime, Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border-crime (“Prüm Decisions”) - statistics and reports on automated data exchange for 2015’, 5129/16, 10 March 2016, <http://statewatch.org/news/2016/apr/eu-council-prum-statistics-2015-dna-fingerprints-vrd-05129-16.pdf>
 101. FBI, ‘CODIS Brochure’, undated, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis_brochure
 102. A caveat notes: “Due to privacy concerns, automated international data exchange to only occur with authorizing legislation.” See: Thomas Callaghan, ‘DNA as a Biometric & FBI International Data Initiatives’, 25 September 2008, http://biometrics.org/bc2008/presentations/199_updated.pdf
 103. As adopted: ‘Draft Internal Security Strategy for the European Union: “Towards a European Security Model”’, 7120/10, 8 March 2010, <http://www.statewatch.org/news/2010/mar/eu-iss-draft-7120-10.pdf>
 104. Ernst & Young et Associés, ‘Evaluation of Aquapol, Tispol and Railpol’, 15 January 2013, p.8, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/police-cooperation/general/docs/eandy_evaluation_of_aquapol_railpol_tispol_final_report_20130115.pdf
 105. Economisti Associati, ‘Evaluation of ‘Prevention and Fight against Crime’ and ‘Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks’ Programs’, 2 December 2010, <http://www.statewatch.org/docbin/eu-com-2010-evaluation-cips-isec.pdf>
 106. Especially given that global financial institutions are deeply embroiled in the practice but rarely face scrutiny or punishment for it. The 2012 HSBC affair was a rare exception although apologies, fines and resignations seem to have served as adequate replacements for criminal prosecutions. See: ‘Outrageous HSBC Settlement Proves the Drug War is a Joke’, *Rolling Stone*, 13 December 2012, <http://www.rollingstone.com/politics/news/outrageous-hsbc-settlement-proves-the-drug-war-is-a-joke-20121213>, accessed 29 April 2016; ‘A word about banks and the laundering of drug money’, *Golem XVI*, 18 August 2012, <http://www.golemxiv.co.uk/2012/08/a-word-about-banks-and-the-laundering-of-drug-money/>, accessed 29 April 2016
 107. Information on the functioning of the system remains beyond the reach even of EU officials. See: ‘Presentation by the European Ombudsman, Emily O’Reilly - Decision of the European Ombudsman closing the inquiry into complaint 1148/2013/TN as regards Europol’, 8 January 2015, <https://www.ombudsman.europa.eu/activities/speech.faces/en/58671/html.bookmark>
 108. European Commission, ‘Questions and Answers: Action Plan to strengthen the fight against terrorist financing’, 2 February 2016, http://europa.eu/rapid/press-release_MEMO-16-209_en.htm
 109. HEMOLIA, http://cordis.europa.eu/project/rcn/98967_en.html
 110. ADVISE, http://cordis.europa.eu/project/rcn/102502_en.html
 111. CAPER, http://cordis.europa.eu/project/rcn/188358_en.html
 112. LASIE, http://cordis.europa.eu/project/rcn/185486_en.html
 113. ePOOLICE, http://cordis.europa.eu/project/rcn/106659_en.html
 114. Which was well-intentioned attention but ended up riddled with “exaggeration and misrepresentation”, as discussed in Ben Hayes, ‘CLEAN IT: the secret EU surveillance plan that wasn’t’, 9 October 2012, <https://www.opendemocracy.net/ben-hayes/clean-it-secret-eu-surveillance-plan-that-wasn-t>. A confidential INDECT paper also became public at some point during the course of the project. See: ‘EU social network spy system brief, INDECT Work Package 4, 2009’, *Wikileaks*, 5 October 2009, https://wikileaks.org/wiki/EU_social_network_spy_system_brief,_INDECT_Work_Package_4,_2009
 115. INDECT, http://cordis.europa.eu/project/rcn/89374_en.html

116. Technopolis Group et al., 'Final Evaluation of Security Research under the Seventh Framework Programme – Final Report', September 2015, p.58, <http://www.statewatch.org/docbin/eu-technopolis-assessment-fp7-esrp-2015.pdf>
117. MOSAIC, http://cordis.europa.eu/project/rcn/98642_en.html
118. ADABTS, http://cordis.europa.eu/project/rcn/91158_en.html
119. P-REACT, http://cordis.europa.eu/project/rcn/185501_en.html
120. TACTICS, http://cordis.europa.eu/project/rcn/104785_en.html
121. iDetect 4ALL, http://cordis.europa.eu/project/rcn/87259_en.html
122. SMARTPREVENT, http://cordis.europa.eu/project/rcn/185481_en.html
123. SAMURAI, http://cordis.europa.eu/project/rcn/89343_en.html
124. ZONESEC, http://cordis.europa.eu/project/rcn/192560_en.html
125. Some useful overviews of existing research are available, such as: 'Review of Studies on Surveillance Camera Effectiveness', *Privacy SOS*, undated, https://privacysos.org/camera_studies/; and Leighton Walter Kille and Martin Maximino, 'The effect of CCTV on public safety: Research roundup', 11 February 2014, <https://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime>
126. See, for example: Fundamental Rights Agency, 'Towards More Effective Policing, Understanding and preventing discriminatory ethnic profiling: A guide', October 2010, pp.25-36, <http://fra.europa.eu/en/publication/2010/towards-more-effective-policing-understanding-and-preventing-discriminatory-ethnic>; Open Society Foundations, 'Ethnic profiling in Europe', last updated 26 March 2015, <https://www.opensocietyfoundations.org/projects/ethnic-profiling-europe>; Asociación Pro Derechos Humanos de Andalucía, 'Identificaciones policiales basadas en perfil étnico en Granada', 11 October 2016, <http://www.apdha.org/identificaciones-policiales-basadas-en-perfil-etnico-en-granada/>
127. Angelique Chrisafis, 'France awaits landmark ruling on 'racial profiling' ID checks', *The Guardian*, 25 February 2015, <https://www.theguardian.com/world/2015/feb/25/france-landmark-ruling-racial-profiling-checks-police-paris-terror-attacks>; Anthony Faiola, 'Racial profiling seems to be a weapon in Europe's war on terrorism', *The Washington Post*, 15 February 2016, https://www.washingtonpost.com/world/europe/racial-profiling-seems-to-be-a-weapon-in-europes-war-on-terrorism/2016/02/15/78788aea-cb91-11e5-b9ab-26591104bb19_story.html
128. Rosamunde van Brakel, 'Pre-emptive Big Data Surveillance and its (Dis)Empowering Consequences: the Case of Predictive Policing' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds.), *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, pp.123-6, <https://www.ivir.nl/publicaties/download/1764>
129. SAVELEC, http://cordis.europa.eu/project/rcn/102072_en.html;
130. AEROCEPTOR, http://cordis.europa.eu/project/rcn/106475_en.html
131. INGRESS, http://cordis.europa.eu/project/rcn/110929_en.html
132. FIDELITY, http://cordis.europa.eu/project/rcn/102324_en.html
133. BEAT, http://cordis.europa.eu/project/rcn/102363_en.html
134. RAPTOR, http://cordis.europa.eu/result/rcn/157441_en.html
135. SecurEau, http://cordis.europa.eu/project/rcn/92297_en.html
136. SAFEWATER, http://cordis.europa.eu/project/rcn/110459_en.html
137. ISIS, http://cordis.europa.eu/project/rcn/111197_en.html
138. TAWARA_RTM, http://cordis.europa.eu/project/rcn/111061_en.html
139. SNIFFER, http://cordis.europa.eu/project/rcn/102348_en.html
140. SNOOPY, http://cordis.europa.eu/project/rcn/111313_en.html
141. HANDHOLD, http://cordis.europa.eu/project/rcn/102760_en.html
142. DOGGIES, http://cordis.europa.eu/project/rcn/103810_en.html
143. SUBCOP, http://cordis.europa.eu/project/rcn/108806_en.html
144. Dimitri Tokmetzis and Maaïke Goslinga, 'How billions vanish into the black hole that is the security industry', *De Correspondent*, February 2017, <https://thecorrespondent.com/6229/how-billions-vanish-into-the-black-hole-that-is-the-security-industry/303333613-52f43e22>
145. Paras. 56-57, Judgment in Joined Cases C-293/12 and C-594/12, 8 April 2014, <http://statewatch.org/news/2014/apr/eu-ecj-data-ret-judgment.pdf>
146. Presidency of the Council of the EU, 'Access criteria for competent authorities to retained communication data – Exchange of views', 8798/17, 4 May 2017, <http://www.statewatch.org/news/2017/may/eu-council-retained-data-8798-17.pdf>; 'Data retention: Commission still refusing demands for new mass surveillance measures', *Statewatch News Online*, March 2016, <http://database.statewatch.org/article.asp?aid=36221>
147. Steve Peers, 'The proposed European Investigation Order: Assault on human rights and national sovereignty', *Statewatch Analysis*, May 2010, <http://www.statewatch.org/analyses/no-96-european-investigation-order.pdf>
148. European Commission, 'Rights of suspects and accused', http://ec.europa.eu/justice/criminal/criminal-rights/index_en.htm
149. For an overview of how the policy cycle functions, see: Chris Jones, 'EU joint police operations target irregular migrants', *Statewatch Journal*, vol. 23 no. 3/4, February 2014, <http://database.statewatch.org/article.asp?aid=33158>

150. On the line between humanitarian assistance and criminal acts, see: Chris Jones, 'Hindering humanitarianism: European Commission will not ensure protection for those aiding *sans-papiers*', *Statewatch Viewpoint*, April 2017, <http://www.statewatch.org/analyses/no-311-facilitation-directive.pdf>
151. "A huge number of migrants": over 19,000 people apprehended during joint police operation Mos Maiorum', *Statewatch News Online*, January 2015, <http://database.statewatch.org/article.asp?aid=34476>
152. 'Punishing the victims - a beginner's guide to the EU and the crisis', *Corporate Europe Observatory*, 17 February 2014, <http://corporateeurope.org/eu-crisis/2014/02/punishing-victims-beginners-guide-eu-and-crisis>
153. 'The importance of income security', *Citizens Advice*, 13 June 2016, <https://www.citizensadvice.org.uk/about-us/policy/policy-research-topics/welfare-policy-research-surveys-and-consultation-responses/welfare-policy-research/the-importance-of-income-security/>
154. 'High-Level Conference on a Renewed EU Internal Security Strategy – The role of the Private Sector in EU Internal Security, Speech to be released on the 29th Sept. 2014 by Santiago Roura, Chairman of the European Organisation for Security', European Organisation for Security, undated
155. European Commission, 'Commission Staff Working Document – Security Industrial Policy', SWD(2012) 233 final, p.4, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN>
156. 'NeoConOpticon', p.25. The report covers in detail the membership of ESRIFF.
157. http://www.statewatch.org/Targeted-issues/ESRP/documents/esrif_final_report.pdf
158. Istituto Affari Internazionali, Manchester Institute of Innovation Research, Institut des Relations Internationales et Stratégiques, "Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence", 15 June 2010, p.170, http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf
159. For more detail see the case study 'Shaping the end-user landscape in the EU' in Technopolis Group et al., 'Final Evaluation of Security Research under the Seventh Framework Programme – Final Report', September 2015, pp.142-9, <http://www.statewatch.org/docbin/eu-technopolis-assessment-fp7-esrp-2015.pdf>
160. European Commission, 'Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection', SWD(2013) 318 final, 28 August 2013, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf
161. 'Commission proposes military research programme', *Statewatch News Online*, August 2014, <http://database.statewatch.org/article.asp?aid=33894>
162. See, for example: 'Plans emerge for the collection of personal data outside European borders to obtain "comprehensive situational awareness and intelligence support"', *Statewatch News Online*, October 2012, <http://database.statewatch.org/article.asp?aid=31942>
163. European Commission, 'A European Security Research and Innovation Agenda - Commission's initial position on ESRIFF's key findings and recommendations', COM(2009) 691 final, 21 December 2009, http://www.statewatch.org/Targeted-issues/ESRP/documents/com_2009_0691.pdf
164. See: Transparency Register, 'European Organisation for Security', updated 15 April 2016, <http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=32134385519-64>
165. European Organisation for Security, <http://eos-eu.com/?page=home>
166. European Commission Transparency Register, 'European Organisation for Security', <http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=32134385519-64>
167. EOS, 'What is EOS?', undated, <http://www.eos-eu.com/Middle.aspx?Page=whatiseos&tID=1>
168. ARCHIMEDES, http://cordis.europa.eu/project/rcn/101736_en.html
169. These include DESSI ("a highly structured and versatile method for Decision Support on Security Investment", €1.6 million from the EU), SECURECHAINS ("contribute to a more competitive Security technology supply chain," partly by examining "how the experience from the defence market can be transferred into the security market and vice-versa", €820,000), HECTOS and CRISP (market harmonisation through new certification procedures for security technologies, €3.5 million and €2.2 million), INSec ("improving the innovation performance of emergency and rescue services", €1.1 million), VALUESEC ("modeling, weighting and quantifying attributes of costs and benefits, advantages and disadvantages of security measures", €3.4 million), and OSMOSIS (helping small and medium-sized enterprise "understand and focus on security market trend and untapped potentials", €580,000).
170. EOS, 'Proposed End-to-End Approach for Security Research and Innovation', 16 February 2015, p.6, http://www.archimedesfp7-eu.eu/docs/ARCHI_D1.3_Proposed%20End-to-End%20Approach%20for%20Security%20Research%20and%20Innovation_V3%20FINAL%20M36.pdf
171. According to the ARCHIMEDES report: "European and national authorities, regulators and procurement professionals; Representatives from: the civil security authorities; first responders and law enforcement bodies (including, when needed, representatives of the defence sector); Representatives from: private users, owners and operators of infrastructures and services; Representatives from research institutes, universities and NGOs; Representatives from: industry suppliers of security solutions and services; Representatives may also be drawn from the insurance and the financial sector." EOS, 'Proposed End-to-End Approach for Security Research and Innovation', 16 February 2015, p.28
172. Ibid.

173. Civil aviation security (October 2012), CBRN event response (December 2012), cyber-crime and cyber-terrorism (April 2013), external dimension of security (April 2013), smart borders and border surveillance (October 2013), crisis management and civil protection (November 2013), innovation management (January 2014), robotics in security (April 2014), critical infrastructure protection (June 2014), and security in urban areas (October 2014). See: 'Europe: Security recommendations', *Sécurité & Défense*, 7 January 2015, <http://sd-magazine.com/article.php?page=90>; 'ARCHIMEDES Report Summary', *CORDIS*, http://cordis.europa.eu/result/rcn/140295_en.html; 'ARCHIMEDES Thematic Conference on Urban Security', *Market Place of the European Innovation Partnership on Smart Cities and Communities*, <https://eu-smartcities.eu/content/archimedes-thematic-conference-urban-security>; 'End-user innovation needs in cybersecurity', http://www.cspforum.eu/uploads/Csp2014Presentations/Track_3/Claudio%20Telmon_%20ARCHI_CYSPA.pdf
174. 'Europe: Security recommendations', *Sécurité & Défense*, 7 January 2015, <http://sd-magazine.com/article.php?page=90>
175. 'Archimedes high-level conference: establishing a European network of national organisations for security', *Archimedes Newsletter*, 16 May 2014
176. Former Commission official Pierre Defraigne considers that: "there is de facto a systemic collusion between the Commission and business circles, with the asserted justification of the consumer's interest, which is the way in which the European citizen is present as a stake in the European decision-making circuit." See: 'International Trade, Corporate Lobbying, and the European Political Project: A Conversation with Pierre Defraigne', *Corporate Europe Observatory*, 22 April 2015, <https://corporateeurope.org/power-lobbies-economy-finance-international-trade/2015/04/international-trade-corporate-lobbying-and>
177. Teresa Riera Madurell, 'Draft report on the proposal for a Regulation of the European Parliament and of the Council establishing Horizon 2020', *Committee on Industry, Research and Energy*, 15 June 2012, p.147, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-489.637+02+DOC+PDF+V0//EN&language=EN>
178. "The analysis of roll-call votes between 2009 and 2013 reveals three different co-existing winning coalitions in the EP that vary by policy area, but are relatively stable over time: first, a 'grand coalition' between EPP and S&D, often together with ALDE (in total in about 70% of the cases)". See: Valentin Kreilinger, '15 key votes in the 2009-14 European Parliament: main insights', *Jacques Delors Institute/VoteWatch Europe*, 19 May 2014, p.3, <http://www.institutdelors.eu/media/analysisepkeyvotes-kreilinger-ne-jdi-may14.pdf>
179. Christian Ehler, 'Déclaration des intérêts financiers des députés', http://www.europarl.europa.eu/mepdif/28226_DFI_rev0_FR.pdf
180. The others were Roberta Angelilli, Tunne Kelam and Marian-Jean Marinescu (all also from the EPP) and Jan Mulder (Alliance of Liberals and Democrats for Europe, ALDE).
181. Amendment 1674, <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE492.790>
182. European Parliament, 'Horizon 2020 Framework Programme for research and innovation 2014-2020: rules for participation and dissemination', [http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2011/0399\(COD\)&l=en](http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2011/0399(COD)&l=en)
183. Ares(2016)3065685, 29 June 2016, <https://www.asktheeu.org/en/request/3024/response/10666/attach/5/Ares%202016%203065685%20Red.pdf>
184. Council, 'Proposal for a Regulation of the European Parliament and the Council establishing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020) - 4-column document -Annex I - Societal challenges', 7574/13, 15 March 2013, <http://data.consilium.europa.eu/doc/document/ST-7574-2013-INIT/en/pdf>
185. Report from the High-Level Security Roundtable 2012, 21 March 2012, p.10, http://www.eos-eu.com/files/Documents/2012_High_Level_Security_Roundtable_Report_final.pdf
186. 'Explanatory statement' contained in the 'Report on the proposal for a regulation of the European Parliament and of the Council, establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa', 14 January 2014, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0025+0+DOC+XML+V0//EN#title2>
187. See also an earlier report from Corporate Europe Observatory: 'Lobbying warfare', 21 September 2011, <https://corporateeurope.org/power-lobbies/2011/09/lobbying-warfare>
188. The 2011 Roundtable was followed the day after by a joint EOS-SDA conference, entitled 'A new partnership for European security'. Sponsored by BAE Systems, CEA, EADS, G4S, Raytheon, Safran, Selex Sistemi Integrati, Siemens, Smiths Detection and Thales, the participants mainly came from industry. The report from the conference notes the need to give "a 'privacy friendly' aspect to security research" in order to "allay civil rights concerns [and] give European companies a competitive edge as privacy issues become more widespread around the world."
189. Mark Akkerman, 'Border Wars', July 2016, <https://www.tni.org/en/publication/border-wars>;
190. '2012 High Level Security Roundtable - Concept paper', <http://www.statewatch.org/docbin/eu-com-high-level-security-roundtable-concept-paper-21-3-12.pdf>
191. ASD, 'Detailed Programme', 30 April 2014, <http://www.tpeb.cz/wp-content/uploads/2014/05/DETAILED-PROGRAMME-ASD-ANNUAL-CONVENTION-TECHNOLOGY-FORUM-2014.pdf>
192. European Commission, 'Staff Working Document on transport security', SWD(2012) 143 final, <http://www.statewatch.org/news/2012/dec/eu-com-transport-security-swd-143-12.pdf>
193. Letter from Slim Kallas to Luigi Rebuffi and Robert Havas, 3 July 2012, <http://www.statewatch.org/docbin/eu-com-letter-slim-kallas-eos-transport-security-3-7-12.pdf>
194. This eventually emerged as a set of "strategic guidelines", adopted by Member States sitting in the European Council with zero parliamentary discussion or debate: Conclusions of the European Council, 26/27 June 2014, <http://statewatch.org/news/2014/jun/eu-council-conclusions-jha.pdf>

195. The 2015 Agenda on Security notes: "Research and innovation is essential if the EU is to keep up-to-date with evolving security needs," (p.11) and: "A competitive EU security industry can also contribute to the EU's autonomy in meeting security needs." See: European Commission, 'The European Agenda on Security', COM(2015) 185 final, 28 April 2015, <http://www.statewatch.org/news/2015/apr/eu-com-agenda-on-security-com-185-15.pdf>
196. European Commission, Italian Presidency of the Council of the EU and EU Committee of the Regions, 'Protecting our societies and citizens' rights – Renewing the EU Internal Security Strategy', 29 September 2014, http://ec.europa.eu/dgs/home-affairs/pdf/eu_iss_conference_programme_20140929_en.pdf
197. Roura left Indra in September 2015 with a reported €4.8 million farewell payment. In an ongoing case, he is accused of delivering a €10,000 cash payment to one Alejandro de Pedro Llorca, known for undertaking "reputational works on the internet for leaders of the Popular Party," Spain's governing conservative formation. Other Indra executives have also been accused relation to these undertakings. The *Guardia Civil* reportedly photographed Roura "in a car park in Madrid" where is alleged to have delivered "an envelope with wads of notes to... Pedro Llorca.". See: Agustín Marco, 'Indra paga indemnizaciones millonarias a directivos tras despedir a 3.000 empleados', *El Confidencial*, 10 September 2015, http://www.elconfidencial.com/empresas/2015-09-10/indra-paga-indemnizaciones-millonarias-a-directivos-tras-despedir-a-3-000-empleados_1008559/; José Precado, 'ICM y Canal de Isabel II: dos empresas públicas sin control convertidas en cajeros automáticos del PP de Madrid', *El Diario*, 1 May 2017, http://www.eldiario.es/politica/Ignacio-Gonzalez-Agencia-Informatica-PP_0_635886619.html; Irene Castro, 'El seguidor de Púnica: "He quedado con el tío de Indra que nos va a pagar en La Moraleja"', *El Diario*, 28 March 2017, http://www.eldiario.es/politica/conseguidor-Punica-queda-do-Indra-Moraleja_0_627138281.html; and Antonio M. Vélez, 'El número dos de Indra, un superviviente imputado en Púnica y bajo la sospecha de la Operación Lezo', *El Diario*, 21 April 2017, http://www.eldiario.es/economia/CEO-Indra-Punica-Operacion-Lezo_0_635537411.html
198. Santiago Roura, 'The role of the Private Sector in EU Internal Security', text of a speech given at the High-Level Conference on a Renewed EU Internal Security Strategy, 29 September 2014
199. Ares(2016)3065685, 29 June 2016, https://www.asktheeu.org/en/request/request_for_minutes_and_document_5
200. Dimitri Tokmetzis, 'Request for minutes and documents on staff meetings', [asktheeu.org](https://www.asktheeu.org/en/request/request_for_minutes_and_document_5), 10 June 2016, https://www.asktheeu.org/en/request/request_for_minutes_and_document_5
201. See also: Crina Boros, 'How the EU cosied up to the defence lobby', *Investigate Europe*, 21 December 2016, <http://www.investigate-europe.eu/en/how-the-eu-cosied-up-to-the-defence-lobby/>
202. Secure Societies Advisory Group, 'Strategic input for 2016-17 call', July 2014, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=15204&no=1>
203. Ares(2016)3065318, 29 June 2016, https://www.asktheeu.org/en/request/request_for_minutes_and_document_5
204. It was not until 2016 that the Commission adopted rules making it "mandatory for Commission departments to select all expert group members through public calls for applications," but even so it is not clear that personal invitations would have been in line with the previous rules. See: European Commission, 'More transparent and balanced interest representation: Commission adopts new expert group rules', 30 May 2016, http://europa.eu/rapid/press-release_IP-16-1923_en.htm; and European Commission, 'Horizontal rules for Commission expert groups', C(2010)7649 final, 10 November 2010, http://ec.europa.eu/transparency/regexpert/PDF/C_2010_EN.pdf
205. The industry seems to be satisfied with the resolution to the disagreement, which presumably means that companies will be more easily to keep hold of the intellectual property generated during research projects. Specific rules were introduced in Horizon 2020 for security research projects to try to ensure wider use of results. See: Crina Boros, 'How the EU cosied up to the defence lobby', *Investigate Europe*, 21 December 2016, <http://www.investigate-europe.eu/en/how-the-eu-cosied-up-to-the-defence-lobby/>; and 'Funding programmes and intellectual property' in Chris Jones, 'The visible hand: the European Union's Security Industrial Policy', August 2016, p.12, <http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf>
206. Mr Schmitt, meanwhile, is "a full-time ASD employee. He [was] recruited last year [2014] by ASD, coming from DG MARKT, where he was the pen on all matters related to Defence and Security for nearly ten years." See: Ares(2016)3065318, 29 June 2016, https://www.asktheeu.org/en/request/request_for_minutes_and_document_5
207. ASD, 'Quarterly Newsletter', October 2015, http://www.asd-europe.org/fileadmin/user_upload/Client_documents/ASD_Contents/2_COMMUNICATION/2.1_Highlights/ASD_newsletter_10_2015-4.pdf
208. 'Declaration of interests', *Register of Commission Expert Groups*, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=memberDetail.memberDetail&memberID=60924>
209. 'Declaration of interests', *Register of Commission Expert Groups*, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=memberDetail.memberDetail&memberID=60401>
210. Multisense Chip, http://cordis.europa.eu/project/rcn/99656_en.html
211. EDEN, http://cordis.europa.eu/project/rcn/110015_en.html
212. ROCSAFE, http://cordis.europa.eu/project/rcn/203295_en.html
213. ASD, 'Quarterly Newsletter', October 2015, http://www.asd-europe.org/fileadmin/user_upload/Client_documents/ASD_Contents/2_COMMUNICATION/2.1_Highlights/ASD_newsletter_10_2015-4.pdf
214. 'EU funding for network developing surveillance, intelligence-gathering and remote vehicle stopping tools', *Statewatch News Online*, January 2015, <http://database.statewatch.org/article.asp?aid=34440>

215. 'New police cooperation plan includes surveillance, intelligence-gathering and remote vehicle stopping technology', *Statewatch News Online*, January 2014, <http://database.statewatch.org/article.asp?aid=33159>
216. 'Police forces get ready for multi-billion euro policing and security funds', *Statewatch News Online*, June 2014, <http://database.statewatch.org/article.asp?aid=33609>
217. See: 'Report on the meeting of ENLETS held on 29-30 September 2014 in Rome', 15000/14, 4 November 2014, <http://www.statewatch.org/news/2015/jan/eu-council-2014-11-24-15000-enlets-september-report.pdf>
218. Peter J. Burgess, 'The Future of Security Research in the Social Sciences and Humanities', *European Science Foundation*, July 2014, p.18, http://archives.esf.org/uploads/media/future_security_research.pdf
219. European Commission, 'Commission Staff Working Paper – Security Industrial Policy', SWD(2012) 233 final, p.4, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN>
220. The 'digital security' theme, however, is managed by DG CONNECT, responsible for communications networks, content and technology; while under Article 37 of the new Frontex Regulation agreed in September 2016 the EU's border agency has a role in "identifying key research themes," and is responsible for implementing "the parts of the Framework Programme for Research and Innovation which relate to border security." See: Regulation (EU) 2016/2624 of the European Parliament and the of the Council of 14 September 2016 on the European Border and Coast Guard, <http://statewatch.org/news/2016/oct/eu-council-border-agency-regulation.pdf>
221. Santiago Roura, 'The role of the Private Sector in EU Internal Security', text of a speech given at the High-Level Conference on a Renewed EU Internal Security Strategy, 29 September 2014
222. PASAG, 'Report of the Protection and Security Advisory Group (PASAG)', July 2016, p.4, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28826&no=1>
223. 'Report of the Protection and Security Advisory Group (PASAG)', p.7
224. Ares(2016)3065318, https://www.asktheeu.org/en/request/request_for_minutes_and_document_5
225. Paulo Pena, '76 Million Euros: EU shops for drones to survey migration routes', *Investigate Europe*, 18 March 2017, <http://www.investigate-europe.eu/en/76-million-to-survey-migration-routes-largest-eu-public-drone-tender-decided/>
226. '€67 million for maritime surveillance drones', *Statewatch News Online*, 13 October 2016, <http://www.statewatch.org/news/2016/oct/eu-emsadrones1.htm>
227. These schemes are examined in more detail in an earlier article. See the section 'Bringing the state to market: pre-commercial procurement' in Chris Jones, 'The visible hand: the European Union's Security Industrial Policy', August 2016, pp.13-15, <http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf>
228. EOS, 'Proposed End-to-End Approach for Security Research and Innovation', 16 February 2015, p.20, http://www.archimedesfp7-eu.eu/docs/ARCHI_D1.3_Proposed%20End-to-End%20Approach%20for%20Security%20Research%20and%20Innovation_V3%20FINAL%20M36.pdf, accessed 25 May 2016
229. 'Review of security measures in the 7th Research Framework Programme FP7 2007-2013', *European Parliament Directorate-General for Internal Policies*, April 2014, p.29, <http://statewatch.org/news/2015/jan/ep-2014-04-fp7-security-research.pdf>
230. "Surveillance over freedoms, for safety's sake" - Belgian PM on possible Schengen limiting', RT, 23 August 2015, <https://www.rt.com/news/313152-belgian-eu-surveillance-borders/>
231. Tova Cohen, 'Israeli defence firm Elbit eyes growing homeland security market', Reuters, 8 June 2016, <http://www.reuters.com/article/security-elbit-systems-idUSL8N1902H8>
232. European Commission, 'First progress report towards an effective and genuine Security Union', COM(2016) 670 final, 12 October 2016, p.2, <http://www.statewatch.org/news/2016/oct/eu-com-1st-new-security-report-com-670-16.pdf>
233. European Commission, 'Overview', last updated 27 May 2017, https://ec.europa.eu/home-affairs/financing/fundings/index_funding_en. The funds noted in the main text are far from exhaustive. The July 2016 PASAG report argued that "ICT, Transport, Energy, Climate action and Space are just a few areas where Security needs to be built into the design of new solutions and capabilities and where the cross-border impact has important security implications." When it comes to border security, the EU's newer states all received significant funding from the PHARE programme and other sources. See: PASAG, 'Report of the Protection and Security Advisory Group (PASAG)', July 2016, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28826&no=1>; Mark Akkerman, 'Border Wars', July 2016, <https://www.tni.org/en/publication/border-wars/>;
234. The Eurostat total for "public order and safety" includes "police services, fire-protection services, law courts, prisons, R&D public order and safety" and other unclassified expenditure under the same heading. The figures for spending between EU Member States and the EU itself are thus not easily comparable, especially as Member State expenditure will include some EU funding. Nevertheless, the statistics give some idea of the numbers involved at national and European level. See: Eurostat, 'Government expenditure on public order and safety', February 2017, http://ec.europa.eu/eurostat/statistics-explained/index.php/Government_expenditure_on_public_order_and_safety
235. European Commission, 'Commissioner Malmström welcomes the Parliament's vote on the new EU Home Affairs' Funds 2014-2020', 13 March 2014, <http://www.statewatch.org/docbin/eu-2014-03-13-com-parl-vote-pr.pdf>

236. As a Commission document stated: "In order to... avoid putting at risk the timely approval of NPs [national programmes], it has been agreed during the policy dialogues that MS [Member States] would informally submit their draft NPs... before the entry into force of the basic acts and the relevant implementing acts... they will give the opportunity to MS and the Commission to move towards a shared understanding of the strategies and the priorities proposed in the programmes in view of their efficient finalisation and approval by the Commission." See: DG HOME, 'Manual to assist Member States in Programming for the Asylum, Migration and Integration and Internal Security Funds of the Multiannual Financial Framework period 2014-20', draft version 8, 31 March 2014, p.8, <http://www.statewatch.org/docbin/eu-com-2014-isf-amif-programming-manual-for-ms.pdf>
237. As adopted: 'Draft Council Conclusions on the Renewed European Internal Security Strategy 2015-20', 9416/15, 1 June 2015, <http://statewatch.org/news/2015/jun/eu-council-iss-draft-conclusions-9416-15.pdf>. Confusingly, the aims and intentions of the Renewed ISS are spread across this and two other documents, the European Commission's 'European Agenda on Security' (<http://statewatch.org/news/2015/apr/eu-com-agenda-on-security-com-185-15.pdf>) and the Council's conclusions on the development of the renewed European Union Internal Security Strategy of 4-5 December 2014 (https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/146042.pdf)
238. For an overview of ongoing work and the responsible bodies, see: 'Internal security: "common risk indicators", internet monitoring, a European police register, entry bans and more', *Statewatch News Online*, December 2015, <http://database.statewatch.org/article.asp?aid=35804>; and 'Implementing the Internal Security Strategy: planning documents', *Statewatch News Online*, August 2015, <http://database.statewatch.org/article.asp?aid=35274>
239. 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy', June 2016, p.45, <http://statewatch.org/news/2016/jul/eu-global-security-strategy.pdf>
240. One should be wary of predictions from those with vested interests, but it is worth noting that numerous reports suggest significant growth in "homeland security" due to terrorist attacks and perceived the lack of "border security" in Europe. See, for example: 'Global Homeland Security & Public Safety Industry, Technologies Market 2015-2022', *ASD Reports*, January 2015, <https://www.asdreports.com/market-research-report-180074/global-homeland-security-public-safety-industry-technologies-market>; 'Homeland Security Market worth \$544.02 Billion – 2018', *Markets and Markets*, undated, <http://www.marketsandmarkets.com/PressReleases/homeland-security-emergency-management.asp>; 'European Counter-Terror and Public Safety Market Surge', *Homeland Security Research*, 2 May 2016, <http://www.marketwired.com/press-release/european-counter-terror-public-safety-market-surge-from-2008-2014-cagr-35-2016-2020-2120146.htm>; 'Homeland Security Market Forecast 2014-2024', *Visiongain*, 8 October 2014, <https://www.visiongain.com/Report/1329/Homeland-Security-Market-Forecast-2014-2024>
241. Eliav Lieblich and Adam Shinar, 'The Case Against Police Militarization', 10 January 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2840715
242. 'Orwellian counter-terrorism laws stripping rights under guise of defending them', *Amnesty International*, 17 January 2017, <https://www.amnesty.org/en/latest/news/2017/01/eu-orwellian-counter-terrorism-laws-stripping-rights-under-guise-of-defending-them/>
243. 'Dangerously disproportionate: the ever-expanding national security state in Europe', *Amnesty International*, 17 January 2017, <https://www.amnesty.org/en/documents/eur01/5342/2017/en/>
244. European Commission, 'Towards a more competitive and efficient defence and security sector', COM(2013) 542 final, 24 July 2013, p.11, <http://statewatch.org/news/2013/jul/eu-com-defence-security-sector-com-542-13.pdf>
245. Council Decision 2013/743/EU of 3 December 2013 establishing the specific programme implementing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020), p.66, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0965:1041:EN:PDF>
246. 'High-level group of personalities on defence research', <http://statewatch.org/news/2016/mar/eu-defence-research-gop-members.pdf>
247. Group of Personalities, 'The case for an EU-funded defence R&T programme', February 2016, p.27, <http://statewatch.org/news/2016/mar/eu-defence-research-gop-again.pdf>
248. European Commission, 'European Defence Action Plan: Towards a European Defence Fund', 30 November 2016, http://europa.eu/rapid/press-release_IP-16-4088_en.htm
249. European Defence Agency, 'Commission proposes EU Defence Fund as "crucial step" to boost defence industry', *European Defence Matters*, no. 12, <https://www.eda.europa.eu/webzine/issue12/cover-story/commission-proposes-eu-defence-fund-as-crucial-step-to-boost-defence-industry>
250. COMPOSITE, 'ICT Trends in European Policing', 2011, http://composite-project.eu/tl_files/fM_k0005/download/COMPOSITE%20ICT%20Trends.pdf
251. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, PE-CONS 71/15, 15 April 2016, <http://statewatch.org/news/2016/apr/eu-council-eu-pnr-dir-16.pdf>. See also: European Parliament, 'Parliament backs EU directive on use of Passenger Name Records (PNR)', 14 April 2016, <http://statewatch.org/news/2016/apr/ep-press-rel-eu-pnr-passed.pdf>
252. Belgian, Danish, German, Spanish, French, Dutch, Polish and UK delegations, 'Foreign fighters: Conclusions of the meeting of Ministers of Belgium, Denmark, France, Germany, Poland, Spain, the Netherlands and the United Kingdom, held on 7 July 2014 in Milan', 12757/14, <http://statewatch.org/news/2016/mar/eu-council-foreign-fighters-meeting-pnr-agreement-12757-14.pdf>

253. 'Travel surveillance: PNR by the back door', *Statewatch News Online*, October 2014, <http://database.statewatch.org/article.asp?aid=34058>
254. Nikolaj Nielsen, 'Governments eschew urgency of passenger flight data law', *EUobserver*, 7 October 2016, <https://euobserver.com/justice/135412>
255. Estelle Massé and Joe Macnamee, 'The curious tale of the French prime minister, PNR and peculiar patterns', *EurActiv*, 4 October 2016, <http://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesday-the-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/>
256. Belgian national ISF programme, <http://www.statewatch.org/docbin/be-isf-national-programme.pdf>
257. 'PNR: €70 million for swift implementation of travel surveillance and profiling infrastructure', *Statewatch News Online*, 21 December 2016, <http://statewatch.org/news/2016/dec/eu-pnr-implementation.htm>
258. As the minutes of a March 2015 meeting of the Secure Societies Advisory Group record, one working group discussed "a typical proposal: what are and should be the police robots?"
259. ASGARD, http://cordis.europa.eu/project/rcn/203297_en.html
260. TENSOR, http://cordis.europa.eu/project/rcn/203292_en.html
261. DANTE, http://cordis.europa.eu/project/rcn/202691_en.html
262. MEDIA4SEC, http://cordis.europa.eu/project/rcn/204503_en.html
263. European Forum for Urban Security, <https://efus.eu/en/>
264. 'Can Member States still use: DATA RETENTION?', *Statewatch News Online*, November 2015, <http://database.statewatch.org/article.asp?aid=35773>
265. 'Data retention: Commission still refusing demands for new mass surveillance measures', *Statewatch News Online*, March 2016, <http://database.statewatch.org/article.asp?aid=36221>
266. Greek national ISF programme, <http://statewatch.org/news/2015/sep/eu-isf-nat-programme.pdf>
267. Hungarian national ISF programme, <http://www.statewatch.org/docbin/hu-isf-national-programme.pdf>
268. Belgian national ISF programme, <http://www.statewatch.org/docbin/be-isf-national-programme.pdf>
269. Croatian national ISF programme, <http://www.statewatch.org/docbin/hr-isf-national-programme.pdf>
270. Maltese national ISF programme, <http://www.statewatch.org/docbin/mt-isf-national-programme.pdf>
271. Romanian national ISF programme, <http://www.statewatch.org/docbin/ro-isf-national-programme.pdf>
272. 'Romanian Secret Services uses European Funding for mass surveillance project disguised as eGovernment services', ApTI, 8 August 2016, <https://privacy.apti.ro/2016/08/08/romanian-secret-services-uses-european-funding-for-mass-surveillance-project-disguised-as-egovernment-services/>
273. Sam Morgan, 'Romanian EU-funded project accused of data protection violations', 13 April 2017, <https://www.euractiv.com/section/data-protection/news/romanian-eu-funded-project-accused-of-data-protection-violations/>
274. INSPEC2T (€5 million), http://cordis.europa.eu/project/rcn/194895_en.html; TRILLION (€4.3 million), http://cordis.europa.eu/project/rcn/194841_en.html; Unity (€4.3 million), http://cordis.europa.eu/project/rcn/194893_en.html; CityCop (€5.6 million), http://cordis.europa.eu/project/rcn/197273_en.html
275. European Commission, 'Horizon 2020 Work Programme 2016-17 – 14. Secure societies', 13 October 2015, p.22, <http://statewatch.org/news/2015/nov/eu-secure-societies-wp-2016-17.pdf>
276. 'Prevent strategy 'sowing mistrust and fear in Muslim communities'', *The Guardian*, 3 February 2016, <https://www.theguardian.com/uk-news/2016/feb/03/prevent-strategy-sowing-mistrust-fear-muslim-communities>
277. Sean Coughlan, 'Teachers warn extremism policy prevents open debate', *BBC News*, 28 March 2016, <http://www.bbc.com/news/education-35907831>. For detailed investigation of the effects of the Prevent policy in schools, see: 'Preventing education? Human rights and UK counter-terrorism policy in schools', *Rights Watch UK*, July 2016, <http://www.statewatch.org/news/2016/jul/preventing-education-final-to-print-3.compressed-1.pdf>
278. 'Anti-radicalisation strategy lacks evidence base in science', *The Guardian*, 29 September 2016, <https://www.theguardian.com/politics/2016/sep/29/anti-radicalisation-strategy-lacks-evidence-base-in-science>
279. Ian Cobain, Alice Ross, Rob Evans and Mona Mahmood, 'Inside Ricu, the shadowy propaganda unit inspired by the cold war', *The Guardian*, 2 May 2016, <https://www.theguardian.com/politics/2016/may/02/inside-ricu-the-shadowy-propaganda-unit-inspired-by-the-cold-war>. See also: Ben Hayes and Asim Qureshi, 'Going global: the UK government's 'CVE' agenda, counter-radicalisation and covert propaganda', *OpenDemocracy*, 4 May 2016, <https://www.opendemocracy.net/ben-hayes-asim-qureshi/going-global-uk-government-s-propaganda-and-censorship-silicon-valley-and-cve>
280. Joint Select Committee on Human Rights, 'Government should consider extremism strategy', 22 July 2016, <http://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/news-parliament-2015/counter-extremism-report-published-16-17/>; see also the summary of the Committee's report, <https://www.publications.parliament.uk/pa/jt201617/jtselect/jtrights/105/10503.htm>
281. United Nations Human Rights, 'Do not criminalize extreme views – UN Special Rapporteur on counterterrorism', 15 March 2016, <http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=17229&LangID=E>
282. European Commission, 'Frequently asked questions: Stronger action at EU level to better tackle violent radicalisation', 14 June 2016, http://europa.eu/rapid/press-release_MEMO-16-2179_en.htm
283. For example: PRIME, http://cordis.europa.eu/project/rcn/185518_en.html; IMPACT Europe, http://cordis.europa.eu/project/rcn/111492_en.html; VOX-Pol, http://cordis.europa.eu/project/rcn/111495_en.html;
284. SAFIRE, http://cordis.europa.eu/project/rcn/94537_en.html

285. Presidency, 'Renewed European Union Internal Security Strategy Implementation Paper', 10854/15, 14 July 2015, p.12, <http://www.statewatch.org/news/2015/aug/eu-council-cosi-renewed-internal-security-strategy-10854-15.pdf>
286. 'Internal security: Project Harmony', *Statewatch News Online*, September 2011, <http://database.statewatch.org/article.asp?aid=30910>
287. NOTE from: Presidency to: Standing Committee on Operational Cooperation on Internal Security (COSI), 'EU Policy Cycle – Implementation monitoring – First progress reports 2016', 9926/1/16 REV 1, 16 June 2016, <http://www.statewatch.org/docbin/eu-council-policy-cycle-implementation-reports-9926-16-rev1.pdf>
288. Belgian national ISF programme, <http://www.statewatch.org/docbin/be-isf-national-programme.pdf>
289. Croatian national ISF programme, <http://www.statewatch.org/docbin/hr-isf-national-programme.pdf>
290. Hungarian national ISF programme, <http://www.statewatch.org/docbin/hu-isf-national-programme.pdf>
291. Latvian national ISF programme, <http://www.statewatch.org/docbin/lv-isf-national-programme.pdf>
292. Romanian national ISF programme, <http://www.statewatch.org/docbin/ro-isf-national-programme.pdf>
293. Alain Cadec MEP, Question for written answer to the Council: Conclusions of 8 and 9 November 2010 on the creation and implementation of an EU policy cycle for organised and serious international crime, E-005690-14, 9 July 2014, <http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2014-005690&language=EN>
294. Council of the European Union, Reply to written question E-005690-14, 15 September 2014, <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-005690&language=EN>
295. Aero Sekur, <http://aerosekur.com/intro/>
296. NOSY, http://cordis.europa.eu/project/rcn/196895_en.html
297. FORENSOR, http://cordis.europa.eu/project/rcn/194854_en.html
298. microMole, http://cordis.europa.eu/project/rcn/194878_en.html
299. BIWAS, http://cordis.europa.eu/project/rcn/197291_en.html
300. ROCSAFE, http://cordis.europa.eu/project/rcn/203295_en.html
301. European Commission, 'Horizon 2020 Work Programme 2016-17 – 14. Secure societies', 13 October 2015, p.14, <http://statewatch.org/news/2015/nov/eu-secure-societies-wp-2016-17.pdf>
302. Something with which the EU has long been concerned and for which the European Police College, CEPOL, now based in Budapest, was established. In 2013, for example, the Agency spent €300,000 on 19 separate courses related to its priorities. Its 2016 work programme notes that priority is being given "to the Policy Cycle and counter-terrorism activities in line with the priorities of the European Agenda of Security [sic]." See: CEPOL, 'Section III – Work Programme 2016', 17 November 2015, p.39, <https://www.cepol.europa.eu/sites/default/files/work-programme-2016.pdf>
303. LAW-TRAIN, http://cordis.europa.eu/project/rcn/194874_en.html
304. Some see significant potential for Israeli companies in Europe: "For the Europeans, this is a new challenge; but we've been dealing with lone terrorists with a Kalashnikov for years; and Israel has a lot of know-how when it comes to early detection and coping with a terrorist incident." See: 'Europe turns to Israeli know-how to fight terror', *Ynetnews.com*, 19 January 2015, <http://www.ynetnews.com/articles/0,7340,L-4616769,00.html>
305. AUGGMED, http://cordis.europa.eu/project/rcn/194875_en.html
306. Isra-Team 98, <http://www.israteam.com/>
307. TARGET, http://cordis.europa.eu/project/rcn/194852_en.html
308. Gaming for Peace, http://cordis.europa.eu/project/rcn/202705_en.html
309. ARIES, http://cordis.europa.eu/project/rcn/202675_en.html
310. FLYSEC, http://cordis.europa.eu/project/rcn/194906_en.html
311. Most recently this has involved the possibility of assistance to the dictatorial government of Ethiopia and other dubious regimes in and around the Horn of Africa. A useful overview of the EU's "external" migration projects and processes is available online. See: 'Beyond the borders', *Statewatch News Online*, August 2016, <http://statewatch.org/news/2016/aug/eu-migration-overview.htm>
312. WIMAAS, http://cordis.europa.eu/project/rcn/88640_en.html
313. European Commission, 'A European Agenda on Migration', COM(2015) 240 final, 13 May 2015, <http://statewatch.org/news/2015/may/eu-com-migration-agenda-com-240-15.pdf>
314. Sergio Carrera, Steven Blockmans, Daniel Gros and Elspeth Guild, 'The EU's Response to the Refugee Crisis: Taking Stock and Setting Policy Priorities', December 2015, p.2, https://www.ceps.eu/system/files/EU%20Response%20to%20the%202015%20Refugee%20Crisis_0.pdf
315. Ruben Andersson, 'Why Europe's border security approach has failed – and how to replace it', February 2016, http://www.securityintransition.org/wp-content/uploads/2016/02/WP08_Migration_FinalEditedVersion.pdf
316. The report 'Death by Rescue' makes particularly incisive arguments on this point. See: <https://deathbyrescue.org/>
317. '2016 deadliest year ever for migrants crossing Mediterranean – UN agency', *UN News Centre*, 6 January 2017, <http://www.un.org/apps/news/story.asp?NewsID=55919>
318. Frontex, 'Eurosur', undated, <http://frontex.europa.eu/intelligence/eurosur/>
319. At least €87 million from the FP6 and FP7 budgets had been spent on at least 17 projects concerned with Eurosur and related initiatives. For an overview of projects funded up to June 2012, see: Ben Hayes and Matthias Vermeulen, 'Borderline: The EU's New Border Surveillance Initiatives', *Heinrich Böll Stiftung*, June 2012, <http://www.statewatch.org/news/2012/jun/borderline.pdf>

320. 'Eurosur extended: all participating states now connected to border surveillance system', *Statewatch News Online*, December 2014, <http://database.statewatch.org/article.asp?aid=34324>
321. Bulgarian national ISF programme, <http://www.statewatch.org/docbin/bg-isf-national-programme.pdf>
322. Estonian national ISF programme, <http://www.statewatch.org/docbin/ee-isf-national-programme.pdf>
323. Nikolaj Nielsen, 'EU border surveillance system not helping to save lives', 14 May 2014, <https://euobserver.com/justice/124136>
324. 'GMV wins the EUROSUR project', *GMV*, 11 March 2014, http://www.gmv.com/en/Company/Communication/PressReleases/2014/NP_005_Frontex.html
325. 'GMV strengthens its position in the international defense and security market', *Homsec*, 20 June 2017, <http://www.homsec.es/gmv-strengthens-its-position-in-the-international-defense-and-security-market/>
326. SafeShore, http://cordis.europa.eu/project/rcn/203302_en.html. It should be noted that it is highly unlikely that a "small RPAS" would ever be able to carry a human being or a boat.
327. The EU has now been promoting the introduction of drones into civil airspace for over a decade. Their emergence as a new "threat" can perhaps be seen as a form of "blowback". It certainly serves as a boon for security technology companies. See: 'Eurodrones, Inc.', February 2014, <http://www.statewatch.org/eurodrones/>
328. RANGER, http://cordis.europa.eu/project/rcn/203301_en.html
329. European Commission, 'Communication on a draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain', COM(2010) 584 final, p.10, http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/documents/integrating_maritime_surveillance_en.pdf
330. 'Data adrift on the high seas: work continues on connecting maritime surveillance systems', *Statewatch News Online*, August 2014, <http://database.statewatch.org/article.asp?aid=33873>
331. EU CISE 2020, http://cordis.europa.eu/project/rcn/192603_en.html
332. The price tag and the list of participants demonstrate the serious nature of the EU CISE 2020, project, but "governance" of the CISE initiative as a whole has so far largely involved decisions taken by "expert groups" and EU and national officials. In an October 2010 resolution, the European Parliament requested that the Commission "propose a legal framework for the integration of maritime surveillance with a view to a common information sharing environment." In July 2014, the Commission said in a Communication that it "does not see a need to put in place a cross-sector legislative initiative," although it was not opposed to abolishing legislation – the same Communication said it would keep working "to remove possible remaining legal barriers to cross-sectorial information sharing while ensuring compliance with relevant data protection requirements." See: European Parliament, 'European Parliament resolution of 21 October 2010 on Integrated Maritime Policy (IMP) - Evaluation of progress made and new challenges', 2010/2040(INI), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2010-386>; and European Commission, 'Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain', COM(2014) 451 final, 8 July 2014, <http://www.statewatch.org/news/2014/jul/eu-com-2014-07-maritime-cise-com-451-final.pdf>
333. For example: 'Long-distance border controls to "check travellers data along his/her journey" and remotely detect "abnormal behaviour"' and 'EU seeks autonomous drones, "data fusion" and "enhanced command and control centres" for border control', *Statewatch News Online*, November 2015, <http://database.statewatch.org/article.asp?aid=35670> and <http://database.statewatch.org/article.asp?aid=35672>
334. NOTE from: Presidency to: Strategic Committee on Immigration, Frontiers and Asylum/Mixed Committee (EU-Iceland/Liechtenstein/Norway/Switzerland), 'Discussion paper on a European electronic travel authorisation system', 8590/16, 3 May 2016, <http://statewatch.org/news/2016/may/eu-council-esta-8590-16.pdf>
335. European Data Protection Supervisor, 'EDPS calls for consistent improvements in the approach to EU border policy', March 2017, <http://statewatch.org/news/2017/mar/eu-edps-etias-pr.pdf>; 'Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)', March 2017, <http://statewatch.org/news/2017/mar/eu-edps-etias-opinion.pdf>
336. A term which, it should be noted, appears to have been lifted wholesale from the marketing literature of various multinational consulting and IT companies.
337. Juliean Jeandesboz, Jorrit Rijpma and Didier Bigo, 'Smart Borders Revisited: An assessment of the Commission's revised Smart Borders proposal', October 2016, [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571381/IPOL_STU\(2016\)571381_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571381/IPOL_STU(2016)571381_EN.pdf)
338. See: NOTE from: the Presidency to: Strategic Committee on Immigration, Frontiers and Asylum (SCIFA)/Mixed Committee (EU-Iceland/Liechtenstein/Norway/Switzerland), 16 June 2016, 10424/16, <http://statewatch.org/news/2016/jul/eu-council-ees-note-scifa-10424-16.pdf>; and: 'Fingerprinting for all? Inclusion of all travellers in new border database to be discussed by 'High Level Expert Group'', *Statewatch News Online*, 4 July 2016, <http://statewatch.org/news/2016/jul/eu-ees-fingerprints.htm>
339. Aline Fontaine and Morgane Remy, 'Surveillance of Everyone: Europe's "Smart Borders" Would Automatically Monitor Individuals', *Truthout*, 2 August 2016, <http://www.truth-out.org/news/item/37067-surveillance-of-everyone-europe-s-proposed-smart-borders-would-automatically-monitor-individuals>
340. European Commission, 'Impact Assessment Report on the establishment of an EU Entry Exit System', SWD(2016) 115 final, 6 April 2016, p.10, http://eur-lex.europa.eu/resource.html?uri=cellar:5c20aef7-fca4-11e5-b713-01aa75ed71a1.0001.02/DOC_2&format=PDF

341. For example: ABC4EU, http://cordis.europa.eu/project/rcn/111518_en.html, EFFISEC, http://cordis.europa.eu/project/rcn/90955_en.html, FASTPASS, http://cordis.europa.eu/project/rcn/106743_en.html, FIDELITY, http://cordis.europa.eu/project/rcn/102324_en.html, INGRESS, http://cordis.europa.eu/project/rcn/110929_en.html and MOBILEPASS, http://cordis.europa.eu/project/rcn/185506_en.html
342. For an overview from the years up to 2009, see 'The dawning of the biometric age' in *'NeoConOpticon'*, pp.46-49, <http://www.statewatch.org/analyses/neoconopticon-report.pdf>
343. PROTECT, http://cordis.europa.eu/project/rcn/202685_en.html
344. BODEGA, http://cordis.europa.eu/project/rcn/196892_en.html
345. The network was initially known as e-MOBidIG but was recently folded into the European Network of Law Enforcement Technology Services (ENLETS), which is in turn overseen by the Council's Law Enforcement Working Party. For some background on e-MOBidIG, see: 'Europe's police and immigration "mobile identification" enthusiasts prepare to regroup during Irish Presidency of the EU', *Statewatch News Online*, January 2013, <http://database.statewatch.org/article.asp?aid=32091>
346. As examined, for example, in the MESMERISE project and C-BORD, which has received €11.8 million for "5 complementary innovative detection technologies: delivering improved X-rays, Target Neutron Interrogation, Photofission, Sniffing and Passive Detection"). MESMERISE, http://cordis.europa.eu/project/rcn/203299_en.html; C-BORD, http://cordis.europa.eu/project/rcn/194848_en.html
347. 'Smart borders: "no sufficient evidence" to justify law enforcement access to proposed Entry/Exit System travel database', *Statewatch News Online*, September 2014, <http://database.statewatch.org/article.asp?aid=33953>
348. The website of the 'Let'sFly2Europe' campaign has disappeared, despite official registration of the campaign by the European Commission in July 2016. It is unclear whether it will re-emerge, but it sought to abolish the EU's 2001 'carrier sanctions' Directive (2001/51/EC). As the website said: "When the Directive 2001/51/EC is abolished, the refugees have the possibility, to buy a ticket to use a regular airline to come to Europe and do not need smugglers anymore. This initiative provides a solution to end human smuggling and trafficking... Every human has the right, to apply for asylum. Our initiative turns that theoretical right into a realistic chance." From: 'Benefits', undated, <http://www.letsfly2europe.eu/benefits/>. See also: European Commission, 'Commission registers 'Let'sFly2Europe' and 'People4Soil' European Citizens' Initiatives', 27 July 2016, http://europa.eu/rapid/press-release_IP-16-2653_en.htm
349. Such as the long-running Euro-African network Migreurop (<http://www.migreurop.org>) and more recent initiative such as 'Cities of Refuge'. See: 'Cities of refuge: EUROCITIES members take leadership', EUROCITIES, 10 September 2015, <http://www.eurocities.eu/eurocities/events/Cities-of-refuge-EUROCITIES-members-take-leadership-WSP0-A28BTU>; Costas Douzinas, 'Cities of refuge', *OpenDemocracy*, 26 March 2016, <https://www.opendemocracy.net/can-europe-make-it/costas-douzinas/cities-of-refuge>
350. European Commission, 'Towards the 2018-2020 Work Programme – Border and External Security', 19 October 2016, <http://www.statewatch.org/docbin/eu-com-presentation-horizon2020-bes-18-20-experts-meeting-19-10-16.pdf>
351. Alec Ross, 'Want job security? Try online security', *Wired*, 25 April 2016, <http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross>
352. Although on this point it is also wise to seek out some of the more critical voices. See, for example, 'Squirrel 'threat' to critical infrastructure', *BBC News*, <http://www.bbc.com/news/technology-38650436>
353. Consider, for example, the "cyber repression" that has been pursued by many states. See: Alex Grigsby, "'Closing that Internet Up": The Rise of Cyber Repression', *Council on Foreign Relations*, 13 January, <https://www.cfr.org/blog-post/closing-internet-rise-cyber-repression>
354. 'Senate Intelligence Committee Advances Terrible Surveillance Bill in Secret Session', *Electronic Frontier Foundation*, 19 March 2015, <https://www.eff.org/deeplinks/2015/03/senate-intelligence-committee-advances-terrible-cybersecurity-bill-surveillance>
355. Gordon Corera, 'Cyber-security strategy launched', *BBC News*, 25 June 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm. The frequent use of Cold War metaphors was insightfully criticised in a 2011 piece that suggested an alternative historical parallel for current "cyber" dilemmas – the golden age of maritime piracy in the 19th century and the gradual, global crackdown that it faced. See: 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive', *Brookings Institute*, 15 August 2011, <https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/>. The two authors do not mention that for all its ills, the largely ungoverned and ungovernable maritime world of the 19th century also allowed for some remarkable experiments in freedom and democracy. See: 'The Many-Headed Hydra: The Hidden History of the Revolutionary Atlantic', *Verso Books*, <https://www.versobooks.com/books/1128-the-many-headed-hydra>
356. 'China: Abusive Cybersecurity Law Set to be Passed', *Human Rights Watch*, 6 November 2016, <https://www.hrw.org/news/2016/11/06/china-abusive-cybersecurity-law-set-be-passed>
357. 'UAE Cybersecurity Law Threatens Freedom of Expression', *Americans for Democracy & Human Rights in Bahrain*, 27 July 2016, <http://www.adhrb.org/2016/07/uae-toughens/>
358. Steve Morgan, 'Worldwide cybersecurity market continues its upward trend', *CSO*, 9 July 2015, <http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html>; 'Cybersecurity: A compelling growth area for defense companies?', *Alix Partners*, undated, <http://www.alixpartners.com/en/Publications/AllArticles/tabid/635/articleType/ArticleView/articleId/815/Cybersecurity-A-compelling-growth-area-for-defense-companies.aspx>
359. European Commission, 'Cybersecurity industry', 6 July 2016, <https://ec.europa.eu/digital-single-market/en/cybersecurity-industry>

360. EOS, 'Moving towards a sustainable European cybersecurity industry', July 2014, p.1, http://www.eos-eu.com/files/Documents/Position%20papers/Moving%20towards%20a%20sustainable%20cybersecurity%20industry_EOS%20Position%20Paper_July%202014.pdf
361. ENISA, 'National Cyber Security Strategies', undated, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map>
362. The Directive emerged from earlier efforts to increase coordination amongst national cybersecurity policies, for example through the Policy in Critical Information Infrastructure. See: European Commission, 'Policy on Critical Information Infrastructure Protection (CIIP)', 7 February 2013, <https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip>. For more on the Directive itself, see: European Commission, 'Directive on Security of Network and Information Systems – Questions and Answers', 6 July 2016, http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm
363. NOTE from: Presidency to: Delegations, 'EU Cybersecurity Strategy: Road map development', 6183/1/15 REV 1, 4 March 2015, <http://statewatch.org/news/2015/apr/eu-council-cyber-security-roadmap-6183-rev1-15.pdf>
364. Jay Stanley, 'Cybersecurity Myths: Beware the Hype', *American Civil Liberties Union*, 26 April 2012, <https://www.aclu.org/blog/cybersecurity-myths-beware-hype>; Murad Ahmed, 'Investors cool on cyber security start-ups that promise silver bullets', *Financial Times*, 16 March 2016, <https://www.ft.com/content/7bee038e-be8b-11e5-9fdb-87b8d15baec2>; Ben Rossi, 'The life and times of the cyber security hype curve', *Information Age*, <http://www.information-age.com/technology/security/123460727/life-and-times-cyber-security-hype-curve>
365. EOS, 'Towards a concerted EU approach to cyber security', July 2010, p.3, http://eos-eu.com/files/Documents/WhitePapers/EOS_ICTWG_CyberSec_v5%200.pdf
366. Cyspa, http://cordis.europa.eu/project/rcn/106313_en.html
367. CAPITAL, http://cordis.europa.eu/project/rcn/110714_en.html. EOS was also involved in the COuRAGE project ('Cybercrime and cyberterrorisM (E)uropeanResearch AGEnda'), funded by the FP7 ESRP and which aimed to "deliver a measured, comprehensive, relevant research agenda for Cyber Crime and Cyber Terrorism"- similar aims to the CYBERROAD project. See: COuRAGE, http://cordis.europa.eu/project/rcn/185504_en.html and CYBERROAD, http://cordis.europa.eu/project/rcn/188603_en.html
368. For example, a January 2016 report from "European Cybersecurity Industry Leaders" suggested ways the EU could "make the EU more trustworthy and digitally secure" and ensure the "successful development of European cybersecurity champions". See: 'Recommendations on Cybersecurity for Europe', 25 January 2016, available via the European Commission website: <https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders>
369. European Commission, 'Call: Digital Security focus area – call summary', undated, https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2016-2017.html#_c.topics=callIdentifier/t/H2020-DS-2016-2017/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc
370. 'European Organisation for Security calls for European industrial strategy in cyber security', *European Defence Matters*, Issue 9, 2015, p.19, <https://www.eda.europa.eu/docs/default-source/eda-magazine/edm9downloadopt140>
371. 'Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union and the European Cybersecurity Organisation', 5 July 2016, p.3, <http://ecs-org.eu/documents/contract.pdf>
372. Ibid.
373. See the Directive on data protection in the law enforcement and criminal justice sectors: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG; and the proposed ePrivacy Regulation: Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), [http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003\(COD\)](http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD))
374. Larry Leob, 'Privacy Protection Meets State Surveillance in Europe', *SecurityIntelligence*, 14 November 2016, <https://securityintelligence.com/news/privacy-protection-meets-state-surveillance-in-europe/>
375. Chris Jones, 'The visible hand: the European Union's Security Industrial Policy', *Statewatch Analysis*, August 2016, p.21, <http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf>
376. PRIVACY FLAG, http://cordis.europa.eu/project/rcn/194864_en.html
377. OPERANDO, http://cordis.europa.eu/project/rcn/194891_en.html
378. TYPES, http://cordis.europa.eu/project/rcn/194867_en.html
379. VisiOn, http://cordis.europa.eu/project/rcn/194888_en.html
380. PANORAMIX, http://cordis.europa.eu/project/rcn/194872_en.html
381. SafeCloud, http://cordis.europa.eu/project/rcn/194907_en.html
382. SHIELD, http://cordis.europa.eu/project/rcn/207185_en.html

383. KONFIDO, http://cordis.europa.eu/project/rcn/207188_en.html
384. But neither is the right to total anonymity necessarily a useful solution to the issues posed by the mass data-gathering and analysis undertaken by governments and corporations alike in today's world, as Evgeny Morozov has thoughtfully highlighted. See: 'The Real Privacy Problem', *MIT Technology Review*, 22 October 2013, <https://www.technologyreview.com/s/520426/the-real-privacy-problem/>
385. OCTAVE, http://cordis.europa.eu/project/rcn/194511_en.html
386. SpeechXRays, http://cordis.europa.eu/project/rcn/194884_en.html
387. DOGANA, http://cordis.europa.eu/project/rcn/194877_en.html. The Commission has also called for project proposals on "insider threats" as part of the ISF-Police programme. See: European Commission, 'Implementation of the EU CBRN Action Plan, the EU Action Plan on enhancing the security of explosives and the European programme for critical infrastructure protection', undated, p.4, http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/calls/2015/cbrn/docs/call_for_proposals_cbrn_2015_en.pdf
388. WISER, http://cordis.europa.eu/project/rcn/194847_en.html
389. DISIEM, http://cordis.europa.eu/project/rcn/202707_en.html; CISP, http://cordis.europa.eu/project/rcn/202687_en.html; PROTECTIVE, http://cordis.europa.eu/project/rcn/202674_en.html; SHIELD, http://cordis.europa.eu/project/rcn/202684_en.html; SSSDEN, http://cordis.europa.eu/project/rcn/202679_en.html
390. FutureTrust, http://cordis.europa.eu/project/rcn/202698_en.html; LIGHTest, http://cordis.europa.eu/project/rcn/203437_en.html
391. certMILS, http://cordis.europa.eu/project/rcn/207195_en.html; ANASTACIA, http://cordis.europa.eu/project/rcn/207199_en.html; VESSEDIA, http://cordis.europa.eu/project/rcn/207194_en.html
392. CANVAS, http://cordis.europa.eu/project/rcn/202697_en.html
393. Andrew Puddephatt and Lea Kaspar, 'Cybersecurity is the new battleground for human rights', *OpenDemocracy*, 18 November 2015, <https://www.opendemocracy.net/wfd/andrew-puddephatt-lea-kaspar/cybersecurity-is-new-battleground-for-human-rights>
394. Alex Comminos and Gareth Seneque, 'Cyber security, civil society and vulnerability in an age of communications surveillance', *Global Information Society Watch*, 2014, <https://giswatch.org/en/communications-surveillance/cyber-security-civil-society-and-vulnerability-age-communications-sur>
395. 'Horizon 2020 work programme 2014-15 - 14. Secure societies - Protecting freedom and security of Europe and its citizens', 10 December 2013, p.9, http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_v1.0_en.pdf
396. Slovenian national ISF programme, <http://www.statewatch.org/docbin/si-isf-national-programme.pdf>
397. David A. Graham, 'Rumsfeld's Knowns and Unknowns: The Intellectual History of a Quip', *The Atlantic*, 27 March 2014, <https://www.theatlantic.com/politics/archive/2014/03/rumsfelds-knowns-and-unknowns-the-intellectual-history-of-a-quip/359719/>
398. European Commission, 'Commission Staff Working Document on the review of the European Programme for Critical Infrastructure Protection (EPCIP)', SWD(2012) 190 final, 22 June 2012, http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf
399. European Commission, 'Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure more secure', SWD(2013) 318 final, 28 August 2013, p.7, http://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf
400. RESOLUTE, http://cordis.europa.eu/project/rcn/194870_en.html
401. IMPROVER, http://cordis.europa.eu/project/rcn/196889_en.html
402. ResiStand, http://cordis.europa.eu/project/rcn/202694_en.html
403. CLISEL, http://cordis.europa.eu/project/rcn/202693_en.html
404. ANYWHERE, http://cordis.europa.eu/project/rcn/203293_en.html
405. I-REACT, http://cordis.europa.eu/project/rcn/203294_en.html
406. ANYWHERE, http://cordis.europa.eu/project/rcn/203293_en.html
407. Reaching out, http://cordis.europa.eu/project/rcn/204900_en.html
408. beAWARE, http://cordis.europa.eu/project/rcn/207286_en.html
409. BRIGAD, http://cordis.europa.eu/project/rcn/202708_en.html
410. PANDEM, http://cordis.europa.eu/project/rcn/197272_en.html
411. TOXI-TRIAGE, http://cordis.europa.eu/project/rcn/194860_en.html
412. IMPACT, http://cordis.europa.eu/project/rcn/194857_en.html
413. CUIDAR, http://cordis.europa.eu/project/rcn/194896_en.html
414. EDUCEN, http://cordis.europa.eu/project/rcn/194905_en.html
415. ChemSniff, http://cordis.europa.eu/project/rcn/198741_en.html
416. ACES, http://cordis.europa.eu/project/rcn/198733_en.html
417. SPIDERS, http://cordis.europa.eu/project/rcn/198738_en.html
418. Bio-Ax, http://cordis.europa.eu/project/rcn/197964_en.html
419. ART, http://cordis.europa.eu/project/rcn/197971_en.html

420. AIRS, http://cordis.europa.eu/project/rcn/198400_en.html
421. INNOPROCITI, http://cordis.europa.eu/project/rcn/198535_en.html
422. SEREN 3, http://cordis.europa.eu/project/rcn/194868_en.html
423. SafeSky, http://cordis.europa.eu/project/rcn/197958_en.html
424. DAPS, http://cordis.europa.eu/project/rcn/201773_en.html
425. SURVEIRON, http://cordis.europa.eu/project/rcn/201667_en.html
426. ROBIN, http://cordis.europa.eu/project/rcn/197963_en.html
427. AquaSHIELD, http://cordis.europa.eu/project/rcn/197303_en.html
428. WATERGUARD, http://cordis.europa.eu/project/rcn/197951_en.html
429. Andrupos, http://cordis.europa.eu/project/rcn/197945_en.html
430. AIRIMGO, http://cordis.europa.eu/project/rcn/197961_en.html
431. Invest, http://cordis.europa.eu/project/rcn/197290_en.html
432. Starlight, http://cordis.europa.eu/project/rcn/196927_en.html
433. For more on the EU's plans for the 'security industry' see: 'The visible hand: the European Union's Security Industrial Policy', August 2016, <http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf>
434. 'NeoConOpticon', p.61
435. Marieke de Goede, 'Beyond Risk: Premediation and the Post-9/11 Security Imagination', *Security Dialogue*, Vol. 39(2-3), pp.155-176, <http://journals.sagepub.com/doi/abs/10.1177/0967010608088773>

AUTHOR: Chris Jones

EDITORS: Nick Buxton, Tony Bunyan

DESIGN: Evan Clayburg

PRINTER: Jubels

IMAGE CREDITS: Images used in this report are not subject to its copyright restrictions and may have their own licence.

Sources (Flickr unless otherwise indicated):

p4, @european_parliament; p.6, @securitydefenceagenda; p.7, @idarrenj; p.11, @idarrenj; p.13, @robdeman; p.20, @131253119@N03; p.28, @benjaminchodroff; p.55, @megantrace; p.54, Twitter/@eulisaconf; p.56, @greensefa; p.59, Twitter@rriescog; p.62, <http://impactcee.com>; p63, @mac_ivan

Published by Transnational Institute – www.TNI.org
and Statewatch – www.Statewatch.org

© Statewatch ISBN 978-1- 874481-70- 6. Personal usage as private individuals/"fair dealing" is allowed. Usage by those working for organisations is allowed only if the organisation holds an appropriate licence from the relevant reprographic rights organisation (e.g. Copyright Licensing Agency in the UK) with such usage being subject to the terms and conditions of that licence and to local copyright law.

Statewatch is the operating name of the Libertarian Research & Education Trust. UK charity number: 1154784, UK company number: 08480724.

Contents of the report may be quoted or reproduced for non-commercial purposes, provided that the source of information is properly cited. TNI would appreciate receiving a copy or link of the text in which this document is used or cited. Please note that for some images the copyright may lie elsewhere and copyright conditions of those images should be based on the copyright terms of the original source.

<http://www.tni.org/copyright>

ACKNOWLEDGEMENTS

This report would not have been possible without the support and assistance of all at Statewatch. Thanks also go to Eric Töpfer, Marie Martin, Ben Hayes, Nick Buxton, Paddy Hillyard and the many others who have offered suggestions, advice and information, as well as the Polden-Puckham Charitable Foundation which provided financial support via a three-year grant to Statewatch.



The Transnational Institute (TNI) is an international research and advocacy institute committed to building a just, democratic and sustainable planet. For more than 40 years, TNI has served as a unique nexus between social movements, engaged scholars and policy makers.

www.TNI.org



Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness.

www.Statewatch.org