Challenges and Critiques of the EU Internal Security Strategy

Rights, Power and Security

Edited by Maria O'Neill and Ken Swinton

Challenges and Critiques of the EU Internal Security Strategy

Challenges and Critiques of the EU Internal Security Strategy:

Rights, Power and Security

Edited by

Maria O'Neill and Ken Swinton

Cambridge
Scholars
Publishing

Challenges and Critiques of the EU Internal Security Strategy:
Rights, Power and Security

Edited by Maria O'Neill and Ken Swinton

This book first published 2017

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-4438-9165-7
ISBN (13): 978-1-4438-9165-3

TABLE OF CONTENTS

Data

Environment

List of Acronyms

AFSJ	Area of Freedom Security and Justice
AG	Advocate General
AS	aerial surveillance
AWFs	Analysis Work Files
CERTs	computer emergency response teams
CFCs	chlorofluorocarbons
CFSP	Common Foreign and Security Policy
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIPS	financial instrument for "the protection of citizens and critical infrastructures against terrorist attacks and other security-related incidents"
CIWIN	Critical Infrastructure Warning and Information Network
CJEU	Court of Justice of the EU
CLC	Civil Liabilities Convention 1992
CoE	Council of Europe
CT	Counter-terrorism
DDoS	distributed denial of service
DGs	Directorate Generals (European Commission)
DNA	Deoxyribonucleic acid
DPAs	(national) Data protection authorities
DPO	Data Protection Office (Europol)
DPWP	Data Protection Working Party
EAS	External Action Service
ECD	Europol Council Decision
ECHR	European Convention on Human Rights
ECI	European Critical Infrastructures
ECIM	European Criminal Intelligence Model
ECIP-POC	network of national points of contact on European Critical Infrastructure Protection
ECJ	European Court of Justice
ECD	Europol Council Decision
ECtHR	European Court of Human Rights
EC3	European Cybercrime centre
EDA	European Defence Agency

EDPS	European Data Protection Supervisor
EEA	European Economic Area
EEAS	European External Action Service
EED	Energy Efficient Design Index
EIS	Europol Information System
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
ENP	European Neighbourhood Policy
ENTSOE	European energy providers and regulators
ENU	Europol National Units
EP	European Parliament
EPCIP	European Programme for Critical Infrastructure Protection
ERN-CIP	European Reference Network – Critical Infrastructure Protection
EU	European Union
EUCFR	EU Charter of Fundamental Rights
Euro-Med	Euro-Mediterranean
ESS	European Security Strategy
E3PR	European Public + Private Partnership for Resilience
FIU	Financial Intelligence Unit
FP	Focal Point (Europol)
GESAMP	Group of Experts on the Scientific Aspects of Marine Environmental Protection
GHGs	greenhouse gas emissions
HRW	Human Rights Watch
HMICS	HM Inspectorate of Constabulary for Scotland
HNS convention	International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, 1996
IT	Information Technology
IGO	Inter-Governmental Organisation
ICT	Information and Communication Technology
IPS	Inspectorate of Prosecution in Scotland
IMDG Code	International Maritime Dangerous Goods Code
IMO	International Maritime Organisation
ISS	Internal Security Strategy
JHA	Justice and Home Affairs
JRC	Joint Research Centre (European Commission)
JITs	Joint Investigation Teams
JSB	(Europol) Joint Supervisory Body

MARPOL	International Convention for the Prevention of Pollution from Ships 1973
MEPC	Marine Environmental Protection Committee (of the IMO)
NATO	North Atlantic Treaty Organisation
NGO	Non Governmental Organisations
NIM	National Intelligence Model
NIS	Network and Information Security
NLSs	Noxious Liquid Substances
NOx	nitrogen oxides
NSA	U.S.'s National Security Agency
OECD	Organisation for Economic Cooperation and Development
OLAF	European Anti-Fraud Office
OSPAR	Convention for the Protection of the Marine Environment of the North-East Atlantic 1992
PRFs	Port Reception Facilities
PJCCM	Police and Judicial Co-operation in Criminal Matters
RoI	Republic of Ireland
SAs	Special Areas
SCEDA	Scottish Crime and Drug Enforcement Agency (since merged into Police Scotland)
SECAs	Sulphur Emission Control Areas
SEEMP	Ship Energy Efficiency Management Plan
SID	Scottish Intelligence Database
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SOC	Serious and Organised Crime
SOx	sulphur oxides
SS	satellite imager
SYRIZA	Coalition of the Radical Left, Greece
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
UN	United Nations
UNCTAD	UN Conference on Trade and Development
UNHCR	United Nations High Commissioner for Refugees
US(A)	United States of America
USE	Unified Search Engine (Europol)
VIS	Visa Information System
VOCs	volatile organic compounds
WTO	World Trade Organisation

CHAPTER ONE

INTRODUCTION AND OVERVIEW

MARIA O'NEILL

The European Union's (EU's) Area of Freedom, Security and Justice (AFSJ) has entered a new period of development. Since the publication of *New Challenges for the EU Internal Security Strateg*y with Cambridge Scholars in 2013,[1] the original implementation period of the Stockholm Programme – an open and secure Europe serving and protecting citizens[2] has come to an end, with some of its issues still having to be properly addressed. The new security programme for the EU, the European Agenda on Security,[3] has since been written. The external relations of the EU, a subject covered in the 2013 book, have now come centre stage. Human trafficking, another subject explored in the 2013 book, is now gaining attention at both the legislative and operational law enforcement level in many EU member states. The other 2013 themes, the business of crime and the policing of ports are still receiving day to day law enforcement attention across the EU.

The post Lisbon EU Internal Security Strategy of 2010 has been in place for a number of years, and many of the provisions of the Stockholm Programme have been legislated for. The European Agenda on Security states that the EU Internal Security Strategy strategic objectives "remain valid and should continue to be pursued".[4] It is now necessary, however, to empirically analyse the exact levels of policy and practice developments

[1] O'Neill, Swinton and Winter, *New Challenges for the EU Internal Security Strategy* (Newcastle-upon-Tyne: Cambridge Scholars 2013).
[2] Stockholm Programme – an open and secure Europe serving and protecting citizens OJ 2010 C115/1.
[3] Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions - *The European Agenda on Security*, COM(2015) 185 final.
[4] Ibid., 2.

of the various provisions of the internal security strategy, in order to ensure that no gaps remain where laws and practices are supposed, under the Stockholm Programme, to be in place, so that the implementation of the EU Internal Security Strategy does not end up being merely a paper based exercise. What works well, and is of considerable added value for some EU member states, may prove to be a mis-fit for others, leading to the argument that the provisions on enhanced cooperation[5] should be used more frequently in this area. In addition the specific "accelerator"[6] and "emergency brake"[7] provisions for the AFSJ could be utilised more often to deliver an EU legal and practice framework that adds value to cross border justice and law enforcement provisions without adding new stumbling blocks and obstacles at the level of national implementation or operationalisation of what are otherwise well intentioned EU measures. This will require greater consultation in the design of proposals, and willingness to engage in greater levels of complexity at the development stage, by both EU officials and their counterparts within member states. It is also arguable that those provisions currently in place should be evaluated for their level of effectiveness, and fitness for purpose, for all and each of the EU member states, with any appropriate modifications being made at either the policy, legislative, implementation or practice level, as appropriate. However this is a matter for further research by other colleagues, both in law enforcement practice and academia.

Further challenges, with respect to the UK (subject to any post-Brexit agreement) and the Republic of Ireland (RoI), will be the impact of Protocol No 21 to both countries, and the impact of Protocol No 36 (Article 10.4) to the UK. Protocol No 21 looks forward from the date of the Lisbon Treaty, basically stating that any new measures under the AFSJ, (for which there were already similar, but differing UK and RoI opt outs for measures building on the Schengen *acquis*, predominantly in the area of "visas, asylum and immigration and other matters dealing with the free movement of [third country nationals]",) are not to apply to them, unless that particular country opts back into the provision "within three

[5] TEU, Article 20 and Articles 326 and 327 TFEU. Also relevant are Articles 329 to 334 TFEU.

[6] Specific enhanced cooperation provisions for EU policing being provided for in TFEU Article 87.3, second paragraph. Article 83.3 second paragraph for Judicial Co-operation in Criminal Matters, and Article 86.1 second paragraph *et seq*. TFEU for the European Public Prosecutor.

[7] TFEU Article 82.3 and Article 83.3 first paragraph for Judicial Co-operation in Criminal Matters.

months after a proposal or initiative has been presented to the Council."[8] It is unclear what exact impact this will have as the UK (subject to any post-Brexit agreement) and RoI have already opted back into many, but perhaps not all, of the post Lisbon measures. A full audit of the impact of this provision still has to be conducted. Under Protocol No 36, Article 10.4 the UK additionally had the option to opt out of all of the pre-Lisbon AFSJ measures that it was originally party to, with the option to "at any time afterwards, notify the Council of its wish to participate in acts which have ceased to apply to it" under the above provisions.[9] The UK notified the EU of its intention to exercise its rights under Protocol no 36, Article 10.4 and issued a 158 page Command Paper on the UK's view of the matter,[10] leading to a block opt out, and the UK opting back into what it considered to be the 35 most important pre-Lisbon EU AFSJ measures.[11] It is to be remembered that the UK (subject to any post-Brexit agreement) can seek to re-join measures "at any time." At the time of writing negotiations are ongoing with the EU as to how matters are to proceed. A challenge for both the UK (subject to any post-Brexit agreement) and the RoI will be to negotiate these changing relationships with the EU in this area. It will also pose a challenge for other member states of the EU in dealing with both these countries. However, despite the rhetoric in public, it is hoped that the level of UK and RoI disengagement with the AFSJ, outwith matters pertaining to their original Schengen opt outs, to include post-Brexit, may not be as great as originally feared.

Ensuring that no gaps remain in the EU legal and policy framework, while respecting national sovereignty, and the EU's principle of subsidiarity,[12] where this applies, such as in the EU's AFSJ,[13] is one of the EU's key challenges, an issue taken up by Bossong. In his chapter on the EU's Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) he starts the empirical analysis that he says is required to establish the exact level of development of the EU's security profile given the considerable obstacles that the EU has faced to "translate its ambitions" into practice. The same argument could be made for all

[8] Protocol No 21, Article 3.1.
[9] Protocol No 36, Article 10.5.
[10] HM Government, *Decision pursuant to Article 10 of Protocol 36 to The Treaty on the Functioning of the European Union*, July 2013, Cm 8671.
[11] Miller, V., In brief: the 2014 block opt-out and selective opt-back-ins, Standard Note: SN/IA/6684.
[12] TEU, Article 5.1.
[13] TFEU, Article 4.2.j.

aspects of the EU internal security strategy. Separately the issue of CIIP is taken up later by Dewar, in his analysis of the EU's Cybersecurity provisions. Dewar talks about the lack of cohesion which has been seen at various stages of the development of the EU's Cybersecurity strategy, covering both the civilian and military response to this threat in Europe. Dewar concludes that the EU has maintained "consistent priorities but shifting approaches" during the course of the evolution of the strategy. In the context of Bossong's chapter this writer would argue that it is possible that the European Network and Information Security Agency (ENISA) could network capacities between more advanced member states in the context of cyber-security, while providing coverage, and protection, for those EU member states which are less developed in this area, particularly given that the EU is supposed to be providing additionality in this area.

As alluded to in the European Agenda on Security,[14] it cannot be assumed that all issues raised in Stockholm Programme have in fact been adequately addressed, or that those which have been addressed are in fact effective in practice. A number of further provisions in the Stockholm Programme are now only beginning to see the light of day. Equally new internal security threats continue to emerge. Two non-traditional security threats are getting particular attention in this publication, environmental crime, often associated with organised crime, and a security issue of the 21st Century, cyber-security, which needs to be distinguished from cyber-crime. A further example of emerging security issues is the Joint Communication from the High Representative for the Common Foreign and Security Policy (CFSP) and the Commission on the need for a maritime security strategy.[15] With external agencies expressly referred to in the communication, Carpenter's examination of the provisions for monitoring and controlling ship source pollution as an environmental crime is highly relevant.

As international maritime environmental provisions are a well-developed area of international law and practice, Carpenter's analysis of the state of play and operation of the ship source pollution provisions, in the various seas which surround the EU, and of interest to the UK post Brexit. The method of surveillance used when combating ship source pollution,

[14] Communication from the Commission, *The European Agenda on Security*, 2.
[15] High Representative of the European Union for foreign Affairs and Security Policy and European Commission: Joint Communication to the European Parliament and the Council; *For an open and secure global maritime domain: elements for a European Union maritime security strategy*, JOIN(2014) 9 final.

through satellite tracking, is a method which could be adapted for other law enforcement and public safety functions, and has been recommended for the tracking of commercial aircraft. It is worth noting in this context that the EU does have a (civilian) space programme, the European Space Agency (also referred to in the Joint Communication on maritime security), Ariane rockets, which take off from the EU's space port in French Guyana, and is developing the Galileo navigation system, which, when completed, will have 30 satellites in near earth orbit, with a number already deployed. The EU is also operating other systems, such as the Sentinel system, as well as the various commercial operations based within the EU, such as Inmarsat, which is already involved with maritime and aviation work. The issue of how existing maritime pollution reporting systems will interact with Europol, and law enforcement generally, an issue introduced by Blasi Casagran in her chapter on reform of Europol through the Europol regulation, is not addressed by Carpenter. No doubt this will be the subject matter of further academic research.

The 2009 Stockholm Programme, and the 2010 Internal Security Strategy had an ambitious vision. Each of their provisions must be implemented adequately in order to ensure a secure Europe for all of its citizens, while also reflecting the vision for a free and just Europe. Once the legal and policy frameworks have been properly designed, they then need to be implemented effectively. This implementation needs to be done by the relevant security, investigatory or judicial staff. The approach of the law enforcement community to the operationalization of EU policies, and their own impact on those policies, is an issue which attracts the attention of two contributors to this book, Skleparis and Egan, building on case studies in Greece and Scotland, UK, respectively, for their work. Of particular interest in the context of both of these chapters is Egan's examination of the development of police knowledge and whether the police can be considered to be an epistemic community. If this type of analysis is transferred to the subject matter of Skleparis' chapter, some interesting analysis could develop, particularly in the broader (than the subject matter of both chapters) context of EU cross border policing and counter-terrorism. A further challenge for the future effective development of the AFSJ, is that the approach taken in these two cases studies which would need to be adopted in each of the EU member states, in each of the key security threat areas, in order to develop an accurate picture of the effect and implementation of EU policies going forward.

At the power/security/rights nexus is an issue which gained prominence during 2013-2014, and still highly relevant today, the use of data by law enforcement agencies (and, outside the EU legal framework, the intelligence services,) also gets prominent attention in this 2014 Cambridge Scholars collection. Data can be collected by private parties for commercial purposes. This can then be transferred to law enforcement authorities for law enforcement purposes. Equally data can be collected by law enforcement authorities for intra-EU law enforcement purposes, but then be exported outside the EU, to countries which may or may not recognise the EU's data protection regime and associated rights. The number of countries to which this data can be exported is currently limited, although not unproblematic, particularly in the context of data transfer to the USA. With the external dimension of EU cross-border law enforcement anticipated to be developed in the future, to include with the UK post Brexit, but also in the ongoing relationships under the European Neighbourhood Policy and Euro-Mediterranean Policy, further, highly complex, challenges are expected to arise. Negotiations on cross-border law enforcement with Russia have floundered on the issue of effective data protection regulation (and practice) in Russia.[16]

Equally the issue now arising is where private parties are being tasked with collecting data for law enforcement purposes, and then storing that data until it is required, that data being stored either inside or outside the EU, with the possibility of leaks or non-authorised use of that data to third parties. The issues which surround data protection and data security are multiplying as the EU, and the world, becomes increasingly digitally interconnected. Furthermore, the issue of the collection of data following intelligence led policing,[17] when suspected individuals are targeted, following the issuing of warrants, mediated by independent parties such as the judiciary, has to be juxtaposed with the increasing creep of mass surveillance through the storage of data which may or may not relate to a suspected individual, may or may not be connected to a particular crime, with that data being used by way of massive data processing methods, known in the law enforcement world as profiling, an issue which itself raises very serious issues with regard to the presumption of innocence, human and fundamental rights. It also raises the issue of wasting limited

[16] Commission staff working document accompanying the communication from the Commission to the Council - *Review of EU-Russia relations pursuant to conclusions of the Extraordinary European Council of September 1, 2008*, COM(2008) 740 final, paragraph 40.
[17] Radcliffe, J., *Intelligence Led Policing* (Cullompton: Willan Publishing, 2008).

law enforcement resources in building large data handling centres, when funds are still restricted for protecting society from known or legitimately suspected offenders or terrorists.

As the greatest bulk of EU cross-border law enforcement activities involve the transfer and analysis of personal data, this issue has attracted the attention of three contributors to this book, analysing this issue from three different perspectives. Gaps and conflicts have clearly emerged between the different legal tools, both planned, and in force, in this area. The attitudes of individual law enforcement officers, or their organisations, when processing such data, also needs to be examined, as officers, as either individuals or through a community of practitioners, can often bring their own prejudices to an activity, giving it an effect in practice which was not intended by either the policy makers or the legislatures, or which would find favour with relevant judiciary.

The underpinning legal framework for the EU AFSJ is also undergoing rapid change, with the five year phase in period of the Lisbon Treaty now over. The new legal and institutional framework began working in earnest from December 2014. The Court of Justice of the EU (CJEU) has now obtained its full powers,[18] bringing with it the full impact of the upgrade in legal status of the EU Charter of Fundamental Rights (EUCFR). (This was one of the key points of contention with the UK in the AFSJ). The proposed accession of the EU to the Council of Europe's European Convention on Human Rights (ECHR) still has to be completed. There is a changing institutional balance within the EU, and a rebalance between the AFSJ's three themes. The widely accepted imbalance in favour of the more developed EU transnational security provisions is expected to be addressed by an improvement of the provisions of the EU transnational freedom and justice provisions. This is echoed in the European Agenda on Security.[19] Equally there will be an increase in involvement of the Commission and European Parliament in law making for the AFSJ. However, even with the increased balance and robustness of the post Lisbon AFSJ legal framework, part of the EU, the CFSP, remains intergovernmental, outside the scope of review of the CJEU, and lacking a rights based legal system. This lack of judicial oversight for CFSP activities is an issue raised by Grant in her chapter on data protection. If a legal system has been developed, it needs to operate in all relevant areas. It is clear from Grant's

[18] Protocol No 36 on Transitional Provisions attached to the TEU and the TFEU post Lisbon.
[19] Communication from the Commission, *The European Agenda on Security*, 3.

chapter that a serious gap has emerged in the outward facing external activities of EU, as exemplified in her analysis of the activities of the External Action Service (EAS) as it handles personal data.

Independent of overarching EU legal and policy developments, details in the EU's legal and institutional provisions in the AFSJ are also developing. The Europol regulation has changed Europol's internal competences and operations, and adding a couple of new crime areas, as with ship source pollution, discussed above. The issue of rights, to offset the power which individual EU member states can maintain over individuals, in the context of EU law enforcement agencies activities, however, needs to be addressed. Both old and new provisions in the AFSJ now have to be fully EUCFR and ECHR compliant, and have been subject to adjudication to that effect since December 2014.

These significant developments will further involve policy makers, lawyers, criminologists and the law enforcement professionals across the EU. Each stage of the policy and practice development process needs to be examined, together with the sites or locations where security, and its counterpoints, freedom and justice, become an issue. The challenges for, and the critiques of the EU Internal Security strategy, from the perspective of rights, power and security, continue to multiply. This publication will address a number of these issues.

This collection, building on original research by its contributors, comprises work by authors from a wide variety of academic and professional areas and perspectives, as well as from different countries, on a variety of areas and issues related to or raised by the EU's Internal Security Strategy, from critical infrastructure protection to the data handling systems at Europol, from the implementation by the border police in Greece of EU external border policies, to the impact of the change of legal status of former Police and Judicial Co-operation in Criminal Matters (PJCCM) provisions, post Lisbon, the upgrade in legal status of the EUCFR, and the changing role of the CJEU in this area. This book examines, from a wide variety of discipline perspectives, to include law, geography and politics, both the changing legal landscape of the EU, and its response to new security threats, such as cyber security and the new role of Europol, under the Europol regulation, of the enforcement of ship source pollution.

The collection is divided into four parts. After this initial introduction, the second part examines some of the paradigm shifts which will be necessary

for the further development and deepening of the EU Internal Security Strategy. Both the changing legal system at the EU, and the need to empirically analyse the implementation of varying aspects of the EU security policy are covered here. The third part provides an analysis of the EU's data processing provisions from a law enforcement perspective, with three chapters taking differing approaches to this issue. The fourth part of this publication analyses the new security threat of environmental crime. Within each part the contributors examine different, but overlapping, legal, political, practical and analytical cases, themes and issues.

The second part of this book focuses on some of the paradigm shifts which will be necessary for the further development of security within the EU. While the initial policy and legal framework was set out in 2010, as the strategy develops, and is implemented, against a changing legal and security threat landscape, new approaches will be required to ensure that all aspects of its effective implementation and further development are addressed. The initial provisions of the law enforcement aspects of the AFSJ were designed, from the bottom up, by law enforcement personnel, using a constructivist approach. This has served the security aspect of the AFSJ well. However, as there is now an emphasis on the development of the "freedom" and "justice" aspects of the AFSJ, a new approach is required. This is a theme echoed by Grant in her later data protection chapter. While there is no intention to cross the treaty based red lines of EU competence, such as member state internal security or national security, and while recognising that the AFSJ is an area of shared competence subject to the principle of subsidiarity, an argument can still be made for a constitutionalist approach to the further development of the AFSJ, in light of the upgrade in legal status of PJCCM provisions, and the improved legal status of both the CJEU and the EUCFR post Lisbon. In addition, Bossong argues that for a proper further development of the security aspect of the AFSJ there is a need for a "cross-cutting empirical survey from a governance perspective", in order to establish where exactly we are in the development of the EU's internal security provisions, and in establishing what are the best approaches in closing off any gaps which may have developed.

O'Neill analyses the changing legal landscape of the AFSJ, which includes the post-Lisbon upgrade in status of the Court of Justice, which gained its full capacity in December 2014, the upgrade in legal status of the EUCFR 2000, and the anticipated accession of the EU to the Council of Europe's ECHR. Also covered is the much delayed EU road map on procedural

rights, now in the course of implementation. All of these developments will have a considerable impact on how cross-border law enforcement operations and prosecutions will be conducted, with one eye being kept at all times on the preparation of cases, and the collection of supporting evidence, for hearing in a court of at least one EU member state.

Bossong's chapter focuses on CIP. He addresses the "empirical complexity" of this area of governance at an EU level, which includes policy instruments, legislative provisions, and "financial incentives and involves a wide variety of actors, institutions and networks." He covers the separate tracks of development of "energy and transport networks," and "critical information infrastructures, which can mean any major IT-based communication and control system." He sheds light on this complex and rapidly evolving area, concluding that "sector-specific binding regulation and considerable institutional capacity-building at the EU level," rather than the much vaunted "public-private partnerships and networking across policy fields," appear to be the most effective approach to security governance in the area of CIP.

The third part of this book focuses on new security challenges for the EU Internal Security Strategy. While the EU and its member states may have thought that they had written a definitive strategy document, such as the EU Internal Security Strategy in 2010, new security threats continue to emerge, as reflected in the European Agenda on Security. As existing strategies are put into operation, new issues arise, such as how exactly Greek security professionals implement the EU's immigration regime, as analysed in Skleparis' chapter, and new or emerging security threats, such as cyber-security, as analysed by Dewar. With the ever changing security landscape, both at an international relations and internal crime level, the EU and its member states need to be constantly alert, and ready to respond with appropriate measures, in order to ensure that the EU really does provide security within the EU, and that either all or parts of the AFSJ do not just end up as very impressive, but ineffective, paper based exercises.

Skleparis' chapter can be seen as a case study of one of the user groups of the intelligence analysed by O'Neill, Blasi Casagran and Grant in their chapters. Equally a link between Egan's epistemic communities and Skleparis' work should be made. Skleparis' work focuses on the attitudes of Greek security professionals, whether they be the Hellenic Police or Coast Guard, in implementing the EU's border security provisions. He examines some "deeply embedded negative attitudes" to "various key

issues related to migration," in a country located at a "busy land and sea crossing route for illegal migrants." The chapter provides the Greek security professional's view of the "migration-security nexus," and their conceptualisation of the migrant as the "other" in the context of globalisation and multiculturalism. This is done through using data obtained from 20 face to face semi-structured interviews, and applying discourse analysis to 11 master's dissertations produced by high-ranking officers in the Hellenic Police and Coast Guard. The chapter goes on to examine the impact of Frontex and their training products on this situation.

Dewar's chapter examines the EU's civilian response to cyber-security, acknowledging that the North Atlantic Treaty Organisation (NATO) is the key player in the military approach to cyber-security in most EU member states. His chapter starts with an historical analysis of EU cybersecurity policy. The chapter brings the reader through three distinct phases of this development, from the "first attempts to codify the field in the EU in 2001," the impact of the change in EU focus after the failure of the draft EU Constitutional Treaty, and "subsequent attempts to revitalise interest in cybersecurity in 2006." Dewar analyses the publication of the EU's Cybersecurity Strategy, published in February 2013, and its supporting directive, examining what was the "first consolidated strategic response of the Union to cybersecurity issues."

The fourth part of this book covers the highly contentious issue of data in a law enforcement context. Three chapters in this part tackle this issue, all written from quite distinct perspectives. In the absence of direct law enforcement powers and law enforcement agencies at EU level, the principal way in which the EU adds value to member states security in the context of transnational crime and counter-terrorism operations is in the sharing, and further analysis of data. Data processing brings with it the traditional issues of data protection, from a data subject perspective, and data security, from a law-enforcement perspective. Additionally the issue of massive data capture by law enforcement authorities, and private bodies acting on behalf of law enforcement authorities, has come to the fore, with many, including this writer, arguing that intelligence led policing should be maintained as the EU preferred method for transnational law enforcement, rather than mass data surveillance, which could lead to the highly problematic issue of reliance on profiling. A number of the relevant issues are addressed by contributors to this publication, with Blasi Casagran, writing with the benefit of the experience of a posting to Europol, on the Europol legal framework, and its impact on data

processing at Europol. Grant takes a rights and personal data approach to the issue of the free movement of data for security purposes, and also tackles the issue of internal EU law enforcement data being "exported" to third countries via the EU's CFSP actors and mechanisms. Egan addresses the issue of police practitioners as an "epistemic community" and the approach of police professionals, in a Scottish financial investigation context to the issue of data in the context of law enforcement.

Blasi Casagran approaches the issue of EU law enforcement data processing from the perspective of Europol, both under the former provisions and under the Europol regulation. The main purpose of her study is to identify and analyse the new rules that will impact on the processing of personal data at Europol. She examines the many criticisms of the Europol regulation, from diverse pro-privacy interest groups, which argue that the regulation will make the former Europol data protection and data security schemes less restrictive, with less protection for the individual than was previously the case. She goes on to demonstrate that Europol can and will maintain and improve the robust data protection regime that the agency had already created.

Grant develops this theme of law enforcement data processing, taking a wider view than Blasi Casagran's focus on Europol, and arguing her points from a data protection perspective. Building on both EU policy documents and case law of both the European Court of Human Rights (ECtHR) and the CJEU, she analyses proposals for reform, and the subsequent enactment, of the EU wide data protection within the now unified supranational legal framework of mainstream EU law. Grant also takes on the challenge of analysing the activities of the remaining intergovernmental activities of the EU, under the CFSP, in particular through the EU's EAS. She examines the exact legal status of data protection in this intergovernmental area, and the gaps in data protection for data which is otherwise legally transferred from internal EU law enforcement bodies to, for example, the European Economic Area, for onward transmission to third countries for extra-EU law enforcement activities.

Egan's chapter is based on earlier doctoral research with territorial Scottish police forces, focusing on the financial investigation community's expertise. While the Scottish police structure has now changed, her work remains relevant to ongoing financial investigations, and its implications are transferrable to the wider policing community across the EU.

Specifically, she examines how the work of the Financial Intelligence Unit (FIU) contributes to the creation of police knowledge and its subsequent dissemination. She points out that the creation and dissemination of police knowledge is of concern because claims to knowledge can be exercised to influence the policy and law.[20] Boswell argues exercising these claims to knowledge can serve a legitimising and substantiating function.[21] This means the knowledge can be drawn upon by an organisation to "bolster claims to resources or jurisdiction*"* or to justify policy preferences and marginalise competing interests.[22] It has been argued by Ericson that police officers produce and distribute knowledge for the management of risk.[23] However, Ericson claims that police officers offer distinctive knowledge about such risks, and it is this distinctive contribution to the "security quilt" that provides their legitimacy as an aspect of government.[24] This author would argue, that in some areas of policing, and perhaps not those covered by Egan, the subjective nature of this police knowledge can be quite worrying, needing a stronger fundamental, human and due process legal framework.

Similarly challenging, Egan goes on to discuss the fact that the developing AFSJ places continued pressure on EU agencies to shore up the available evidence base for policy development.[25] The implementation of the EU Internal Security Strategy constructively demonstrates how such evidence is incorporated within policy development at the EU level. However, as acknowledged by Parkin, many of these EU agencies derive such evidence from member states' various data repositories. Consequently, domestic organisations/agencies responsible for such data collection can influence EU level policy. Against this background, this chapter examines the interaction of national police practitioners as "experts in their field," assessing the validity of their knowledge as a foundation for such policy and increasingly, law making.

---

[20] Boswell, C., *The Political Uses of Expert Knowledge: Immigration policy and Social Research* (Cambridge: Cambridge University Press, 2013), 7.
[21] Ibid.
[22] Ibid.
[23] Ericson, R., "The division of expert knowledge in policing and security", *BJS* 45(2) (1994): 149-175. 151.
[24] Ibid. 153.
[25] Parkin, J., *EU Home Affairs Agencies and the Construction of EU Internal Security Strategy*, (Brussels: CEPS Paper in Liberty and Security in Europe No 53, December 2012).

The final part of this book focuses on the emerging area in the context of cross-border law enforcement, environmental crime. Often connected with the activities of organised crime groups, environmental crime, both terrestrial and maritime, is gaining an increasing profile at an EU level. Environmental crime generally is seen as "being a serious and growing problem that needs to be tackled at European level".[26] With the Europol regulation expressly granting Europol competence to address ship source pollution, the issue arises as to how Europol is to operate in this area. In particular, Europol's interaction with not only national law enforcement in the context of environmental crime, but also the EU's Environment Agency and national environmental agencies need to be examined. In addition, as many of the laws in force in this area are international treaties, with both EU and non-EU contracting parties, Europol needs to develop operational relationships with these non-EU countries in the context of ship source pollution law enforcement. As Eurojust is competent to act in all crimes in which Europol is competent to act, transnational (EU and non-EU) prosecutions in the context of ship-source pollution also merit further academic, policy and practitioner examination. Separate from the above challenging issues, is where Carpenter's analysis fits into the more broadly focused EU maritime security strategy.

Carpenter, in her chapter, examines the provisions on ship-source pollution as an environmental crime on the basis of EU and International law, leaving it to future researchers to examine how exactly both Europol and Eurojust will interact with the other key stakeholders in implementing its law enforcement and prosecution capacity in this area. Arguing that the ship-source pollution regime could provide a model for further developments for both territorially based environmental crime and transnational surveillance frameworks more generally, Carpenter's chapter examines the MARPOL Convention,[27] which aims to prevent pollution by oil, noxious liquids and garbage, for example, through the use of standards for ships and also zones where the discharge of wastes is prohibited into the sea. The chapter also examines the EU Directive on Port Reception Facilities for ship-generated waste and cargo residues[28] and the role of the

[26] http://ec.europa.eu/environment/legal/crime/index.htm (last accessed: 21/7/17).
[27] International Convention for the Prevention of Pollution from Ships 1973, as amended by its Protocol of 1978.
[28] Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues, OJ 2000 L332/81.

EU's European Maritime Safety Agency (EMSA).[29] The chapter then goes on to examine three specific regimes, those covering the Baltic Sea, Mediterranean Sea and the North Sea, (adjacent to the post-Brexit UK), and the use of aerial surveillance is used to detect oil pollution and, through the use of satellites and in co-operation with the EMSA, to hindcast (back-track) oil pollution to a specific ship at sea. The chapter focuses, in particular on the regime covering the North Sea, together with the expansion of its regime into the North-East Atlantic.

Increasing complexity is emerging as the EU Internal Security Strategy develops over time, and moves from a paper based exercise to one that has to be implemented in practice, and deliver results, and against the back ground of a continuing diversity in legal and law enforcement systems across EU member states. These challenges are multiplied as new EU systems need to be integrated with existing communities of practices, with law enforcement agencies, and individual agents putting their own interpretation on what has been designed "in Brussels." In addition the imbalance between the rights, power and security elements of the AFSJ has been recognised, and needs to be rebalanced. It is clear that the Internal Security Strategy is, and will continue to be for a long time, a work in progress, as reflected in the European Agenda on Security,[30] not only addressing traditional transnational security threats, but in reacting to emerging issues which appear over time, either as new crime areas, or issues which arise during the implementation of earlier phases of the strategy. This will be a subject matter for academic discourse for many discipline areas for some time to come.

Bibliography

Boswell, C. *The Political Uses of Expert Knowledge: Immigration policy and Social Research*. Cambridge: Cambridge University Press, 2013.

Commission staff working document accompanying the communication from the Commission to the Council - *Review of EU-Russia relations pursuant to conclusions of the Extraordinary European Council of September 1, 2008*, COM(2008) 740 final.

[29] Regulation (EC) No 1406/2002 of the European Parliament and of the Council of 27 June 2002 establishing a European Maritime Safety Agency (Text with EEA relevance), OJ 2002 L208/1.

[30] Communication from the Commission, *European Agenda on Security*, 2.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – *The European Agenda on Security*, COM(2015) 185 final.

Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues, OJ 2000 L332/81.

Ericson, R. "The division of expert knowledge in policing and security," *BJS* 45(2) (1994): 149-175.

High Representative of the European Union for foreign Affairs and Security Policy and European Commission: Joint Communication to the European Parliament and the Council; *For an open and secure global maritime domain: elements for a European Union maritime security strategy*, JOIN(2014) 9 final.

HM Government, *Decision pursuant to Article 10 of Protocol 36 to The Treaty on the Functioning of the European Union*, July 2013, Cm 8671. https://www.gov.uk/government/publications/decision-pursuant-to-article-10-of-protocol-36-to-the-treaty-on-the-functioning-of-the-european-union (last accessed: 21/7/17).

International Convention for the Prevention of Pollution from Ships 1973, as amended by its Protocol of 1978.

Miller, V., In brief: the 2014 block opt-out and selective opt-back-ins, Standard note: SN/IA/6684.

O'Neill, Swinton and Winter; *New Challenges for the EU Internal Security Strategy*, Newcastle-upon-Tyne, Cambridge Scholars 2013.

Parkin, J., *EU Home Affairs Agencies and the Construction of EU Internal Security Strategy*, Brussels: CEPS Paper in Liberty and Security in Europe No 53. December (2012).

Protocol No 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom Security and Justice.

Protocol No 36 on Transitional Provisions attached to the TEU and the TFEU post Lisbon.

Radcliffe, J.; *Intelligence Led Policing*, Collompton, Willan Publishing, 2008.

Regulation (EC) No 1406/2002 of the European Parliament and of the Council of 27 June 2002 establishing a European Maritime Safety Agency (Text with EEA relevance), OJ 2002 L208/1.

Stockholm Programme – an open and secure Europe serving and protecting citizens, OJ 2010 C115/1.

Treaty on European Union

Treaty on the Functioning of the European Union

PARADIGM SHIFTS FOR THE EU

CHAPTER TWO

A FIRST MAPPING OF THE POTENTIAL IMPACT OF THE JUSTICE DEVELOPMENTS ON THE AREA OF FREEDOM SECURITY AND JUSTICE

MARIA O'NEILL

Introduction

We are entering into a new phase in the construction of what is now known as the Area of Freedom, Security and Justice (AFSJ). Early developments on the security side, led predominantly by law enforcement professionals, following an Onuf[1] style constructivist methodology, are now nearing completion. While a few specific crime areas still need to be addressed, the current areas of rapid development are in the freedom and justice aspects of the AFSJ. A new prism needs to be adopted, namely one of European Union (EU) constitutionalism, further refining what it means to be an EU citizen. The Lisbon Treaty gave a massive impetus to these new areas of development, giving a substantial upgrading in the legal framework for ex. Police and Judicial Co-operation in Criminal Matters (PJCCM) matters. These provisions also become subject to adjudication by the Court of Justice (CJEU), formerly the European Court of Justice (ECJ), and benefit from the Lisbon Treaty upgrade of the EU Charter of Fundamental Rights (EUCFR), and the anticipated accession of the EU to the European Convention on Human Rights (ECHR). This area of law "is still in its infancy."[2] These changes should equally affect the UK (subject to any post-Brexit agreement) and Poland, despite their opt-out positions

[1] Onuf, N., "Constructivism: A User's Manual", in *International Relations in a Constructed world*, eds. V. Kubálková, N. Onuf and P. Kowert. (New York: M.E. Sharpe, 1998), 58.

[2] Luchtman, M. "Principles of European Criminal Law: Jurisdiction, Choice of Forum, and the Legality Principle in the Area of Freedom, Security, and Justice," *European Review of Private Law* 2012, 347-380, 347.

pursuant to Protocol No. 30 post-Lisbon, with regard to the EUCFR. The imbalance between security and freedom and justice in the AFSJ is causing problems. Guild talks about "unleashing the power of the Member States to exercise punishment at the edges of their own constitutional settlements."[3] Equally, problems arise when only the "enforcement mechanisms of criminal law" is given equal status across borders.[4] However, constitutional problems arise, as while the AFSJ is clearly a matter for the EU, "criminal law in general" is not.[5] The development of powers at an EU level "as a means to cope with the increasing transnational crimes as a result of European integration" needs therefore, to be matched "by appropriate protection of fundamental rights at that level."[6]

The member states of the EU, however, come from three main legal traditions, "the inquisitorial, adversarial, and post-state socialist."[7] In addition, "criminal procedures vary enormously," as do "the level of legal protection offered to suspects in criminal proceedings,"[8] with court procedures and decisions reflecting "the very different constitutional traditions of each country."[9] These fundamental differences, in areas outside the EU's competence, allied with the increase in numbers of people in transnational criminal investigations and decisions, involving possibly more than two EU member states,[10] are leading to some very complex problems.

In addition to examining the very real instrumentalist issues which arise, questions as to the constitutional impact of these developments also need

[3] Guild, E., "Crime and the EU's Constitutional future in the Area of Freedom Security and Justice," *European Law Journal*, 10(2): 220.
[4] Ibid. 219.
[5] Luchtman, "Principles of European Criminal Law," 358.
[6] Ibid. 366.
[7] Vocht, D.L.F. de & Spronken, T.N.B.M., "EU Policy to Guarantee Procedural Rights in Criminal Proceedings: 'Step by Step'", *North Carolina Journal of International Law and Commercial Regulation*, 37 (2011): 436-488, 238.
[8] Ibid., 237.
[9] Ziamou, T., "New process rights for citizens? The American tradition and the German legal perspective in procedural review of rulemaking", *Public Law* (1999), Win.: 726-742, 726.
[10] De Bondt W. and Vermeulen, G., "The Procedural Rights Debate A Bridge Too Far or Still Not Far Enough?" *EUCRIM (FREIBURG)*, 4 (2010): 163-167, 163.

to be addressed, as pointed out by Gibbs.[11] While constructivism might be an appropriate prism through which to examine the development of the mechanistic elements of cross-border law enforcement, this jigsaw approach to a development of an understanding by doing, is far from ideal with regard to issues which have "a profound effect on individual rights and political freedom."[12] As will be evidenced by this paper, these are developments which will have a profound effect not just on the EU, but also on individuals. Issues of "accountability," "democratic legitimacy" and "human rights" are coming to the fore, with the EU's "understanding as to how internal security integration forms an integral part" of how we perceive the EU needing to be critically examined.[13] Some provisions relevant to ex. PJCCM measures post-Lisbon can be brought forward from the pre-Lisbon EU legal framework. However, as this area of law is only now beginning to develop its own legal dynamic, this paper can only provide an initial assessment of the law in this area. In addition the road map on procedural rights[14] and its allied directives,[15] will have a serious impact on how investigations and prosecutions are conducted. The case law of the CJEU and the European Court of Human Rights (ECtHR), both pre- and post- EU accession, will have to fill in the many gaps in the legal framework in the years to come.

Oversight role to the Court of Justice

Pre-Lisbon Article 35 TEU, with its three options for preliminary reference procedures, has been replaced, post Lisbon, by integration of

[11] Gibbs, A.H., *Constitutional Life and Europe's Area of Freedom, Security and Justice* (Farnham: Ashgate, 2011), 7.
[12] Ibid, 7.
[13] Ibid, 7.
[14] Council of the EU. *EU road map on procedural rights Roadmap with a view to fostering protection of suspected and accused persons in criminal proceedings*. Brussels, 1 July 2009, 11457/09.
[15] Such as the directives on the right to information in criminal proceedings and the right to translation and interpretation and the rights of victims of crimes; Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012, on the right to information in criminal proceedings, OJ 2012 L142/1, Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ 2010 L280, Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ 2012 L315/57.

PJCCM matters into the mainstream preliminary reference procedure. The resulting oversight role of the CJEU is, however, limited. It can only overview those areas of AFSJ competences which have actually been transferred by member states to the EU. As the Treaty on European Union (TEU) states, the Union will respect members'

> "essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."[16]

This is reinforced by Article 72 Treaty on the Functioning of the European Union (TFEU) which provides that the EU "will not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security." In addition Article 73 TFEU makes it clear that national security and intelligence services are not under the control of the EU, and therefore are not subject to review by the CJEU. These treaty provisions would appear to draw some very clear red lines in the treaty for the whole of the AFSJ. There are further specific provisions dealing with policing and law enforcement matters, in Article 276 TFEU.[17] This relates to the powers and competences of the CJEU, providing that it "shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State," on actions taken by that state "with regard to the maintenance of law and order and safeguarding of internal security." This Article 276 TFEU limitation is not only with regard to preliminary reference proceedings, but also member state infringement proceedings in this area.[18] It is unlikely that EU institutions would attempt to regulate a member state's internal law enforcement provisions in light of the very clear provisions in Articles 72 and 73 TFEU. Non-involvement of the EU in internal law enforcement and internal security provisions is understandable when one takes into account the quite varying approaches to policing and justice procedures, measures which are closely tied to the internal constitutional structure of each individual member state, and their lengthy historical developments. An interesting point however, as noted by Hinarejos, Article 276 TFEU

[16] Article 4.2 TEU.
[17] Hinarejos, A., "Law and order and internal security provisions in the Area of Freedom, Security and Justice: before and after Lisbon," in *Crime within the Area of Freedom, Security and Justice, A European Public Order*, eds. C. Eckes and T. Konstadinides (Cambridge: Cambridge University Press, 2011), 265.
[18] Ibid. 265.

limitation "does not catch the reintroduction of Schengen internal borders."[19] In addition, issues of "public emergencies," such as arise with regard to major terrorist incidents, and how to tackle them, have clearly been recognised as issues for the particular member state, by both the ECtHR, in the *Brannigan* case,[20] and the CJEU in AG Maduro's opinion in the 05 *Kadi* ruling.[21]

Hinarejos offers a different perspective on Article 72 TFEU.[22] She makes the comparison to other areas of EU law where there are current derogations. This author would be of the view that Hinarejos' comparator policy areas, "public health, public security and public policy in the realm of the common market,"[23] would be less sensitive politically than law enforcement and internal and national security measures, and that her second line of argument, that there are "limits of Union legislative competence," would be much more persuasive in this particular context.[24] Hinarejos however does make a cogent point that "actions of law-enforcement service[s] that have their origins in EU law" not being "controlled by the ECJ in any way" could "be considered unsatisfactory." She points out that "such actions may be controlled by national courts,"[25] and that there is a need for the CJEU and the national courts to "strive to cooperate"[26] in practice, in order to ensure that there is, in fact, no gap in the judicial oversight of cross-border law enforcement and prosecution activity.

Hinarejos states that the CJEU would be unlikely to seek jurisdiction to review actions for human rights compliance standards, which would more properly be a matter for the national courts, and their own legal relationship with the ECtHR.[27] Using Tridimas,[28] she points out that the then ECJ was "prepared to review the proportionality of member states actions even where issues of national security are at stake," relying on the

[19] Ibid. 266.
[20] *Brannigan and McBride* v *the United Kingdom*, app no 5/1992, 26-5-1993, paragraph 43.
[21] Joined Case C-402/05 and C-415/05 *Yassin Abdullah Kadi*, [2008] ECR I-06351. Opinion of Advocate General Maduro, at paragraph 35 of his opinion.
[22] Hinarejos, "Law and order and internal security provisions," 264.
[23] Ibid. 264.
[24] Ibid. 264.
[25] Ibid. 260.
[26] Ibid. 270.
[27] Ibid. 264.
[28] Tridimas, T., *The General Principles of EU Law* (2nd edn, Oxford: Oxford University Press, 2006) 225–9, 229.

case of *Alfredo Albore*.[29] It has to be pointed out that the *Albore* case dealt with free movement of capital, and the purchase of property near a military base. It did not deal with cross border law enforcement or criminal law, such as would come into play in the context of a cross border drug trafficking operation or prosecution, matters which were the focus of the ex. PJCCM provisions.

There are a number of cases similar to *Albore* which have appeared before the ECJ over the years, which touch on national security issues,[30] but are really matters covered by other policy areas of the EU legal framework, such as employment law.[31] There is a grey area between what is legitimately a national security issue, and what is not, however these are somewhat removed from the area of cross border law enforcement, as engaged with on a daily basis by EU agencies such as Europol and Eurojust, and therefore do not form part of the subject matter of this paper.

The CJEU will necessarily be required to give preliminary rulings in ex. PJCCM matters, "where law and order and internal security occupy the centre stage."[32] There will be a need for judicial practices to develop, allowing the CJEU to rule on the substance of EU law, but not crossing the red lines of member state internal security provisions. Preliminary ruling requests will have to be phrased by national courts accordingly, with national courts needing to review national activities "not only with national law, but also with EU law."[33] Outside the treaty based red lines, this subject matter is an area of shared competence,[34] subject to the principle of subsidiarity. The general view here is that "subsidiarity and proportionality are likely to be raised more often" post-Lisbon, with greater likelihood of success.[35]

---

[29] C-423/98 *Alfredo Albore* [2000] ECR I-5965.
[30] Hinarejos, "Law and order and internal security provisions," 265.
[31] Case 222/84 *Johnston* v *Chief Constable of the Royal Ulster Constabulary* [1986] ECR 1651.
[32] Hinarejos, "Law and order and internal security provisions," 271.
[33] Ibid. 268.
[34] Article 4.2.j TFEU.
[35] Fletcher, M., "EU criminal justice: beyond Lisbon," in *Crime within the Area of Freedom, Security and Justice A European Public Order*, eds. C. Eckes and T. Konstadinides (Cambridge: Cambridge University Press, 2011), 10- 42, 22, referring to Sir Francis Jacobs in House of Lords Select Committee, "The Treaty of Lisbon: An Impact Assessment", para. 11.43.

Criminal law and detention cases need to be dealt with much more rapidly than commercial law cases, the traditional case law of the ECJ. Article 267 TFEU provides that the CJEU will act "with the minimum of delay" "with regard to a person in custody." Post Lisbon, the Consolidated Version of the Statute of the Court of Justice of the EU provides for an urgent procedure for AFSJ provisions, being a sub set of an expedited or accelerated procedure, (which is not limited to AFSJ matters),[36] in the context of a reference for a preliminary ruling relating to the area of freedom, security and justice.[37] An urgent procedure can also be used in the context of a file forwarded from the General Court to the CJEU.[38] Urgent preliminary procedures are provided for in Title III Chapter 3, of the Court's rules of procedure,[39] for questions arising under Title V part 3 of the TFEU, the AFSJ. As stated by the editors of the Common Market Law Review, "respect for fundamental rights of individuals required that request for preliminary rulings be handled with the minimum delay."[40] Worth noting in this context is that the CJEU is empowered by Article 279 TFEU to "prescribe any necessary interim measures" in "any cases before it." It is highly possible that this provision may be used in the context of cross border AFSJ referrals in order to assist in respecting individual's fundamental rights. Provisions are now also in the Statute for specialised courts,[41] something which may well develop in the future if large number of criminal cases arrive before the Court.

As pointed out by Fletcher, Article 263 TFEU brings both Europol[42] and Eurojust[43] within the ambit of judicial review actions at the CJEU,[44] as the

---

[36] Lenaerts, K., "The contribution of the European Court of Justice to the area of freedom, security and justice," *International & Comparative Law Quarterly*, 59(2), (2010): 255-301, 273.

[37] Consolidated Version of the Statute of the Court of Justice of the European Union, Protocol No 3, as amended, Article 23a, available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-10/staut_cons_en.pdf.

[38] Ibid. Article 62a.

[39] Consolidated Rules of Procedure of the Court of Justice, OJ 2010 C177/5, Article 107 to 114.

[40] Editorial comments, "Preliminary rulings and the area of freedom, security and justice," *CMLRev* 44: 1-7, 2007, 7.

[41] Article 62c of the Consolidated Version of the Statute of the Court of Justice of the European Union, Protocol No 3, as amended.

[42] Article 88 TFEU.

[43] Article 85 TFEU.

[44] Fletcher, "EU criminal justice: beyond Lisbon,"40.

actions of both these bodies clearly are "intended to produce legal effects *vis-à-vis* third parties,"[45] with natural or legal persons being able to institute judicial review proceedings against acts "addressed to that person or which is of direct or individual concern to them."[46] This is a long standing provision in EU law. However it still has to be seen how this provision will operate in the context of a cross border law enforcement or criminal prosecution, where the prosecution or investigation is against that individual, and whether the judicial review proceedings will be dealt with by the CJEU by way of the expedited or accelerated procedures, discussed above, in the context of preliminary reference procedures. Eurojust and Europol activities were clearly not in the minds of the drafters of the original version of the judicial review treaty provisions, which are substantially un-amended in the post-Lisbon treaty framework.

EU Charter of Fundamental Rights

The EU Charter of Fundamental Rights (EUCFR) was adopted in October 2000, with an uncertain legal status. It binds EU member states when they implement EU law.[47] It built on the earlier Community Charter of the Fundamental Social Rights of Workers, and other international documents, including the Council of Europe's European Social Charter, which was adopted in 1961, and revised in 1996. Pre-Lisbon EC law had long established that, independent of other sources, that fundamental rights were one of the general principles of EC law.[48] The EUCFR has clearly also been inspired by the ECHR, however there are significant differences between the two documents. In particular Article 52(3) of the Charter "explicitly allows the court to afford a more extensive level of protection

[45] Article 263(1) TFEU.
[46] Article 263(1) TFEU.
[47] Sarmiento, D., "Who's afraid of the Charter? The court of Justice, national courts and the new framework of fundamental rights protection in Europe," *C.M.L. Rev.* 50(5), (2013):1267-1304, 1274.
[48] Barnard, C., *The "Opt-Out" for the UK and Poland form the charter of Fundamental Rights: Triumph of Rhetoric over Reality?*, available on line at http://www.law.cam.ac.uk/faculty-resources/download/barnard-uk-opt-out-and-the-charter-of-fundamental-rights/7309/pdf, 5, relying on Case 29/69 *Erich Stauder* v *City of Ulm – Sozialamt* [1969] ECR 419 and Case 11/70 *Inernationale Handelsgesellschaft mbH* v *Einfuhr und Vorratsstelle für Getreide und Futtermittel* [1970] ECR 1125, paragraph 4.

than that offered by Strasbourg."[49] However, as Carrera *et al.* have pointed out, this article "provides the [CJEU][50] with an additional incentive to take the Strasbourg Court case law into account when developing its own fundamental rights jurisprudence."[51] A post-Lisbon innovation is Article 263 TFEU, "which foresees the possibility that when acts of EU agencies produce 'legal effects', these can fall under the judicial scrutiny of the [CJEU]."[52] While Carrera *et al.* go on to discuss the potential impact for Frontex, the same analysis could be applied to the ex. PJCCM agencies, such as Europol, Eurojust, etc. in their transnational prosecution and law enforcement activities.

Despite the lack of clarity on the exact legal status of the pre-Lisbon EU Charter, it featured in a number of cases before the then ECJ, being "referred to by a number of Advocate Generals."[53] Barnard has reported that more recently, in the 2003 to 2009 period the "Court of Justice had finally come off the fence and started to refer to the Charter" itself, but that "reference to the Charter [was] merely to buttress or confirm the interpretation of a Union measure."[54] Sarmiento argues, however, that "the Court of Justice has put the Charter at the forefront of European integration."[55]

With the Lisbon Treaty in 2009 the EU Charter has now gained full legal status, and is now fully justiciable given that the five year phase-in period of the powers of the now renamed Court of Justice, in particular over ex. PJCCM provisions, has expired.[56] This change in status to a charter which is legally binding should not, according to Article 6 TEU, lead to the Charter extending "in any way the competences of the Union as defined in

---

[49] Carrera, S., De Somer M., and Petkova, B., *The Court of Justice of the European Union as a Fundamental Rights Tribunal, Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice*, CEPS Paper in Liberty and Security, (Brussels, , CEPS, 2012), 7, available on-line at http://www.ceps.eu/book/court-justice-european-union-fundamental-rights-tribunal-challenges-effective-delivery-fundamen.

[50] Court of Justice of the EU.

[51] Carrera *et al*., *The court of Justice of the European Union*, 15.

[52] Ibid. 6.

[53] Barnard, *The "Opt-Out" for the UK and Poland*, 19.

[54] Ibid.

[55] Sarmiento, "Who's afraid of the Charter?" 1267.

[56] Pursuant to Protocol (No 36) on Transitional Provisions attached to the post Lisbon TEU and TFEU.

the Treaties." Barnard expressed the view[57] that the Charter "does not identify which provisions contain rights and which principles," with the explanations to the chapter only stating that these two categories can be found in the document.[58] Herlin-Karnell also points out that Article 51 of the Charter is "directed at the Union's institutions and to Member States when they are implementing EU law,"[59] or as Barnard has stated, "purely national issues will not be affected by the Charter,"[60] as evidenced in the *Walloon Government* v *Flemish Government* case.[61]

Article 51.2 of the Charter reinforces the fact that the Charter does "not extend the field of application of Union law… or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties." The competence of the EU to act must therefore be examined before the provisions of the Charter can be examined. In addition Protocol No. 30 attached to the TEU/TFEU limits the legal effect of the Charter to the United Kingdom (subject to the final Brexit agreement) and to Poland.[62] The protocol provides, at Article 1.1 that the Charter does not have the capacity to strike down any "laws, regulations or administrative provisions, practices or actions of Poland or of the United Kingdom," and at Article 1.2, that nothing in Title IV of the Charter creates justiciable rights applicable to Poland or the United Kingdom (subject to the final Brexit agreement) except in so far as Poland or the United Kingdom have provided for such rights in its national law. However, Title IV of the Charter covers the Solidarity headings,[63] which are part of employment law.

---

[57] Referring to HoL EU Select Committee, *The Treaty of Lisbon: An Impact Assessment 10th Report*, 2007/8, HL Paper 62, paragraphs 5.15, 5.18-5.20.
[58] Barnard, *The "Opt-Out" for the UK and Poland*, 4.
[59] Herlin-Karnell, E., *The Constitutional dimension of European Criminal Law*, (Oxford: Hart Publishing Ltd. 2012), 38.
[60] Barnard, *The "Opt-Out" for the UK and Poland*, 4.
[61] Case C-212/06 *Government of the French Community and Walloon Government* v *Flemish Government* [2007] ECR I-00, paragraph 38.
[62] Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and the United Kingdom.
[63] Title IV covers what are essentially employment related rights, however Article 32, which covers the "Prohibition of child labour and protection of young people at work", and Article 35 Health care" might be of relevance in the context of trafficking of human beings, and Article 37, which covers Environmental protection, might be of relevance in the context of Environmental crime, should these provisions not be already to be found in the national legislation of the UK and Poland.

Prior to the Lisbon Treaty upgrade, which UK and Poland have opted out of, the Charter had already begun to have an effect in ex. PJCCM type cases. As Guild has pointed out, the rights in the Charter come from two main sources, those rights "which already existed in EU law," which therefore would not be affected by whether or not the Charter, post Lisbon, was to have legal effect in any individual EU member state, and the ECHR, and its protocols, which also apply to all of the EU member states as part of their domestic laws.[64] Pre-existing EU rights were recognised by the then ECJ in the *Stauder* case.[65] Here the court recognised that "fundamental human rights [are] enshrined in the general principles of community [now EU] law and protected by the Court." Similarly, the *Internationale Handelsgesellschaft* case[66] held that "the protection of such rights, whilst inspired by the constitutional traditions common to the Member States, must be ensured within the framework of the structure and objectives of the Community." Again, in the *Nold* case[67] the court held[68] that "International treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories, can supply guidelines which should be followed within the framework of Community law." The approach exemplified in these and subsequent cases would presumably still apply to the UK (subject to the final Brexit agreement) and Poland, post Lisbon.

The limits put on the effectiveness of the Charter under Article 51 have been challenged by Herlin-Karnell, when she comments that the Charter was "given a free-standing value as a source of interpretation," which appeared to go beyond the limits set upon it in Article 51 in the *Kükükdeveci* case,[69] on the basis of concerns for "effectiveness."[70] She points out that similar considerations seem to have underpinned the *Unibet*[71] ruling. In *Unibet* the point at issue was that "national rules [should] not undermine the right to effective judicial protection," on the

[64] Guild, E., *The European Union after the Treaty of Lisbon Fundamental Rights and EU Citizenship*, (Brussels: CEPS 2010), available on-line at CEPS.eu.
[65] Case 29/69 *Stauder* v *City of Ulm*, paragraph 7.
[66] Case 11/70 *Internaitonale Handelsgesellschaft*, paragraph 4.
[67] Case 4/73 *Nold* v *Commission* [1974] ECR 491.
[68] Ibid. paragraph 13
[69] Case C-555/07 *Kükükdeveci* v *Swedex GmbH & Co. KG*, [2010] ECR, 00000.
[70] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 49.
[71] Case C-432/05 *Unibet (London) Ltd and Unibet (International) Ltd* v *Justitiekanslern*, [2007] ECR, I-02271, point made a number of times in the judgment.

basis of Article 47 of the Charter, "which provides the right to an effective remedy."[72] As Carerra *et al.* have stated, "through Article 47 … the Luxembourg Court has a consolidated role and reinforced legal mandate in fundamental rights protection."[73]

Article 19 TEU, as pointed out by Herlin-Karnell,[74] also provides the right to "effective legal protection," with Article 19 TEU not being subject to the Charter opt outs. The Court has declared "that the right to judicial protection is one of the general principles of law stemming from the constitutional traditions of Member States."[75] It is questionable, therefore, what the value of the opt outs to Article 47 of the Charter will be, given that very similar provisions are provided elsewhere in the EU legal framework, and any ruling from the CJEU is unlikely to divide the case law seamlessly between Charter and non-Charter EU rights. The general consensus is that Articles 47 to 49 of the Charter are likely to "have a huge influence as they set the framework for the EU's action" in ex. PJCCM matters.[76] Article 48, covering the "presumption of innocence and right of defence," is clearly a spin off from the Article 47, "right to an effective remedy and a fair trial." However, as pointed out by the European Parliament,[77] this is a pre-Lisbon Treaty right under *Johnston*[78] and *Pecastaing*.[79]

It is arguable that the Article 49 provisions on "principles of legality and proportionality of criminal offences and penalties" would also be subsumed into a non-Charter interpretation of Article 19 TEU "effective legal protection" for the two Charter opt-out states. Herlin-Karnell points out that this right, while "codified in Article 49 of the Charter,"[80] had already appeared in a number of pre-Lisbon cases, such as *Pupino*,[81] but

---

[72] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 50.
[73] Carrera *et al*., *The court of Justice of the European Union*, 19.
[74] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 47.
[75] Ibid.
[76] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 38.
[77] European Parliament Fact Sheets, 2.1.1. Respect for fundamental rights in the EU – general development, available at http://www.europarl.europa.eu/factsheets/2_1_1_en.htm.
[78] Case 222/84 *Johnston* v *Chief Constable of the Royal Ulster Constabulary*, paragraph 19.
[79] Case 98/79 *Pecastaing* v *Belgium* [1980] 691, at para 10.
[80] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 54.
[81] Case C-105/03 *Criminal proceedings against Maria Pupino* [2005] ECR 2005, I-05285.

she did state that "the issue is far more complicated when dealing with procedural legality in the context of criminal law cooperation."[82] She expressed concern as to EU developments in this area, with over emphasis on security at the expense of justice, stating that "it appears as though the shield has been lost in the effective enforcement fight across the EU's borders."[83]

While national law of the two opt out states may not be struck down for illegality, it is highly likely that an individual suspect who claims Article 19 TEU rights in appropriate cross-border prosecutions and law enforcement cases would benefit from the same rights as he or she would benefit from in fully Charter compliant EU member states. It is therefore to be expected that the Charter (and corresponding rights scattered throughout the EU legal framework) will have "a real impact on criminal law."[84] However, as Barnard has pointed out, the "Charter will therefore apply to states only when implementing Union law."[85] There remains a lack of clarity, however, as to the exact nature of the UK and Polish "opt-out," as the protocol states that "Noting the wish of Poland and the United Kingdom to clarify certain aspects of the application of the Charter."[86] If this means that there is no change from the UK (subject to the final Brexit agreement) and Poland's pre-Lisbon status, then the "opt-out" will, beyond the employment law relevant provisions, have little impact.

Fundamental rights at an EU level, once they can be established, are not however absolute. The interpretation of fundamental rights at an EU level is subject to a number of limitations. The use of these rights must be in line with the principle of proportionality, which permeates all of EU law, and the Community or now the Union, must "not affect the essential content of that right" [87] as ruled on in the *Schräder* case.[88] Equally, as pointed out by Sarmiento, "fundamental rights protection is one of the few areas in which constitutional courts are willing to scrutinise EU law."[89]

---

[82] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 54.
[83] Ibid. 55.
[84] Ibid. 38.
[85] Barnard, *The "Opt-Out" for the UK and Poland*, 5.
[86] Ibid. 9, and eight recital.
[87] European Parliament Fact Sheets, 2.1.1. Respect for fundamental rights in the EU – general development, available at http://www.europarl.europa.eu/factsheets/2_1_1_en.htm.
[88] Case 265/87 *Schräder* v *Hauptzollamt Gronau* [1989] ECR 2237, paragraph 15.
[89] Sarmiento, "Who's afraid of the Charter?", 1268.

In the specific context of the impact of the Charter on ex. PJCCM matters previous cases at the ECtHR may be indicative of the type of cases which may come before the CJEU on Charter related matters. One case, dealing with the broad discretion in the UK in "laws permitting police officers to stop and search individuals," the case of *Gillan and Quinton* v *UK*[90] before the ECtHR, was held to be "in violation of the right to private life."[91] As stated by Guild, while "this case may be at the edges of EU competences," the ECtHR case *S & Marper* v *UK*[92] on the UK's (England and Wales and Northern Ireland) DNA database would directly relate to EU transnational law enforcement activities,[93] as there are EU provisions on the transmission of DNA, fingerprint and other personal information and data. Guild points[94] out that the Stockholm Programme, for the future development of the ex. PJCCM area, has requested the Commission to "explore if and how authorities of one Member State could obtain information rapidly from private or public entities of another Member State without use of coercive measures or by using judicial authorities of the other Member State."[95] This provision, certainly, would raise a myriad of Charter related issues.

Anticipated accession of the EU to the ECHR

A new era in the legal relationship between the EU and the ECHR is provided for in Article 6 TEU, post Lisbon, which provides that the EU is to accede to the ECHR, with Protocol No. 8, attached to the TEU and TFEU adding details on this accession.[96] From the ECHR perspective, Article 17(1) of Protocol No.14 ECHR has now amended Article 59 ECHR to add that "[t]he European Union may accede to this Convention," with Russia, the last contracting party to the ECHR approving these developments in February 2010, and the EU submitting proposals for

[90] *Gillan and Quinton* v *UK* [2010] ECHR 28.
[91] Guild, The European Union after the Treaty of Lisbon, 4.
[92] *S & Marper* v *UK* [2008] ECHR 1581.
[93] Guild, The European Union after the Treaty of Lisbon, 4.
[94] Ibid.
[95] Stockholm Programme - An open and secure Europe serving and protecting citizens, OJ 2010 C115/1, 3.1. Furthering the implementation of mutual recognition**,** 3.1.1. *Criminal law, fifth paragraph, fourth indent.*
[96] Protocol (No 8) relating to Article 6(2) of the Treaty on European Union on the accession of the Union to the European Convention on the protection of Human Rights and Fundamental Freedoms.

negotiation directives in March 2010.[97] The results of these negotiations were referred to the CJEU for a formal Opinion, leading to *Opinion 2/13*,[98] which ruled, for a number of reasons, that the then draft agreement was incompatible with EU law. It will therefore need to be re-drafted. The then version of the draft agreement contains "co-respondent" and "prior-involvement" mechanisms. The co-respondent mechanism avoided the need to address in human rights relevant cases the difficult issues of the division of competence between the EU and its member states,[99] which have frequently arisen in EU external relations situations, as in the World Trade Organisation (WTO) case of *Opinion 1/94*.[100] Baretta has described the prior-involvement mechanism as a way of preserving the CJEU "monopoly on the interpretation of EU law,"[101] one of the issues in *Opinion 2/13*. It can also be seen as echoing the standard ECtHR prerequisite of exhausting national remedies. The key point, which will need to be reflected in any new draft agreement, will be the need to maintain the "autonomy of the EU legal order," despite the then proposed external supervision mechanism.[102]

As Lock has pointed out, these are "two very different legal orders," and they need to be "brought into line" while still maintaining "the autonomy of the EU legal order."[103] In addition, nothing in the provisions dealing with the EU's accession to the ECHR shall affect Article 344 TFEU,[104] which in turn provides that "Member States undertake not to submit a dispute concerning the interpretation or application of the Treaties to any method of settlement other than those provided for therein." The Republic of Ireland fell foul of this provision in *Commission* v *Ireland* (*re MOX plant*),[105] when they submitted a matter to an international arbitral tribunal rather than submitting the matter to the then ECJ. The proposed "co-

[97] Editorial Staff of the Maastricht Journal, "Recent legal developments; EU Accession to the ECHR – The Commission Proposal for Negotiating Directives," 17 *MH* 2 (2010), 206.
[98] *Opinion 2/13* [2014] ECR 2014, page 0000.
[99] Lock T., "Walking on a tightrope: the Draft ECHR Accession Agreement and the autonomy of the EU legal order," *C.M.L.Rev.* 48(4) (2011): 1025-1054**,** 1040.
[100] *Opinion 1/94* (re WTO) [1994] ECR, I-05267.
[101] Baratta, R., "Accession of the EU to the ECHR: the rationale for the ECJ's prior involvement mechanism," *C.M.L.Rev*. 50(5) (2013): 1305-1332, 1316.
[102] Lock, "Walking on a tightrope," 1025.
[103] Ibid. 1025.
[104] Article 3 of Protocol No. 8 TEU/TFEU.
[105] Case C-459/03 *Commission* v *Ireland* (Dispute relating to the MOX plant at Sellafield, United Kingdom) [2006] ECR page I-04635 (Grand Chamber).

respondent" and "prior-involvement" mechanisms should assist in avoiding similar cases in the context of the CJEU-ECtHR relationship. The Strasbourg court's remit will not, however, be "to tell the ECJ what the content of the EU substantive law would generally be."[106] Equally the two senior courts should not be seen as one "of rivals," as their remits and legal frameworks are quite different, but "rather [as] complementary partners for progressive evolution in the interest of improving individual protection" within the EU.[107]

In addition to the points raised above, not only the treaty provisions on subsidiarity, but also the EU treaty red lines in the context of internal and national security, would come into play. These in particular would be Article 4.2 TEU,[108] Article 72 TFEU[109] and Article 73 TFEU.[110] Protocol No. 8, point 2 provides that nothing in the EU treaties "affects the situation of Member States, in relation to the European Convention" to include provisions of individual member states set out in protocols attached to the ECHR, or individual derogations from the ECHR.[111] At the time of writing 13 EU member states have derogations attached to the ECHR. Other derogations relevant to the subject matter of this paper can be anticipated.

Despite these mechanisms the issue of the exact legal relationship between the two legal regimes still needs to be examined. As pointed out by Lord Hoffmann, there is "a huge distinction" between the two legal systems.[112] The relationship between the ECHR and its contracting parties is subject

[106] Baratta, "Accession of the EU to the ECHR," 1326.
[107] Ibid. 1332.
[108] Article 4.2 TEU provides that the Union will respect members' "essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."
[109] Article 72 TFEU: This title shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.
[110] Article 73 TFEU: It shall be open to member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the component departments of their administrations responsible for safeguarding national security.
[111] Article 2 of Protocol No. 8 TEU/TFEU.
[112] Martinico, G., "Is the European Convention going to be 'supreme'? A comparative-constitutional overview of ECHR and EU law before national courts," *E.J.I.L.* 23(2) (2012): 401-424, 402, quoting Lord Hoffmann, "The Universality of Human Rights", Judicial Studies Board Annual Lecture, London, 19 Mar. 2009.

to the constitutional make-up of the individual states, including the monist/dualist dichotomy. This is very different from the supremacy and direct effect of EU law. In addition, as Martinico has pointed out, the EU institutions, to include the CJEU in Luxembourg, "were given a mandate to unify the laws of Europe."[113] There was no such mandate given to the Council of Europe and the human rights court based in Strasbourg.[114] In addition, while EU law works pretty effectively, given that it is being implemented in 28 very diverse member states, which are at different levels of development, there is a significant gap between "the formal status of ECHR norms and their real value and nature" in the CoE's 47 countries,[115] which stretch from the Atlantic to the Pacific. Martinico refers to the distinction between the "'static approach' (what national constitutions say) and a 'dynamic approach' (concerned with the actual force of these laws, as emerges in the case law)."[116] These distinctions will affect the direct relationship between the EU and the ECHR. The nature of the relationship between the EU and the ECHR may well be dualist, following the EU's approach in the WTO case of *Portugal* v *Council*,[117] relying on the earlier cases of *Fediol*[118] and *Nakajima*.[119]

In addition the distinction between a static and a dynamic relationship also needs to be examined in the context of the relationship between the two senior courts, the CJEU and the ECtHR. There has been some academic argument to the effect that national judges are unaware of, or unwilling to, acknowledge the distinction between these two different legal systems. Nevertheless, there appears to be already "a partial convergence in the application of EU and ECHR's norms," independent of the actual accession of the EU to the ECHR.[120] It is clear from the study conducted by Martinico and Pollicino[121] that the automatic supremacy of ECHR law is not guaranteed within EU member states, in the same way as EU law is recognised as being supreme. In addition, occasional problems continue to

[113] Ibid.
[114] Ibid.
[115] Ibid. 403.
[116] Ibid. 403.
[117] Case C-149/96 *Portugal* v *Council*, OJ 2000 C47/8.
[118] Case 70/87 *Fediol* v *Commission* [1989] ECR 1781.
[119] Case C-69/89 *Nakajima All Precision* v. *Council* [1991] ECR I-2069.
[120] Martinico, "Is the European Convention going to be 'supreme'?" 402.
[121] Martinico G. and Pollicino, O., *The Interaction between Europe's Legal Systems; Judicial Dialogue and the Creation of Supranational Laws* (Cheltenham: Edward Elgar 2010).

arise in the supremacy of EU law at Constitutional Court level of the EU member states – where the most senior judges in a member state can be reluctant to overly defer to another court. Although efforts are made at Constitutional Court level to accommodate EU law into national law, there do appear to be judicial red lines[122] over which EU law is not permitted to cross, for example, issues surrounding abortion in the Republic of Ireland. It is quite likely that more of these judicial red lines will emerge in the context of the AFSJ post Lisbon. At an EU/ECHR level Martinico and Pollicino have developed the "impression that we are dealing with a sort of cooperative climate between judges," particularly with the aim of protecting fundamental rights.[123] They also point out that "[m]any fundamental judgments of the ECJ are [already] very rich in references to the judgments of the ECtHR or to the provisions of the ECHR."[124]

At the time of writing a Draft Accession Agreement has still to be formally approved, so it is not certain what mechanisms will finally be put in place for articulating the relationship between the EU and the ECHR. However, academics are pointing out that once the agreement has been finalised, and approved by the CJEU, ratification of the agreement will be required in all CoE High Contracting Parties, "in accordance with their constitutional traditions," which may require domestic legislation and/ or a referendum, and separately, in all EU member states. As O'Meara has pointed out, "securing 47 approvals could be a tall order and may take some time."[125] Once the currently proposed mechanisms are in place Groussot *et al.* argue that the proposed co-respondent mechanism looks quite lengthy and complicated.[126] This is to be contrasted with the need for speed generally in criminal matters, and in particular when an individual's liberty is at stake. The EU has acknowledged this factor in the current version of the preliminary reference procedure, now in Article 267 TFEU, which provides that "with regard to a person in custody, the Court of

[122] The only exceptions to this would appear to be Estonia, Belgium (but this is disputed), Luxembourg and the Netherlands. Martinico and Pollicino, 134.
[123] Martinico and Pollicino, *The Interaction between Europe's Legal Systems*, 16.
[124] Ibid. 7.
[125] O'Meara, N., "'A More Secure Europe of Rights?' The European Court of Human Rights, the Court of Justice of the European Union and EU Accession to the ECHR," *German Law Journal* 12(10) (2011): 1813 – 1832, 1830.
[126] Groussot, X., Lock, T., and Pech, L., *EU Accession to the European Convention on Human Rights: a Legal Assessment of the Draft Accession Agreement of 14th October 2011*, European issues no 218 (Brussels and Paris: Robert Schuman Foundation, Brussels and Paris, (2011), 11.

Justice of the European Union shall act with the minimum of delay." It must be envisaged that these cases will queue jump the cases waiting to be heard at the CJEU. The real impact of EU accession to the ECHR on the criminal litigation process "will not be clear until tested in practice."[127]

From being a clear statement of rights, the ECHR has given rise to "complex case law,"[128] with it being "difficult to determine the outer boundaries" of some of its provisions, in particular Article 6, right to a fair trial,[129] with the UK, for example, having had "difficulties" in deciding whether its provisions are applicable to cases before the UK courts.[130] Craig has described Article 6 jurisprudence as being "complex and unsatisfactory."[131] Article 6 rights are generally understood to be a right to "fair and public hearing within a reasonable time by an independent and impartial tribunal established by law."[132] However, the right to silence, not explicitly referred to in Article 6 ECHR, has led to a number of ECtHR cases, particularly in the context of terrorism cases referred from Ireland, *Heaney* v *Ireland*[133] and *Quinn* v *Ireland*.[134] This dealt with adverse consequences following on a suspect's refusal to answer police questions under the Irish Offences Against the State Act 1939.[135] A similar UK case would be the commercial case of *Saunders* v *UK*,[136] where evidence obtained under compulsion was held not to be useable in criminal proceedings. While the right to silence is recognised by the ECtHR, it "is not absolute," and "its scope depends upon the setting in which self-incriminatory information is sought."[137] Self-incrimination issues also arise from "an official demand for documents or identification information."[138] The combined rulings lead to an obligation on the

[127] O'Meara, "A More Secure Europe of Rights?", 1830.
[128] Craig, P., "The Human Rights Act, Article 6 and procedural rights," *Public Law* (2003), Win: 753-773, 755.
[129] Ibid. 756.
[130] Ibid. 759.
[131] Ibid. 754.
[132] Ibid. 754.
[133] *Heaney* v *Ireland* (2001) 33 EHRR 12.
[134] *Quinn* v *Ireland* (App. No.36887/97), (2000).
[135] Berger, M., "Self-incrimination and the European Court of Human Rights: procedural issues in the enforcement of the right to silence," *European Human Rights Law Review* 5 (2007): 514-533, 515.
[136] *Saunders* v *United Kingdom*, (Application no. 19187/91), ECHR, Judgment, (1996), para. 69 et seq. of the judgment of the court.
[137] Ibid.
[138] Ibid. 525.

national courts to decide on the matter in each particular case.[139] The two senior courts have engaged in "a regular dialogue," with this dialogue likely to be "reinforced when the Union accedes to that Convention."[140] The "increasing complexity" of both the EU and ECHR legal systems[141] will require greater efforts of coordination between the two senior courts, at both the formal (court ruling) and informal (liaison and meeting) level.

Pre-Lisbon the ECtHR's view of the EU was covered in the *Matthews* case,[142] which provided that the transfer of sovereignty from a member state to the EU "did not negate State responsibility" under the ECHR, which "continues after such a transfer."[143] The later ECtHR ruling in *Bosphorus*[144] developed this point further, leading to the "equivalent protection test,"[145] being a default position that, while the ECtHR maintains the right of that court to review EU acts, the presumption was that "EU fundamental rights" were "considered equivalent to that" of the ECHR.[146] This presumption put the EU in a privileged position vis-à-vis the ECtHR, some would argue for too long,[147] questioning whether this *Bosphorus* position would survive the combined impact of the Lisbon Treaty, the increased volume of ex. PJCCM matters anticipated to come before the CJEU, and the anticipated accession of the EU to the ECHR.[148] The ECHR rights have only been incorporated into EU law to date, in a "piecemeal" manner, with White arguing that reliance on the current "'principles of EC law' just lacks credibility" when it comes to procedural

[139] Ibid. 527.
[140] First working meeting of the CDDH informal working group on the accession of the European Union to the European Convention on Human Rights (CDDH-UE) with the European Commission; Extracts of relevant texts of the European Union on the accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms, Strasbourg, Tuesday 6 July (2.30 pm) – Wednesday 7 July 2010 (1.30 pm), 4.
[141] O'Meara, "A More Secure Europe of Rights?", 1829.
[142] *Matthews* v *UK*, [1999] *ECHR* (Ser. A), 45.
[143] O'Meara, "'A More Secure Europe of Rights?'", 1816.
[144] *Bosphorous Hava Yollari Turizm Ticaket Anonim Şirketi* v *Ireland*, Application no. 45036/98, (2005).
[145] Groussot *et. al*. *EU Accession to the European Convention on Human Rights*, 4.
[146] Ibid.
[147] O'Meara, "'A More Secure Europe of Rights?'", 1828.
[148] Ibid. 1816.

matters.[149] In addition, the EUCFR makes it clear, at Article 53, that its rights "must be at least as high as that of the Convention."[150] The potential for some very complex case law arises.

Some have argued that "the potential impact of the accession agreement [of the EU to the ECHR] has been perhaps exaggerated,"[151] on the basis that "the ECtHR, unlike the ECJ, was never going to gain the power to annul an EU act."[152] However, post accession "individual applicants" may well have the right to directly address the issue of ECHR violations by the EU.[153] Lock points out that these violations could "potentially be found in primary law, in secondary law, in executive actions or omissions and in decisions of the Union's courts."[154] To that list could be added police practice manuals for transnational law enforcement, activities of the EU's agencies, such as Europol and Eurojust, and the EU's data protection standards for law enforcement purposes. Doubts are being expressed as to whether the ECtHR can "offer sufficient protection to suspects and defendants in criminal proceedings,"[155] given the nature of the legal system and the very different ways it is implemented in ECHR contracting states. The very high number of violations also have to be taken into account, as is the fact that the ECtHR has been recognised as having a serious backlog of cases,[156] with 82,100 cases pending on 1st October 2005 with an exponential rise then anticipated to 250,000 by 2010.[157] A new Protocol No. 14 was ratified, bringing in a new single-judge formation,

[149] White, S., "The EU's accession to the Convention on Human Rights; A new era of closer cooperation between the Council of Europe and the EU?" *New Journal of European Criminal Law*, 1(4) (2010): 433-446, 433.
[150] Ibid. 436.
[151] Groussot *et. al*. *EU Accession to the European Convention on Human Rights*, 5.
[152] Ibid.
[153] Lock, "Walking on a tightrope," 1034.
[154] Ibid.
[155] van Puyenbroeck L. and Vermeulen, G., "Towards minimum procedural guarantees for the defence in criminal proceedings in the EU," *International and Comparative Law Quarterly*, 60(4), (2011): 1017-1038, 3.
[156] Woolf, Lord, *et al*., *Review of the Working Methods of the European Court of Human Rights*, December, (Strasbourg: CoE, 2005), available on the ECHR web site at http://www.echr.coe.int/Documents/2005_Lord_Woolf_working_methods_ENG.pdf.
[157] Woolf *et al*., *Review of the Working Methods of the European Court of Human Rights*, 8.

"with competence to declare applications inadmissible,"[158] which by 2012 had "decided approximately 81,700 applications" in that year.[159] In addition, under Protocol No. 14 the three-judge committees were given power to decide cases "if the underlying question in the case [was] already the subject of well-established case law of the Court."[160] Pending applications had been reduced down to 128,000 by the end of 2012.[161] In addition the *Broniowski* v *Poland*[162] development of the "pilot" judgment practice of adjourning "its consideration of applications deriving from the same general cause,"[163] also assisted in clearing the backlog of pending cases. However, given these ongoing delays at the ECtHR, and despite some radical reforms, the potential impact of the EUCFR from within the EU legal system, together with the EU's own interpretation of ECtHR standards, is likely to have a much more profound effect on the AFSJ in the long run. As stated by Baratta, given the "multifaceted implications for the EU legal order" of these developments, the "full impact of the accession is however impossible to predict."[164]

Road map on procedural rights

The final stream of development flowing into the rapidly growing area of ex. PJCCM matters is the EU road map on procedural rights.[165] The anticipated development of ex. PJCCM matters post Lisbon will lead to "an unprecedented level of coordination" at both the "procedural and substantive levels" in the context of a developing EU criminal law, with a "respect for fundamental rights" being the "unifying factor" binding all of these issues together.[166] However this "will remain work in progress… for a considerable time."[167] The current work plan in this area is the road map

[158] European Court of Human Rights Annual Report 2005, 12, available at www.echr.coe.int.
[159] European Court of Human Rights Annual Report 2012, 6, available at www.echr.coe.int.
[160] European Court of Human Rights Annual Report 2005, 12/13, available at www.echr.coe.int.
[161] European Court of Human Rights Annual Report 2012, 6, available at www.echr.coe.int.
[162] ECtHR case of *Broniowski* v *Poland* (Application no. 31443/96).
[163] Para 35 of the final judgment.
[164] Baratta, "Accession of the EU to the ECHR," 1331.
[165] Council of the EU. *EU road map on procedural rights*.
[166] Lenaerts, "The contribution of the European Court of Justice," 301.
[167] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 41.

on procedural rights, which covered six separate legal measures which were to be adopted. Problems arose, however, with the conception of these rights, with "increasing opposition to the proposal" emerging.[168] The main issue was whether the EU should restrict itself to cross-border cases, and not get involved in "purely domestic proceedings."[169] Some argued that there was "no direct link to the protection of rights in transnational cases", a matter in which the EU could "legitimately exercise its competence" under Article 82 TFEU.[170] However, it is arguable that rights in themselves are not sufficient, as an "effective criminal defence" required an "interrelationship between, a range of principles, laws, practices, and cultures,"[171] the full range of which is clearly outside the competence of the EU. Also affecting the debate in this area was the belief that many of the proposed rights were merely reproducing rights already provided for by the ECHR, and that any attempt to replicate them within EU law was "actually useless."[172] The difference in quality of the EU and ECHR legal framework may have brought a more nuanced perspective to this debate. A proposal for a framework decision on procedural rights in criminal proceedings was abandoned.[173]

Given the political and legal problems in how exactly to draft measures which were Article 82 TFEU compliant, but did not overly extend into matters of exclusive member state sovereignty, the approach was to use a "step-by-step approach," and to tackle the least controversial issues first.[174] On this basis the provisions on translation and interpretation rights were the first to be enacted,[175] followed by measures dealing with the provision of information during a criminal proceeding.[176] Provisions on legal advice and legal aid have recently been enacted in the context of the operation of the European Arrest Warrant as Directive (EU) 2016/1919,[177] and Directive

[168] van Puyenbroeck and Vermeulen, "Towards minimum procedural guarantees," 20.
[169] Ibid.
[170] Rafaraci, T., "The Right of Defence in EU Judicial Cooperation in Criminal Matters", in *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, ed. S. Ruggeri (New York: Springer, 2013), 340.
[171] Vocht, de & Spronken, "EU Policy to Guarantee Procedural Rights," 482.
[172] Rafaraci, "The Right of Defence," 334.
[173] Ibid.
[174] Vocht, de & Spronken, "EU Policy to Guarantee Procedural Rights," 459.
[175] Directive 2010/64/EU.
[176] Directive 2012/13/EU.
[177] Directive 2016/1919/EU of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal

2013/48/EU.[178] More generally the ECJ ruled on the issue of legal privilege in the Competition law case of *AM&S*,[179] as confirmed in the *Akzo Nobel* case.[180] Pre-trial detention provisions are also still at proposal stage.[181] Separate safeguards for vulnerable suspects or accused persons have not been addressed. However there are now legal provisions on the rights of victims of crimes,[182] which have been complemented, as stated by the House of Lords,[183] by the trafficking in human beings directive,[184] and the directive on the sexual abuse of children.[185] Lenaerts points out that the double jeopardy rules (*ne bis in idem*) set out in Article 54 of the Schengen Convention[186] would also be relevant here.[187] ECJ case law[188] has already covered the issue of "the refusal to hear the defence of an

---

proceedings and for requested persons in European arrest warrant proceedings, OJ 2016 L297/1.

[178] Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ 2013 L294/1.

[179] Case 155/79 *AM&S* v *Commission*, [1982] ECR 1575.

[180] Case C-550/07 *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd.* v *European Commission*, 2010 [ECR] I-8739, para. 155.

[181] Strengthening mutual trust in the European judicial area – A Green Paper on the application of EU criminal justice legislation in the field of detention, COM(2011) 327 final.

[182] Directive 2012/29/EU.

[183] House of Lords European Union Committee, 30th Report of Session 2010–12, The European Union's Policy on Criminal Procedure, 26th April 2012, HL Paper 288, para. 44.

[184] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, OJ 2011 L101/1.

[185] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ 2011 L335/1.

[186] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders, OJ 2000 L239/19.

[187] Lenaerts, "The contribution of the European Court of Justice," 300.

[188] Case C-7/98 *Krombach* v *Bambersk*, [2000] ECR I-01935, paras 38-40.

accused person who is not present at the hearing" being "a manifest breach of fundamental rights."[189]

It is important to note that rights considered to be standard in many EU member states, "such as the right to remain silent, to have access to the file and to call and/or examine witnesses or experts," are not available in all EU member states.[190] One can well ask how strong is the mutual trust, in reality, between the different EU legal jurisdictions. While "no political agreement could be reached" the Commission has not given up on the road map.[191] There clearly "remain key differences in procedural systems of protection,"[192] as Murphy states with regard to the European Evidence Warrant, with EU criminal justice cooperation being pursued despite, rather than because of, the level of trust between member state criminal justice systems.[193] Rafaraci is of the view that this "common minimum guarantees" of procedural rights would "represent an effective enhancement of the principle of mutual recognition,"[194] which is probably true, as long as the EU does not encroach onto member state sovereignty.

Murphy goes on to state that while the *Advocaten voor de Wereld*[195] ruling proved that harmonisation is not a precondition" for mutual recognition, that mutual recognition is "easier said than done."[196] As the ex. PJCCM area generates more and more case law, and perhaps between non-traditional partnership countries, more of these issues are likely to arise in practice. It would also appear that the EU is now prepared to address "future actions [in the development of the road map on procedural rights]

---

[189] Lenaerts, "The contribution of the European Court of Justice," 284.
[190] van Puyenbroeck and Vermeulen, "Towards minimum procedural guarantees," 22.
[191] Ibid. 21.
[192] Murphy, C., "The European Evidence Warrant: Mutual Recognition and Mutual (Dis) Trust?," in *Crime within the Area of Freedom, Security and Justice A European Public Order*, eds. Eckes, C. and Konstadinides, T. (Cambridge: Cambridge University Press, 2011), 237.
[193] Ibid. 238.
[194] Rafaraci, "The Right of Defence," 341.
[195] Case C-303/05 *Advocaten voor de Wereld* v *Leden van de Ministerraad* [2007] ECR I-3633.
[196] Konstadinides, T., "The Europeanisation of extradition: how many light years away to mutual confidence?" in *Crime within the Area of Freedom, Security and Justice A European Public Order* eds. Eckes, C. and Konstadinides, T. (Cambridge: Cambridge University Press, 2011), 214.

one area at a time."[197] Whether the CJEU gets to deal with a particular procedural rights issue, under either the ECHR or the EUCFR or other general principles of EU law, before the Commission has managed to enact the perceived necessary provision, awaits to be seen.

Other EU case law will prove useful in filling in some of the gaps in the only partially enacted road map on procedural rights. Lenaerts has undertaken a study of pre-existing rights under ECJ case law which could be used.[198] He points out that the "right to an effective remedy against the violation of freedoms and rights guaranteed by EU law"[199] has been long recognised. As he points out,[200] "the right to be notified of procedural documents" and the right to be heard were recognised in *Eurofood*.[201] In addition *ASML*[202] held that respect for fundamental rights required a defendant, in that instance in a civil case, to know the contents of a judgment, and for documents to be "served on him in sufficient time to enable him to arrange his defence."[203] Equally, free movement of civil judgments was "not to be achieved at the expense… of a right to a fair hearing."[204] Lenaerts work goes on to examine other possible ECJ case law which could be useful in the absence of any further developments in the road map on procedural rights.[205]

Conclusion

The likely impact of EU accession to the ECHR has provided a fertile area for academic debate. It is interesting to recall that the EU has always defended its "external autonomy," guaranteeing that "the content of the EU's internal rules are not determined by the interpretations of an outside body."[206] Even Protocol No. 8 to the Lisbon Treaty speaks about the

[197] van Puyenbroeck and Vermeulen, "Towards minimum procedural guarantees," 21.
[198] Lenaerts "The contribution of the European Court of Justice".
[199] Ibid. 265.
[200] Ibid. 284.
[201] Case C-341/04 *Eurofood* [2006] ECR I-3813, at paragraph 66 of the ruling.
[202] Case C-283/05 *ASML Netherlands BV* v *Semiconductor Industry Services GmbH (SEMIS)*, [2006] ECR I-12041.
[203] Lenaerts, "The contribution of the European Court of Justice," 284.
[204] Ibid. 285.
[205] Ibid.
[206] Lock, "Walking on a tightrope," 1032.

"preservation of the autonomy of EU law."[207] This accession will "provide an interesting legacy for both legal orders,"[208] and it is to be expected that the EU Commission will "monitor the dynamics between [the] courts following accession."[209] While ECHR accession is clearly an important matter, and is likely to throw up a number of complex legal issues, it is arguable that a much more profound legal change to ex. PJCCM matters is likely to arise from the recent changes within the EU. The increased role of the CJEU, allied to the upgrade in legal status of the EUCFR, and the, all be it, slowly developing road map on procedural rights, is likely to have a much more profound effect. The UK (subject to the final Brexit agreement) and Polish "opt outs" to the upgrade in legal status of the EUCFR are likely to be limited to employment law measures, and have little impact on ex. PJCCM matters. Complex issues of EU competence and member state sovereignty remain.

Clearly the issue of rights in the context of ex. PJCCM measures arises from the national constitutional traditions of individual member state legal systems, and is reliant on the "interrelationship between, a range of principles, laws, practices, and cultures"[210] in which they operate. However, mutual trust between legal systems requires some base line rights to be recognised and fully respected in all, and not just some EU member states. Complicating developments at this level is the fact that the "Commission does not enjoy a monopoly over initiative,"[211] and the provision for an "'emergency' brake over proposed legislation" if a particular proposal would substantially adversely affect an individual member state's criminal justice system.[212]

The imbalance between security and rights needs to be addressed at the EU level. We need to ask who is the "public" that the EU is seeking to protect,[213] particularly "in light of relations with non-EU Member States," such as under the Euro-Med[214] and ENP[215] agreements.[216] Those "values",

[207] Ibid. 1033.
[208] O'Meara, "'A More Secure Europe of Rights?'", 1832.
[209] Ibid. 1830.
[210] Vocht, de & Spronken, "EU Policy to Guarantee Procedural Rights," 482.
[211] Gibbs, *Constitutional Life*, 18.
[212] Ibid. 18.
[213] Ibid. 16.
[214] Euro-Mediterranean Agreements.
[215] European Neighbourhood Partnership Agreements.
[216] De Bondt and Vermeulen, "The Procedural Rights Debate," 167.

which Gibbs refers to as "constitutional public goods,"[217] that the EU wishes to promote, need to be "scrutinised in detail,"[218] particularly as, following on the writings of Foucault, "'security" has emerged as a technique of governance."[219] Some clarity needs to be brought to what exactly the EU means by "'justice' …in a transnational setting."[220] In addition, the broader discussion "surrounding the issue of constitutional legitimacy in the EU"[221] need to be addressed, to include issues of democratic accountability and legitimacy. As Gibbs points out, there is a need to examine how exactly we conceptualise criminal justice[222] in a transnational context, as cross border law enforcement and prosecution needs to operate in a way which preserves "the liberal and democratic achievements of the national state."[223] The traditional constructivist approach taken to developing the EU cross-border law enforcement framework will not lead to an effective development of the freedom and justice aspects of the AFSJ. An EU constitutionalist approach needs to be developed. As Eckes has pointed out, interpretations of human rights have been closely linked with identity and sovereignty, traditionally in the context of a particular state.[224] If we are now to develop an effective EU concept of human rights, the concept of EU citizenship need to be more fully explored, in light of the fact that we will not be a United States of Europe, but be living in a more complex legal and political arrangement, needing to negotiate "margin[s] of appreciation, subsidiarity, discretion and proportionality," while still preserving individual member state differences, and overcoming, as best we may, the inevitable resulting tensions.[225]

[217] Gibbs, *Constitutional Life*, 47.
[218] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 111.
[219] Gibbs, *Constitutional Life*, 66.
[220] Herlin-Karnell, *The Constitutional dimension of European Criminal Law*, 111.
[221] Gibbs, *Constitutional Life*, 14.
[222] Ibid. 125.
[223] Ibid. 9.
[224] Eckes, C., "EU Accession to the ECHR: Between Autonomy and Adaptation," 76(2) *MLR* (2013), 254–285, 285.
[225] Ibid.

Bibliography

Baratta, R. "Accession of the EU to the ECHR: the rationale for the ECJ's prior involvement mechanism." *C.M.L.Rev*. 2013, 50(5): 1305-1332.

Barnard, C., *The "Opt-Out" for the UK and Poland form the charter of Fundamental Rights: Triumph of Rhetoric over Reality?*, available on line at http://www.law.cam.ac.uk/faculty-resources/download/barnard-uk-opt-out-and-the-charter-of-fundamental-rights/7309/pdf.

Berger, M. "Self-incrimination and the European Court of Human Rights: procedural issues in the enforcement of the right to silence." *E.H.R.L.R. (European Human Rights Law Review)* 2007, 5: 514-533.

Bosphorous Hava Yollari Turizm Ticaket Anonim Şirketi v *Ireland*, Application no. 45036/98, (2005).

Branningan and McBride v *the United Kingdom*, app no 5/1992, 26-5-1993.

Broniowski v *Poland* (Application no. 31443/96).

Carrera, S., De Somer M., and Petkova, B. *The Court of Justice of the European Union as a Fundamental Rights Tribunal, Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice*. CEPS Paper in Liberty and Security, Brussels: CEPS, 2012.

Case C-555/07 *Kükükdeveci* v *Swedex GmbH & Co. KG*, [2010] ECR, 00000.

—. C-550/07 *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd.* v *European Commission*, 2010 [ECR] page 00000.

—. C-212/06 *Government of the French Community and Walloon Government* v *Flemish Government* [2007] ECR I-00.

—. C-432/05 *Unibet (London) Ltd and Unibet (International) Ltd* v *Justitiekanslern*, [2007] ECR, I-02271.

—. C-303/05 *Advocaten voor de Wereld* v *Leden van de Ministerraad* [2007] ECR I-3633.

—. C-283/05 *ASML Netherlands BV* v *Semiconductor Industry Services GmbH (SEMIS)*, [2006] ECR I-12041.

—. C-341/04 *Eurofood* [2006] ECR I-3813.

—. C-459/03 *Commission* v *Ireland* (Dispute relating to the MOX plant at Sellafield, United Kingdom) [2006] ECR I-04635.

—. C-105/03 *Criminal proceedings against Maria Pupino* [2005] ECR 2005, I-05285.

—. C-423/98 *Alfredo Albore* [2000] ECR I-5965.

—. C-7/98 *Krombach* v *Bambersk*, [2000] ECR I-01935.

—. C-149/96 *Portugal* v *Council* OJ 2000 C 47/8.

—. C-69/89 *Nakajima All Precision* v *Council* [1991] ECR I-2069.
—. 265/87 *Schräder* v *Hauptzollamt Gronau* [1989] ECR 2237.
—. 70/87 *Fediol* v *Commission* [1989] ECR 1781.
—. 222/84 *Johnston* v *Chief Constable of the Royal Ulster Constabulary* [1986] ECR 1651.
—. 155/79 *AM&S* v *Commission*, [1982] ECR 1575.
—. 98/79 *Pecastaing* v *Belgium* [1980] 691.
—. 4/73 *Nold* v *Commission* [1974] ECR 491.
—. 11/70 *Inernationale Handelsgesellschaft mbH* v *Einfuhr und Vorratsstelle für Getreide und Futtermittel* [1970] ECR 1125
—. 29/69 *Erich Stauder* v *City of Ulm – Sozialamt* [1969] ECR 419.
Consolidated Rules of Procedure of the Court of Justice, OJ 2010 C177/5.
Consolidated Version of the Statute of the Court of Justice of the European Union, available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-10/staut_cons_en.pdf.
Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders, OJ 2000 L239/19.
Council of the EU: EU road map on procedural rights Roadmap with a view to fostering protection of suspected and accused persons in criminal proceedings, Brussels, 1 July 2009, 11457/09.
Craig, P. "The Human Rights Act, Article 6 and procedural rights." *Public Law* 2003, Win: 753-773.
De Bondt W. and Vermeulen, G. "The Procedural Rights Debate A Bridge Too Far or Still Not Far Enough?" (2010) 4 *EUCRIM (FREIBURG):* 163-167.
Directive 2016/1919/EU of the European Parliament of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ 2016 L297/1.
—. 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ 2013 L294/1.
—. 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support

and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ 2012 L315/57.
—. 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ 2012 L142/1.
—. 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ 2012 L26/1.
—. 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, OJ 2011 L308/27.
—. 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ 2010 L280/1.
Eckes, C. "EU Accession to the ECHR: Between Autonomy and Adaptation." (2013) 76(2) *MLR*: 254–285.
Editorial comments. "Preliminary rulings and the area of freedom, security and justice." (2007) *CMLRev* 44: 1-7.
Editorial Staff of the Maastricht Journal. "Recent legal developments; EU Accession to the ECHR – The Commission Proposal for Negotiating Directives," 17 MJ (2010): (2010).
European Court of Human Rights Annual Report 2012, available at www.echr.coe.int.
—. 2005, available at www.echr.coe.int.
European Parliament Fact Sheets, 2.1.1. Respect for fundamental rights in the EU – general development, available at http://www.europarl.europa.eu/factsheets/2_1_1_en.htm.
First working meeting of the CDDH informal working group on the accession of the European Union to the European Convention on Human Rights (CDDH-UE) with the European Commission; Extracts of relevant texts of the European Union on the accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms, Strasbourg, Tuesday 6 July (2.30 pm) – Wednesday 7 July 2010 (1.30 pm), 4.
Fletcher, M. "EU criminal justice: beyond Lisbon," in *Crime within the Area of Freedom, Security and Justice A European Public Order*, (eds.) C. Eckes and T. Konstadinides. Cambridge: Cambridge University Press, 2011, 10- 42.

Gibbs, A.H. *Constitutional Life and Europe's Area of Freedom, Security and Justice*. Farnham: Ashgate, 2011.

Gillan and Quinton v *UK* [2010] ECHR 28.

Groussot, X., Lock, T., and Pech, L. *EU Accession to the European Convention on Human Rights: a Legal Assessment of the Draft Accession Agreement of 14th October 2011*. Paris and Brussels: Robert Schuman Foundation, European issues no 218, 7th November 2011.

Guild, E. *The European Union after the Treaty of Lisbon Fundamental Rights and EU Citizenship*, Brussels: CEPS, 2010, available on-line at CEPS.eu.

—. "Crime and the EU's Constitutional future in the Area of Freedom Security and Justice". *European Law Journal*, 10, no 2: 220.

Heaney v *Ireland* (2001) 33 EHRR 12.

Herlin-Karnell, E. *The Constitutional dimension of European Criminal Law*. Oxford: Hart Publishing Ltd., 2012.

Hinarejos, A. "Law and order and internal security provisions in the Area of Freedom, Security and Justice: before and after Lisbon." In *Crime within the Area of Freedom, Security and Justice, A European Public Order*, eds. C. Eckes and T. Konstadinides. Cambridge: Cambridge University Press, 2011.

House of Lords European Union Committee, 30th Report of Session 2010–12, The European Union's Policy on Criminal Procedure, 26th April 2012, HL Paper 288.

—. The Treaty of Lisbon: An Impact Assessment 10th Report, 2007/8, HL Paper 62.

Joined Case C-402/05 and C-415/05 *Yassin Abdullah Kadi*, [2008] ECR I-06351.

Konstadinides, T. "The Europeanisation of extradition: how many light years away to mutual confidence?" In *Crime within the Area of Freedom, Security and Justice A European Public Order* eds. Eckes, C. and Konstadinides, T. Cambridge: Cambridge University Press, 2011, 192-223.

Lenaerts, K. "The contribution of the European Court of Justice to the area of freedom, security and justice." *I.C.L.Q.* 2010, 59(2): 255-301.

Lock T. "Walking on a tightrope: the Draft ECHR Accession Agreement and the autonomy of the EU legal order." *C.M.L.Rev.* 2011, 48(4): 1025-1054.

Luchtman, M. "Principles of European Criminal Law: Jurisdiction, Choice of Forum, and the Legality Principle in the Area of Freedom, Security, and Justice." *European Review of Private Law* 2-2012: 347-380.

Martinico, G. "Is the European Convention going to be 'supreme'? A comparative-constitutional overview of ECHR and EU law before national courts." E.J.I.L. 2012, 23(2): 401-424.

Martinico G. and Pollicino, O. *The Interaction between Europe's Legal Systems; Judicial Dialogue and the Creation of Supranational Laws*. Cheltenham: Edward Elgar 2010.

Matthews v *UK*, [1999] *ECHR* (Ser. A), 45.

Murphy, C., "The European Evidence Warrant: Mutual Recognition and Mutual (Dis) Trust?," in *Crime within the Area of Freedom, Security and Justice A European Public Order* (eds.) Eckes, C. and Konstadinides, T. Cambridge: Cambridge University Press, 2011, 224-248.

O'Meara, N. "'A More Secure Europe of Rights?' The European Court of Human Rights, the Court of Justice of the European Union and EU Accession to the ECHR," *German Law Journal* 12(10): 1813-1832.

Onuf, N. "Constructivism: A User's Manual", in *International Relations in a Constructed world*, eds. V. Kubálková, N. Onuf and P. Kowert. New York: M.E. Sharpe, 1998.

Opinion 2/13 (re ECHR) [2014] ECR 0000.

—. *1/94* (re WTO) [1994] ECR, I-05267.

Protocol (No 36) on Transitional Provisions attached to the post Lisbon TEU and TFEU.

—. (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and the United Kingdom.

—. (No 8) relating to Article 6(2) of the Treaty on European Union on the accession of the Union to the European Convention on the protection of Human Rights and Fundamental Freedoms.

Quinn v *Ireland* (App. No.36887/97), (2000).

Rafaraci, T., "The Right of Defence in EU Judicial Cooperation in Criminal Matters". In *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, ed. S. Ruggeri. New York: Springer, 2013.

S & Marper v *UK* [2008] ECHR 1581.

Sarmiento, D. "Who's afraid of the Charter? The court of Justice, national courts and the new framework of fundamental rights protection in Europe." (2013) *CMLRev* 50: 1267-1304.

Saunders v *United Kingdom*, (Application no. 19187/91) ECHR (1996).

Stockholm Programme - An open and secure Europe serving and protecting citizens, OJ 2010 C115/1.

Strengthening mutual trust in the European judicial area – A Green Paper on the application of EU criminal justice legislation in the field of detention, COM(2011) 327 final.

Treaty on the European Union.

Treaty on the Functioning of the European Union.

Tridimas, T. *The General Principles of EU Law* 2nd edn. Oxford University Press, 2006.

van Puyenbroeck L. and Vermeulen, G. "Towards minimum procedural guarantees for the defence in criminal proceedings in the EU," *International and Comparative Law Quarterly*, 60(4), (2011): 1017-1038.

Vocht, D.L.F. de & Spronken, T.N.B.M. "EU Policy to Guarantee Procedural Rights in Criminal Proceedings: 'Step by Step'", *North Carolina Journal of International Law and Commercial Regulation*, 37 (2011): 436-488.

White, S. "The EU's accession to the Convention on Human Rights; A new era of closer cooperation between the Council of Europe and the EU?" *New Journal of European Criminal Law*, 1(4), (2010): 433-446.

Woolf, Lord, *et al*., Review of the Working Methods of the European Court of Human Rights, December, 2005, CoE, available on the ECHR web site at http://www.echr.coe.int/Documents/2005_Lord_Woolf_working_methods_ENG.pdf.

Ziamou, T. "New process rights for citizens? The American tradition and the German legal perspective in procedural review of rulemaking", *Public Law* (1999), Win: 726-742.

CHAPTER THREE

CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: THE NEW FRONTIER OF EU INTERNAL SECURITY?

RAPHAEL BOSSONG

Introduction

Critical infrastructure protection (CIP) is an increasingly prominent component of security policy in advanced industrialised countries. The European Union, too, has sought a role in this area for nearly a decade. Beyond political rhetoric, however, little is currently known about the significance and impact of these efforts to expand the scope of the EU's internal security profile. EU critical infrastructure policy is made up of a variety of policy instruments, a growing body of legislative initiatives, financial incentives, and involves a wide variety of actors, institutions and networks. To capture this empirical complexity, this contribution presents a cross-cutting empirical survey from a governance perspective. The EU faced considerable obstacles to translate its ambitions for a comprehensive approach to critical infrastructure protection into practice. Furthermore, the governance of "classic" critical infrastructures, such as energy and transport networks, and of so-called critical information infrastructures, which can mean any major IT-based communication and control system, has developed in separate tracks at the EU level, even though those tracks are increasingly interlinked in practice. In sum, sector-specific binding regulation and considerable institutional capacity-building at the EU level, rather than innovative public-private partnerships and networking across policy fields, seem to remain the most effective, if conventional, approach to security governance in this area.

The practice of critical infrastructure protection (CIP) is, in principle, not a new idea, since conventional defence planning revolves around the protection of central communication, supply and production lines.[1] Similarly, the European integration project started out in the crucial economic sectors for war-fighting, i.e. coal and steel, quickly to be followed by nuclear power. The following decades of European integration could similarly be read as a project to modernise as well as to protect central economic sectors and infrastructures,[2] first in response to international competition, and later also to major technological risks.[3]

The explicit concept of CIP, however, developed in the mid-1990s, when globalisation, new terrorist attacks and the growing dependency on information technologies generated new threat perceptions.[4] The events of 9/11, a growing appreciation for causal complexity and environmental risks, an issue developed further by Carpenter in her chapter to this book, led to a further elaboration and diffusion of concerns across the OECD[5] world.[6] Thus, social and economic infrastructures of advanced industrialised countries are now regarded as highly vulnerable due to the:

- increasingly efficient use of resources or timing of production processes, which leads to "tight coupling"[7] and a lack of robustness,

[1] Collier, S. J. and Lakoff, A., "The Vulnerability of Vital Systems: How Critical Infrastructure Became a Security Problem" in *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security* ed. M. Dunn Cavelty (London: Routledge, 2008).
[2] Badenoch, A. and Fickers, A., *Materializing Europe infrastructures and the project of Europe*. (Basingstoke: Palgrave Macmillan, 2010).
[3] Beck, U., *Risikogesellschaft: Auf dem Weg in eine andere Moderne* (Frankfurt: Suhrkamp, 1986).
[4] Beckworth, D., 1999. Critical infrastructure protection: a new dimension of U.S. National Security Strategy. AWC Strategy Research Project 19990618 084, US Army War College, Bendrath, R., The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information & Security*, 7(1) (2001): 80-103.
[5] Organisation for Economic Cooperation and Development.
[6] Maurer, V. and Dunn, M., 2006. International CIIP Handbook 2006 Vol. II. Analyzing issues, challenges and prospects. Zürich, Center for Security Studies; World Economic Forum, 2012. Global Risks, Seventh Report. An initiative of the Risk Response Network. (Geneva: World Economic Forum, 2012).
[7] Perrow, C., *The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters*. (Princeton: Princeton University Press, 2007).

- ever growing economic and technological interdependence, which leads to unforeseen feedback effects and "systemic risks,"[8]
- reliance on networked information technologies that are used to manage industrial production and energy networks,[9] or increasingly all technological appliances and devices ("the internet of things"),
- the potential of terrorists, hackers and hostile regimes to exploit these vulnerabilities by "asymmetric" strategies (un-attributable attack, sabotage, "blackmail").

This explains why critical infrastructure protection is central to contemporary "risk governance."[10] Such risk governance needs to involve private actors, since public ownership of economic assets and infrastructures has declined steeply over the last two decades, while governmental actors are often unable to keep up with the speed of technological change, especially in the Information Technology (IT) sector. Yet one cannot simply speak of public-private partnerships in the field of CIP.[11] Public-private partnerships typically mean the profit-oriented delivery of public goods and services by private actors. CIP, in contrast, mostly requires "unproductive" investments, such as excess capacity for robustness, and is therefore more likely to be a burden on private actors. As such, mandatory regulation by public authorities, as in other areas of health and safety, is likely to be a central component of CIP policies. Nevertheless, the complexity and dynamism of the issue area also calls for positive incentives to stimulate the exchange of information, and to build capacities for joint risk management beyond individual firms and regulators.

---

[8] Cleeland, B., "Contributing Factors to the Emergence of Systemic Risks", *Technikfolgenabschätzung – Theorie und Praxis*, 20(3) (2011): 1-21.

[9] Orwat, C., Büscher, C. and Raabe, O., *Governance of Critical Infrastructures, Systemic Risks, and Dependable Software* (2010) Available at: http://pp.info.uni-karlsruhe.de/dsci/material/Governance.pdf.

[10] Renn, O., Klinke, A. and van Asselt, M., "Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis" *AMBIO: A Journal of the Human Environment*, 40(2) (2011): 231-246.

[11] Dunn-Cavelty, M. and Suter, M., "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection*, 2(4) (2009): 179-187; Koski, C., "Committed to Protection? Partnerships in Critical Infrastructure Protection," *Journal of Homeland Security and Emergency Management*, 8(1) (2011): 1-25.

Vulnerable critical infrastructures cut across state borders and different sectors of the economy generating further challenges. Information and energy networks illustrate such "transboundary" risks, whereby failure in one node of the network can spread at lightning speed to others. In such a scenario, jurisdictional conflicts, the sheer number of possible stakeholders and technical complexity add to the crisis dynamics.[12] In sum, conflicting interests or competences of public and private actors and obstacles to transboundary risk management partially explain why even the U.S., which pioneered the concept of CIP, has struggled to form a coherent and effective regime.[13]

Against this background, this contribution surveys and assesses the EU's efforts in this field. The EU appears fairly well-placed to address the regulatory challenges across borders and support technical capacity building.[14] Yet the initial ambitions to enact a comprehensive European Programme on Critical Infrastructure Protection[15] have not come to fruition, leaving the EU with a shallow regulatory framework and weak networks. In contrast, the area of critical information infrastructures, or Network Information Security and Cybersecurity, which are related EU terms, is still in a formative period. Here the EU has developed a significant role via regulation, network formation and the growth of the European Network and Information Security Agency (ENISA).[16]

Theoretical framework

Due to its empirical research interests, this chapter does not engage with the normative literature on the securitisation dynamics of critical

[12] Boin, A. and McConnell, A., "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience," *Journal of Contingencies and Crisis Management*, 15(1) (2007): 50-59.
[13] May, P. J., Jochim, M. and Sapotichne, J., "Constructing Homeland Security: An Anemic Policy Regime," *Policy Studies Journal*, 39(2) (2011): 285-307.
[14] House of Lords. *Protecting Europe against large-scale cyber-attacks*. European Union Committee 5th Report of Session 2009–10 (2010), 18. http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf.
[15] Commission, of the European Communities, 2006. Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final.
[16] See also Dewar's chapter 5 in this book.

infrastructures[17] or cyber threats.[18] Instead, the concept of "meta-governance,"[19] which has already been employed in the context of CIP,[20] is utilised to survey the EU's efforts. Meta-governance broadly denotes the "governance of governance," i.e. attempts by (public) actors to organise, stimulate or steer multiple forms of coordination among other (private) actors by means of direct, indirect and/or identity-forming practices.[21] Baker and Stoke[22] provided an encompassing, but more manageable, operationalisation of this broad meta-governance perspective. In their comparative analysis of different national governance regimes for nuclear power they apply the following four categories:

1. Authority denotes the degree of legislative control or regulatory competence by the governance actor under investigation. The term authority remains useful in so far as it foregrounds the issue of legitimacy or acceptance which needs to be constructed in absence of clear hierarchy.
2. Nodality may be defined by networks that have been stimulated or steered by the governing actor. While this category should ideally include various forms of informal networks or professional communities, this paper limits itself to formal groups that are related to EU policy-making.
3. Treasure denotes fungible assets that the governing actor can expend to influence the behaviour of others. In the context of the EU, which does not own assets, such as land, this is limited to budgetary resources and attached financial incentives.

---

[17] Burgess, P., "Social values and material threat: the European Programme for Critical Infrastructure Protection", *International Journal of Critical Infrastructures*, 3(3-4) (2007): 471-487; Aradau, C., "Security That Matters: Critical Infrastructure and Objects of Protection," *Security Dialogue*, 41(5) (2010): 491-514.

[18] Guinchard, A. "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy," *Journal of Strategic Security*, 4(2) (2011): 75-96.

[19] Sørensen, E. and Torfing, J., "Making the governance of networks effective and democratic through metagovernance," *Public Administration*, 87(2) (2009): 234-258.

[20] Dunn-Cavelty and Suter, "Public–Private Partnerships are no silver bullet."

[21] Crisis and Risk Network. *Focal Report 2. Critical Infrastructure Protection*. CRN Report 2009, http://www.css.ethz.ch/publications/pdfs/Focal-Report-2-CIP.pdf.

[22] Baker, K. and Stoker, G., "Metagovernance and Nuclear Power in Europe," *Journal of European Public Policy*, 19(7) (2012): 1026 –1051.

4. Capacity is understood as non-fungible organisational assets for achieving governance objectives, such as capacities for administration or other tasks (e.g. analysis, data collection). This mostly corresponds to institutionalisation (agency formation) and organisational growth or coordination within public bureaucracies.

Surveying the European Programme for Critical Infrastructure Protection

The above four categories structure the following survey and comparison of the EU's governance efforts for CIP and Critical Information Infrastructure Protection (CIIP).

Authority

Following the 2004 terrorist attacks in Madrid, the EU set itself the goal of developing a European Programme for Critical Infrastructure Protection (EPCIP).[23] Previously, the UK, Sweden, the Netherlands and Germany as well as NATO[24] and the G8[25] had taken up the notion of CIP. Information infrastructure security had already been discussed in various European fora since the turn of the millennium.[26] In particular, the notion of a single digital market, which could complement the EU's core competences, and a corresponding mechanism to safeguard e-commerce against cyber-risks and cyber-crime was envisaged.[27]

The London bombings in July 2005 could have been expected to add momentum to the first Commission green paper on critical infrastructure

---

[23] Commission, of the European Communities. *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, COM (2004)702 final, Council, of the European Union, 2004. *Brussels European Council. 16/17 December 2004. Presidency conclusions.* 16238/1/04 REV 1.

[24] North Atlantic Treaty Organisation.

[25] Abele-Wigert, I. and M. Dunn. International CIIP Handbook 2006, Center for Security Studies, Zurich: ETH, 2006, kms2.isn.ethz.ch/serviceengine/Files/.../CIIP_HB_06_Vol.1.pdf.

[26] Rathmell, A. *Building partnerships to protect Europe's critical information infrastructures*. Cambridge and Brussels: RAND Corporation, 2003, http://www.prgs.edu/content/dam/rand/pubs/papers/2008/P8063.pdf.

[27] Commission, of the European Communities. *Network and Information Security: proposal for a European Policy Approach*, COM(2001) 298 final.

protection.[28] But when moving from general concepts to more specific proposals, EU member states revealed their reluctance.[29] The initial link between CIP and the fight against terrorism was changed to an "all-hazards approach"[30] due to the divergent threat perceptions of member states. Moreover, member states emphasised that private owners remained mainly responsible for adequate security levels.[31] The EU added value would need to be limited to clearly defined cases of cross-border vulnerabilities of infrastructures. Arguments by the Commission to create a level playing field for European utility and infrastructure companies by harmonised security provisions were not taken up.

The very definition, scope and nature of critical infrastructures emerged as a serious stumbling block.[32] Early EU documents on CIP were forwarded to fourteen technical Council working groups, which adopted an approach which contrasted with the prevailing attitude of experts and industry representatives about the need to treat such security information in a highly confidential manner. This added to the technical and legal complexities when trying to design an overarching framework for several economic sectors. In the end, this led to a major scaling back of the proposal for a Directive on the Identification of European Critical Infrastructures (ECI), which would be limited to energy and transport infrastructures only. In these sectors cross-border effects were readily evident and the process could be organised among DG Home and the then integrated DG Energy and Transport, of the European Commission. Nevertheless, decision-making was held up by the problem of how to provide a workable yet flexible definition of ECIs, since their identification

[28] Commission, European. *Green paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final.
[29] Lindstroem, M., "The European Programme for Critical Infrastructure Protection", in *Crisis Management in the European Union. Cooperation in the Face of Emergencies*, ed. S. Olsson, (Stockholm: Springer. 2009), 37-60.
[30] Commission, of the European Communities. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM(2006) 786 final.
[31] Council, of the European Union. *Adoption of the Council Conclusions on a European Programme for Critical Infrastructure Protection* (2007). 7743/07.
[32] Pursiainen, C., "The Challenges for European Critical Infrastructure Protection," *Journal of European Integration*, 31(6) (2009): 724-5.

was the core objective of the directive. It was eventually formulated as follows:[33]

> (a) "critical infrastructure" now means an asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions - health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions;
> (b) "European critical infrastructure" or "ECI" now means critical infrastructure located in member states the disruption or destruction of which would have a significant impact on at least two member states. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

The key elements were the emphasis on the need to involve two member states and multiple forms for impact assessment. This left much room for interpretation on how to model the effects of infrastructure failure. Still, member states were required to identify potential ECIs in energy and transport within their borders, designate corresponding points of contact, and ensure the existence of suitable security and contingency plans. After a first implementation round taking four years, the member states would review the possible extension of the directive to other sectors.

This seemed like a pragmatic approach to bridge the gap between initial ambitions and the limited scope of the first ECI directive. Yet the exclusion of cyber-security and critical information infrastructures (CIIP) from the start of the process, despite the 2007 crisis in Estonia, which were often cited as the first large-scale cyber-attacks (denial of service), set the scene for the subsequent divergence of these two policy areas. By March 2009 the Commission brought out a new Commission communication on CIIP,[34] which mirrored the initial European Programme on Critical

[33] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 2008 L345/75, Article 2.
[34] Commission, of the European Communities. *Communication from the Commission to the Council and the European Parliament on Critical Information Infrastructure Protection Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM(2009) 149 final.

Infrastructure Protection.[35] The new communication sought to outline criteria for the identification of Critical Information Structures and set out strategic objectives for preventing and responding to cyber threats. Furthermore, it suggested the creation of a number of networks and organisational capacities that will be discussed further below.

So even though the reintegration with the ECI directive was formally possible, discussions soon went off on separate tracks. The 2010 revelation of the Stuxnet computer virus and a hacking attack on the European institutions in March 2011 underlined the salience of the threat. Later that year, the Commission,[36] the member states[37] as well as the European Parliament[38] all underlined the need to work on information infrastructures. By 2013 these discussions culminated in the publication of standalone cybersecurity strategy,[39] which aimed to develop the internal as well as global profile of the EU in this issue area. In particular, the strategy listed "cyber resilience," which largely coincides with the notion of CIIP, as the first of several strategic objectives.

Finally, the Commission[40] tabled a proposal for an extensive directive to "ensure a high common level of network and information security across the Union." The now commonly called NIS (network and information security) directive contains multiple obligations, such as the creation of so-called Computer Emergency Response Teams and the designation of a main responsible authority for cybersecurity in all member states. Moreover, it introduces a duty requiring private actors to notify public

---

[35] Commission, of the European Communities. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM(2006) 786 final.

[36] Commission, European. *Critical Information Infrastructure Protection. Achievements and next steps: towards global cyber-security*, COM(2011) 163 final.

[37] Presidency of the EU. *European Union Ministerial Conference on Critical Information Protection, Balatonfüred 14-15 April 2011*, http://www.eu2011.hu/files/bveu/documents/HU_CIIP_Conference_Presidency_Statement_final.pdf.

[38] Parliament, European. *Report on critical information infrastructure protection – achievements and next steps: towards global cyber-security*. 2011/2284(INI).

[39] EU, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN(2013) 1 final.

[40] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48.

authorities in cases of serious breaches of IT security, which could also be extended to other infrastructure sectors.

These obligations reflected the different level of member states' capacities to manage cyber-incidents, as only a handful of member states have, at the time of writing, set up such response teams. The duty to notify seeks to address the well-known structural problem in CIP to estimate the true extent of vulnerabilities, while private actors are reluctant to share information for fear of high financial and reputational costs. As the directive on network and information security remained controversial and technologically complex[41] it passed with a two year delay in July 2016. Already in September 2013 the EU had passed a directive[42] revising the 2005 Framework Directive criminalising attacks on information systems. This directive, though originally somewhat separate from CIP concerns, could be seen as supporting CIIP, not only by aiming to harmonise and sharpen criminal sanctions against hackers, but also by requiring member states to systematically collect data on cyber-attacks.

The 2008 ECI directive,[43] in contrast, was overtaken by discussions on critical information infrastructures and cybersecurity. A technical study in preparation of the planned Commission review of the ECI directive[44] highlighted numerous problems which remain unresolved.[45] The 2008 directive, which was adopted in all member states, has led to the

[41] Rand Europe. *Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts.* Study for European Parliament, Directorate-General for Internal Policies, Policy Department A: Economic and Scientific Policy EP-5039. Cambridge and Brussels: Rand Europe, 2013.

[42] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ 2013 L218/8.

[43] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*,* OJ 2008 L345/75.

[44] Commission, European, Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD (2012) 190.

[45] Booz & Company. *Study to support the preparation of the review of the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection.* Final Report (Draft) HOME/2011/CIPS/PR/001-A1. The study, which is referred to in the cited Commission working paper (2012) has not been published, but was made available to the author upon request.

identification of thirteen European critical infrastructures. However, it did not lead to notable changes in security practices and investments, as transport and energy infrastructures were already heavily regulated at national, European and global levels. The lack of on-site monitoring mechanisms for the ECI directive, as exist, for instance, in the case of EU aviation security, did not allow for independent assessments of operational security provisions.[46] The study revealed additional gaps and deficits in the designation of ECIs. For the first implementation period, national authorities drew on their previous assessment of national infrastructures to identify potential ECIs. This side-lined the potential input of private actors, and missed out on infrastructures that could not be assigned to a particular nation state, such as European aviation control systems.

A new Commission working document[47] accepted most of these criticisms, and moved away from the initially envisaged extension of the 2008 directive to further economic sectors. Instead, it was argued that the EU should focus on four European-wide infrastructures that had hitherto fallen through the net of national risk assessments, namely the European aviation control system EUROCONTROL, the satellite-based navigation system GALILEO, and transnational energy and gas transmission networks. These four infrastructures should be subjected to new risk analyses, leading to new risk prevention or mitigation activities, as well as provisions for their eventual breakdown. At the time of writing, these activities still have to take place, at least in so far as can be inferred from publicly accessible sources.

In summary, the initial objective for an integrated and authoritative EU framework for CIP policy could not be realised. Energy and transport policy were already strongly integrated in various sector-specific regulations, including those emanating from the EU, so that the additional framing of CIP would not bring an immediate benefit or be readily accepted. In contrast, CIIP policies took a higher profile from 2009 onwards, due to the pressure of events and overlapping agendas, such as

[46] The doubtful impact of the Directive was aggravated by lack of data or baselines, as various member states started independent policy initiatives on CIP between 2005 and 2012. Only Slovenia and Bulgaria cited EPCIP as a direct reference for the development of national policy frameworks.

[47] Commission Staff Working Document. *On a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure*, SWD(2013) 318 final.

the so-called Digital Agenda. Here further developments are to be expected, as is also elaborated in the following sections.

Nodality

The comparison of networks that could support or supplant regulatory activities presents a similar picture. The area of CIP or the European Programme of Critical Infrastructure Protection (EPCIP) is again discussed first before turning to activities in the area of CIIP.

Four different types of networks have been generated by the EPCIP: 1.) the network of national points of contact on European Critical Infrastructure Protection (ECIP PoC); 2.) the Critical Infrastructure Warning and Information Network (CIWIN); 3.) the European Reference Network – Critical Infrastructure Protection (ERN-CIP); 4.) and sector-specific networks by private actors.

National contact points have become a component of EU counterterrorism coordination since the 2004 Madrid terrorist attacks. This explains why the comparable ECIP network was set up in 2006, which has met with Commission representatives two to three times a year since then.[48] The evaluation report on the ECI directive maintained that most member states considered the contact points to be a useful trust building instrument.[49] However, the lack of further public information about the activities of the network and the aforementioned lack of momentum behind the ECI directive cast doubt over the political impact of this network.

The fate of the so-called CIWIN network, which is supposedly linked with the points of contact,[50] highlights further obstacles. The initial Commission concept for CIP[51] drew direct inspiration from the U.S., where the so-called CWIN network was set up in 2003 to minimise response times to

[48] Commission, of the European Communities. *Accompanying document to the Proposal for a Council Decision on creating a Critical Infrastructure Warning Information Network (CIWIN)*, COM(2008) 676 final, 7.

[49] Booz & Company. Study to support the preparation of the review of the Council Directive 2008/114/EC.

[50] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm.

[51] Commission, of the European Communities. *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, COM(2004)702 final.

infrastructure failures. CWIN should also collect information and allow for more accurate assessment of existing hazards and threats at the strategic level. Comparable warning and information networks were set up in some EU member states.[52] Yet at the EU level, member states and private actors highlighted serious concerns over the confidentiality of data when a related EU network (CIWIN) was proposed. They were not ready to accept more than a voluntary system for the exchange of best practices,[53] which undercut the main rationale for the creation of CIWIN, namely a reliable alert system. Consequently, a legislative proposal for CIWIN drifted into irrelevance and was withdrawn several years later.[54] The Commission instead recently created a CIWIN website on its own account, which emphasises the principles of voluntary participation and high standards for data protection.[55] It remains to be seen whether this voluntary initiative will attract a sufficient number of participants and can be relied upon as a warning mechanism.

Scientific exchanges were a less controversial issue, and could be stimulated with EU funds. In 2009 the Commission developed the idea for a "European Reference Network for CIP" (ERN-CIP), which would link laboratories and experimental facilities working on critical infrastructure vulnerabilities. According to official presentations, the number of ERN-CIP stakeholders is growing fast, and includes several thematic sub-groups beyond the energy and transport sectors covered by the EPCIP 2008 directive.[56] In addition, in autumn 2013 the Commission sponsored a large-scale research network that pursues similar activities for four years.[57]

The Thematic Network on Critical Energy Infrastructure Protection (TNCEIP), which is an off-shoot of the well-established and operationally active network of European energy providers and regulators (ENTSO-E), could be taken as evidence of the necessary public-private dialogues.

---

[52] See, for instance, http://www.warp.gov.uk/.

[53] Commission, European. *Green paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final, 14.

[54] EU. *Withdrawal of obsolete Commission Proposals* List of proposals withdrawn, OJ 2012 C156/10.

[55] https://ciwin.europa.eu/Pages/Home.aspx.

[56] Lewis, A., *The European Reference Network on Critical Infrastructure Protection,* (CIP Conference. 27-28 October 2011, Bucharest). The ERN-CIP network will be returned to below when discussing the institutional capacities of the EU, since it is linked to the EU Joint Research Centre.

[57] www.ciprnet.eu.

While ENTSO-E is a core partner in the formulation of EU energy policy, the activities of TNCEIP appear however, to be comparatively limited. To date it has consulted on an occasional basis with DG Energy and issued a statement on the ECI 2008 directive.[58] A related study funded by DG Energy explored the financial implications of CIP policies from the perspective of industry.[59] In short, interactions between private actors and the Commission appear limited and emphasise regulatory costs over common projects or genuine partnership.

When turning to the EU's governance efforts on CIIP, a parallel set of networks can be identified, i.e. professional, warning, research and public-private networks. To take them in order, networking between national computer emergency response teams (CERTs) has developed since 2006 onwards. At the time, a few member states had started to create such units, emulating the U.S. By 2012, a separate EU CERT was created,[60] while regular network activities and standardisation of procedures to coordinate the work of national CERTs were underway.[61] The web presence of the EU CERT further includes regular news items on cyber threats and vulnerabilities of various applications. Even though the EU CERT remains relatively small and is only available during regular office hours, falling short of a major investment in 24/7 IT security by the EU, this network favourably contrasts with the limited activities of the points of contact for CIP.

Second, the creation of a European Information Sharing and Alert System, which essentially mirrors the rationale of the CIWIN network, is foreseen. While the creation of the system has also been fraught with various technical and financial obstacles, it has received repeated support in pilot

[58] TNCEIP. *Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection* (2012). Available at: http://ec.europa.eu/energy/infrastructure/doc/20121114_tnceip_eupolicy_position_paper.pdf.

[59] Harnser Group. *The Financial Aspects of the Security of Assets and Infrastructure in the Energy Sector. A Set of Guidelines Prepared by the Harnser Group for the European Commission* (2012). ENER/B1/ETU/42-2011/SI2.611505.

[60] http://cert.europa.eu/cert/plainedition/en/cert_about.html. This will also be taken up further under section 3.4.

[61] For instance, one could point to frameworks for data sharing or best practice collection, see http://www.enisa.europa.eu/activities/cert/support/data-sharing, http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems.

studies and is, so far, expected to be rolled out in coming years.[62] If and when the directive on network and information security is adopted, one can expect a push to implement such an Information Sharing and Alert System, which should help to fulfil the statutory requirements for alerts and data collection on cyber-incidents.

Third, EU research support for network and information security is extensive. Since the 6th Framework Research Programme a dedicated administrative unit for "ICT Trust and Security Research" had been set up.[63] By 2011 the majority of research projects under the security theme, including those that were officially labelled under the wider framework of CIP, focused on ICT-based vulnerabilities or mechanisms of risk management. Yet these research activities were not more dispersed than the activities of the ERN-CIP network, which formally aims to support the development of technical standards and comparative specialisation of research centres.

Finally, network and information security has given rise to relatively high density of public-private consultations. The first platform is the so-called "European Public + Private Partnership for Resilience" (or E3PR) that had been mandated by the 2009 Communication on CIIP[64] and should stimulate more private efforts to increase IT security. At the time of writing, the E3PR format generated a number of thematic working and expert groups that should offer various options, standards and frameworks for private industry.[65] However, this open-ended and bottom-up approach, while laudable in the abstract, seems to have led to limited tangible results due to the diversity of stakeholders and possible avenues for action.[66]

---

[62] http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas.

[63] http://cordis.europa.eu/ist/trust-security/index.html.

[64] Commission, of the European Communities. *Communication from the Commission to the Council and the European Parliament on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*, COM(2009) 149 final.

[65] ENISA. *European Public+Private Partnership for Resilience*. *Activity Report* 2012, https://resilience.enisa.europa.eu/ep3r/2012-activity-report.

[66] Irion, K., "The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R)", in *The Secure Information Society*, eds. J. Krüger, B. Nickolay, and S. Gaycken, (Berlin: Springer, 2012): 83-116.

Therefore, the 2013 EU Cybersecurity Strategy[67] led to the creation of another public-private platform on "Network Information Security and Resilience."[68] By the end of 2013, this reformed platform had met for two major conferences, and was expected to provide specific policy recommendations to the Commission.[69]

In addition, private companies have already formed an additional "Alliance for Cyber Security"[70] and the EU-wide interest group of security companies, EOS, adds another platform on cybersecurity.[71] Nonetheless, the standalone impact of these networks and platforms is not readily evident, and are not likely to go beyond classic interest representations in legislative processes, and bidding for EU research money.

In summary, the EU has stimulated and created various networks in the area of CIP and CIIP, but these could, at best, play a supportive role in the field of research and non-urgent technical information exchange, rather than make up for a lack of central political authority by means of more horizontal and voluntary forms of coordination. As will be developed below, an institutional anchoring of such networks, as in the Joint Research Centre or ENISA is also necessary to sustain such networks.

Budget

While the EU's total financial budget is considerable, neither CIP nor CIIP have emerged as major and important funding objectives. With the exception of research, where comparatively small sums can be leveraged, the impact of EU governance efforts in this highly cost-intensive area is therefore strictly limited.

The EU financial perspective for 2008-2013 included a financial instrument for "the protection of citizens and critical infrastructures against terrorist

---

[67] Commission, European and High Representative of the European Union for Foreign Affairs and Security Policy, 2013. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final.
[68] https://resilience.enisa.europa.eu/nis-platform.
[69] http://ec.europa.eu/digital-agenda/en/news/second-meeting-network-and-information-security-nis-platform-plenary-0.
[70] www.ecns.eu.
[71] http://www.eos-eu.com/?page=cyber%20security%20menu.

attacks and other security-related incidents" (CIPS). The €140 million set aside for CIPS was intended to stimulate research activities, networking and standard-setting across member states. A mid-term review of CIPS highlighted limited results in this regard.[72] Most funds had been attracted by two member states and have been mainly spent on meetings, which have not translated into tangible project outcomes or EU-wide networks. The EU's seventh research framework (Framework Programme 7 (FP7), 2007-13) led to a simultaneous growth of scientific research on CIP. Fourteen pertinent projects added up to approximately €40 million of EU co-funding to national research efforts. As outlined above, in the area of information network security, the number of projects has been consistently much larger and, while difficult to aggregate due to the technical complexity and diversity of projects that are arranged under the theme of "Pervasive and Trustworthy Network and Service Infrastructures," running into several hundred million Euros.

As FP7 remained research-oriented rather than specification, or customer-driven, one can assume a positive contribution to scientific innovation, but leading to only rare instances when new security technologies or processes could be applied by public and private actors. This is also implicitly acknowledged by the next EU research framework programme (Horizon 2020), which, for better or for worse, prioritises industrial application and direct support to competitiveness.[73]

The EU financial perspective for 2014-20 leads to an increase of funding for security purposes. An "Internal Security Fund" has streamlined related funding instruments and provides approx. €560 million for the purposes of police cooperation, preventing and combating crime, and crisis management, which includes CIP.[74] This constitutes a notable increase in comparison to what preceded it, and could lead to further networking activities among public authorities and experts in this field. The sums, however, are clearly insufficient to directly stimulate security investments

[72] Commission, European. *Communication from the Commission to the European Parliament and the Council on the mid-term evaluation of the Framework Programme Security and Safeguarding Liberties (2007-2013)*, COM(2011) 318 final.
[73] Commission, European. *Security Industrial Policy. Action Plan for an innovative and competitive Security Industry*, SWD(2012) 233 final.
[74] Commission, European. *Building an open and secure Europe: the home affairs budget for 2014-2020*, COM(2011) 749 final.

in large and complex technological infrastructures, even if the funding was focused on the poorest and technologically disadvantaged member states.

DG Home officials[75] have therefore argued that CIP concerns should be reflected in investment criteria for the EU's regional cohesion funds. This line of reasoning was applied to the so-called "Connecting Europe Facility," which the Commission proposed as one of the largest items for the next funding period and could be mobilised for energy and transport projects. Yet during intense negotiations over the Multiannual Financial Framework between the European Parliament and the Council, the Connecting Europe Facility was drastically reduced from €50bn to €20bn, while the ongoing economic crisis put a premium on "conventional"' infrastructure projects rather than those with security objectives.

For the foreseeable future it would appear that the EU is not likely to make a significant difference to existing levels of CIP and CIIP at the national level via its financial instruments. This assessment could also be seen in the context of the discussions that emerged in the aftermath of the Snowden revelations on the surveillance activities of the U.S.'s National Security Agency (NSA). While the European Parliament sought a strong common European stance and condemnation of the US activities, the response of member states was only weakly, if at all, coordinated. Aside from diplomatic and security relations with the US, the debate on the need to construct a "European internet" to decrease the vulnerability of communications, never moved beyond initial stages. The required sums were far too high, especially in the context of the financial crisis, while the real security benefits remained unclear. Last, but not least, the existing stand-alone infrastructure projects that had been financed by the EU to increase their independence and competitiveness vis-à-vis the US, namely the European fusion reactor ITER and the satellite navigation system GALILEO, discussed above, have severely overrun their budgets, straining political relations, and have not led to quick results. All that may now be realistically expected at this time is a limited "hardening" of Community institutions and their communication networks, rather than large-scale and EU-wide investments in CIP or CIIP.

[75] Krassnig, C. *European Programme on Critical Infrastructure Protection (EPCIP). 1st international Workshop on Regional Critical infrastructures Protection Programmes.* 17-18 November 2011, Milan.

Capacity

There are some serious capacity issues at the EU level in this area. In contrast to a number of member states[76] the EU did not create a senior political unit, or designate a lead agency to coordinate CIP activities. Only a few EU Commission officials housed within the Unit on Terrorism and Crisis Management at DG Home were responsible for the original European Programme on Critical Infrastructure Protection. This meagre human resource base explains the reliance of DG Home on external management consultants, and external actors, in the design and review of the ECI directive. Institutional deficits are aggravated by the fact that there is no clear counterpart in the working groups of the Council of Ministers, which remain separated by sectors or thematic ministerial councils. The only official institutional EU platform has been the so-called "Sub-group on Critical Infrastructure Protection on the Inter-Service Group on the Internal Aspects of Terrorism," which includes 16 Commission directorates and Commission services, mainly communicating by email.[77] It is this author's view that such a forum may, at best, manage possible competence disputes, but cannot provide a coherent political leadership, driving change and building capacity.

However, the Commission's Joint Research Centre (JRC) maintains a genuinely cross-sectoral approach in this field.[78] The so-called Institute for the Protection of the Citizen within the JRC formed a task force[79] to support the designation of infrastructures as required by the ECI directive, in a manner comparable to the JRC's historical mission in support of nuclear technology.[80] Aside from a series of workshops and exercises,[81] its main contribution to date has been the formation of the ERN-CIP network mentioned above. The considerable investment of the JRC into ERN-CIP comprises twelve research officers and a multifunctional IT network.[82]

---

[76] Abele-Wigert and Dunn. *International CIIP Handbook* 2006.

[77] Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN), COM/2008/0676 final.

[78] http://sta.jrc.ec.europa.eu/index.php/cip-home.

[79] Heimans, D., *Critical Infrastructure Protection. Recent EU developments.* London, Royal Institute of International Affairs, 2009, http://rusi.org/downloads/assets/Dick_Heimans_-_European_Commission.pdf.

[80] http://ec.europa.eu/dgs/jrc/index.cfm?id=2260.

[81] JRC. *Risk Assessment and Resilience for Critical Infrastructures. Workshop Proceedings* 25-26 April 2012. JRC71923.

[82] http://ipsc.jrc.ec.europa.eu/?id=775.

The JRC can thus support technological exchanges, but should not be compared with the stand-alone regulatory agencies which proliferate across other EU policy fields.

One of the most important developments in EU CIIP policy has been the growth and consolidation of the European Network and Information Security Agency (ENISA).[83] ENISA was created on a temporary basis, and with limited means, in 2004, while its politically motivated location on Crete, Greece, cast doubt over the real commitment of the EU to CIIP.[84] Yet over time ENISA has managed to establish its authority, particularly with regard to those member states that do not boast strong national agencies and competences on IT security. It generated a large volume of conceptual papers and hosted various workshops and expert meetings on cybersecurity, including with private industry. ENISA also serves as host of the EU Computer Emergency Response Teams (EU CERT), and coordinates various dialogues with private industry (E3PR), which were already referred to above. While cybersecurity is defined in a wide sense in all these study and network activities, the protection of critical information infrastructures is still presented as the first objective of ENISA. This is illustrated by the recent report on the interdependence of modern or "smart" energy grids with ICT infrastructures.[85]

Importantly, ENISA has coordinated numerous Information and Communications Technology (ICT) incident exercises for EU member states ever since 2010. These exercises were called for by Commission and Council conclusions in 2009 in the aftermath of the Estonian cyber-attacks, with NATO undertaking similar military led exercises in response. Assessments of these exercises are limited to official documents, where the large number of participants (500+) and the positive resonance had been praised,[86] but there is little reason to doubt the overall use and

[83] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance), OJ 2013 L165/41.
[84] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ 2004 L77/1
[85] ENISA. Smart Grid Threat Landscape and Good Practice Guide. 2013, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/smart-grid-threat-landscape-and-good-practice-guide.
[86] ENISA. *Cyber Europe 2012. Key Findings and Recommendations*.

successful conduct of the exercises. The 2014 pan-European exercise, for instance, fulfilled the ambition of the 2009 Communication on CIIP, which argued that "regular exercises for large scale network security incident response and disaster recovery" should be organised.[87] For a further discussion on the role of NATO, and cybersecurity more generally, see Dewar's chapter 5 in this book.

ENISA is well on track to becoming the central authoritative EU-level agency, which addresses a widely perceived need of public actors to become more active on IT security. In 2013, ENISA was given an expanded and permanent legal basis under Regulation (EU) No 526/2013.[88] It also opened an additional office in Athens, which partially addressed the perceived marginal position of the main agency located on the island of Crete. Since then, ENISA has also taken on a greater role in the monitoring and development of EU regulatory frameworks discussed above, especially with regard to the 2016 NIS directive, and develop structural links to the new cybercrime centre of Europol.[89] The current director of ENISA previously served as the head of the equivalent German agency for the security of information technology, which signals the growing political significance of ENISA. ENISA's possible role as a standard-setting body could, for instance, also be illustrated the recent completion of Standard Operation Procedures during cyber crises, which will cover all EU and European Free Trade Association (EFTA)[90] member states.[91]

Further research needs to investigate this relatively new, or hitherto unnoticed, player in EU internal security. Aside from the positive

---

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1.

[87] Commission, of the European Communities. Communication from the Commission to the Council and the European Parliament on Critical Information Infrastructure Protection *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, (2009)10.

[88] Regulation (EU) No 526/2013.

[89] The Europol Cybercrime Centre cannot be discussed in the context of this contribution, but underlines the increasing accent and perceived niche or "added value" of an increased EU role in this area.

[90] Norway, Iceland, Switzerland and Liechtenstein.

[91] http://www.enisa.europa.eu/media/press-releases/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa.

developments outlined here one may critically investigate the control mechanisms of the agency, as well as its overall size and means, in comparison to the size of potential challenges in the area of cyber threats. It is sufficient to allude once again to the NSA crises, and lack of willingness of EU member states to invest more substantial sums in more independent information infrastructures, while some national security services, in particular the UK's Government Communications Head Quarters (GCHQ) are clearly far more advanced and capable than any nascent EU organisation, or even most national agencies specialising in network and information security.

Conclusions

The EU has followed the wider trend of Western societies in treating critical infrastructure protection, and especially critical information infrastructure protection, as a rising security concern. Spurred on by terrorist attacks and various cyber events between 2004 and 2010, one could point to a growing body of comprehensive action programmes, networks and governance instruments in these areas, which demonstrate the expanding scope and ambition of EU internal security policy.

However, the EU has suffered from a considerable gap between its initial ambitions and eventual actions, especially in the case of more "conventional" critical infrastructure protection. As outlined at the beginning of this chapter, it is necessary to have realistic expectations of the level of trans-boundary cooperation that can be expected among public and private actors, and across different economic sectors. This is not only another case of the familiar "rhetoric-reality" gap in EU security policy. States are equally searching for additional and supposedly more effective strategies, as is reflected in the growing discourse on the need to stimulate "resilience" in a decentralised, bottom-up manner.

Beyond such general critiques, the main object of this chapter has been to analyse more specific strengths and weaknesses of the EU's approach on the basis of the meta-governance framework. The following main trends can be identified. First, authoritative EU regulation has been more difficult to enact than expected, but is expanding in the area of cyber- and critical information infrastructure protection. The main objective of this regulatory framework is to address structural disincentives to cooperation, for example the duty to notify, and mandatory security investments, while the penal sanctions for "attacks against information systems" are on a path of

upward harmonisation. In contrast, the further development of the Directive on the Identification of European Critical Infrastructures has not been realised, and further legislative actions on CIP are likely to remain fragmented across the relevant economic sectors.

Second, the weakness of the European Programme of Critical Infrastructure Protection and the comparable dynamism of related instruments for CIIP apply to almost all dimensions of the meta-governance framework, namely the role of networks, financial resources, and EU-level institutional capacities. In other words, there is no compensation for a lack of regulatory competence by means of other and softer governance mechanisms.

Furthermore, voluntary consultation forums with private actors, or scientific and professional networks, will remain weak and ineffective if there continues to be no firm institutional anchoring, and without the necessary substantial financial resources being made available. Those limited successes to date of the EU in the area of CIP are mainly due to the use of research funds under (earlier EU) FP7 research funding programme, and the support from a dedicated team on the Joint Research Centre. In the area of CIIP, research funding and in particular the dynamic development of ENISA have been critical.

The case of ENISA demonstrates again that the EU is good at incremental institutionalisation, assuming that there is a nucleus to start with. The absence of a comparable institution or major unit within the Commission that could guide and promote CIP policy beyond the initial conceptual papers provides the matching counter-example. While a new "critical infrastructure" coordinator or similar post is not likely, there clearly is a need for institutional reform if CIP is to remain a meaningful policy objective of the EU. For instance, it is not clear who should conduct or coordinate the required analysis of the protection of transnational European infrastructures, in particular those which were missed out in the first round of the operation of the ECI directive, in particular GALILEO and EUROCONTROL, with some core energy and transport corridors still remaining to be covered. Equally external consultancies, which conducted the first review of the ECI directive, are clearly only a temporary solution.

Last but not least, the EU has treated neither CIP nor CIIP as a financial priority. Even within the expanded Internal Security Fund, under 2014-2020 EU financial perspective, CIP issues have remained a minor concern. Ideas about linking CIP-related criteria to investments under an umbrella

of regional funds or other large EU financial instruments may receive renewed attention, once the economic crisis recedes. Compared to the overheated debate on "cyberwars" in the US, however, one could also welcome the relative restraint of the EU. Aside from further support to ENISA, continued EU research money are a minimal and necessary commitment to move from speculative threat scenarios to realistic assessments of infrastructure vulnerability.

In summary, the scope and content of the EU's internal security policy is in flux, whereas policy-making and implementation is faced with many familiar obstacles, such as the acceptance of binding regulation, the use of voluntary networks, the appropriation of funds, and the construction of dedicated institutional capacities. The development of CIP and CIIP, therefore, do not a constitute paradigm shift in EU security policy, even if there may be a need for a comparatively higher involvement of private actors. Furthermore, and when compared to issues such as border security or the fight against organised crime, CIP and CIIP are not truly salient or dominant concerns of EU decision-makers. Nevertheless, scholars of EU security must expand their knowledge to these areas, if only to engage with the debate on the potential securitisation of evermore aspects of social and economic life.

Bibliography

Abele-Wigert, I. and M. Dunn. *International CIIP Handbook 2006.* Zurich: ETH, 2006.

Aradau, C., "Security That Matters: Critical Infrastructure and Objects of Protection." *Security Dialogue*, 41(5) (2010): 491-514.

Badenoch, A. and Fickers, A. *Materializing Europe infrastructures and the project of Europe*. Basingstoke, Palgrave Macmillan, 2010.

Baker, K. and Stoker, G. "Metagovernance and Nuclear Power in Europe." *Journal of European Public Policy,* 19(7) (2012): 1026 –1051.

Beck, U. *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt, Suhrkamp, 1986.

Beckworth, D. *Critical infrastructure protection: a new dimension of U.S. National Security Strategy*. AWC Strategy Research Project 19990618 084, US Army War College, 1999.

Bendrath, R. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." *Information & Security*, 7(1) (2001): 80-103.

Boin, A. and McConnell, A. "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience." *Journal of Contingencies and Crisis Management,* 15(1) (2007): 50-59.

Booz & Company. *Study to support the preparation of the review of the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection.* Final Report (2011) (Draft) HOME/2011/CIPS/PR/001-A1.

Burgess, P. "Social values and material threat: the European Programme for Critical Infrastructure Protection." *International Journal of Critical Infrastructures,* 3(3-4) (2007): 471-487.

Cleeland, B. "Contributing Factors to the Emergence of Systemic Risks." *Technikfolgenabschätzung – Theorie und Praxis*, 20(3) (2011): 1-21.

Collier, S. J. and Lakoff, A. "The Vulnerability of Vital Systems: How Critical Infrastructure" Became a Security Problem. In: Dunn Cavelty, M. ed. *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security*. London, Routledge, 2008.

Commission, of the European Communities. Communication from the Commission to the Council and the European Parliament on Critical Information Infrastructure Protection *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM(2009) 149 final.

—. *Accompanying document to the Proposal for a Council Decision on creating a Critical Infrastructure Warning Information Network (CIWIN)*, COM(2008) 676 final.

—. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM(2006) 786 final.

—. *Green paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final.

—. Communication from the Commission to the Council and the European Parliament - *Critical Infrastructure Protection in the fight against terrorism*, COM(2004)702 final.

—. *Network and Information Security: proposal for a European Policy Approach*, COM(2001) 298 final.

—. *Moving towards improved protection. Energy and transport infrastructure in Europe*. MEMO, DG Energy and Transport, http://ec.europa.eu/energy/infrastructure/doc/critical/2006_12_15_critical_infrastructures_memo.pdf.

European Commission. *Commission Staff Working Document. On a new approach to the European Programme for Critical Infrastructure*

Protection. Making European Critical Infrastructures more secure, SWD(2013) 318 final.

—. *Security Industrial Policy. Action Plan for an innovative and competitive Security Industry*, SWD(2012) 233 final.

—. *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)*, SWD(2012) 190.

—. *Building an open and secure Europe: the home affairs budget for 2014-2020*, COM(2011) 749 final.

—. *Communication from the Commission to the European Parliament and the Council on the mid-term evaluation of the Framework Programme Security and Safeguarding Liberties (2007-2013)*, COM(2011)318 final.

—. *Critical Information Infrastructure Protection. Achievements and next steps: towards global cyber-security*, COM(2011) 163 final.

Commission, European and High Representative of the European Union for Foreign Affairs and Security Policy, 2013. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 2008 L345/75.

Council, of the European Union, *Adoption of the Council Conclusions on a European Programme for Critical Infrastructure Protection* (2007). 7743/07.

—. 2004. *Brussels European Council. 16/17 December 2004. Presidency conclusions*. 16238/1/04 REV 1.

Crisis and Risk Network, 2009. F*ocal Report 2. Critical Infrastructure Protection. CRN Report*, http://www.css.ethz.ch/publications/pdfs/Focal-Report-2-CIP.pdf.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ 2013 L218/8.

Dunn-Cavelty, M. and Suter, M. “Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection.” *International Journal of Critical Infrastructure Protection,* 2(4) (2009): 179-187.

ENISA. *Smart Grid Threat Landscape and Good Practice Guide* (2013),

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/smart-grid-threat-landscape-and-good-practice-guide.

—. *European Public+Private Partnership for Resilience*. *Activity Report* 2012, https://resilience.enisa.europa.eu/ep3r/2012-activity-report.

—. *Cyber Europe 2012. Key Findings and Recommendations* (2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1.

EU. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final.

—. *Withdrawal of obsolete Commission Proposals* List of proposals withdrawn, OJ 2012 C156/10.

Guinchard, A. Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy. *Journal of Strategic Security,* 4(2) (2011): 75-96.

Harnser Group. *The Financial Aspects of the Security of Assets and Infrastructure in the Energy Sector. A Set of Guidelines Prepared by the Harnser Group for the European Commission* (2012). ENER/B1/ETU/42-2011/SI2.611505.

Heimans, D. *Critical Infrastructure Protection. Recent EU developments.* London, Royal Institute of International Affairs, 2009, http://rusi.org/downloads/assets/Dick_Heimans_-_European_Commission.pdf.

House of Lords. *Protecting Europe against large-scale cyber-attacks. European Union Committee 5th Report of Session 2009–10* (2010), http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf.

Institute for the Protection and Security of the Citizen. *ERNCIP newsletter 2*. (2012), http://ipsc.jrc.ec.europa.eu/fileadmin/repository/sta/cinet/docs/erncip/ERNCIPnewsletter-No2.pdf.

Irion, K. "The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R)." In: *The Secure Information Society*. Eds. J. Krüger, B. Nickolay, S. Gaycken. Berlin: Springer, 2012.

JRC. *Risk Assessment and Resilience for Critical Infrastructures*. Workshop Proceedings 25-26 April 2012. JRC71923.

Koski, C. Committed to Protection? Partnerships in Critical Infrastructure Protection. *Journal of Homeland Security and Emergency Management,* 8(1) (2011): 1-25.

Krassnig, C. *European Programme on Critical Infrastructure Protection (EPCIP).* 1st international Workshop on Regional Critical infrastructures Protection Programmes. 17-18 November 2011, Milan.

Lewis, A. *The European Reference Network on Critical Infrastructure Protection*. CIP Conference. 27-28 October 2011, Bucharest

Lindstroem, M. "The European Programme for Critical Infrastructure Protection." In Olsson, S., ed. *Crisis Management in the European Union. Cooperation in the Face of Emergencies*. Stockholm, Springer, 2009.

Maurer, V. and Dunn, M. *International CIIP Handbook 2006 Vol.II. Analyzing issues, challenges and prospects.* Zürich, Center for Security Studies, 2006.

May, P. J., Jochim, M. and Sapotichne, J. "Constructing Homeland Security: An Anemic Policy Regime." *Policy Studies Journal,* 39(2) (2011): 285-307.

Orwat, C., Büscher, C. and Raabe, O., 2010. *Governance of Critical Infrastructures, Systemic Risks, and Dependable Software.* http://pp.info.uni-karlsruhe.de/dsci/material/Governance.pdf.

Parliament, European. *Report on critical information infrastructure protection – achievements and next steps: towards global cyber-security*. 2011/2284(INI).

Perrow, C. *The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton, Princeton University Press, 2007.

Presidency of the EU. *European Union Ministerial Conference on Critical Information Information Protection, Balatonfüred 14-15 April 2011*, http://www.eu2011.hu/files/bveu/documents/HU_CIIP_Conference_Presidency_Statement_final.pdf.

Proposal for a a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48.

—.Council Decision on a Critical Infrastructure Warning Information Network (CIWIN), COM/2008/0676 final.

Pursiainen, C. "The Challenges for European Critical Infrastructure Protection." *Journal of European Integration,* 31(6) (2009): 721-739.

Rand Europe. *Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts*. Study for European Parliament, Directorate-General for Internal Policies, Policy

Department A: Economic and Scientific Policy EP-50395, Cambridge and Brussels: Rand Europe, 2013.

Rathmell, A. *Building partnerships to protect Europe's critical information infrastructures*. Cambridge and Brussels: Rand Corporation, 2013, at: http://www.prgs.edu/content/dam/rand/pubs/papers/2008/P8063.pdf.

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance), OJ 2013 L165/41.

—. (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ 2004 L77/1.

Renn, O., Klinke, A. and van Asselt, M. Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis. *AMBIO: A Journal of the Human Environment*, 40(2) (2011): 231-246.

Sørensen, E. and Torfing, J. "Making the governance of networks effective and democratic through metagovernance," *Public Administration*, 87(2) (2009): 234-258.

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final.

TNCEIP, 2012. *Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection*, http://ec.europa.eu/energy/infrastructure/doc/20121114_tnceip_eupolicy_position_paper.pdf.

World Economic Forum. *Global Risks 2012. Seventh Report. An initiative of the Risk Response Network*. Geneva, World Economic Forum.

NEW SECURITY CHALLENGES

CHAPTER FOUR

RATIONALISING HUMAN RIGHTS VIOLATIONS IN IMMIGRATION ENFORCEMENT: THE CASE OF GREEK SECURITY PROFESSIONALS

DIMITRIS SKLEPARIS

Introduction

The links between migration and security in Greece started to form in the early 1990s, once the country became an immigration host.[1] Indeed, "[t]he result [of migration to Greece was] [...] the creation of a ubiquitous 'moral panic' [...] among the public, the media, and very importantly the police."[2] These flows were comprised of people from former socialist countries in Eastern Europe and the Balkans, for whom Greece was a final destination. In the early part of the 21st century, Greece also became a transit country for undocumented migrants coming mainly from Asia and Africa. Their final destination is usually in Central, Western and Northern Europe. However, due to the Dublin II regulation[3] and the intensification of

[1] Karyotis, G. "Securitization of Migration in Greece: Process, Motives, and Implications," *International Political Sociology* 6, no. 4 (2012): 390-408; Karyotis, G. and Patrikios, S. "Religion, Securitization and Anti-Immigration Attitudes: The Case of Greece," *Journal of Peace Research* 47, no. 1 (2010): 43-57; Swarts, J. and Karakatsanis, N. M. "The Securitization of Migration: Greece in the 1990s," *Journal of Balkan and Near Eastern Studies* 14, no. 1 (2012): 33-51; Swarts, J. and Karakatsanis, N. M. "Challenges to Desecuritizing Migration in Greece," *Journal of Balkan and Near Eastern Studies* 15, no. 1 (2013): 97-120.

[2] Antonopoulos, G. A. "The Limitations of Official Statistics in Relation to the Criminality of Migrants in Greece," *Police Practice and Research* 6, no. 3 (2005), 251.

[3] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for

internal EU border controls they became trapped in Greece, a country which faces an important challenge regarding irregular migration, as its borders are almost all external borders of the EU, except for the Greek-Bulgarian one.[4] These relatively new flows from Turkey to Greece have significantly increased since 2007.[5] Thus, because of its geographic location and international obligations, Greece plays an important role in the EU's Internal Security Strategy[6] and in the external dimension of EU's migration policy.[7]

In this respect, Greece undertook various measures to enhance its external border control, such as establishing the border guard force in 1998, signing bilateral readmission and police cooperation agreements with a number of countries[8] and cooperating closely with Frontex, among others. Yet, in general terms, the state's reaction to the influx of migrants has been characterised by unpreparedness, inconsistencies and short-termism.[9] It is within this context that human rights violations in immigration enforcement

---

examining an asylum application lodged in one of the Member States by a third-country national, OJ 2003 L50/1, now replaced by Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), OJ 2013 L180/31.

[4] Triandafyllidou, A., Maroufof, M. and Nikolova, M. "Greece: Immigration Towards Greece at the Eve of the 21st Century. A Critical Assessment," *Athens: ELIAMEP IDEAS Working Paper* 4 (2009), 46.

[5] IOM, *Migration in Greece: a country profile 2008* (Geneva: International Organization for Migration, 2009), 40.

[6] Council Document, *Internal Security Strategy for the European Union: Towards a European Security Model*, 5842/2/2010.

[7] Geddes, A. and Lazarou, E. *Europeanization of Migration Policy and Narratives of Migration Management: The case of Greece*, Sussex: Paper presented at EPRC Workshop Narratives of Migration Management and Cooperation Sussex Centre for Migration Research, University of Sussex (2008).

[8] Bosnia and Herzegovina (3547/2007), Bulgaria (2406/1996), Croatia (2350/1995), France (2917/2001), Hungary (3321/2005), Italy (2857/2000), Latvia (2861/2000), Lithuania (2911/2001), Poland (2384/1996), Romania (2301/1995), Slovenia (2353/1995), Switzerland (3726/2008), and Turkey (3030/2002).

[9] Karyotis, *Securitization*; Triandafyllidou, A. "Greek Immigration Policy at the Turn of the 21st Century. Lack of Political Will or Purposeful Mismanagement?" *European Journal of Migration and Law* 11, no. 2 (2009): 159-178; Triandafyllidou, A., Dimitriadi, A., Maroufof, M., Hatziprokopiou, P., Gemi, E., Nikolova, M., and Yousef, K. *Migration in Greece: People, Policies and Practices* (Athens: ELIAMEP and EUI, 2013).

in Greece emerge. The detrimental impact of the "migration-security nexus" for migrants in Greece is not in question.[10] In this respect, Greece has lost a number of European Court of Human Rights cases with regard to its treatment of migrants.[11] A broad non-academic literature produced by human rights Non-Governmental Organisations (NGOs) and Intergovernmental Organisations (IGOs) has examined the effects of this "nexus" on migrants, refugees and asylum seekers by extensively documenting the unfair deterrence, apprehension and detention practices of the Hellenic Police and Coast Guard.[12]

---

[10] Karyotis, G. and Skleparis, D. "Qui Bono? The Winners and Losers of Securitising Migration," *Griffith Law Review* 22, no. 3 (2013); Karyotis, G. and Skleparis, D. "Migrant Mobilisation during the Economic Crisis: Identity Formation and Dilemmas," in *Remapping "Crisis": A Guide to Athens*, eds. M. Tsilimpounidi, and A. Walsh, (London: Zero Books, 2013); Lazaridis, G. and Skleparis, D. "Securitization of migration and the far right: the case of Greek security professionals," International Migration 54, no. 2 (2016); Skleparis, D. "(In)securitization and illiberal practices on the fringe of the EU," *European Security* 25, no. 1 (2016).

[11] Recent cases include *SD* v *Greece* (53541/2007, 11.6.2009), *Tabesh* v *Greece* (8256/2007, 26.11.2009), *AA* v *Greece* (12186/2008, 22.7.2010), *RU* v *Greece* (2237/2008, 7.6.2011), *Rahimi* v *Greece* (8687/2008, 4.7.2011), *Grand Chamber MSS* v *Belgium and Greece* (30696/2009, 21.1.2011).

[12] *E.g.* CPT, *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 20 to 27 February 2007* (Strasbourg: Council of Europe, 2008); CPT, *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 23 to 29 September 2008* (Strasbourg: Council of Europe, 2009); CPT, *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 17 to 29 September 2009* (Strasbourg: Council of Europe, 2010); CPT, *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 19 to 27 January 2011* (Strasbourg: Council of Europe, 2012); FRA, *Coping with a Fundamental Rights Emergency: The Situation of Persons Crossing the Greek Land Border in an Irregular Manner* (Vienna: European Union Agency for Fundamental Rights, 2011); HRW, *Stuck in a revolving door: Iraqis and other asylum seekers and migrants at the Greece/Turkey entrance to the European Union* (New York: Human Rights Watch, 2008); HRW, *No refuge: migrants in Greece* (New York: Human Rights Watch, 2009); HRW, *Unwelcome Guests: Greek Police abuses of migrants in Athens* (New York: Human Rights Watch, 2013); Pro Asyl, *The truth may be bitter, but it must be told* (Frankfurt: Friends of Pro Asyl, 2007); Pro Asyl,

The UN High Commissioner for Refugees (UNHCR) has described the situation for asylum seekers and migrants in Greece as a "humanitarian crisis."[13] A recent report by Human Rights Watch (HRW) criticises specific practices implemented under the "Xenios Zeus" operation, which in August 2012 became the main internal migration control measure, enforced by the Hellenic Police.[14] The report states that the "lengthy and intrusive procedure" of "stop and search" identity checks "amounts to arbitrary and discriminatory deprivation of liberty"[15] and is unlawful, as it discriminates against people based on their physical characteristics, ethnic and racial profile.[16] Body pat-downs, bag searches, disrespectful treatment, rude, insulting and threatening behaviour, even physical violence are described as routine.[17] In the same manner, external border control practices, such as interceptions and systematic push-backs by the Hellenic Police and Coast Guard have been widely criticised for violating the principle of *non-refoulement*.[18] Moreover, the detention facilities of migrants, particularly in Evros, near Greece's northern land borders, are characterised as "grim" and equated with "medieval dungeons."[19] Overcrowding, poor hygiene, sporadic violence and lack of access to legal aid, information and translators, make the facilities "synonymous with brutality, despair and dehumanisation."[20]

The situation is out of control (Frankfurt: Friends of Pro Asyl, 2008); Pro Asyl, *Walls of Shame: Accounts from the inside* (Frankfurt: Friends of Pro Asyl, 2012); Pro Asyl, *Pushed back: systematic human rights violations against refugees in the Aegean Sea and at the Greek-Turkish land border* (Frankfurt: Friends of Pro Asyl, 2013).

[13] "UNHCR says asylum situation in Greece is 'a humanitarian crisis'", *UNHCR Briefing Notes*, 21 September 2010, available at http://www.unhcr.org/4c98a0ac9.html (last visited 28 January 2014).

[14] HRW, *Unwelcome*.

[15] Ibid, 2.

[16] Ibid, 3, 5.

[17] Ibid, 4.

[18] See UNHCR, *Observations on Greece as a country of asylum* (Geneva: Office of the United Nations High Commissioner for Refugees, 2009); Amnesty International, *Frontier Europe: Human Rights Abuses on Greece's Border with Turkey* (London: Amnesty International, International Secretariat, United Kingdom, 2013); Pro Asyl, *Pushed*.

[19] Hellenic League for Human Rights, *Report about the detention facilities of undocumented migrants in Rodopi and Evros* (Athens: Hellenic League for Human Rights, 2009), 10.

[20] Pro Asyl, *Pushed*, 3.

However, these unfair internal/external control and detention practices have been largely treated by NGOs and IGOs as isolated cases despite their frequent occurrence, which has been mainly blamed on the lack of resources, infrastructure and education in human rights, and on bureaucratic deficiencies.[21] In contrast, this chapter argues that the repetition of illicit practices by Greek security professionals derives to a great extent from deeply embedded negative attitudes towards various key issues related to migration in their field.

In this respect, twenty interviews with Greek security professionals in Athens, Lesvos, Orestiada and Alexandroupoli in 2012 and the discourse of eleven master's dissertations[22] produced by high-ranking officers during their study at the School of National Security and the Hellenic National Defence College - which train elite security professionals - was analysed. The views expressed in this sample definitely do not reflect the opinions of all Greek security professionals. Yet, they do manifest a particular and quite widespread ethos among them, which was also reflected in the recent polls, where "[m]ore than half of all police officers in Greece voted for the far-right ultra-nationalist party Golden Dawn."[23] Thus, the aim of this chapter is to map out the rationalities that inform the unlawful practices of the Hellenic Police and Coast Guard. In this respect, it provides an overview of the security professionals' understanding of the Greek "migration-security nexus," the migrant "other", the "self", globalisation and multiculturalism. Additionally, it puts forward an outline of their perceptions of Islam, Turkey, and the role of Greek NGOs. Finally, it presents their reflections on EU and national migration policies, the role of Frontex migration controls, and their own practices.

Framing Theory and Migration

The framing literature offers a useful angle for studying the rationalities, perceptions and opinions that inform the unlawful practices of the Hellenic Police and Coast Guard. Framing involves highlighting some aspects of a perceived reality in discourse "in such a way as to promote a particular

[21] See FRA, *Coping*.
[22] Access to these unclassified dissertations was granted to the researcher after a formal request was submitted to both the School of National Security and the Hellenic National Defence College.
[23] "Half of Greek cops go ultra-nationalist at elections", *Russia Today*, 16 May 2012, available at http://rt.com/news/greek-police-vote-nazis-350/ (last visited 28 January 2014).

problem definition, causal interpretation, moral evaluation, and/or treatment recommendation."[24] In other words, frames call attention to some elements of reality, while obscuring other aspects.[25] They establish the parameters and points of reference for audiences to interpret, categorise and evaluate complex or ambiguous events,[26] such as irregular migration. This may be achieved through subtly altering the presentation of an issue or through more direct attempts to draw attention to certain elements of an issue, while ignoring others.[27] Thus, frames function like lenses, which are capable of shaping the opinions of individuals regarding a specific issue.[28]

Broadly speaking then, frames are "schemata of interpretation" that allow individuals to "locate, perceive, identify and label" occurrences within the world, rendering them meaningful,[29] and thereby functioning as experienced organisers and action guides.[30] In this respect, frames are "action-oriented sets of beliefs and meanings that inspire and legitimate the activities" of those who construct and adhere to them by simplifying and condensing elements of the world,[31] while they "are not merely aggregations of individual attitudes and perceptions but also the outcome of negotiating shared meaning."[32]

In the political and social realms, actors with vested interests are constantly debating with each other the correct or standard way to define/present an issue, each putting forward a specific set of values, actions and policy recommendations.[33] This means that frames do not exist

---

[24] Entman, R. M. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43, no. 4 (1993), 52.
[25] Ibid, 55.
[26] Benford, R, and Snow, D. "Framing process and social movements: An overview and assessment" *Annual Review of Sociology* 26, no. 1 (2000): 611-639.
[27] Nelson, T. E., Clawson, R. A. and Oxley, Z. M. "Media Framing of a Civil Liberties Conflict and Its Effect on Tolerance." *American Political Science Review* (1997): 567-583.
[28] Iyengar, S. *Is Anyone Responsible? How Television Frames Political Issues* (Chicago: University of Chicago Press, 1994).
[29] Goffman, E. *Frame Analysis: An Essay on the Organization of Experience* (Cambridge MA: Harvard University Press, 1974), 21.
[30] Benford and Snow, "Framing," 614.
[31] Ibid.
[32] Gamson, W. A. *Talking Politics* (Cambridge: Cambridge University Press, 1992), 111.
[33] Lavenex, S. "Migration and the EU's New Eastern Border: Between Realism and Liberalism," *Journal of European Public Policy* 8, no. 1 (2001): 24-42; Scheufele,

within a vacuum, but they typically compete directly with each other, while also constrained by "pre-existing meaning, structures or schemas."[34] Those frames that can relate more closely to the specific socio-political and historical context and which can be easily retrieved from memory are more likely to dominate.[35]

Two main frames compete for dominance with regard to migration.[36] On the one hand, the "realist policy frame" predominantly presents migration as a security problem. Following a state-centric approach, the realist frame emphasises "the need to secure borders, restrict migration and homogenise all categories of migrants into a single policing-repression scheme."[37] More particularly, irregular migration is perceived as a direct threat to the state's legitimacy, as it damages the myth of control of its borders and many of its key institutions, such as the government, the army and the police.[38] Moreover, it is perceived as a threat to "our" jobs, personal and social security, moral values, collective identities, and cultural homogeneity.[39] When it comes to the control and management of irregular migration then, the only appropriate response from this perspective is to employ a hard stance to suppress it, with the emphasis placed on the strengthening of internal and external border controls as deterrent measures.

On the other hand, the "liberal policy frame" focuses more on the individual, rather than the state. The preoccupation with human rights constitutes the core of this approach, which criticises the consequences of restrictive policies on migrants' living conditions and human rights.[40] Moving away from the realist frame that sees migrants as inferior and/or threatening, the liberal frame perceives them as beneficial to the economy and deserving of respect, regardless of their legal status, favouring

---

D. A. "Framing as a Theory of Media Effects," *Journal of Communication* 49, no. 1 (1999): 103-122.

[34] Scheufele, "Framing," 105.

[35] Nelson, Clawson and Oxley, "Media."

[36] Lavenex, "Migration".

[37] Karyotis, G. "The Fallacy of Securitizing Migration: Elite Rationality and Unintended Consequences," in *Security, Insecurity and Migration in Europe,* ed. Lazaridis, G. (Farnham: Ashgate, 2011), 13-14.

[38] Anderson, B. R. O.G. *Imagined Communities: Reflections on the Origin and Spread of Nationalism,* (Brooklyn: Verso, 1991).

[39] Faist, T. "The Migration-Security Nexus: International Migration and Security before and after 9/11." *Migration, citizenship, ethnos* (2006): 103-20.

[40] Lavenex, "Migration."

ethnically diverse and multicultural societies. In turn, migration is understood as a natural right, as a symptom of global poverty and war, rather than as a problem in itself that needs to be tackled by any means. In this respect, when it comes to the control and management of irregular migration, the most suitable response from this perspective is to adopt a much more lenient stance, with the emphasis placed on regularisation schemes, integration, and the provision of international protection to those who need it.

The remainder of this chapter aims to map the rationalities, attitudes, perceptions and opinions that constitute the Greek security professionals' frame with regard to various key issues related to migration. It is argued that this frame heavily draws on the "realist policy frame" described above, which, in turn, informs restrictive policies and practices. However, it also deviates from it, towards a more extreme and radical version. Those very departures from the classic "realist policy frame" inform and guide Greek security professionals' unlawful practices in the control and management of irregular migration.

In what follows, this chapter applies Entman's definition of the frame to Greek security professionals' opinions, beliefs, rationalities, reflections and evaluations regarding various issues related to migration. First it presents the definition of migration as a problem according to Greek security professionals, which is followed by their interpretation of the causes of the problem. The security professionals' moral evaluations of migrants in Greece and the attitudes of Greeks towards them, as well as the role of NGOs and Frontex in managing and controlling migration are put forward next. The chapter continues with the treatment recommendation according to Greek security professionals, which is accompanied by their reflections on their own security practices. Finally, the conclusion summarises the findings and assesses the challenges that occur for the EU's Internal Security Strategy.

Defining the Problem: Migration as a Security Threat

This section presents the way in which Greek security professionals frame migration. Instead of portraying it as a social issue, they choose to interpret it as a social problem and security threat by drawing attention to particular negative elements of it, while ignoring the positive ones that exist in the "liberal policy frame" discourse. Thus, Greek security professionals frame migration as a public health, political, social and

societal, asymmetric, and economic threat to the country. In this respect, they promote a specific definition of the phenomenon of migration as a multi-level security threat, which constitutes a core element of their frame.

According to one of the interviewed police officers, "[...] migrants are a public health bomb."[41] New/unknown contagious diseases are brought into the country by illegal migrants,[42] or their emergence is fostered by migrants' grave living conditions.[43] Additionally, the unregulated inclusion of illegal migrants in the labour market, without any sanitary controls, is another potential factor for the spread of diseases,[44] as well as prostitution networks that operate without any healthcare monitoring and control.[45]

Moreover, migration creates implications for the diplomatic relations between Greece and other Schengen countries. Drymousis argues that Greece has been repeatedly accused in the past that it doesn't contribute efficiently to the deterrence of international migration flows that use the country as a gateway to Europe,[46] which has resulted in the dispersing of these migrants to other EU and Schengen member states.[47] Migration also exacerbates the diplomatic relations between Greece and third countries. Koukouras[48] refers specifically to the issue of Kurdish migrants and refugees in Greece, which has occasionally undermined the Greek-Turkish diplomatic relations. Finally, migration can potentially lead to the creation of large and solid religious/ethnic/national minorities with leverage in the Greek state with the ability to influence its foreign policy. In this regard,

---

[41] Hellenic Police Officer, Hellenic Police Directorate, Orestiada, 6 April 2012.
[42] Manos, D. "Muslim economic migrants in Greece and the relevant Greek policy: approach, weaknesses, problems, and national planning within the context of the European reality and the Middle Eastern instability", *MA Dissertation*, Hellenic National Defence College, 2011, 35.
[43] Kokkinis, N. "National security and migration policy", *MA Dissertation*, School of National Security, 2009, 151.
[44] Ibid, 152.
[45] Ibid.
[46] Drymousis, I. "The Muslim economic migrants in Greece and the relevant Greek political approach (weaknesses, problems and national planning within the context of the European reality and the Middle Eastern systemic instability)", *MA Dissertation*, Hellenic National Defence College, 2012, 39.
[47] See "EU plans to exclude wayward Schengen nations", *Financial Times*, 12 September 2011, available at http://www.ft.com/cms/s/0/bb2a9b0e-da0e-11e0-b199-00144feabdc0.html#axzz2UiJQfe7U (last visited 28 January 2014).
[48] Koukouras, A. "The criminality of aliens in Greece. Myths and reality", *MA Dissertation*, School of National Security, 2003, 47.

Drymousis expresses his concerns about the size of the Albanian minority in Greece, which, in combination with Albanian nationalism, can potentially harm Greece.[49]

Additionally, migration poses a social and societal threat to Greece by undermining the demographic, ethnic, cultural and religious homogeneity of the country. Indeed, the regularisation of hundreds of thousands of migrants, in combination with their high fertility rates and the persistent Greek demographic problem will result in Greeks becoming a minority in their own country in the future.[50] Migration is also linked to the increase of criminality and organised crime and the resulting rise of fear, insecurity and racism that leads to social segregation and racist violence.[51] In this respect, Kokkinis argues that racism and xenophobia appeared in Greece simultaneously with the increase of criminality, which was caused by mass migration.[52] However, according to academic studies, the involvement of migrants in serious criminality was not significant enough to justify the widespread "Albanophobia" in Greece in the 1990s.[53]

Furthermore, security professionals frame migration as an asymmetric threat to Greece, which is "a threat that does not aim to overpower the defences of its target, but rather to surpass them and attack its weak points." [54] Dimitriadis suggests that the possibility of infiltration of terrorists in Greece through illegal migration channels should not be excluded,[55] as illegal migration always goes hand-in-hand with the terrorist threat.[56] Barla and

[49] Drymousis, "The Muslim,"43.
[50] Manos, "Muslim," 32.
[51] Dimitriadis, V. "Migration, illegal migration and criminality in modern Greece", *MA Dissertation*, School of National Security, 2005, 5; Drymousis, "The Muslim," 40; Koukouras, "The Criminality," 87; Tsironis, D., Stamatiadis, G., Daviotis, L., Tsitsimpikos, N., Liakos, G., Papathanasiou, V., Kamnis, I., Varzakis, A., Lerakis, K., Diamantaki, I., and Barkatsas, G. "Guarding land and sea borders and illegal migration in Greece and the European Union", *MA Dissertation*, Hellenic National Defence College, 2009, 8.
[52] Kokkinis, "National," 142.
[53] Karydis, V. "Criminality or Criminalization of Migrants in Greece? An Attempt at Synthesis" in *The new European criminology: Crime and social order in Europe*, eds. V. Ruggiero, N. South, and I. Taylor, (Abington: Routledge, 1998).
[54] Kordalis, V. "New dimensions in Police work as a consequence of the recent policies for legal and illegal immigrants in the European Union and Greece", *MA Dissertation*, School of National Security, 2006, 135.
[55] Dimitriadis, "Migration," 82.
[56] Kokkinis, "National," 144.

colleagues suggest that there is fertile ground for the eruption of terrorism in Greece due to the widespread poverty, the large migrant population, their grave living conditions, their illegal status, and their socialisation with outlaws.[57] Moreover, Greek security professionals believe that Turkey is using illegal migration as a weapon of asymmetric warfare against Greece. Tsironis and colleagues maintain that "Turkey can potentially recruit spies and saboteurs among illegal immigrants that are willing to serve Turkish interests against our own country."[58]

Finally, migration is framed as an economic threat to Greece. There is a shared belief among Greek security professionals that migration creates parallel economies, leads to a drop in public revenues, burdens social welfare services, and increases unemployment. Drymousis argues that unskilled illegal migrants strengthen the parallel economy, as they are excluded from the labour market regulations.[59] In turn, this reduces public revenues, as employers still hire illegal migrants but refrain from paying for their social security, which leads to the burdening of the government budget.[60] Moreover, migrants are threatening the social welfare system with collapse,[61] as they benefit from it but they don't contribute anything to it, which leads to the increase of public spending on healthcare, education and national security.[62] Furthermore, Tsironis and colleagues argue that migration is linked to the rise of unemployment as the native workforce is substituted by the foreign one, which is preferred by the labour market because it is cheaper and more hard-working.[63] In contrast, however, a number of academic studies have highlighted the diachronic positive impact of migrants in Greek economy, who, for years, filled in labour shortfalls in vital economic sectors, such as agriculture, and helped keep the country's inflation low.[64]

---

[57] Barla, S., Kokkoros, E., Eteridis, N., and Velentzas, A. "Consequences of the demographic problem and illegal migration in national security: threat or opportunity?", *MA Dissertation*, School of National Security, 2004, 66.
[58] Tsironis *et al*, "Guarding," 9.
[59] Drymousis, "The Muslim," 36.
[60] Ibid.
[61] Ibid.
[62] Manos, "Muslim," 35.
[63] Tsironis *et al*, "Guarding," 8.
[64] Antonopoulos, G. A., Tierney, J. and Webster, C. "Police Perception of Migration and Migrants in Greece." *Eur. J. Crime Crim. L. & Crim. Just.* 16 (2008): 353-378; Ioakeimoglou, E. "Migrants and Employment" in *Migrants in Greece*, eds. A. Marvakis, D. Parsanoglou, and M. Pavlou, (Athens: Ellinika Grammata, 2001), 81-94; Lyberaki A., and Pelagidis, T. *The "fear of the*

Causal Interpretation of the Problem

The definition of migration as a problem in the Greek security professionals' frame is followed by the causal interpretation of the issue. The majority of security professionals' master's dissertations provide a detailed description of the push and pull factors that lead people to migrate to Greece: globalisation and multiculturalism, the nature of Islam, the rivalry and proximity with Turkey, and the EU and national migration policies, all feature as key push/pull factors of migration to Greece. In contrast, a large number of academic studies have put forward their own interpretation of the phenomenon. Push factors include the socio-political changes in former socialist countries in the late 1980s and early 1990s, the civil wars in the Balkans, the collapse of the Albanian regime, and the demographic push in many Third World countries.[65] Additionally, several pull factors have been suggested by the relevant literature, such as the growing underground economy, the relatively limited flexibility of the Greek labour market, the high seasonality of the Greek economy, and the financial and political stability of the country in the 1990s and 2000s.[66] Against these explanations, Greek security professionals put forward an altered presentation of the causes of migration to Greece.

Globalisation and Multiculturalism

A number of master's dissertations identify globalisation as the driving force of international migration. These studies present a radical understanding of the notion of globalisation, and, by extension, proceed to a distorted perception of multiculturalism. Elements of various conspiracy

---

foreigner" in the labour market: Tolerations and prejudices in development, (Athens: Polis, 2000).

[65] Alipranti-Maratou, L. "Migration to Greece: A New Type and Emerging Problems" in *Greek Research in Australia: Proceedings of the Sixth Biennial International Conference of Greek Studies, Flinders University June 2005*, eds. E., Close, M. Tsianikas, and G. Couvalis, (Adelaide: Flinders University Department of Languages - Modern Greek, 2007), 187.

[66] Alipranti-Maratou, *Migration*; Antonopoulos, G. A. and Winterdyk, J. "The Smuggling of Migrants in Greece an Examination of Its Social Organization," *European Journal of Criminology* 3, no. 4 (2006): 439-461; Baldwin-Edwards, M. and Arango, J. *Immigrants and the Informal Economy in Southern Europe*. Vol. 3: (Abingdon: Psychology Press, 1999); King, R., Lazaridis, G. and Tsardanidis, C. G. *Eldorado or Fortress? Migration in Southern Europe,* (New York: St. Martin's Press, 2000).

theories are predominant in this frame. Kokkinis suggests that international migration is caused by globalisation, which was planned and organised after the end of the Cold War by external forces, and more specifically, the USA. [67] Globalisation aims at the creation of an "ultra-neoliberal international economic system of trade and a unified global market" with loose national borders.[68] This process, by definition, leads large masses of people to migrate.[69] A similar opinion is echoed by Manos, who takes this idea a step further and argues that globalisation is an integral part of the "New World Order," which involves the loosening and discredit of national borders, and the consistent internal subversion of a state's national existence in order for peoples with national history, sovereignty, collective consciousness and memory to be substituted by multicultural populations.[70] In this manner, the nation-state is rendered an outmoded way of organisation, while the dedication to national identity and patriotism is demonised and presented as racist nationalism and xenophobia.[71] With specific regard to Greece, Kokkinis claims that the "New World Order" aims at the "Balkanisation" of the country by dismantling its national identity through the strengthening of the Muslim element in its society in order to act as an antagonist to Russia,[72] since Islam is de facto antagonistic towards the Russian Orthodox influence in the Balkans.[73]

In turn, this framing of globalisation produces a very specific understanding of multiculturalism as a tool of restructuring countries for geopolitical and economic reasons. According to this line of thinking, since multiculturalism is a project enforced on Greece by external powers, it has to be resisted. Tsironis and colleagues suggest that it would be a tragedy for Greek people to be deceived and fall for the destruction of their national identity "with these nice words about humanitarianism, universalism, and multiculturalism," which are presented as an ostensible progressive feat.[74] Multiculturalism poses "a direct threat to the ethnic and social coherence, national security, and political and state stability of the country"[75] and it is

[67] Kokkinis, "National," 100.
[68] Ibid, 120.
[69] Ibid.
[70] Manos, "Muslim," 33.
[71] Ibid.
[72] Kokkinis, "National," 101.
[73] Ibid, 136.
[74] Tsironis *et al*, "Guarding," E4.
[75] Kokkinis, "National," 119.

the duty of the Greek people to resist it, since "the political, social and spiritual elites of the country seem to have utterly and unquestionably accepted it."[76]

Islam and Turkey

Two other factors that cause the migration problem in Greece according to Greek security professionals are the nature of Islam and Greece's proximity and rivalry with Turkey. Again there are elements of conspiracy theories evident in this frame, which are, however, expressed by a minority. Yet, they are indicative of the suspicion and bias, with which the Greek security professionals' frame is instilled.

Kokkinis suggests that Islam is "impossible to be assimilated by Western civilisation", as it is a "foreign body" and "incompatible with democracy."[77] This deeply negative framing of Islam is combined with a profound sense of suspicion. Drymousis argues that Muslims migrate to Europe in order to take advantage of the favourable legislation and discourse that allow them to reproduce their own cultural lifestyle.[78] Kokkinis maintains that Muslim migrants "despise the European lifestyle and conspire to take it over,"[79] while Barla and colleagues take this idea a step further by arguing that the migration of Muslims to Europe is organised and financed by economically powerful actors that aim to create a strong Muslim enclave in Europe.[80] In this respect, Drymousis talks about "a crude and ruthless Islamic imperialism" that threatens the existence of the peoples of Europe.[81]

The way in which Islam and Muslim migrants are framed by Greek security professionals also informs their understanding of Turkey and its role in the mass migration of people to Greece. Turkey is generally viewed with suspicion by Greek security professionals, some of whom argue that the problem of irregular migration starts with the fact that "[w]e [i.e. Greeks] have a neighbouring country [i.e. Turkey], with which we have

[76] Ibid.
[77] Ibid, 150.
[78] Drymousis, "The Muslim," 13-14.
[79] Kokkinis, "National," 146.
[80] Barla *et al*, "Consequences," 11.
[81] Drymousis, "The Muslim," 30.

national sovereignty problems and which also is a Muslim country."[82] In this respect, some security professionals argue that Turkey has important national interests in using migration to Europe and Greece for its own benefit. Tsironis and colleagues argue that Turkey is using migrant smuggling as a means to promote its unsubstantiated claims in the Aegean Sea through the conduct of search and rescue operations in Greek territorial waters.[83] Manos suggests that migrant smuggling brings great economic benefits to Turkey and argues that the Turkish state foments illegal smuggling networks in its territory.[84] Finally, Greek security professionals also believe that Turkey is using migration "as a weapon to destabilise Greece,"[85] as migrants "create terrible social problems, problems in the healthcare system etc."[86]

EU and National Migration Policies

EU and Greek immigration policies are also considered as constitutive factors of the migration problem in Greece, according to the security professionals' frame. Some security professionals reveal their concerns and disappointment with specific EU policies, such as the family reunification directive[87] and the (then) Dublin II regulation.[88] Tsironis and colleagues argue that the application of the family reunification directive means that an additional 3-4 million migrants will come to Greece,[89] and for this reason "the Greek government must abolish the family reunification

[82] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 18 January 2012.
[83] Tsironis *et al*, "Guarding," 1.
[84] Manos, "Muslim," 40.
[85] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[86] Ibid.
[87] Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification, OJ 2003 L251/12.
[88] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ 2003 L50/1, now replaced by Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), OJ 2013 L180/31.
[89] Tsironis *et al*, "Guarding," E4.

measure."[90] Furthermore, Manos argues that the Dublin II regulation constitutes "a huge problem for Greece" as it obliges the country to keep all undocumented migrants that cross its borders.[91]

National migration policies have also played their role in the creation of the migration problem in Greece, according to this frame. There is a shared understanding of the relevant legislation as "largely pro-migrant,"[92] which is seen, however, as a negative characteristic and it is even treated with suspicion: "our country's migration policy is characterised by a weird tolerance towards migration, which constitutes a pull-factor for waves of illegal migrants." [93] Security professionals are also critical of the regularisation programmes that were implemented in the country in the past as they "rewarded the migrants who entered the country illegally" and they "gave incentive to other migrants to enter the country illegally, hoping that someday they will be regularised too."[94] Finally, security professionals are critical of the (then) suggested change in the nationality law, which would incorporate elements of *jus soli*[95] into the legislation. Manos claims that this would constitute a potential national security threat, adding that such a change would be "the pinnacle of the malaise, weakness, and suspicious indifference of our political system."[96]

Moral Evaluation of the Problem

Greek security professionals' frame of migration-related issues also includes the moral evaluation of the roles and qualities of key actors involved in the migration problem. More specifically, security professionals assess the attitudes of Greek people towards migrants *vis-à-vis* the quality of migrants themselves, and they evaluate the role and contribution of NGOs and Frontex in the management and control of irregular migration. In this respect, Greek security professionals' moral evaluations together with the problem definition and causal interpretation

[90] Drymousis, "The Muslim," 47.
[91] Manos, "Muslim," 37.
[92] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[93] Manos, "Muslim," 33.
[94] Tsironis *et al*, "Guarding," E8.
[95] *Jus soli*, or else the "right of the soil", defines citizenship as a territorial birth right. See Brubaker, R. *Citizenship and nationhood in France and Germany*, (Cambridge: Cambridge University Press, 1992).
[96] Manos, "Muslim," 39-40.

described above, serve as experience organisers and action guides that inspire and legitimate the treatment recommendation that will be presented in the last section of the chapter.

"Us" v the "Others"

The analysis of Greek security professionals' interviews and master's dissertations reveals the moral evaluation of the attitudes of Greek people towards migrants *vis-à-vis* the migrants themselves. There seems to be a shared understanding of "us," as "friendly," "hospitable," "humanitarian" and characterised by a "keen sense of honour" (*philotimo* in Greek). Koukouras maintains that Greeks always had a highly developed sense of hospitality towards the "foreigner."[97] In the same manner, Tsironis and colleagues argue that "Greece was always ecumenical and open towards all other people,"[98] while one of the interviewees argued that "Greece has humanitarianism and hospitality as its flag."[99] Additionally, another interviewee stated that "Greeks were never racist."[100] Indeed, these findings are in line with Antonopoulos.[101] Yet, it is common for the police in Greece to adopt racist attitudes towards migrants and to employ various offensive practices.[102]

As far as the framing of the migrant "Other" is concerned, all interviewees referred to migrants as "illegal migrants" ("*lathrometanastes*" in Greek), a term that fails to capture the important distinction between regular/irregular migrants, asylum seekers and refugees. The specific choice of this term derives from a certain logic, according to which "in Greece, we don't have migrants; we only have illegal migrants."[103] Moreover, in its heart this frame sees migrants in Greece as inferior people of lower quality and culture. Kokkinis considers immigrants as "pathetic individuals"[104] and "the contemporary version of the barbaric tribes."[105]

---

[97] Koukouras, "The Criminality," 50.
[98] Tsironis *et al*, "Guarding," E4.
[99] Hellenic Police Officer, Hellenic Police Directorate, Orestiada, 6 April 2012.
[100] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 24 January 2012.
[101] Antonopoulos, G. A. "Greece: Policing Racist Violence in the 'Fenceless Vineyard'." *Race & Class* 48, no. 2 (2006), 92-100.
[102] Ibid, 95.
[103] Kokkinis, "National," 127.
[104] Ibid, 115.
[105] Ibid, 96.

Barla and colleagues refer to them as "uncivilised Third Worlders,"[106] while a few security professionals used in our informal discussions extremely demeaning terms to describe them, such as "niggers," "monkeys," "apes," "animals" and "stinkers." Yet, one of the interviewed police officers was explicit during the formal interview too and used degrading terms, such as "stinkers" and "animals" to portray them.[107] Finally, some of the master's dissertations employ heavily loaded terms to describe the phenomenon of migration. Manos, for instance, talks about the "whirlwind of illegal migration,"[108] while others, use war-like metaphors, such as "migrant invasion," "[Greece became] the target of migrants,"[109] and "the armies of miserable migrants."[110]

The NGOs

Greek security professionals' frame also includes the moral evaluation of NGOs. A number of master's dissertations and interviewees put forward their negative opinions, suspicions and distorted picture in general of NGOs. Moreover, this frame manifests Greek security professionals' attitude towards human rights. For instance, a Coast Guard officer in Lesvos argued that NGOs "are dealing with human rights, while we [i.e. the Coast Guard] are dealing with border guarding. We respect human rights, but we are not interested in them."[111] Another interviewee suggested that members of NGOs are bringing their political ideas with them at work,[112] while a third interviewee, moving in the same direction, stated that only people who support SYRIZA[113] are involved in NGOs and human rights protection, adding that "SYRIZA do not like the police."[114] As these quotes manifest, there is a deep misunderstanding regarding what NGOs really are and do. Moreover, they reveal that security professionals see NGOs as politicised actors and bearers of a political agenda.

[106] Barla *et al*, "Consequences," 65.
[107] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 18 January 2012.
[108] Manos, "Muslim," 39.
[109] Kokkinis, "National," 98.
[110] Barla *et al*, "Consequences," 64.
[111] Hellenic Coast Guard Officer, Lesvos Port Authority, Mitilene, 8 March 2012.
[112] Hellenic Police Officer, Hellenic Police Directorate, Orestiada, 6 April 2012.
[113] SYRIZA, or else the Coalition of the Radical Left.
[114] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 18 January 2012.

Additionally, they uncover a very specific attitude towards human rights, which are considered of secondary importance.

Indeed, this misunderstanding of the role and mission of NGOs goes deeper. Drymousis suggests that NGOs "are pushing for the admission of mass illegal migration, adopting a discourse of universal human rights, usually ignoring the fact that the source of power at the international level is always the nation-state."[115] One interviewee also argued that the NGOs' jobs are not hard compared to what the police officers are doing.[116] Finally, other security professionals stated that they couldn't understand why NGOs even exist as "they are just in it for the money" and "they simply make our [i.e. the police's] job harder."[117]

Frontex

Some security professionals, particularly those involved in asylum procedures, the detention, internal control and management of migrants,[118] share a negative evaluation of the role of Frontex in Greece. More specifically, there is a common belief that Frontex has a minimal contribution to the reduction of irregular migration flows. In this respect, one of the interviewees suggested that Frontex can do "nothing at all" about irregular migrants, as "[...] from the moment somebody enters your country illegally [...] you can't send him back where he came from, since refoulement is not permitted."[119] The same interviewee argued that "what Frontex does is to record these people and let them go. This is the two-faced Europe."[120] Echoing these views, another interviewee stated that Frontex officers have been deployed in Greece in order to record all foreigners that enter the country, so that when irregular migrants registered in Greece get arrested in Germany, for instance, then Greece is obliged to accept them back according to the Dublin II regulation.[121] In this regard,

[115] Drymousis, "The Muslim," 34.
[116] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 18 January 2012.
[117] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[118] In other words, in processes where Frontex has no involvement at all.
[119] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[120] Ibid.
[121] Ibid.

"[i]t's in their [i.e. Frontex's] interests to record foreigners, because they are incapable of deterring them."[122]

Thus, Frontex is framed by Greek security professionals as a force that has been deployed in Greece in order to serve the interests of Central and Western European states. All in all, the stance of the EU is largely perceived as hypocritical. More specifically, security professionals express their disappointment with the lack of solidarity and the unequal responsibility-sharing among EU member states regarding the management of undocumented migrants: "if the EU really wanted to support Greece, then the burden of illegal migrants would be shared among all member states. There is hypocrisy on behalf of the EU."[123]

Treatment Recommendation

The chapter has presented so far the definition of migration as a problem, the causal interpretation of the issue and the moral evaluation of the role of various actors involved therein, according to the Greek security professionals' frame. Nevertheless, frames often include a treatment recommendation of the problem, as was stated above, which informs their action-oriented nature by organising the experience and guiding the practices of those who construct and adhere to them. The treatment recommendation in the Greek security professionals' frame is partly shaped by their reflections on their very own migration control and management practices presented below.

Greek Security Professionals' Practices

Security professionals' reflections revolve around the idea that "the control and deterrence of illegal migration is futile,"[124] as "migrants will attempt sooner or later to cross the borders illegally using a different route."[125] In this respect, one of the interviewees argued that "there is no way to stop somebody from entering Greece; deterrence is impossible."[126] In the same manner another interviewee claimed that patrols are pointless, since they do not contribute anything to the control of illegal migration

[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Tsironis *et al*, "Guarding," H2.
[126] Hellenic Police Officer, Hellenic Police Directorate, Lesvos, 9 March 2012.

due to the complex methods employed by the smugglers.[127] However, another factor that renders patrolling and deterrence methods ineffective is the willingness of illegal migrants to be arrested.[128] Indeed, "illegal migrants want to be arrested [...] because they are aware that being detained is part of their journey,"[129] but also because "the conditions in detention centres are better compared to the outside world."[130] Yet, Greek security professionals express deep resentment regarding their internal migration control mechanisms too. According to one of them "'sweep operations' are a smokescreen,"[131] as "illegal migrants just move to a different area; we [i.e. the police] are just transferring the problem."[132] Indeed, one of the interviewees stated that "sweep operations"' are just "part of the political parties' political calculations."[133]

In this respect, the Hellenic Police seem to have adopted a rather controversial migration control practice: "we detain them [i.e. the irregular migrants] for a few hours, then we release them, and then we arrest and detain them again. In this way we are breaking their nerves and we push them to go to Europe or back to their home countries."[134] Indeed, this practice seems to be openly admitted by a member of parliament of the New Democracy party, the main actor of the Greek coalition government: "we must make their [i.e. the irregular migrants'] lives hard in order for them to understand that they are unwanted in the country and leave."[135] In the same manner, one of the interviewed police officers in Athens stated that "we must make Greece inhospitable to migrants. I mean that all Greeks must stop our financial relations with them in order to make them

[127] Hellenic Police Officer, Hellenic Police Directorate, Orestiada, 6 April 2012.
[128] Manos, "Muslim," 37.
[129] Hellenic Coast Guard Officer, Sea Borders Protection Directorate, Athens, 19 January 2012.
[130] Border Guard Officer, Attica Aliens' Police Directorate, Athens, 24 January 2012.
[131] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[132] Border Guard Officer, Attica Aliens' Police Directorate, Athens, 24 January 2012.
[133] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[134] Border Guard Officer, Attica Aliens' Police Directorate, Athens, 24 January 2012.
[135] "Adonis: We must make migrants' lives hard", *Proto Thema*, 10 June 2013, available at http://www.protothema.gr/politics/article/?aid=285345 (last visited 28 January 2014).

understand that there is nothing here. No charity, no philanthropy, no job offers."[136]

This treatment recommendation, as radical as it sounds, guides the repeated illicit migration control practices employed by Greek security professionals. Indeed, this logic has been identified by Mauro Palma, President of the Committee for the Prevention of Torture, who has argued that Greek authorities intentionally create inhuman detention conditions in order to send a message to would-be migrants that "they will have a hard time in Greece."[137]

Conclusions

This chapter attempted to shed some light on the frame that guides the recurrent unlawful migration control practices of Greek security professionals. More specifically, it put forward the dominant realist understanding among Greek security professionals of migration as a public health, political, social and societal, asymmetric, and economic threat to Greece. Moreover, it presented their interpretation of the causes of the migration problem that focuses on globalisation and multiculturalism, the nature of Islam, the rivalry and proximity with Turkey, and the ineffective EU and national migration policies. Furthermore, the chapter demonstrated their moral evaluations of the attitudes of Greeks towards migration, migrants themselves, and the role and contribution of NGOs and Frontex in the management and control of migration. Finally, it introduced the treatment of the problem recommended by Greek security professionals that is shaped by their reflections on their very own security practices. These four elements make up the Greek security professionals' frame of migration and inform, guide and legitimate the recurrent illicit migration control practices of the Greek authorities.

This frame, which is a radical and extreme variation of the "realist policy frame," and the resulting unlawful security practices pose some serious challenges to the EU Internal Security Strategy. For example, the data processing by law enforcement officers examined by O'Neill, Grant and Blasi Casagran in their chapters to this book would be seriously affected

[136] Hellenic Police Officer, Attica Aliens' Police Directorate, Athens, 19 January 2012.
[137] See "Greece says to illegal immigrants 'You will have a hard time'", *To Vima*, 13 January 2012, available at http://www.tovima.gr/society/article/?aid=438602 (last visited 28 January 2014).

by these frames, particularly in the context of the "epistemic community" as examined by Egan. First, they are placing obstacles to the development of a coherent long-term immigration policy in Greece, and they are undermining the full implementation of integrated border management. Second, they increase the death toll of immigrants at the external borders of the EU and damage the Union's reputation as a defender of human rights, despite the fact that individual member states are held responsible for human rights violations. Third, they compromise the application of the principles of solidarity and cooperation among EU member states and agencies by instilling biases and suspicions in inter-state and inter-agency relations. All in all, they end up jeopardising national and EU security, the very essences of which they aimed to protect in the first place.

One needs to ask if there is a way to alleviate the consequences of this frame and the resulting unlawful security practices on national security and the EU Internal Security Strategy. By building upon the works of sociological institutionalists, Horii explores the impact that Frontex border guard training has brought to the EU external border regime and argues that it has had an integrative effect on it, as it has promoted the socialisation and professionalisation of border guards.[138] Indeed, the interviewed security professionals that expressed the most negative opinions across the board were those that had not received any kind of Frontex training and were not involved in procedures where socialisation with Frontex officers was mandatory. In contrast, officers who had attended Frontex training seminars and/or were cooperating regularly with foreign officers expressed more moderate opinions. The answer to the above question then could be the expansion of Frontex training programmes across all Greek security professionals, and the introduction of similar "anti-radicalisation" training programmes in the Hellenic Police and Coast Guard Academies, the School of National Security and the Hellenic National Defence College. However, any solution implemented in this regard, should go hand-in-hand with further research on the real and perceived impact of EU migration policies on the member states' national security and the field of security professionals.

[138] Horii, S. "It Is About More Than Just Training: The Effect of Frontex Border Guard Training," *Refugee Survey Quarterly* 31, no. 4 (2012): 158-177.

Bibliography

AA v *Greece* (12186/2008, 22.7.2010).

Alipranti-Maratou, L. "Migration to Greece: A New Type and Emerging Problems." In *Greek Research in Australia: Proceedings of the Sixth Biennial International Conference of Greek Studies, Flinders University June 2005*, 185-198. Adelaide: Flinders University Department of Languages - Modern Greek, 2007.

Amnesty International. "Frontier Europe: Human Rights Abuses on Greece's Border with Turkey". London: Amnesty International, International Secretariat, United Kingdom, 2013.

Anderson, B. R. O.G. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. Brooklyn: Verso, 1991.

Antonopoulos, G. A. "Greece: Policing Racist Violence in the 'Fenceless Vineyard'." *Race & Class* 48, 2 (2006): 92-100.

—. "The Limitations of Official Statistics in Relation to the Criminality of Migrants in Greece." *Police Practice and Research* 6, 3 (2005): 251-260.

Antonopoulos, G. A., Tierney, J. and Webster, C. "Police Perception of Migration and Migrants in Greece." *Eur. J. Crime Crim. L. & Crim. Just.* 16 (2008): 353-378.

Antonopoulos, G. A. and Winterdyk, J. "The Smuggling of Migrants in Greece an Examination of Its Social Organization." *European Journal of Criminology* 3, 4 (2006): 439-461.

Baldwin-Edwards, M. and Arango, J. *Immigrants and the Informal Economy in Southern Europe*. Vol. 3. Abingdon: Psychology Press, 1999.

Barla, S., Kokkoros, E., Eteridis, N., and Velentzas, A. *Consequences of the demographic problem and illegal migration in national security: threat or opportunity?*, MA Dissertation: School of National Security, 2004.

Benford, R, and Snow, D. "Framing process and social movements: An overview and assessment". *Annual Review of Sociology* 26, 1 (2000): 611-639.

Brubaker, R. *Citizenship and nationhood in France and Germany*. Cambridge: Cambridge University Press, 1992.

Council Document, Internal Security Strategy for the European Union: Towards a European Security Model, 5842/2/2010.

Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification, OJ 2003 L251/12.

Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third- country national, OJ 2003 L50/1.

CPT, *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 19 to 27 January 2011*, Strasbourg, Council of Europe, 2012.

—. *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 17 to 29 September 2009*, Strasbourg, Council of Europe, 2010.

—. *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 23 to 29 September 2008*, Strasbourg, Council of Europe, 2009.

—. *Report to the Government of Greece on the visit to Greece carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 20 to 27 February 2007*, Strasbourg, Council of Europe, 2008.

Dimitriadis, V. *Migration, illegal migration and criminality in modern Greece*, MA Dissertation: School of National Security, 2005.

Drymousis, I. *The Muslim economic migrants in Greece and the relevant Greek political approach (weaknesses, problems and national planning within the context of the European reality and the Middle Eastern systemic instability)*, MA Dissertation: Hellenic National Defence College, 2012.

Entman, R. M. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43, 4 (1993): 51-58.

Faist, T. "The Migration-Security Nexus: International Migration and Security before and after 9/11." *Migration, citizenship, ethnos* (2006) 103-20.

Financial Times, 12 September 2011, available at http://www.ft.com/.

FRA. *Coping with a Fundamental Rights Emergency: The Situation of Persons Crossing the Greek Land Border in an Irregular Manner*. Vienna, European Union Agency for Fundamental Rights, 2011.

Gamson, W. A. *Talking Politics*: Cambridge University Press, 1992.

Geddes, A. and Lazarou, E. *Europeanization of Migration Policy and Narratives of Migration Management: The case of Greece*, Sussex: Paper presented at EPRC Workshop Narratives of Migration

Management and Cooperation. Sussex Centre for Migration Research, University of Sussex, 2008.
Goffman, E. *Frame Analysis: An Essay on the Organization of Experience*. Cambridge MA: Harvard University Press, 1974.
Grand Chamber MSS v. *Belgium and Greece* (30696/2009, 21.1.2011).
Hellenic League for Human Rights. *Report about the detention facilities of undocumented migrants in Rodopi and Evros*. Athens, Hellenic League for Human Rights, 2009.
Horii, S. "It Is About More Than Just Training: The Effect of Frontex Border Guard Training." *Refugee Survey Quarterly* 31, 4 (2012): 158-177.
HRW, *Unwelcome Guests: Greek Police abuses of migrants in Athens*, New York, Human Rights Watch, 2013.
—. *No refuge: migrants in Greece,* New York, Human Rights Watch, 2009.
—. *Stuck in a revolving door: Iraqis and other asylum seekers and migrants at the Greece/Turkey entrance to the European Union*, New York, Human Rights Watch, 2008.
Ioakeimoglou, E. "Migrants and Employment". In *Migrants in Greece*, 81-94. Athens: Ellinika Grammata, 2001.
IOM. *Migration in Greece: a country profile 2008*, Geneva, International Organization for Migration, 2009.
Iyengar, S. *Is Anyone Responsible? How Television Frames Political Issues*. Chicago: University of Chicago Press, 1994.
Karydis, V. "Criminality or Criminalization of Migrants in Greece? An Attempt at Synthesis". In *The new European criminology: Crime and social order in Europe*, 350-367: Abingdon: Routledge, 1998.
Karyotis, G. "Securitization of Migration in Greece: Process, Motives, and Implications." *International Political Sociology* 6, 4 (2012): 390-408.
—. "The Fallacy of Securitizing Migration: Elite Rationality and Unintended Consequences." In *Security, Insecurity and Migration in Europe,* 13-30. Aldershot: Ashgate, 2011.
Karyotis, G. and Patrikios, S. "Religion, Securitization and Anti-Immigration Attitudes: The Case of Greece." *Journal of Peace Research* 47, 1 (2010): 43-57.
Karyotis, G. and Skleparis, D. "Qui Bono? The Winners and Losers of Securitising Migration." *Griffith Law Review* 22, 3 (2013)
—. "Migrant Mobilisation during the Economic Crisis: Identity Formation and Dilemmas." In *Remapping "Crisis": A Guide to Athens*. Ropley, London: Zero Books, 2013.

King, R., Lazaridis, G. and Tsardanidis, C. G. *Eldorado or Fortress? Migration in Southern Europe*. New York: St. Martin's Press, 2000.

Kokkinis, N. *National security and migration policy*. MA Dissertation: School of National Security, 2009.

Kordalis, V. *New dimensions in Police work as a consequence of the recent policies for legal and illegal immigrants in the European Union and Greece*. MA Dissertation: School of National Security, 2006.

Koukouras, A. *The criminality of aliens in Greece. Myths and reality*. MA Dissertation: School of National Security, 2003.

Lavenex, S. "Migration and the EU's New Eastern Border: Between Realism and Liberalism." *Journal of European Public Policy* 8, 1 (2001): 24-42.

Lazaridis, G., and Skleparis, D. "Securitization of migration and the far right: the case of Greek security professionals." *International Migration* 54, 2 (2016): 176-192.

Lyberaki A., and Pelagidis, T. *The "fear of the foreigner" in the labour market: Tolerations and prejudices in development*. Athens: Polis, 2000.

Manos, D. *Muslim economic migrants in Greece and the relevant Greek policy: approach, weaknesses, problems, and national planning within the context of the European reality and the Middle Eastern instability*. MA Dissertation: Hellenic National Defence College, 2011.

Nelson, T. E., Clawson, R. A. and Oxley, Z. M. "Media Framing of a Civil Liberties Conflict and Its Effect on Tolerance." *American Political Science Review* (1997): 567-583.

Pro Asyl. *Pushed back: systematic human rights violations against refugees in the Aegean Sea and at the Greek-Turkish land border*. Frankfurt, Friends of Pro Asyl, 2013.

—. *Walls of Shame: Accounts from the inside*. Frankfurt, Friends of Pro Asyl, 2012.

—. *The situation is out of control*. Frankfurt, Friends of Pro Asyl, 2008.

—. *The truth may be bitter, but it must be told*. Frankfurt, Friends of Pro Asyl, 2007.

Proto Thema. 10 June 2013, available at http://www.protothema.gr/.

Rahimi v *Greece* (8687/2008, 4.7.2011).

Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), OJ 2013 L180/31.

RU v *Greece* (2237/2008, 7.6.2011).
Russia Today, 16 May 2012, available at http://rt.com/.
Scheufele, D. A. "Framing as a Theory of Media Effects." *Journal of Communication* 49, 1 (1999): 103-122.
SD v *Greece* (53541/2007, 11.6.2009).
Skleparis, D. "(In)securitization and illiberal practices on the fringe of the EU." *European Security* 25, 1 (2016): 92-111.
Swarts, J. and Karakatsanis, N. M. "Challenges to Desecuritizing Migration in Greece." *Journal of Balkan and Near Eastern Studies* 15, (2013): 97-120.
—. "The Securitization of Migration: Greece in the 1990s." *Journal of Balkan and Near Eastern Studies* 14, (2012): 33-51.
Tabesh v *Greece* (8256/2007, 26.11.2009).
Triandafyllidou, A. "Greek Immigration Policy at the Turn of the 21st Century. Lack of Political Will or Purposeful Mismanagement?" *European Journal of Migration and Law* 11, 2 (2009): 159-178.
Triandafyllidou, A., Dimitriadi, A., Maroufof, M., Hatziprokopiou, P., Gemi, E., Nikolova, M., and Yousef, K. *Migration in Greece: People, Policies and Practices*. Athens: ELIAMEP and EUI, 2013.
Triandafyllidou, A., Maroufof, M. and Nikolova, M. *Greece: Immigration Towards Greece at the Eve of the 21st Century. A Critical Assessment*. Athens: ELIAMEP IDEAS Working Paper 4, 2009.
Tsironis, D., Stamatiadis, G., Daviotis, L., Tsitsimpikos, N., Liakos, G., Papathanasiou, V., Kamnis, I., Varzakis, A., Lerakis, K., Diamantaki, I., and Barkatsas, G. *Guarding land and sea borders and illegal migration in Greece and the European Union*. MA Dissertation: Hellenic National Defence College, 2009.
UNHCR. Briefing Notes, 21 September 2010, http://www.unhcr.org/4c98a0ac9.html.
UNHCR. *Observations on Greece as a country of asylum,* Geneva, Office of the United Nations High Commissioner for Refugees, 2009.
Vima. 13 January 2012, http://www.tovima.gr/.

CHAPTER FIVE

THE EUROPEAN UNION AND CYBERSECURITY: A HISTORIOGRAPHY OF AN EMERGING ACTOR'S RESPONSE TO A GLOBAL SECURITY CONCERN

ROBERT S. DEWAR

Introduction

Over the past decade cyberspace has been acknowledged by the European Union (EU) as essential for daily life, protecting fundamental rights and ensuring economic development.[1] In addition, information and communications technology (ICT) has become vital for the smooth operation and functioning of critical infrastructures such as water and electricity supply.[2] Of equal importance is the security and protection of the information and communications networks on which these infrastructures

[1] European Commission. "Final Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime," COM(2000) 890 final, 2.

[2] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance), OJ 2009 L337/37; European Commission, Final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - *"Achievements and next Steps: Towards Global Cyber-Security,"* COM(2011) 163 final.

rely. Despite the importance placed on the role of cyberspace in everyday life, however, the EU's approach to cybersecurity has historically been disjointed and fragmented.[3] The approach has a broad remit, addressing issues as diverse as child pornography, digital copyright infringement, privacy, the protection of critical physical infrastructures and the synergies between civilian and military capabilities.[4] Furthermore, the EU did not use the term "cybersecurity" in legal documents until 2011,[5] referring instead to "network and information security" challenges.[6]

Despite the lack of coherence in EU cybersecurity policy, it is possible to identify five important goals which have endured throughout that policy's development. These goals are: ensuring the economic viability of the online sphere, critical information infrastructure protection (which is addressed in more detail by Bossong in chapter 3), system and network resilience, co-operation and information-sharing amongst vital stakeholders and the reduction of cybercrime. During the course of developing policy in this field, the EU has adhered to these five goals. What has changed over time, however, is the approach taken to achieving these goals. Due to the effects of the political forces at play during key phases of policy development, the EU's approach has shifted from a hard-line, quasi-statist position to an arms-length facilitation role and finally to a middle ground between these two extremes.

This chapter will provide a historiographical examination of the development of EU cybersecurity policy. The aim is to demonstrate the continuity of thematic goals as well as to examine the historical and political context in which policy in this area developed. As a result of this examination it is possible to identify the EU's conceptualisation of cybersecurity: as a set of economic, civilian challenges solved through resilient infrastructures,

---

[3] Klimburg, A., and H. Tiirmaa-Klaar. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU* (Brussels: European Parliament, April 2011), 29.

[4] European Commission, Communication, *Joint Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN(2013) 1 final, 11.

[5] European Commission, "*Achievements and next Steps: Towards Global Cyber-Security."*

[6] As a consequence to this, "network and information security" had become synonymous with "cybersecurity" and the terms are used interchangeably. This chapter adopts this approach.

criminal justice measures and actor co-operation. This conceptualisation sits in contrast to more militarist approaches of other actors such as the North Atlantic Treaty Organisation (NATO).

The development of EU policy in cybersecurity can be divided into three distinct phases, each coinciding with the publication of a strategy document. The initial phase began with the publication in 2001 of a proposal for a European approach to network and information security. This was the first attempt to develop an over-arching cybersecurity strategy.[7] This document was highly prescriptive and sought to codify and define key terms. Instead of using the word "cybersecurity," the EU utilised the phrase "network and information security (NIS)" and provided detailed and specific definitions of the problems faced. Concomitantly, it provided solutions to these problems including requirements for action from key actors. It was in this first phase that the five goals of EU cybersecurity policy were first promulgated.

The second phase began in 2006 with the publication of a strategy for a secure information society.[8] Released in the shadow of the failure of the proposed Constitutional Treaty this strategy moved away from hard-line regulation and prescribed action while continuing to focus on the NIS goals established in 2001. It sought to establish an arms-length approach, facilitating and encouraging voluntary action and co-operation, reflecting attempts to rein in what was seen at the time as a drive towards the establishment of a European super-state.[9]

The third and final phase of this developmental process began in 2013, with the publication of the Cybersecurity Strategy of the EU.[10] While this strategy continued the policy goals established by its predecessors, it sought to ensure that cooperation was both facilitated and if necessary

[7] European Commission, Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - *Network and Information Security: Proposal for A European Policy Approach*, COM(2001) 298 final.
[8] European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A Strategy for a Secure Information Society – 'Dialogue, Partnership and Empowerment,'* COM(2006) 251 final.
[9] Bache, I., S. George, and S. Bulmer, *Politics in the European Union*. (Oxford: Oxford University Press, 2011), 212.
[10] European Commission, *Cybersecurity Strategy.*

enforced in certain vital areas. This represents a middle-ground between the hard-line regulatory and integrationist approach of 2001, and the arms-length approach of 2006. This was due to the publication of the 2013 strategy following a period of major institutional change in the EU. In 2009 the Treaty of Lisbon came into force, abolishing the pillar structure of European governance, and enabling a number of agencies and Directorates-General (DGs) to work together. This created a more streamlined approach to a number of policy areas, including cybersecurity. These agencies and DGs had previously been working independently on aspects of cybersecurity, but with considerable overlap. The result was that the 2013 strategy consolidated, under a single banner, a number of measures and initiatives, including those addressed in other EU strategies such as the Internal Security Strategy[11] and the Digital Agenda.[12]

Phase 1: 2001 to 2006 – the Era of Definition

Defining the Problem and Creating Path Dependency - The Core Tenets of EU Cybersecurity

Prior to 2001, the EU's approach to cybersecurity consisted of a primordial soup of varying types of legislation. An array of regulations, policies and Council resolutions addressed issues ranging from establishing generic research programmes[13] to the disposal of electronic devices,[14] as well as more recognisable issues such as personal privacy[15] and unauthorised

[11] European Commission, Final Communication from the Commission to the European Parliament and the Council - *The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe*. Communication. European Commission, November 22, 2010, COM(2010) 673 final.

[12] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - *A Digital Agenda for Europe*, COM(2010) 245 final.

[13] Council Decision 85/141/EEC of 11 February 1985 adopting the 1985 work programme for the European Strategic Programme for Research and Development in Information Technologies: ESPRIT, OJ 1985 L55/1.

[14] Council Regulation (EC) No 2937/95 of 20 December 1995 amending Regulation (EEC) No 2887/93 by imposing an additional anti-dumping duty on imports of certain electronic weighing scales originating in Singapore, OJ 1995 L307/30.

[15] EEA Joint Parliamentary Committee, *Recommendations of the EEA Joint Parliamentary Committee Adopted in Brussels on 13 October 1994*, October 13, 1994, 21994D1217(12); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

access to the communications of the European Commission.[16] Criminal activity enabled by online communications was addressed in specific policy documents including a Commission Communication of 2000, entitled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime."[17] There was, however, no overarching strategy covering security issues in cyberspace.

Seeing the need to ensure popular trust and confidence in an increasingly interconnected society and information-driven economy, the European Council, under the presidency of Sweden, resolved in 2001 to work with the Commission to develop a "comprehensive strategy on the security of electronic networks including practical implementing action."[18] The driving force for this move was the recognition that ICT was becoming increasingly important to economic growth, competitiveness and the development of a more inclusive society.[19] The result of this impetus was the first formal attempt to produce a unified EU policy dealing with cybersecurity; a document entitled "Network and Information Security: Proposal for a European Policy Approach" published by the European Commission in 2001.

The 2001 Proposal was influential in the development of EU cybersecurity policy for two reasons. First, it provided a definition of network and information security (NIS) which would be the cornerstone of EU policy in this field for twelve years, establishing the conceptual basis on which to build policy, strategy and solutions. This brought a level of clarity, consistency and commonality of understanding to EU policy in this field and set the tone for future attempts to revise or revivify policy in this area. While some commentators have argued that the European cybersecurity policy at the time suffered from a lack of cohesion, a high level of fragmentation and duplication[20] amongst competing legislation, strategy

processing of personal data and on the free movement of such data, OJ 1995 L281/31.

[16] Council Decision 86/23/EEC of 4 February 1986 Relating to the Coordinated Development of Computerized Administrative Procedures (CD Project), 1986, OJ 1986 L33/28.

[17] European Commission, "Creating a Safer Information Society".

[18] European Council. "Conclusions of the European Council - Stockholm 23-24 March 2001." European Union, March 24, 2001.

[19] Ibid.; European Commission, "Creating a Safer Information Society", 2.

[20] Cornish, P. *Cyber Security and Politically, Socially and Religiously Motivated*

initiatives and agencies, the overall themes identified here endure and can be found in the EU cybersecurity strategy. Predicated upon ensuring the confidentiality, integrity, authentication and availability of data,[21] NIS was defined as "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems".[22]

In addition to a definition of NIS itself, the 2001 Proposal laid out a specific threat typology comprising six areas of risk. These areas were:

1. Interception of communications;
2. Unauthorised access into (*sic*) computers and computer networks;
3. Disruption of the Internet and telephone networks;
4. Execution of malicious software that modifies or destroys data;
5. Malicious misrepresentation;
6. Environmental and unintentional events.[23]

The aim of providing these definitions was to give a comprehensive breakdown of the types of risks faced by national and private operators.

The second reason for the 2001 NIS Proposal's importance was that, in addition to providing definitions which have endured, it established a number of policies and goals which have also endured throughout the development of EU cybersecurity policy and continue to define the European approach to security challenges in cyberspace. These are: a prioritisation on securing the economic potential and viability of cyberspace; protecting critical information networks on which financial and other infrastructures rely; ensuring the resilience of systems and networks; a focus on facilitating and enabling co-operation between actors; and finally

---

Cyber Attacks. Study. Directorate General External Policies of the Union. (Brussels: European Parliament, 2009), 3; Klimburg and Tiirmaa-Klaar, *Cybersecurity*, 29.

[21] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 9. This is the so-called "CIA Triangle" of information security. See Ning, H., H. Liu, and L.T. Yang. "Cyberentity Security in the Internet of Things," *Computer* 46, 4 (2013): 46–53.

[22] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 9.

[23] Ibid., 5.

a focus on cybercrime – the criminal use of information and communications technology.

The NIS Proposal was published in 2001 under the aegis of the Communities' pillar of EU governance, as it then was. Its primary aim, therefore, was "to ensure the economic viability of information networks and infrastructures," going so far as to argue that security itself was a commodity bought and sold on the open market.[24] Its rationale was to focus on data protection, ensuring a functioning economy, national security in the form of protecting critical physical infrastructures and the promotion of e-commerce. This established the clear financial focus of EU policy towards cybersecurity, and ensured that what were termed "market imperfections" (gaps caused by security solutions not being considered profitable) were addressed.[25] The EU therefore sought to implement specific information security measures which would have two goals: the first was to support the market-oriented standardisation of communications protocols and interfaces. This was in order that private companies' networks can be interoperable, and hence be able to take up standard security solutions.[26] The second goal was to harmonise the regulatory framework then in place regarding telecommunications, data protection and cybercrime. In short, legislation current at that time regarding privacy and access, which is addressed by Grant in chapter 7, was to be extended into the information technology sphere, as there was already "a legal obligation for operators and service providers to ensure a certain level of security."[27] What was illegal offline would be illegal online. In addition to the prioritisation of the economic viability of the information sphere, the definition of NIS and its accompanying threat typology pointed to two further strategic goals: Critical Information Infrastructure Protection (CIIP) and resilience.

The asset being protected in the NIS Proposal, identified in the definition of network and information security and its threat typology, is the electronic network infrastructure; computer data and the networks used to transmit that data. Hardware may become corrupted due to malicious or accidental damage or human error. In addition data can become corrupted or be falsified. These scenarios are key threats due to the potential cascading impact of an incident from information systems into the

[24] Ibid., 2.
[25] Ibid.
[26] Ibid., 23.
[27] Ibid., 19.

physical infrastructures that rely on functioning communications networks. Such acts are illegal and are prosecuted in the same manner as criminal damage and financial fraud in the physical world.[28] Information networks must therefore be protected in order to prevent such scenarios occurring, or to minimise the damage if they do. CIIP has become fundamental in the EU cybersecurity strategy.

What was vital to the EU model of NIS and its focus on CIIP was the ability of systems and networks to withstand the threats identified in the typology published in the NIS Proposal of 2001. CIIP was described here as a process of ensuring that the hardware, software and electronic data required to support networked communications was able to resist the consequences of accidental or malicious incidents, in order to continue functioning, and providing the services for which they were designed.[29] The ability of a system to recover from a natural or man-made shock and continue functioning is more commonly known as resilience,[30] a concept vital for the functioning of financial markets and critical physical infrastructures.

One problem faced by the EU at this point was the ambiguous nature of resilience; it is a concept which has still not been clearly defined when applied to cybersecurity. According to Dunn Cavelty,[31] resilience comes in two types. The first is predicated upon ensuring that networked systems, services and infrastructures continue functioning by being adaptable to the effects of an incident. The second is based on ensuring a return to the *status quo* prior to the occurrence of the incident. If system resilience is what is inferred by the EU in the ability of a network to resist accidental events or malicious actions, the precise nature of that resistance remained unclear. The 2001 NIS Proposal does not stipulate whether systems and networks should be adaptable to events, and thereby continue to provide the services and functions for which they were designed, or have the capability to return to a pre-event situation. Such a lack of clarity is surprising in a document which focusses on defining key terms and

[28] European Commission, "Creating a Safer Information Society", 2.
[29] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 9.
[30] Dunn Cavelty, M., "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15, no. 1 (2013): 105–22, 116.
[31] Dunn Cavelty, M., "Cyber-Security," in *Contemporary Security Studies*, ed. A. Collins, 3rd ed. (Oxford: Oxford University Press, 2012), 19.

extends into solution-building. This raises another problem: how to achieve the goals of protecting critical infrastructures and ensure network resilience for economic purposes, goals set out in the European NIS policy proposal in 2001.

The 2001 NIS Proposal specifies a number of solutions to the threats and risks that it identifies. Among these are the encryption of data and the installation of firewalls and authentication systems by network operators. However, the most prominent measure for ensuring security and minimising risks is actor co-operation, particularly in sharing best practice.[32] One of the most important elements in developing resilient systems to protect critical infrastructures is for the actors involved in service provision and maintenance – the private network operators and national authorities – to exchange information on threats as they occur. It was noted that experienced engineers were surprised by the novelty of some incidents, which identified the need for a reliable warning system and framework for information-sharing across the EU.[33] It was further noted that Computer Emergency Response Teams (CERTs) had been established in some member states – Belgium was specifically mentioned[34] - but also noted that co-operation between these CERTs was problematic due to differing operational parameters and levels of expertise. The Commission therefore proposed to develop measures to strengthen co-operation and facilitate information exchange, and examine with member states "how to best organise at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats."[35] One of the most important developments in this initial phase, intending to facilitate and expedite co-operation between actors and member states, was the establishment of an agency dedicated to NIS issues.

The European Network and Information Security Agency

The European Network and Information Security Agency (ENISA) was established in 2004 with the objective of enhancing the capabilities of the EU, its member states and the business community, to prevent, address

[32] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 21.
[33] Ibid.
[34] Ibid.
[35] Ibid., 22.

and respond to NIS problems.[36] Its mission was to achieve a high level of network and information security within the EU by building on national and Community efforts[37] in the field, and to operate as a point of reference for advice and information. This function was provided not just to EU institutions and member states, but also to other relevant stakeholders including those in the private sector. This was due to the recognition that the electronic networks and services underpinning them are largely privately owned.[38]

ENISA describes itself as an "Advice Broker."[39] It is an intermediary or conduit for information to and from its various stakeholder groups and the European Commission, ensuring that experiences and best practice are effectively shared and communicated. ENISA also helps its stakeholders address, respond to and prevent NIS problems through publishing "soft law", i.e. advice, assistance[40] and guidelines covering a range of issues. These issues include the development of coherent and holistic national cybersecurity strategies,[41] and best practice regarding minimum security standards.[42] Since its inception ENISA developed rapidly,[43] and by 2013 the agency was recognised as being at the forefront of EU cybersecurity co-ordination.[44] ENISA's remit was expanded in 2013, both in a

[36] ENISA. *Activities – ENISA*. (2005), http://www.enisa.europa.eu/about-enisa/activities.
[37] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ 2004 L77/1, repealed in 2013 and replaced with Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance), OJ 2013 L165/41. Although the founding regulation was repealed, its replacement did not substantially alter the principles under which ENISA was to function.
[38] Regulation (EC) No 460/2004, 2.
[39] ENISA, *Activities - ENISA*.
[40] Robinson, N. "European Cybersecurity Policy," in *Cybersecurity: Public Sector Threats and Responses*, ed. K.J. Andreasson, (Abingdon: CRC Press, 2012), 165.
[41] Falessi, N. *et al*. *National Cyber Security Strategies: An Implementation Guide — ENISA*. Report/Study, December 19, 2012, http://www.enisa.europa.eu/.
[42] ENISA. *Technical Guideline on Minimum Security Measures — ENISA*. Report/Study, December 13, 2011, http://www.enisa.europa.eu/.
[43] Dunn Cavelty, Interview - The Role of the European Union as an Institution in the provision and maintenance of cyber security in Europe, Skype, audio recorded, July 2, 2012.
[44] ENISA. *New Regulation for EU Cybersecurity Agency ENISA, with New Duties*

Regulation being passed covering its mandate and the 2013 Cybersecurity Strategy of the European Union.[45] Part of that expansion included the development of tools to assist in another key goal established in 2001; the fight against cybercrime. This is a task which requires it to work closely with Europol.

Europol and the Fight against Cybercrime

Europol became fully operational in 1999[46] as a centre for co-ordinating cooperation between member states' police forces in combatting terrorism, drug trafficking and other transnational crime.[47] In 2002 a "high-tech crime centre" was established,[48] at the beginning of this first phase of EU cybersecurity policy development. This centre involved online crime experts investigating the specialist areas of child sexual exploitation, payment card fraud and cybercrime, described as "crime areas in which the Internet plays a key role."[49] While card fraud emphasises the EU's commitment to treating NIS issues as criminal acts affecting the Union's economic development, the expansion of Europol's remit into the investigation of online child sexual exploitation demonstrates a widening of the issues that the EU considers a part of cybersecurity. Acts that cause harm not just to physical objects but to people are being included in a wider EU cybersecurity approach.[50] A corollary to this was the enhancement of security measures in order to "make the internet safer from fraudsters, harmful content and technology failures to increase trust amongst investors and consumers."[51]

The sum total of all these measures was that the 2001 NIS Proposal set the

— *ENISA*. Press Release, June 18, 2013, http://www.enisa.europa.eu/.

[45] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance), OJ 2013 L165/41.

[46] Europol. *History: The First Years 1992-2004*. (2013), https://www.europol.europa.eu/.

[47] Europol. *History*, (2013), https://www.europol.europa.eu/.

[48] Europol. *Mandate*, (2013), https://www.europol.europa.eu/.

[49] Ibid.

[50] European Commission, Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - *i2010 – A European Information Society for Growth and Employment*, COM(2005) 229 final, 3.

[51] Ibid., 5.

tone and path of European Union cybersecurity. It established certain key policy goals such as CIIP, resilience and co-operation. The ultimate aim of EU NIS policy in the first phase of its development was the protection of economic viability and capabilities through ensuring that the systems and networks which underpin this economic viability are able to continue functioning and providing the services for which they were designed.[52] The NIS Proposal was a key element of this policy, and sought to define exactly what NIS was, clarify the threats involved and provide a clear policy framework in order to address those threats. This framework was based on harmonising private sector protocols, the sharing of information on security breaches, ensuring the continuity of critical services and an explicit commitment to treat malicious incidents as criminal acts.

What differed over the next 12 years was the approach taken to operationalising and achieving these goals. The period following the publication of the NIS Proposal was characterised by the passing of a comparatively large volume of legislation in the field, which addressed the areas of data integrity and privacy protection, but which retained a strong economic focus, an issue further examined by Grant in chapter 7 of this book. Directive 2002/21/EC,[53] for example, required electronic service providers to notify national authorities of security breaches while Directive 2002/58/EC[54] on data protection and privacy sought to enshrine in law key principles of online security in order to encourage businesses and private individuals to conduct commerce via the Internet. In addition, Decision 2005/222/JHA[55] required all member states to introduce

[52] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 3.

[53] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ 2002 L108/33, Article 5; European Commission. *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*, COM(2013) 48 final, 14.

[54] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L201/37.

[55] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ 2005 L69/67, now replaced by Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ 2013 L218/8; Klimburg and Tiirmaa-Klaar, *Cybersecurity*, 30.

legislation to deal with the principal forms of cyber-incidents.

While economic development was clearly the priority for this vision, EU citizens needed to trust the networks and systems which would drive this development. The need to enhance security to ensure this trust led to the conceptualisation of NIS established in 2001 – that set of socio-economic, criminal justice challenges manifested in cyberspace – being revisited in 2006. There was a desire to increase awareness of cybersecurity issues and revitalise the EU's policy in that field, particularly by encouraging co-operation with the private sector. This was manifested in the strategic goal of defining and implementing a strategy for a secure European information society by 2006. This goal was expressed in the EU's i2010 programme,[56] which laid out broad policy orientations for a European Information Society, involving the promotion of a competitive and vibrant digital economy and society.[57]

Phase 2: 2006 to 2013 – A Crisis of Confidence

The second phase in the development of EU cybersecurity began with the publication in 2006 of the Strategy for a Secure Information Society – "Dialogue, partnership and empowerment." This strategy can be seen as a sequel to its predecessor as it continued a number of important themes. It was intended to revitalise and revivify efforts in NIS,[58] and directly quoted the earlier definition of the concept established in 2001. It continued to prioritise economic viability, stating that "the relevance of the ICT sector for the European economy and for European society as a whole is incontestable"[59] as, by 2006, ICT was responsible for nearly 40% of economic productivity.[60] In addition, security breaches eroded trust in electronic communications and therefore citizens' willingness to invest in and use online technologies, which would be detrimental to the EU's economic development.

The goal of protecting critical information infrastructures was reaffirmed given their role in the economic and societal growth of the EU[61] and the reliance of physical infrastructures on ICT. Furthermore, the EU's

[56] European Commission, *i2010*, 6.
[57] Ibid., 3.
[58] European Commission, *A Strategy for a Secure Information Society*, 3.
[59] Ibid., 5.
[60] Ibid.
[61] Ibid.

commitment to fighting cybercrime continued as NIS threats had the potential to affect citizens in their everyday lives. Yet while the 2001 definitions of NIS remained, gone were the detailed, specific typologies of threats and the apportionment of specific responsibilities for addressing those threats.

A Shift of Approach – Partnership, Soft-Law and Encouragement

What differentiated the 2006 Secure Information Society Strategy from the 2001 NIS Proposal was the manner in which the EU sought to achieve its goals. A three-pronged approach was proposed in 2006 comprising specific NIS measures, a regulatory framework for electronic communications and the fight against cybercrime.[62] The second and third prongs found their origins in the proposal of 2001; the regulatory framework sought to ensure a competitive market within the EU and combatting cybercrime was prioritised.

It is the first prong, the "specific NIS measures," which provide the greatest contrast between EU policy in 2001 and 2006. These measures represent a shift in the EU's approach towards facilitating a more holistic, soft-law response to NIS, recognising the roles of the various stakeholders involved.[63] Rather than simply dictating what action public, private and individual actors should take, as was done in 2001, the EU recognised that these actors should be encouraged to be a part of solution-building programmes, and that involvement of the various stakeholders required proper co-ordination.[64]

This represents a shift towards greater inclusiveness and is a significant change in the EU's approach between the Secure Information Society Strategy and its predecessor, not least due to the language used to describe these measures. In 2006 stakeholders were "invited" to enter into partnerships and "encouraged" to share information and best-practice in contrast to earlier provisions which placed requirements on stakeholders. Even the EU's 2009 Communication on CIIP[65] invites member states and

[62] Ibid., 3.
[63] Ibid., 6.
[64] Ibid., 6,10.
[65] European Commission, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions - *Critical Information Infrastructure Protection: Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing*

concerned stakeholders to engage with measures to increase information infrastructure protection through developing national contingencies and co-operating with each other and the EU.[66] ENISA would raise awareness and act as a facilitator. This is in stark contrast to the more definitive language of the 2001 NIS Proposal. While member states and stakeholders were invited and encouraged to engage with certain measures, the NIS Proposal stated that operators should secure networks "as they are required to do under Directive 97/66 EC [on Data Protection in Telecommunications]"[67] and that a balance between network protection and the advantages of open access "must be achieved."[68] By 2006 there had been a clear shift away from a prescriptive attitude of instruction towards a softer tone of encouragement and partnership. That partnership was to involve stakeholders from all areas of NIS and ICT to ensure the availability and integrity of data.[69]

To achieve these goals, the Commission called upon ENISA, in its role as an advice broker, to provide the focal point in this co-ordination, serving as a centre for cooperation, information sharing and the exchange of best practice.[70] One of the methods employed by ENISA to encourage such co-operation was the organisation of a series of international exercises.[71] These simulated a number of NIS incidents targeting critical information infrastructures. The object of these exercises was to examine participants' responses and cooperative capabilities. Named "Cyber Europe," the first exercise took place in November 2010, and brought together representatives from 22 member states and eight observer nations.[72] Two years later Cyber Europe 2012 built on the findings of its predecessor and brought private stakeholders, including financial institutions and internet service providers (ISPs), into the simulations.[73] ENISA also facilitated a transatlantic version of the exercises in 2011 known as Cyber Atlantic. This exercise was carried

---

Preparedness, Security and Resilience, March 30, 2009, COM(2009) 149 final.
[66] Ibid., 8–9.
[67] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 10.
[68] Ibid., 12.
[69] European Commission, *A Strategy for a Secure Information Society*, 8.
[70] Ibid., 6.
[71] European Commission, *Critical Information Infrastructure Protection*, 9.
[72] ENISA. *Cyber Europe 2010 Report — ENISA*. Report/Study, Winter 2011, 3, http://www.enisa.europa.eu/.
[73] ENISA. *Cyber Europe 2012 - Key Findings Report*. ENISA, 2012, 5, http://www.enisa.europa.eu/.

out in co-operation with the EU-US Working Group on Cybersecurity and Cyber Crime.[74] The principal findings of all of these exercises were that, while some work was needed to build capabilities, greater emphasis on training and information-sharing between actors was needed to raise both awareness of existing measures across all stakeholders, and also the level of collective security in the face of large-scale incidents.

What the actions of ENISA and the EU's policy framework at this time demonstrated is that the wider goal in this second phase of cybersecurity policy development was not to establish, identify and publicise EU definitions of terms and challenges, or to prescribe specific courses of action, but to foster an international culture of network and information security[75] where all stakeholders are involved, and NIS is seen as a virtue and commercial opportunity. It is not by accident that the 2006 Strategy was subtitled a "strategy for a secure information society: dialogue, partnership and empowerment." The EU positioned itself as a facilitator of that dialogue, to ensure partnership, and thereby generate empowerment. This is a more arms-length approach to achieving cybersecurity aims and goals. Encouragement, soft-law in the form of strategy documents, and facilitation via ENISA were the new, preferred options. An important factor in this shift away from prescriptive action after only five years was the political climate in which the Secure Information Society Strategy was developed. This was characterised by a wariness of the EU overextending its competences and mandates and adopting the attributes of a state. It led to the constitutional crisis following the failure to ratify the Treaty establishing a Constitution for Europe in 2005. Cybersecurity policy in the mid-2000s was necessarily caught up in this "constitutional impasse."[76]

The 2006 Secure Information Society Strategy was therefore a product of the rejection of certain statist[77] principles proposed in the 2003 draft Constitutional Treaty in favour of a desire to establish an environment where NIS principles would take hold and grow organically, with guidance from the EU. The EU, in turn, adopted a softer stance based on

[74] ENISA. *Cyber Atlantic — ENISA.* 2011, http://www.enisa.europa.eu/.
[75] Robinson, "European Cybersecurity Policy," 165.
[76] Christiansen, T., "The EU Reform Process: From the European Constitution to the Lisbon Treaty," in *National Politics and European Integration: From the Constitution to the Lisbon Treaty*, ed. M. Carbone. (Cheltenham: Edward Elgar Publishing, 2010), 30.
[77] Craig, P., "The Treaty of Lisbon: Process, Architecture and Substance." *European Law Review*, 2 (2008): 137–66, 12.

strategy and policy rather than legislation and prescribed action. However, this then new approach brought into sharp relief a serious problem with the nature of EU cybersecurity in 2006. While the goal was to develop a culture of security, the approach taken by the EU was still highly fragmented. The 2006 strategy sought to galvanise support for a secure information society, building on certain tenets laid down by its 2001 predecessor. However crucial elements of that security were addressed by parallel, often overlapping strategy documents published under the aegis of different Directorates-General. One objective of the 2010 Internal Security Strategy – managed by DG Home Affairs – was "raising levels of security for citizens and businesses in cyberspace."[78] It included provisions for a pan-European office dedicated to cybercrime, a goal officially achieved in 2013 with the establishment of the European Cybercrime Centre at Europol.[79] The 2010 Action Plan adopting the Stockholm Programme for a European "area of freedom, security and justice"[80] sought to promote stakeholder dialogue on illegal online activity related to terrorism and other criminal acts.[81] Finally the 2010 Digital Agenda of the EU – spearheaded by DG CONNECT – aimed to promote the "sustainable economic and social benefits" of digital media.[82] If the period following the publication of the EU's NIS Proposal was characterised by the passing of legislation to protect data integrity and the development of a regulatory framework for electronic communications, then the period after the release of the Secure Information Society Strategy was characterised by the publication of a number of other important documents which overlapped and duplicated key aspects of the remit of that strategy.

A Question of Governance

The reason for the lack of cohesion in 2006 was the governance and policy management system of the EU itself. The Secure Information Society Strategy was a product of "the pillar structure" of policy management[83]

[78] European Commission, *The EU Internal Security Strategy in Action*, 9.
[79] Europol, *A Collective EU Response to Cybercrime*.
[80] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - *Delivering an Area of Freedom, Security and Justice for Europe's Citizens Action Plan Implementing the Stockholm Programme*, COM(2010) 171 final, 2.
[81] Ibid., 39.
[82] European Commission, *A Digital Agenda for Europe*, 3.
[83] Europa, *Pillars of the European Union*.

established by the 1992 Maastricht Treaty. This structure stipulated separate decision-making procedures for certain policy areas.[84] The Secure Information Society Strategy was developed within the framework of Pillar 1 – The Communities – and so focused on matters pertinent to economic development. By contrast, for example, the Internal Security Strategy was developed under the aegis of Pillar 3 – criminal justice and policing. Such a division of remits meant that the stated objective of a holistic multi-stakeholder approach to cybersecurity[85] was still a distant prospect in 2006. Although the NIS Proposal of 2001 had identified important areas of policy and action, drawing these disparate, fragmented and duplicated elements together would require a level of interaction hitherto unknown in EU cybersecurity policy development.

The opportunity to draw these elements together did not come about until 2007, when the Lisbon Treaty created a new legal framework for the re-named European Union[86] and abolished the pillar system. However, the Lisbon Treaty did not come into force until 2009, by which time the EU's Internal Security Strategy, Digital Agenda and Stockholm Programme were at very advanced stages of development and implementation. Nevertheless, the Lisbon Treaty enabled Directorates-General across the former pillars to co-operate rather than duplicate work. This led, for the first time in the history of EU cybersecurity, to a consolidation of all the disparate, fragmented elements, aims, objectives, legislation and policy into a single strategic approach. The result was the Cybersecurity Strategy of the European Union, published in February of 2013. This document ushered in the third phase of EU cybersecurity policy development.

Phase 3: From 2013 – The Era of Consolidation

Whereas the second phase of EU cybersecurity policy development began with the publication of a strategy document amid a major constitutional crisis, the third phase began with the publication of a strategy document following a major constitutional change. A number of separate policy and strategy streams were, post-Lisbon, consolidated into one document representing a unified policy for the EU. This had two profound effects. First, it enabled for the first time Directorates-General of the European Commission to work more closely together to develop a truly holistic

[84] Ibid.
[85] European Commission. *A Strategy for a Secure Information Society*, 10.
[86] Europa. *Pillars of the European Union*.

approach to cybersecurity challenges. Second, it enabled the EU to develop its capacity as an actor in a number of additional areas, most notably cyber-defence. These two fundamental changes were encapsulated in the first unified approach of the EU to network and information security: The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.[87]

Thematic Continuity and Operational Change

From the outset, the 2013 Cybersecurity Strategy continues to focus on goals laid out in the 2001 NIS Proposal and reaffirmed in the 2006 Secure Information Society Strategy, demonstrating a strong thematic continuity between the three documents. Priority was still placed on the economic viability of the online sphere.[88] CIIP is crucial to safeguarding this viability.[89] All three documents were based on the principle that the Internet and cyberspace must remain free and open in order to ensure economic prosperity, and must remain secure in order that citizens have trust and confidence in online commerce.[90] Achieving cyber resilience[91] is retained as a key goal through "developing the industrial and technological resources for cybersecurity,"[92] and reinforcing the EU's commitment to co-operation between public authorities and the private sector. This co-operation is voluntary and further illustrates the EU's commitment to encouragement and facilitation of co-operation rather than hard legislation.

Despite promoting voluntary co-operation and information sharing, the EU acknowledged that encouragement and voluntary codes of practice can only achieve so much. Having regained some of the confidence lost in the 2003-5 constitutional crisis the EU was willing to assert itself and propose legislation in certain key areas such as security breach notification. In what was a step-change in the EU's approach to fostering information-sharing and collaboration, a directive proposed in 2013 concerning measures to ensure a high common level of network and information security across the Union[93] (which is to be considered in parallel to the Cybersecurity

[87] European Commission. *Cybersecurity Strategy*.
[88] Ibid., 2.
[89] Ibid., 3, at footnote 4.
[90] European Commission. *Proposal for a Directive Concerning NIS*, 3.
[91] European Commission. *Cybersecurity Strategy*, 5.
[92] Ibid., 12.
[93] European Commission. *Proposal for a Directive Concerning NIS*.

Strategy[94]) built on the requirements of the 2002 Directive on a regulatory framework for electronic communications.[95] While the 2002 Directive required electronic service providers to notify national authorities of security breaches,[96] the directive proposed in 2013 would expand this requirement to cover hardware manufacturers, financial and health institutions and utilities provider; in short, any area providing "vital economical (sic) or societal functions" in the EU.[97] In addition, the proposal would also require all member states to establish Computer Emergency Response Teams (CERTs) and develop formal cybersecurity strategies with minimum operating capacities,[98] thereby enforcing the harmonisation of cybersecurity responses across the whole of the EU. Under the terms of the 2013 Cybersecurity Strategy, ENISA is tasked with assisting member state governments with developing these strategies. This demonstrates that, while seeking to promote voluntary co-operation, the EU was not afraid to enforce this level of co-operation on its member states when it is not forthcoming.

In a further example of regained confidence, the roles of both ENISA and Europol in the field of cybercrime were being greatly increased. ENISA was tasked with identifying trends and patterns in cybercrime and assisting Union institutions with raising awareness of criminal threats from cyberspace.[99] Europol's internal high-tech crime centre was given greater recognition and was established as the European Cybercrime Centre (EC3). This change came into effect on 1 January 2013. As a result, the EC3 is a "focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and co-operation with international partners in the pursuit of an EU free from cybercrime."[100]

In addition to the establishment of a pan-European cybercrime response via the EC3 at Europol, member states were also advised to adopt the Council of Europe (CoE) Convention on Cybercrime, more commonly

[94] Ibid., 2.
[95] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.
[96] Ibid., 40; European Commission, P*roposal for a Directive Concerning NIS*, 14.
[97] European Commission, *Proposal for a Directive Concerning NIS*, 14.
[98] Ibid., 4.
[99] European Commission, *Cybersecurity Strategy*, 14. See also Regulation (EU) No 526/2013, 44.
[100] Europol, *A Collective EU Response to Cybercrime*.

known as the Budapest Convention,[101] as a framework for their own national legislation. Drafted by a Committee of Experts from CoE member states as well as four observers countries – the United States, Australia, Canada and South Africa[102] – the Budapest Convention was established in 2001 and entered into force in 2004.[103] To date, 55 countries have ratified the Convention, including the United States.[104] It covers a range of agreed crimes including those where computers or computer networks are both the targets and tools of criminal activity[105] as well as content related offences, particularly those relating to child pornography.[106] In essence, the Convention sets out a framework for internationally agreed criminal acts carried out in the online sphere, providing a basis for national policy and legislation. The basic premise is that whatever is illegal in the physical world is illegal in the online world.

Of particular note is the fact that the EU made no mention or endorsement of the Convention in its official policy and strategy literature until 2013. The Convention represents an important but belated addition to the EU's cybersecurity response. One possible reason for this is again the question of competence. The EU has no mandate to adopt the Convention unilaterally and individual member states can only be encouraged to sign up to and ratify it. Nevertheless, it is surprising that the only current international treaty to address a cybersecurity issue was not referred to in any EU strategy or policy before 2013. Although the EU clearly values the Budapest Convention given its endorsement in the Cybersecurity Strategy the reasons for its earlier omission are unclear.

The Cybersecurity Strategy therefore represents another important shift in the dynamic of the EU's response to cybersecurity as a whole. By 2013 the EU had taken on a much more active role in the field, particularly in the area of cybercrime. Previous strategies, while acknowledging the threat of online criminal activity, have nevertheless placed the ultimate responsibility

[101] Council of Europe, "Convention on Cybercrime."
[102] Porcedda, M.G. *Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?* Working Paper, 2012. http://cadmus.eui.eu/handle/1814/23296, 28.
[103] Clough, J., "The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World," *Criminal Law Forum* 23 (2012): 363–91, 368.
[104] Council of Europe, "Council of Europe Convention on Cybercrime Signatories."
[105] Clough, "The Council of Europe Convention on Cybercrime," 371–372.
[106] Porcedda, *Data Protection and the Prevention of Cybercrime*, 36.

for security on the member states themselves.[107] The EU's role was to be one of co-ordinating efforts and ensuring coherence and consistency in national measures. By taking such action as expanding and formalising Europol's cybercrime activities as a European centre, the EU is addressing the problem of cybercrime and engaging in the dismantling and disruption of criminal networks.[108] This was representative of a new-found confidence and affirmative action in EU strategy post-Lisbon. Part of this affirmative action was not only to directly engage in attempts to reduce cybercrime but, according to the strategy's fifth key priority, to raise the EU's international profile by "establishing coherent international policy…and promote core EU values,"[109] thereby increasing its presence on the international stage. This was a clear expression of intent; it could be argued that the EU was establishing itself as an actor in cybersecurity in its own right on the international political stage, beyond the European context, and not merely as a representative of its member states as "the time has come for the EU to step up its actions in [the area of cybersecurity]."[110]

The Impact of the Lisbon Treaty

While the EU was asserting itself in policy goals established in 2001 and reaffirmed in 2006, the 2013 strategy represented a departure from its predecessors in two important ways. The first was the application of wider EU principles to the area of cybersecurity, bringing them into line with other areas of policy and strategy. The second was the recognition of the threat of state-sponsored cyber incidents, discussed further below.

The 2013 strategy avoided definitive descriptions of either threats or solutions. Instead, key strategic priorities for EU-wide cybersecurity were located within a set of broad principles:

1. The EU's core values apply as much in the digital as in the physical world.
2. Protection of fundamental rights, particularly freedom of expression, personal data and privacy.[111]
3. Access for all.

[107] European Commission, *Network and Information Security: Proposal for A European Policy Approach*, 16.
[108] European Commission, *Cybersecurity Strategy*, 11.
[109] Ibid., 14.
[110] Ibid., 3.
[111] Issues further developed by O'Neill in chapter 3, and Grant in chapter 7.

4. Democratic and efficient multi-stakeholder governance.
5. A shared responsibility to ensure security.[112]

These principles mean that cybersecurity issues were not a separate section of policy, but part of the EU's wider vision of a safe space where the fundamental rights of citizens are protected. The Lisbon Treaty changes enabled cybersecurity to be placed within the wider framework of protecting fundamental rights and responsibilities.[113] This in turn allowed for the consolidation into one document of the relevant elements of those strategies published between 2006 and 2013 which contained a component of cybersecurity. The 2013 Cybersecurity Strategy described the EU's space being a safe place to live and conduct business, as further developed by the Stockholm Programme.[114] Digital illiteracy was to be combatted so that everyone could benefit from the economic potential of cyberspace as set out in the Digital Agenda of 2010. Cooperation between all stakeholders was also to be promoted, ensuring that everyone accepts and acts on their shared security responsibilities, as expounded in the Internal Security Strategy of 2010.[115]

Extending this process of consolidating relevant policy areas, the Lisbon Treaty in 2009 enabled policy-makers working on EU cybersecurity to set the strategic priority of "developing cyber-defence policy and capabilities within the Common Security and Defence Policy,"[116] something not previously addressed in the context of cybersecurity. This was potentially the most important policy shift in comparison to the 2001 and 2006 documents. This change was based upon the recognition of the potential for state-sanctioned or state-sponsored cybersecurity incidents,[117] and was a response to several significant recent historical events, discussed below.

Cybersecurity or Cyber-Defence? State-Sponsored Cyber-attacks

Between 2006 and 2013 a number of international incidents occurred which added a new dimension to political discussions of cybersecurity issues. In 2007, following a decision by the Estonian government to move a Soviet-

[112] European Commission, *Cybersecurity Strategy*, 3–4.
[113] The issues of fundamental and human rights in the post-Lisbon era are analysed by O'Neill in chapter 3.
[114] European Commission, *Implementing the Stockholm Programme*.
[115] European Commission, *The EU Internal Security Strategy in Action*, 9.
[116] European Commission, *Cybersecurity Strategy*, 11.
[117] Ibid., 3.

era war memorial from the centre of the capital Tallinn to its outskirts, Estonia experienced a series of distributed denial of service (DDoS) attacks which affected banking and government websites. In 2008, during the Russo-Georgian conflict over the South Ossetia region, Georgian government websites were defaced amid a DDoS attack similar to that experienced by Estonia. In 2010, a computer virus labelled Stuxnet was found to have fed corrupted data into an Iranian nuclear facility, causing a significant number of enrichment centrifuges to spin out of control, damaging them and rendering them inoperative.

Allegations of responsibility were made against Russia in the cases of Estonia and Georgia, due to the political situations of the time, and the Stuxnet virus was alleged to have been an attempt by the USA and Israel to halt or at least hinder Iran's suspected nuclear weapons programme.[118] What made these incidents so significant was that they appeared to indicate a previously unknown level of state involvement in the aggressive, quasi-military use of computer networked technology.[119] While previous incidents alleging state involvement had focussed on espionage, the theft of intellectual property and state governments restricting the internet access of their own citizens,[120] the period between the publication the EU's Safer Information Society Strategy in 2006 and its Cybersecurity Strategy in 2013 saw an apparent escalation of the use of networked computer technology almost to the level of weaponisation.[121]

---

[118] Dunn Cavelty, M., "The Militarisation of Cyber Security as a Source of Global Tension," in *Strategic Trends Analysis*, ed. D. Möckli and A. Wenger (Zurich, Switzerland: Center for Security Studies, 2012), 111-112.

[119] Unknown in the sense of not being in the public domain. There are potentially a much greater number of earlier incidents which have remained classified and so are not matters of public knowledge.

[120] Deibert, R.J. "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace," in *Routledge Handbook of Internet Politics*, ed. A. Chadwick and P. N. Howard, (London: Routledge, 2009), 323–36; Rid, T. "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, 1 (2012): 5–32; Segal, A. "From Titan Rain to Byzantine Hades: Chinese Cyber Espionage," in *A Fierce Domain: Conflict in Cyberspace 1986-2012*, ed. J. Healey, (USA: CCSA, 2013), 165–73.

[121] Langner, R. "Stuxnet: Dissecting a Cyberwarfare Weapon," *Security & Privacy, IEEE* 9, 3 (2011): 49–51. There was a very active debate on whether these incidents classify as armed attacks or were examples of a new form of warfare. For examples of this debate see Schmitt, M.N. "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework," in *Essays on Law and War at the Fault Lines*, (New York: Springer, 2012) 3–48; Rid, "Cyber War."

This led to an increase in the development of national cybersecurity strategies throughout the world,[122] with the UK placing cybersecurity threats on an equal footing with terrorism.[123]

There is always a risk of falling into the trap of hypersecuritising cyber-defence phenomena such as the Estonian, Georgian and Stuxnet examples.[124] Analyses of data concerning cyber-incidents point to such examples being relatively rare.[125] Nevertheless, these three examples indicated a new dimension to the security concerns of the EU. The Union had a responsibility to acknowledge these issues and formulate a policy response, especially as it had taken it upon itself to step up its cybersecurity actions, and to raise its international profile in the field more generally.[126] While responsibility remains primarily with the member states to secure cyberspace for national security purposes,[127] the EU cannot be seen to be ignoring the incidents of 2007-2010.

An issue for the EU in this area was that it had no competence for wide-ranging involvement or engagement in national security issues.[128] Although the European Defence Agency (EDA) was set up in 2004, it existed to support member states in developing collaborative defence capabilities and research. Its cyber-defence project team was intended to be used as a vector for co-ordination.[129] Operational military capabilities

[122] ENISA. *National Cyber Security Strategies in the World — ENISA.* 2013, http://www.enisa.europa.eu/. This website provides a list of published cyber security strategies with their publication dates. Most of these were published 2011-2012. Although some countries, notably the UK and the USA had strategies before 2007, these were updated in 2011.

[123] United Kingdom. *The National Security Strategy - a Strong Britain in an Age of Uncertainty* - Publications - GOV.UK, October 18, 2010, 11.

[124] Hansen, L. and H. Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155–75, 1163; Dunn Cavelty, "Militarisation of Cyber Security," 111.

[125] Valeriano, B. and R. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11," *Journal of Peace Research*, April 2014, 9.

[126] European Commission, *A Strategy for a Secure Information Society*, 4, 7.

[127] European Commission, *Cybersecurity Strategy*, 11.

[128] Robinson, "European Cybersecurity Policy," 161.

[129] Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency, OJ 2004 L245/17, then repealed and replaced by Council Decision 2011/411/CFSP of 12 July 2011 defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action

and mutual assistance between nations were already assured through NATO treaty provisions, many of whose signatories were also EU member states. Under EU treaty stipulations, national and military security matters remain the prerogative of individual member states. Further complicating the political situation, all areas of shared competence, such as the Area of Freedom, Security and Justice, are subject to the principle of subsidiarity, meaning that decisions should be taken at a level as close to the citizen as possible, except where there is a clear, logical and effective reason not to do so.[130] Transnational issues such as organised crime and human trafficking are addressed at the EU level because these issues cross borders. So too, however, do malicious or accidental NIS incidents. It therefore makes sense for the EU to address cybersecurity in the same way as transnational organised crime. Cyber incidents, if severe enough and involving inter-state action, can however threaten the national security of a member state – an individual member state issue – as well as the infrastructure and functioning of the EU as a whole, making them an EU issue.

As a result of treaty-defined competence limitations[131] and the operation of the principle of subsidiarity, the EU must tread a very fine line between not involving itself in national security issues – which might also have potential military applications (at most an EU intergovernmental issue) and which may also overlap with NATO missions – and the need to address the transnational nature of cybersecurity threats. The 2013 Cybersecurity Strategy sought to set out how the EU will tread these lines. It recognised that it was predominantly the task of member states to deal with security in cyberspace, but there were actions the EU could take.[132] These actions are not dissimilar to the EU's wider response to cybersecurity; a focus on co-ordination and leadership in the promotion of cyber-defence capabilities through encouraging interoperability amongst

---

2004/551/CFSP, OJ 2011 L183/16; European Commission, *Cybersecurity Strategy*, 18.

[130] *Treaty on European Union*, Article 5.

[131] There was a very active debate about the precise nature of the security competence of the EU, and whether or not the Treaty of Lisbon abolished the Pillar system *de jure*, but due to the still undefined nature of competence in the area, the CFSP remains a *de facto* pillar. See Craig, *The Lisbon Treaty*; Laursen, Finn. "The EU as an International Political and Security Actor after the Treaty of Lisbon: An Academic Perspective," in *Jean Monnet Conference on the Lisbon Treaty,* (2010), 25–26.

[132] European Commission, *Cybersecurity Strategy*, 11.

stakeholders, working with international partners such as NATO and promoting dialogue between military and civilian actors to promote exchanges of good practice and information.[133] While recognising that cybersecurity is made more complex by the potential for state involvement in destructive incidents, the EU was not engaging directly in military or national security issues. It provided a leadership role in co-ordinating efforts while remaining within its treaty obligations and limitations.

The 2013 Strategy was therefore a crucial document in the development of EU policy and action in the field of cybersecurity. It brought together a number of related, but previously disparate elements. Until 2013 the EU's cybersecurity policy was highly fragmented, with separate strategies such as the Digital Agenda and the Internal Security Strategy making oblique references to its individual elements. The 2013 Cybersecurity Strategy consolidated the relevant policy and legislative provisions into one holistic document. It also showed that the EU was capable of demonstrating strong leadership and could enforce the sharing of information on security breaches, which was an important development. Furthermore, the EU was also responding to then recent events. The development of cyber-defence capabilities demonstrated a willingness both to respond to the cybersecurity climate of the time, but also to increase the EU's international standing. It is perhaps too early to say whether the 2013 strategy represents a "coming of age" for the EU vis-à-vis cybersecurity, but the Union is taking a more direct role in such issues as the fight against cybercrime, and is asserting itself as an actor on this issue at an international level.

Conclusions: A European approach to cybersecurity?

The history of EU cybersecurity policy is one of consistent priorities but shifting approaches. Through the publication of "Network and Information Security: Proposal for a European Policy Approach" in 2001 the EU sought to define both the problem (network and information security) and the solutions to that problem. Critical information infrastructure protection, through resilient networks and systems, was the goal. This was to be achieved through co-operation and reducing cybercrime in order to ensure the economic viability of the online sphere. In addition, specific actions were to be undertaken by specific actors within the framework of existing legislation. In 2006 the EU's Strategy for a Secure Information Society was published in the shadow of the failed Constitutional Treaty.

[133] Ibid., 11–12.

Consequently the EU opted for an arms-length approach predicated on soft-law, recommendations and minimal legislative output. Both documents were hamstrung, however, by the nature of the three-pillar system of governance. Although the 2001 Proposal and 2006 strategy advocated a holistic approach to NIS, such holism was not feasible given the division of remits and responsibilities across the three pillars, namely the European Community, Common Foreign and Security Policy, and post-Amsterdam Treaty provisions on Police and Judicial Co-operation in Criminal Matters.

The 2013 Cybersecurity Strategy was the first EU document to address all aspects of NIS, whether concerned with data, technological infrastructure protection or personal safety from harm. This was only possible under the post-Lisbon legal framework. Eschewing categorical definitions in favour of policy aims within a framework of wider EU principles, 2013 saw the combined activities of ENISA and the EC3 focussing on crime and co-operation firmly establishing an EU conception of cybersecurity as an economic and civilian issue, resolved through resilient infrastructures and actor co-operation.

In addition, the EU needed to cooperate with individual member states and international military partners – such as NATO – in responding to state-sponsored incidents, while still respecting the treaty based limitations on the EU's competences. The EU therefore concentrated predominantly on tackling civilian issues such as cybercrime, while still having its own political response to the precedents of the cyber-incidents in Estonia, Georgia and Iran. National governments had responded to these major international incidents by placing cybersecurity at the forefront of their security policies. The EU, for its part, could not afford to ignore this trend. Such a focus was part of the EU's aim to establish itself as a global actor in this field.

Despite the policy decision to engage in cyber-defence, at least in a nominal capacity, the EU's explicit policy decision was to treat cyber-incidents as primarily economic threats and criminal matters to be prosecuted under national or international civilian law. This is a trait which has endured in spite of many cybersecurity actors adopting militaristic, and what could be described as hypersecuritised, strategies. With its experience of managing and responding to transnational, multilingual and multicultural issues, the EU saw itself as ideally placed to tackle the global issues of cybersecurity head-on. Time will tell whether

this approach to cybersecurity, based on fundamental principles of personal freedom, access for all, democracy and free speech, becomes more widely adopted as a rational paradigm, or is simply a phase in the development of the EU's approach to cybersecurity in a rapidly changing field of global security.

Bibliography

Bache, I., S. George, and S. Bulmer. *Politics in the European Union*. Oxford: Oxford University Press, 2011.

Christiansen, T. "The EU Reform Process: From the European Constitution to the Lisbon Treaty." In *National Politics and European Integration: From the Constitution to the Lisbon Treaty*, ed. M. Carbone. Cheltenham: Edward Elgar Publishing, 2010.

Clough, J. "The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World." *Criminal Law Forum* 23 (2012): 363–91.

Cornish, P. *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*. Study, Directorate General External Policies of the Union. European Parliament, February 2009, http://www.europarl.europa.eu/.

Council Decision 2011/411/CFSP of 12 July 2011 defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFSP, OJ 2011 L183/16.

—. 86/23/EEC of 4 February 1986 Relating to the Coordinated Development of Computerized Administrative Procedures (CD Project), 1986, OJ 1986 L33/28.

—. 85/141/EEC of 11 February 1985 adopting the 1985 work programme for the European Strategic Programme for Research and Development in Information Technologies: ESPRIT, OJ 1985 L55/1.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ 2005 L69/67.

Council of Europe Convention on Cybercrime, November 23, 2001. CETS: 185.

COE.int web site.

Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency, OJ 2004 L245/17.

Council Regulation (EC) No 2937/95 of 20 December 1995 amending Regulation (EEC) No 2887/93 by imposing an additional anti-dumping duty on imports of certain electronic weighing scales originating in Singapore, OJ 1995 L307/30.

Craig, P. *The Lisbon Treaty: Law, Politics, and Treaty Reform*. Oxford:

Oxford University Press, 2010.
—. "The Treaty of Lisbon: Process, Architecture and Substance." *European Law Review*, no. 2 (2008): 137–66.
Deibert, R.J. "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace." In *Routledge Handbook of Internet Politics*, ed. A. Chadwick and P. N. Howard. London: Routledge, 2009.
Dunn Cavelty, M. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15, no. 1 (2013): 105–22.
—. "Cyber-Security." In *Contemporary Security Studies*, ed. A. Collins, 3rd ed. Oxford: Oxford University Press, 2012.
—. Interview - The Role of the European Union as an Institution in the provision and maintenance of cyber security in Europe. Skype, audio recorded, July 2, 2012.
—. "The Militarisation of Cyber Security as a Source of Global Tension." In *Strategic Trends Analysis*, ed. D. Möckli and A. Wenger. Zurich: Center for Security Studies, 2012.
EEA Joint Parliamentary Committee. *Recommendations of the EEA Joint Parliamentary Committee Adopted in Brussels on 13 October 1994*, October 13, 1994, 21994D1217(12).
ENISA. *Activities — ENISA*, http://www.enisa.europa.eu/.
—. *Cyber Atlantic — ENISA*, http://www.enisa.europa.eu/.
—. *New Regulation for EU Cybersecurity Agency ENISA, with New Duties — ENISA. Press Release*, June 18, 2013, http://www.enisa.europa.eu/.
—. *National Cyber Security Strategies in the World — ENISA*. February 7, 2013, http://www.enisa.europa.eu/.
—. *Cyber Europe 2012 - Key Findings Report*. ENISA, December 19, 2012, http://www.enisa.europa.eu/.
—. *Cyber Europe 2010 Report — ENISA*. Report/Study, Winter 2011, http://www.enisa.europa.eu/.
—. *Technical Guideline on Minimum Security Measures — ENISA*. Report/Study, December 13, 2011, http://www.enisa.europa.eu/.
European Commission. *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*, COM(2013) 48 final.
—. *Joint Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN(2013) 1 final.

—. "Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - *on Critical Information Infrastructure Protection - "Achievements and next Steps: Towards Global Cyber-Security"*, COM(2011) 163 final.

—. *Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe*, COM(2010) 673 final.

—. *A Digital Agenda for Europe*, COM(2010) 245 final.

—. *Delivering an Area of Freedom, Security and Justice for Europe's Citizens Action Plan Implementing the Stockholm Programme*. Communication. European Commission, COM(2010) 171 final.

—. *Critical Information Infrastructure Protection: Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience*. March 30, 2009, COM(2009) 149 final.

—. *A Strategy for a Secure Information Society – 'Dialogue, Partnership and Empowerment'*, COM(2006) 251 final.

—. *'i2010 – A European Information Society for Growth and Employment'*, COM(2005) 229 final.

—.*Network and Information Security: Proposal for A European Policy Approach*, COM(2001) 298 final.

—.*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*, COM (2000) 890 final.

European Council. *Conclusions of the European Council - Stockholm 23-24 March 2001*. European Union, March 24, 2001.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ 2013 L218/8.

—. 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance), OJ 2009 L337/37.

—. 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L201/37.

—. 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ 2002 L108/33.
—. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L281/31.
Europol. *A Collective EU Response to Cybercrime*, 2013 https://www.europol.europa.eu/ec3.
—. *History*, 2013, https://www.europol.europa.eu/.
—. *History: The First Years 1992-2004*, 2013, https://www.europol.europa.eu/.
—. *Mandate*, 2013, https://www.europol.europa.eu/.
Falessi, N., R. Gavrila, Maj. R. Klejnstrup, and K. Moulinos. "National Cyber Security Strategies: An Implementation Guide — ENISA." Report/Study, December 19, 2012, http://www.enisa.europa.eu/.
Hansen, L., and H. Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, 4 (2009): 1155–75.
Klimburg, A., and H. Tiirmaa-Klaar. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. Brussels: European Parliament, 2011. Available at http://www.europarl.europa.eu/.
Langner, R. "Stuxnet: Dissecting a Cyberwarfare Weapon." *Security & Privacy, IEEE* 9, 3 (2011): 49–51.
Laursen, F. "The EU as an International Political and Security Actor after the Treaty of Lisbon: An Academic Perspective." In *Jean Monnet Conference on the Lisbon Treaty,* May, 25–26, 2010.
Ning, H., H. Liu, and L.T. Yang. "Cyberentity Security in the Internet of Things." *Computer* 46, no. 4 (2013): 46–53.
Porcedda, M.G. *Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?* Working Paper, 2012, http://cadmus.eui.eu/handle/1814/23296.
Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance), OJ 2013 L165/41.
—. (EC) No 460/2004 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ 2004 L77/1.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

Robinson, N. "European Cybersecurity Policy." In *Cybersecurity: Public Sector Threats and Responses*, ed. K.J. Andreasson. Abingdon: CRC Press, 2012.

Schmitt, M.N. "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework." In *Essays on Law and War at the Fault Lines*, 3–48. New York: Springer, 2012.

Segal, A. "From Titan Rain to Byzantine Hades: Chinese Cyber Espionage." In *A Fierce Domain: Conflict in Cyberspace 1986-2012*, ed. J. Healey, 165–73. USA: CCSA, 2013.

Treaty on European Union.

United Kingdom. *The National Security Strategy - a Strong Britain in an Age of Uncertainty* - Publications - GOV.UK, October 18, 2010.

Valeriano, B. and R. Maness. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11." *Journal of Peace Research*, April 2014.

Data

CHAPTER SIX

THE NEW EUROPOL LEGAL FRAMEWORK: IMPLICATIONS FOR EU EXCHANGES OF INFORMATION IN THE FIELD OF LAW ENFORCEMENT

CRISTINA BLASI CASAGRAN

Introduction

In the aftermath of 9/11, existing counterterrorism laws have been reinforced worldwide. Within the EU, the effort of member states to protect their citizens against other possible attacks is reflected in the increasing number of EU measures adopted within the Area of Freedom, Security and Justice (AFSJ). These measures involve also the enhancement competences of many AFSJ bodies and, particularly, the European Police Office (hereinafter, Europol). Europol was established in 1995 through the Europol Convention, aiming at giving support to member states in preventing and combating serious crimes. That convention was replaced by the Europol Council Decision (ECD) in 2009, the point at which that intergovernmental organisation became an EU agency.

Europol exchanges data on a daily basis, providing a useful tool to law enforcement agencies. Law enforcement authorities in the member states collect a considerable part of the data processed by Europol. Yet, data might also come from other EU agencies (e.g. Eurojust, Frontex, etc.), EU information systems (e.g. the Visa Information System (VIS), the Schengen Information System (SIS), etc.), private entities, third countries and public sources. As a result, Europol is today the EU agency that

processes the greatest volume of information within the EU, exchanging up to 200,000 operational messages in any four-month period.[1]

On 27 March 2013, the Commission launched a proposal for a Europol Regulation, which would repeal the ECD. The explanatory memorandum of the proposal noted that this legal instrument seeks to "grant Europol new responsibilities so that it may provide a more comprehensive support for law enforcement authorities in the Member States."[2] After three years of negotiations, the Europol Regulation came into force in May 2016.[3] The regulation represents a clear enhancement of Europol's competences, which consolidates the value of Europol within and beyond the EU. The regulation introduces some changes, which have been controversial. This chapter will give an overview of the Europol Regulation, and analyse new issues that the Commission has included to improve the coherence and effectiveness of Europol. The primary objective of this study is to identify the new provisions that enhance the ability of Europol to process crime-related information, and conversely identify those provisions which limit Europol when compared to the previous ECD mandate. The interaction of these opposing interests and their implications will be a key factor for the future of Europol, and its operations in the European security environment.

Enhanced competences of Europol in the proposed regulation

This section details how the new regulation enhances Europol competences as regards the processing of information. These new capabilities of Europol can be summarised as follows: i) enhancement of its objectives and tasks, ii) clearer participation in Joint Investigation Teams (JITs), iii) Europol's authority to initiate a criminal investigation, iv) Europol's ability to access and retrieve information from member state's databases; and v) Europol's coordination of an investigation.

---

[1] Communication from the Commission to the European Parliament and the Council. *Second Report on the implementation of the EU Internal Security Strategy*, COM(2013) 179 final, 5.

[2] Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, 5.

[3] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L135/53.

Articles 3 and 4 of the regulation list the objectives and tasks of Europol, which do not vary significantly from those in the previous ECD. Two minor word changes can be identified. First, the emphasis has shifted from "organised crime" to the much broader and less restrictive concept of "serious crime," which will impact on the operation of Europol. Second, Annex I broadens the definition of some of its offences, and adds one completely new one. The broader term "robbery" now replaces "organised robbery;" to the pre-existing swindling and fraud has been expressly added "fraud affecting the financial interests of the Union," and to environmental crimes has been expressly added "including ship source pollution," an issue analysed by Carpenter in chapter 9 of this book. A completely new addition to Europol's competence is the crime of "sexual abuse and exploitation of women and children." As for the new Europol's tasks, the list in Article 4 simplifies the enumeration of the former Article 5 ECD, which was confusingly divided into principal and additional tasks, which were equally important. Lastly, two other new tasks for Europol have been introduced. On the one hand, a provision on technical and financial support to member states' cross-border operations is included. This financial support will be important in the context of current budgetary restraints on many law enforcement agencies. On the other hand, there is now an express legal basis for the development of specialised centres (e.g. the Cybercrime Centre[4] or the office for counterfeiting). It provides a guide to the potential for establishment of other new specially designated centres within Europol in the future.

The alignment of the regulation with the Treaty of Lisbon is manifested in Art. 4(c), which describes the same coordination tasks as those in Art. 88(1)(b) Treaty on the Functioning of the EU (TFEU). According to this provision, Europol is in charge of the "coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States' competent authorities." Thus, Europol is not only able to initiate an investigation, but it can also get the role of coordinating an entire investigation, in conjunction with the member state(s). This role, however, is not further detailed in the regulation. The only reference is found in Art. 4(1)(c) of the regulation, which states that Europol shall "coordinate, organise and implement investigative and operational action" together with member states. Therefore, Europol's Joint Supervisory Body (JSB)[5] argued that specific rules should be included in the text so that

[4] For an analysis on the new Europol Cybercrime Centre in the context of the EU's cyber security strategy, see Dewar's chapter 5 in this book.
[5] This body is examined in the section "Changes on external supervision".

there would be a clear understanding regarding the distribution of competences between Europol and national law enforcement authorities during a criminal investigation.[6]

Article 5 of the regulation brings clarity to Europol's participation in JITs. The important point here is that no prior authorisation is be required for Europol to participate in a JIT. Moreover, Article 5(5) allocates to Europol the task of taking "measures to assist [member states] in setting up the joint investigation team." Although this role is somewhat symbolic, it demonstrates the willingness on behalf of the EU to increase the presence of Europol in such teams.

Article 6 of the regulation allows Europol to initiate and/or conduct a criminal investigation when it considers that it can add value.[7] This provision introduces changes to the previous Article 7(1) ECD. First, it adds a deadline of one month for a member state to reply. Second, it requires a member state that decides not to proceed with an investigation to send a reasoned justification as to why to Europol by a set date.[8] Lastly, Europol now has an obligation to inform Eurojust about the decision made by that member state.

Article 7 of the regulation sets up the conditions under which member states must cooperate with Europol. This provision offers great changes. It establishes the obligation for national law enforcement authorities to provide Europol with relevant criminal-related information. Under the previous legal framework, member states had no obligation to provide any information to Europol.[9] Also, Europol did not have access to member states' national law enforcement databases.[10] In a change to previous practice, in the new legal instrument member states are required to inform Europol about all

[6] JSB Opinion 13/31 with respect to the proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol), 10 June 2013, 6.
[7] Europol Regulation, Recital 10 and Article 6(1).
[8] Europol Regulation, Article 6(4). This was already announced in Council of the European Union, "Revision of Europol's legal basis", Brussels 8261/12, 29 March 2012, 3.
[9] Disley E., Irving B., Hughes W., Patruni B., "Evaluation of the implementation of the Europol Council Decision and of Europol's activities", *Rand Europe* (Cambridge: Rand Europe, 2012), 47.
[10] Ibid., 60.

bilateral and multilateral exchanges which fall under Europol's mandate.[11] Special attention must be given to Article 7(5), which states that contact between Europol and a member state is not to only be established through the Europol National Units (ENUs), but by means of any "competent authority of a Member State." Thus, in some cases, Europol is able to contact directly national law enforcement authorities, without going through the national contact point.[12] Considering that, in some member states, police competences are not centralised, this provision can be seen as positive. For instance, in Spain only the *Policía Nacional* is directly connected to ENU, but Catalan police forces (*Mossos d'Esquadra*) are not. The possibility of establishing direct contact between Europol and *Mossos d'Esquadra* will surely speed up their exchange of information during any ongoing criminal investigation.

It is worth adding that the definition of "competent authorities" is also modified in the regulation. Rather than the previous, "all public bodies" in the member states responsible for preventing and combatting criminal offences (Art. 3 ECD), it now states "all police authorities" in charge of such activities (Art. 2(a) Regulation). It is however unclear what the impact of this change will be, and whether this definition will make any difference in practice.[13]

Based upon the above changes, this author is of the view that Europol has gained some regulatory power under the new regulation. These new powers should lead to a more efficient and coherent framework, making better use of the available information processes, i.e. databases and communication tools, as will be examined below.

Improvements on data quality

In the past, EU member states had responsibility for guaranteeing that the information sent to Europol was accurate and up-to-date. Europol also ensured that data was processed according to the principles of necessity and proportionality,[14] and was subject to frequent reviews to ensure the

[11] Europol Regulation, Article 7(5)(a).
[12] Ibid. Recital 13 and Article 7(4).
[13] This provision could cover civilian agencies which fulfil a police like role, like the old SOCA in the UK, now replaced by a police body (the National Crime Agency).
[14] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ 2009 L121/37, Article 35.

accuracy of its data.[15] Europol is continually working to improve the quality of its data and the primary difficulty it faces is that, in some instances, Europol officials might not introduce data using the same format. This inconsistency will negatively affect the search criteria of "hits," since variations in keywords will not match, and links and relationships will be missed if the word(s) searched do not match exactly. Take for example a search against a hypothetical Spanish suspect named "Jaime Fernández García." In sending data to Europol, a member state creates an "opening order" to input the data to Europol's database. There are spaces to enter the first name, middle name, and surname of the suspect. It is possible that "Fernández," despite being a surname, is entered as a middle name. In this case, the system would not identify or "hit" during a search for "Fernández" and/or "García" because there are currently no provisions for partial word matches. This is an area which needs to be addressed to prevent suspects from evading detection.[16]

The Europol regulation should improve the data quality of information processed by Europol with the introduction of Article 29. The accuracy and reliability of data should be better assessed, as personal data is classified according to factual verification, and according to the reliability of the source. As shown in Table 1 below, there are different source-evaluation codes rating the accuracy on the scale of one to four, as well as letter scale A-B-C-X for reliability.

Table 1: Source Evaluation Codes

	Accuracy	**Reliability**
Not in doubt	1	A
Information known personally to the source / In most instances proved reliable	2	B
Information not known personally to the source but corroborated / In most instances proved unreliable	3	C
Not reliable/accurate	4	X

[15] Europol Council Decision, Article 29.
[16] The author has benefited from a work experience at Europol, and writes from her experience of using such databases.

Adequacy of the retention periods

Data retention is, without doubt, one of the most controversial issues regarding data protection matters.[17] One of the key questions is how long data should be retained. This is already a difficult problem in the context of the commercially focused internal market,[18] however complexity is multiplied in the law enforcement sector. In the ECD Europol opted for keeping data "only for as long as it is necessary for the performance of its tasks."[19] This was determined on a case-by-case basis. Europol had a mandatory review process to make sure that data is not kept any longer than is absolutely necessary. It consisted of regular audits conducted by the Europol data protection office (DPO) in order to determine whether the information stored in the systems was still necessary for an ongoing investigation. In addition, Article 20(2) ECD noted that a review of the information has to be made after three years. Data was automatically deleted unless there is a proven necessity to keep specific data.

It is worth highlighting that the deletion of data always involves the member state which sent the data initially. Therefore, Europol, without exception, must ask the member state if the data which Europol wants to delete is still relevant at the national level. Only after the authorisation of the particular member state, can Europol delete the information. The issue then arises as to what authority Europol does have with regard to data retention. Suppose there is information regarding a drug trafficking investigation introduced to Europol by France in 2006. The Europol DPO conducts an audit and detects that this information has not been used or updated in the past four years. The DPO then asks the particular focal point (FP) to delete such information. The FP is bound by the decision of French law enforcement authorities. If they consider it is necessary to retain the information, it will be kept. Even if the French police authorities fail to supply a proper justification, Europol has no authority to enforce its requirement to delete the information. Primacy in law enforcement matters rests with individual member states under Article 72 TFEU, with EU

[17] For a detailed analysis of this from a data protection perspective, see Grant's chapter 7 in this book.
[18] See the debates about Directive 2006/24/EC on data retention and C-293/12/ C-594/12 *Digital Rights Ireland Ltd)* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* Judgment of the Court (Grand Chamber) of 8 April 2014 discussed in Grant's chapter in particular.
[19] Europol Council Decision, Article 20.

activities in this area being an area of shared competence with EU member states, and subject to the principle of subsidiarity. This is reflected in how Europol operates under the Europol regulation.

Article 37 of the proposed regulation maintained the former legal framework[20] by establishing that "[p]ersonal data processed by Europol shall be stored by Europol only as long as necessary and proportionate for the purposes for which the data are processed." However, the EDPS considered that the provision was too broad, and the terms "for the achievement of its objectives" should be modified by "the purpose for which data are processed."[21] Article 31 of the regulation, now provides that "Personal data processed by Europol shall be stored by Europol only for as long as it necessary and proportionate for the purposes for which the data are processed". This is again determined on a case-by-case basis. Europol keeps the mandatory review process in order to ensure that data is not kept longer than necessary. Suppose it is decided that information of a specific FP is to be deleted in three years, if there is no cross-match or update in the past two years. As in the current ECD, the method of ensuring that data is not kept longer than necessary will be through regular audits from the Europol DPO to determine whether or not the information is still necessary for ongoing investigations.

That said, it can be concluded that the time limits for retention and storage of information still comply with the purpose limitation principle. A problem remains at the domestic level. Adequate audits should also be carried out by the law enforcement agencies of each member state under their own legal frameworks to insure that data is not retained longer than necessary within that state. Currently these audits would follow the national regulations of the state. This author would be of the view that in an ideal world a standardised procedure such as the Europol approach would provide uniform guidance to all member states. Only a single standardised procedure will ensure compliance with data retention goals.

[20] Europol Council Decision, Article 20.

[21] See Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, 31 May, 26.

The new flexible architecture for data processing

The provisions in the Europol Regulation offer, at first sight, greater safeguards for the processing of information by Europol. Yet the new draft legal instrument includes new issues which have been perceived as obscure and vague by the European Data Protection Supervisor (EDPS),[22] member states and even Europol itself. One of the most questioned provisions is, without doubt, Article 18 of the regulation. This provides that:

> "….Europol may process information, including personal data ….only for the purposes of: a) cross-checking aimed at identifying connections and other relevant links between information…., b) analyses of a strategic or thematic nature, c) operational analyses; d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations."

It is essential to first draw a distinction between this article and the former data processing scheme in Europol. In the ECD three specific information processing "systems" delivered operational support to member states, which consisted of Analysis Work Files (AWFs), the Europol Information System (EIS) and its Index Function.

The EIS began operations in 2005 and since then it has become one of Europol's core databases which today contains approximately 200,000 entries.[23] A recent document of the Council of the European Union revealed that Germany provides the most data to the EIS, followed by Belgium, France and Spain.[24] Most of the information stored in the EIS is inserted automatically[25] (occasionally manually) by EU member states. Such information contains data related to suspects, convicted criminals or persons for whom exist "factual indications or reasonable grounds to believe that they will commit crimes that fall within Europol's competence."[26] As for access to the EIS, ENUs used to be the only group

[22] EDPS Opinion, 31.05.2013, 11-13.
[23] Europol, *Data Protection at Europol*, (Luxembourg: Publications Office of the European Union, 2010) 15.
[24] Council of the European Union, *General Report on Europol's activities in 2011*, 10036/12, 24 May 2012, 21.
[25] Thirteen Member States insert criminal data in the EUI using automated data loading systems. See General Report on Europol's activities in 2011, *General Report on Europol's activities in 2011*, 21.
[26] Europol Council Decision, Article12.

with access. A new version of the EIS was later developed to include a hit/no-hit search function which effectively widened its access beyond the ENUs.[27] This right to input data into the EIS is now available to Europol staff, the Europol director and liaison officers under Article 13(1) ECD.

The EIS was not the only information system of Europol. Analysis Work Files were also used. In contrast to the EIS, AWFs were focused on the analysis of a specific crime area (e.g. Islamic terrorism, human trafficking, etc.).[28] Data, including personal data,[29] was collected and analysed in a comprehensive environment in order to provide national law enforcement authorities with; a) general "cross-match reports," b) operational analysis reports of the activities of a specific group of persons, and c) strategic analysis reports.[30] Criminal analysis was divided into two types: i) analysis of a general nature affecting all member states,[31] and ii) analysis of specific cases, concerning only some member states.[32]

AWFs, under Art. 14 ECD, included data not only related to criminals, but also witnesses, victims, associates and contacts. This data was introduced in a file which is opened at Europol's initiative or at the request of member states. The Director had to specify i) the file name, ii) the purpose of the file, iii) the concerned groups of persons, iv) the nature of data, v) the general context, vi) the participants in the analysis, vii) the conditions for data communication, viii) the time limit for examination and storage, and ix) the establishment of the audit log.[33] After that, this data was accessible on a "need to know" basis[34] to Europol staff, liaison officers, experts from

[27] Bigo D., Carrera S., Hayes B., Hernanz N. and Jeandesboz J., "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An Evaluation of Current and Forthcoming Proposals", (Brussels: *CEPS Paper No. 52,* 2012), 22.
[28] *Data Protection at Europol*, 15.
[29] Europol Council Decision, Article 6(2). These include biographical data, physical descriptions, identification means (identity documents but also images or biometrics, including fingerprints, DNA profiles, voice profiles, blood group or dental information), occupational, economic and financial, behavioural data, as well contacts and associates, information relating to criminal activities and so forth. See also Bigo *et al*., "Justice and Home Affairs", 22.
[30] Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ 2009 L325/14, Article 11.
[31] Europol Council Decision, Article 14(1).
[32] Ibid. Article 14(4).
[33] Council Decision 2009/371/JHA, Article 16.
[34] Disley *et al*., "Evaluation of the implementation", 83.

member states and the concerned third countries.[35] There were separate rules on the transfer of data to individual third countries. It is worth adding that Europol Implementing Rules for AWFs were signed on 30 November 2009, one day before the Treaty of Lisbon entered into force.[36] The direct implication of this is that these rules were adopted without the participation of the European Parliament (EP), which is now involved in legislating for most EU cross-border law enforcement under the EU's ordinary legislative procedure,[37] and without the need to comply with the new provisions of the treaty.

Finally, the Index Function could be considered as an extension of the AWFs, as it basically indexed information in the AWFs.[38] This index system allowed member states that are not involved in a given AWF to see what AWFs include, in order to allow them to request to join if they, and the given AWF member states, both desire. However, the Index Function, as well as the EIS and the AWF, disappeared when the Europol Regulation came into force. The Europol Regulation abolished the above three systems in favour of more flexibility. The new system for processing of information is established in Chapter V of the regulation. It introduces, for the first time, one single data processing environment, instead of separated data systems, merging all three of the current databases into one. Processing depends on the specific purpose, and encompasses different conditions for such processing. In other words, different categories of data are collected and processed depending on the purpose.[39]

Article 18 of the regulation distinguishes four different purposes: a) a general cross-checking aim, b) strategic analyses, c) operational analyses, and d) facilitating the exchange of information between Europol and member states. Restrictions in access and use of the information will be determined by the purpose and the corresponding type of processing.[40] Cross-checking and strategic analyses enable member states to search all

[35] *Data Protection at Europol*, 17.
[36] Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files.
[37] The posting of law enforcement officers across borders remains a special legislative procedure, post-Lisbon, under the effective control of the Council, with little involvement of the European Parliament.
[38] The index function allows those searching to determine whether or not there is an item of information in the AWFs. See Europol Council Decision, Article 13(3).
[39] Europol Regulation, Annex 2.
[40] Europol Regulation, Article 25(2).

necessary information stored in the Europol database. In the case of operational analyses, personal data needs to be especially protected, and the accuracy and relevance is essential.[41] Due to this special sensitivity of data processed, a "privacy by design" approach[42] is applied for operational analyses, with access only being possible on a hit/ no-hit basis, when a specific criminal investigation takes place. This system first checks whether the found crime-related information matches with any of the data stored in the agency database,[43] and further information will only be provided in case of a hit, and if a follow-up request has been issued.[44] In that sense, the fully established hit/ no-hit mechanism of Europol ensures better protection of information, especially personal data, than many of the domestic rules and regulations.

As mentioned above, Article 18 of the regulation has been strongly criticised by the EDPS. Criticism of this provision has arisen as it is not clear at all how Europol seeks to implement it. It seems that the idea behind the current Article 18 is to create a big Europol Information System, one single depository composed of different data set levels of processing. The purpose of this change is to enhance the protection of personal data by strictly complying with the purpose limitation principle.[45] Yet, no further explanation of how to put this into practice is included in the legal text. Perhaps, a way of implementing Article 18 could be by adopting a prior privacy impact assessment explaining the purposes, necessity and proportionality of the proposed action before opening any work file. In fact, a memorandum for data protection impact assessments, which is in the Europol Regulation, has also been suggested by the EDPS[46] and the JSB.[47] This author would agree with the JSB that "[p]rinciples of data protection such as necessity and purpose limitation

[41] These are issues which Grant will examine in more detail in Chapter 7 of this book.
[42] This concept is examined in the section "Lack of clarity in the privacy-by-design approach."
[43] Europol Regulation, Article 26(2).
[44] Europol Regulation, 8.
[45] The purpose limitation principle consists of using any personal information strictly for the purposes which intended its original collection. It is regulated in Article 5(b) of 108 Data Protection Convention, Article 6(1)(b) of Directive 95/46/EC and Article 3 of EU Framework Decision 2008/977/JHA.
[46] EDPS Opinion, 31 May 2013, 7.
[47] JSB Opinion 13/31, 6.

should not be made dependant on a choice of IT structure."[48] Yet, privacy impact assessments should be excluded on a case-by-case basis for urgent transnational policing issues, in which a delay could jeopardise the entire operation.

In addition, it is possible to argue that the new flexibility for data processing is unnecessary. In May 2012, Europol decided to reduce the number of AWFs from 23 to 2. After that, there were currently two different AWFs,[49] one referring to terrorism issues (AWF CT) and the other to serious organised crimes (AWF SOC). Each of these AWFs included a list of FPs, separated by crime area. For instance, FP TWINS included data on crimes of sexual exploitation of children, and FP CYBORG refered to Internet and information and telecommunication technology (ICT) related crimes. Data searches could be conducted within the two big databases (SOC and CT), avoiding the need to introduce the very same data twenty-three times. Precisely because of the reduction in the number of crime areas the Europol system was much more flexible than before. The JSB rightly concluded that the current system is flexible enough, and that there was no need to change the current data processing structure. Moreover, Article 10(2) ECD offered the possibility to create new systems if necessary. The fact that this option was never been used[50] demonstrates the high level of functionality of the current data processing framework.

Convergence of and the proposed Europol Regulation and the future EU Data Protection Directive

Another concern that emerged from the proposed Europol Regulation was that there was a risk that the proposed system would not match the same level of safeguards as those currently provided for in the EU Data Protection Directive for police and judicial matters (hereinafter, the directive), which was also released in 2016.[51]

---

[48] Ibid., 3.

[49] Before May 2012 there were twenty-three AWFs, but it was then reduced to two.

[50] JSB Opinion, 13/31, 3.

[51] 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 the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L119/89.

The directive, despite excluding Europol from its scope, impacts directly on the Europol Regulation. Indeed, recital 40 of the Europol Regulation highlights the importance of aligning this law with the draft directive, stating that:

> [T]he data protection rules of Europol should be autonomous while at the same time consistent with other relevant data protection instruments applicable in the area of police cooperation in the Union. Those instruments include, in particular, Directive (EU) 2016/680 of the European Parliament and of the Council, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe and its Recommendation No R(87)15.

The directive regulates the data protection standards applicable within the member states, which in fact are the main sources of Europol's information. Therefore, the long delay in the approval of the directive caused also a suspension in the voting of the Europol regulation by the Parliament.

There are two situations where having the EU data protection directive finalised before the adoption of the Europol Regulation proved to be very useful. The first one refers to data quality issues, and the second one to the purpose limitation principle. On the point of data quality, Art. 7 of the directive deals with different degrees of "accuracy and reliability" of personal data to be established in each member state, which is monitored by the pertinent national data protection authorities. Such general clause is not coincidental. Although the first draft directive included several degrees of accuracy, they were finally removed because they conflicted with Article 29 of the Europol Regulation, which establishes other different degrees of accuracy.

It has been demonstrated that the purpose limitation principle of Article 18 of the Europol Regulation is not sufficiently clear, and that there is confusion on how it is to be implemented. Taking a closer look at the directive, national law enforcement authorities process data depending on the different categories of data subjects, such as suspects, convicts, victims, witnesses, contacts or associated persons, and other persons.[52] It is difficult to envisage how this will be implemented in the different EU member states, but it is possible that the Europol Regulation uses the same

[52] Directive 2016/680, Article 6.

processing system according to Article 18, so as to match the directives provisions.

Therefore, it was important to first adopt the directive and then the Europol Regulation. Since the EU has, at the time of writing, 28 member states and each of them has its own data processing mechanisms, the establishment of a certain harmonization within the EU was first needed. Only then, it made sense to adopt rules on Europol's data processing mechanism. However, it is worth mentioning that a complete harmonisation among member states is still impossible as each state has its own criminal laws. For example, if one of the rules prohibits the processing of data relating to minors who are not criminally responsible, then the question arises as to how to define a responsible minor, as the age for this varies considerably from one member state to another.

Diversity in the area of criminal law is not new, and the general rules on processing information, in line with the purpose limitation principle could be applied in a case-by-case, or rather in a country-by-country, basis. The assessment of this compliance would be carried out by the data protection supervisory authorities of each member state. The next section examines the provisions on supervision in the Europol Regulation, which could inspire and be used as guidelines for establishing common practices on external supervision among member states.

Changes on external supervision

Europol already had a fully-fledged supervision system before the adoption of the regulation. On the one hand, as discussed earlier, there is a DPO, which constitutes the internal supervision of the agency, which is independent from the activities of the other departments, but dependent on Europol's budget. The DPO continues to exist under the Europol Regulation. On the other hand, the agency had an external oversight body called the Joint Supervisory Body (JSB), which was located in Brussels and was composed of data protection authorities of the member states (DPAs). This body disappeared under the regulation.

The new regulation introduces the supervision of Europol's data processing by the EDPS,[53] which excludes any participation of the current JSB. The EDPS, as supervisor of such processing, mainly gives authorisation prior

[53] Europol Regulation, Article 43.

to the automated processing of sensitive personal data, and investigates complaints lodged by data subjects.[54] Likewise, Article 43(3)(f) leaves in the hands of the EDPS the ability to "impose a temporary or definitive ban on processing." Although the body has confirmed that a ban will be an exceptional remedy, this provision has already been met with criticism.

Europol has also cast doubt on its potential future efficiency. As the EDPS has assumed the JSB supervisory tasks, this could potentially delay processing of operational data. Moreover, there is a more general worry about the capabilities of the EDPS in the field of law enforcement. The JSB has gained a very strong expertise on Europol matters over the years, which the EDPS does not currently have. National DPAs are used to conducting audit functions on national law enforcement agencies, and such valuable competence might be lost with the proposed regulation. In this sense, the JSB, in its recent opinion, has suggested creating an independent and effective joint supervision structure with national DPAs and the EDPS, instead of relying solely on the latter.[55] In any event, the regulation has already clarified that the EDPS will carry out "joint supervisions" with national supervisory authorities in some cases.[56]

Besides the new role of the EDPS, the European Parliament (EP) has also gained a stronger supervisory role with the introduction of parliamentary scrutiny in the regulation.[57] This new role for the EP is based on the Commission communication of 2010, where the Commission stressed the necessity of enhancing the scrutiny of Europol's activities by the EP, together with national parliaments.[58] The EP is co-legislator in the AFSJ policies under the Treaty of Lisbon, meaning that it plays an important role in "ensuring that [the AFSJ] agencies fulfil their mandates effectively."[59] Under the current legal framework the EP supervisory role

[54] Ibid., Recital 44.
[55] JSB Opinion 13/31, 3 and 10.
[56] Europol Regulation, Article 44.
[57] Article 88(2) TFEU.
[58] Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national Parliaments, COM(2010) 776 final.
[59] Vermeulen M., Wills A., "Parliamentary oversight of security and intelligence agencies in the European Union", Brussels: European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' rights and Constitutional Affairs, 2011, 19.

is limited to Europol's policies, administration and financial aspects.[60] The Europol Regulation enhances the EP's control over Europol, by providing the following: a) The Management Board will have to consult the EP (and national parliaments) on the annual programme; b) the EP (and national parliaments) will receive strategic analysis and non-confidential threat reports from Europol; c) the EP can make requests for classified information; d) the EP will receive all activity reports from Europol (in addition to the current requirement of receiving reports from the Director).[61]

In summary, the EDPS and the EP will have their role as supervisory bodies enhanced under the regulation. Despite criticisms from Europol on the new competences of the EDPS, it can be concluded that this change should increase the coherence of the oversight mechanisms within the AFSJ. They should also increase the transparency of Europol through the greater involvement of the EP.

Lack of clarity in the privacy-by-design approach

The Europol Regulation refers to the privacy-by-design approach in Article 33. Privacy-by-design can be defined as the principle under which "controllers should be able to demonstrate that appropriate measures have been taken to ensure that privacy requirements have been met in the design of their systems."[62] However, the regulation itself does not include any specific data processing activity that guarantees the implementation of this principle.[63] In particular, the Commission has failed to introduce a legal basis for the two tools which support this principle: the Secure Information Exchange Network Application (SIENA) and handling codes.

SIENA is the current tailor-made communication tool at Europol. In 2012, more than three hundred competent authorities[64] used this tool to share crime-related information, and a total of 414,334 operational messages

[60] Ibid.
[61] Europol Regulation, Article 51 and 52.
[62] Hustinx P., "Ensuring stronger, more effective and more consistent protection of personal data in the EU", *New Europe*, 2 January 2012, http://www.neurope.eu/kn/article/ensuring-stronger-more-effective-and-more-consistent-protection-personal-data-eu.
[63] JSB Opinion 13/31, 4.
[64] These include not only police forces but also customs agents and independent law enforcement bodies (e.g. the Italian *Guardia di Finanzia*).

were exchanged.[65] Europol began using SIENA in 2009 with the purpose of connecting the agency to a fully secure encrypted scheme, through which information could be exchanged according to adequate data protection and data security standards. SIENA is the primary messaging system used to connect ENUs with Europol. The number of users of these tools has increased to the extent that now third countries, liaison officers of the member states, Europol officials and other competent authorities have access.

The Commission, the Council and Europol itself have all urged member states to increase their use of SIENA whenever they need to exchange crime-related information, regardless of whether or not the particular crime is within Europol's mandate. By using SIENA, law enforcement authorities would avoid the use of less data secure channels, such as regular email. However, an issue arises in the use of SIENA as the default communication tool, as the Europol Regulation does not provide any legal framework for its scope and usage in the context of Europol communications. With no rules on the use of SIENA, many member states prefer to use other more flexible channels of communication such as the Interpol channel, mutual legal assistance forms or even regular unencrypted email. The lack of SIENA provisions in the draft regulation is thus a missed opportunity to harmonise the numerous channels that exist today to exchange information within the field of law enforcement.

The same issue arises with handling codes. Any information that a member state transfers to Europol is subject to the "ownership principle." This principle states that the owner keeps full control of that information. For years Europol has used a system whereby the member state can choose the level of accessibility of the specific information it introduces to Europol's database. These restrictions are called handling codes. SIENA integrates a function with four types of codes to be selected by the national law enforcement authorities. First, there is the H0 or no-handling code, by which the information can be distributed to all member states without restriction. Second, there is the H1, which prohibits disclosure of the information in advance of a judicial proceeding without the prior authorisation from the inputting member state. Third, the H2 prevents disseminating cross-matched information without the permission of the provider. Finally, the H3 allows for further restrictions, details of which need to be entered in a free text box (e.g. target group X only). As with

[65] See https://www.europol.europa.eu/content/page/siena-1849.

SIENA, there is a failure to deal with the issue of handling codes in the regulation. As argued by the JSB, an issue may develop as there is no control of a member state's decisions with regard to handling codes. It is possible that member states may automatically use the most restrictive handling code, which would make it more difficult than necessary for Europol to fulfil its tasks.[66]

It can be argued that despite the privacy-by-design intentions in the regulation, there is a failure to specify how this will be implemented in practice. The two operational tools which enforce the privacy-by-design principle, i.e. SIENA and the handling codes, are not explicitly provided for in the regulation. It is impossible, therefore, to determine whether the repeated claims to support of the "privacy-by-design" will in fact make any difference in how Europol will deal with data security going forward.

Conclusions

This study has examined the main changes in the Europol regulation, which will have a direct impact on the processing of crime-related information within the EU. There are positive aspects of the regulation. It provides enhanced competencies for Europol with regard to the initiation and coordination of criminal investigations. It also offers what this author would consider to be adequate standards of data quality and data retention periods. However, the new data processing architecture is also controversial amongst data protection authorities, as is the appointment of the EDPS as the external supervisor body for Europol data exchanges. The most critical issue, however, is that despite the support for the principle of privacy-by-design, adequate provisions dealing with this principle have not been provided for/adequately provided for in the regulation. In the absence of a robust legal, or regulatory, framework doubts will remain as to whether the regulation will effectively improve on the former Europol data protection scheme.

Although the main objective to adopt the regulation was to "reinforce the data protection regime applicable to Europol's activities,"[67] the JSB has declared that it instead "results in a much weaker Europol data protection regime."[68] This author is of the view that the regulation is adequate in

[66] JSB Opinion 13/31, 9.
[67] COM(2013) 173, 8.
[68] JSB Opinion 13/31.

terms of data protection. As demonstrated in this study, this legal instrument maintains the strong and robust data protection framework that Europol has been building since its creation over twenty years ago. Nevertheless, further clarification is needed with regard to Article 18 of the regulation, specific data security measures, and the capabilities of the EDPS as the new supervisory body. In all other respects, the Europol Regulation will hopefully have a positive impact on the overall EU security environment, as it establishes a perfect synergy with the new directive for data protection in police and judicial matters.

Bibliography

Bigo D., Carrera S., Hayes B., Hernanz N. and Jeandesboz J. "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An Evaluation of Current and Forthcoming Proposals". Brussels: *CEPS Paper No. 52*, 2012.

Communication from the Commission to the European Parliament and the Council. Second Report on the implementation of the EU Internal Security Strategy, COM(2013) 179 final.

—. on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national Parliaments, COM(2010) 776 final.

Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ 2009 L325/14.

—. 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ 2009 L121/37.

Council of the European Union. *Revision of Europol's legal basis*. Brussels 8261/12, 29 March 2012.

Council of the European Union. *Target information management architecture (IMS Action 10) - Draft vision on EU law enforcement information exchange*. 7903/13, 25 March 2013.

—. *General Report on Europol's activities in 2011*. 10036/12, 24 May 2012.

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 the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L119/89.

Disley E., Irving B., Hughes W., Patruni B., "Evaluation of the implementation of the Europol Council Decision and of Europol's activities", *Rand Europe* Cambridge: Rand Europe, (2012).

Europol. *Data Protection at Europol*. Luxembourg: Publications Office of the European Union, 2010. http://www.europol.europa.eu.

Hustinx P. "Ensuring stronger, more effective and more consistent protection of personal data in the EU", *New Europe*, 2 January 2012.

JSB Opinion 13/31 with respect to the proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol), 10 June 2013.

Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, 31 May 2013.

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10.

—. Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA and 2009/968/JHA, OJ 2016 L135/53.

Vermeulen M., Wills A. "Parliamentary oversight of security and intelligence agencies in the European Union". Brussels: European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' rights and Constitutional Affairs, 2011.

CHAPTER SEVEN

RIGHTS AND PERSONAL DATA, AND THE FREE MOVEMENT OF SUCH DATA FOR EU SECURITY PURPOSES IN THE CONTEXT OF DIRECTIVE (EU) 2016/680 FOR THE PURPOSES OF PREVENTION, INVESTIGATION, DETECTION OR PROSECUTION OF CRIMINAL OFFENCES OR THE EXECUTION OF CRIMINAL PENALTIES

FIONA GRANT

Introduction

The Commission published two legislative proposals designed to revise a significant part of the EU legal framework pertaining to the protection of personal data in 2012.[1] The instruments had a duality of purpose; to replace (the non-policing) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] with a general Data Protection Regulation[3]

[1] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, the free movement of such data, COM(2012) 10 final. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. See also Blasi Casagran's Chapter 6 in this book.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L281/31.

and to supersede Framework Decision 2008/977/JHA[4] for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters with a sector-specific directive.[5] A key element of the EU's Area of Freedom Security and Justice (AFSJ) is the legitimate collection, storage, processing, analysis and intra-EU cross-border exchange of relevant information in the form of personal data in the area of police cooperation[6] and judicial cooperation in criminal matters.[7] This can only proceed on the basis of common action if appropriate safeguards on the protection of personal data are achieved. One inherent limitation of Framework Decision 2008/977/JHA is the prohibition on sharing personal data processed by the police and judiciary at a purely national level. This has led to practical difficulty in distinguishing between purely domestic and cross-border processing requirements and predicting whether certain "national" data may become the object of a cross border exchange at a later date.[8]

Post-Amsterdam, with police and judicial co-operation on criminal matters (PJCCM) continuing to proceed on an intergovernmental rather than supranational basis,[9] convergence of PJCCM issues of common concern was furthered through the adoption of consecutive five year programmes defining objectives and results to be achieved. The penultimate pre-Lisbon Hague Programme 2005-2010 recognised that an "innovative approach to the cross-border exchange of law-enforcement information"[10] would

[3] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L350/60.

[5] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

[6] TEU, Article 30(1) (b).

[7] Ibid. Article 31(1) (a).

[8] Proposal for a Directive - on the protection of individuals with regard to the processing of personal data, Recital 1.

[9] Title VI TEU, Police and Judicial Co-operation in Criminal Matters.

[10] *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, OJ 2005 C53/1.

require cultivation, if the EU was to meet the commitment to strengthen freedom, justice and security and guarantee a high level of public safety.

This imperative culminated in a more detailed commitment by the Council in the post-Lisbon Stockholm programme 2010-2014[11] to develop a comprehensive internal security strategy to combat, primarily, cross border crime through enhanced border controls. To that end, the Council adopted a draft strategy in 2010,[12] and the Commission, through an earlier action plan, separately published a Communication[13] outlining an internal security strategy (ISS) predicated on, *inter alia*, enhanced co-operation in the sphere of intra-member state law enforcement and judicial cooperation. The basis for any legislative innovation[14] is highlighted in the text, to include due respect for shared European values, the rule of law and respect for fundamental rights. The ISS incorporates these imperatives stating that the attainment of "efficient" law enforcement through co-ordinated intra-EU information exchange is not to be at the expense of individual privacy and the fundamental right to protection of personal data.[15]

In the context of the incremental revision of the EU data protection landscape and ISS objectives two initial and inter-related issues were raised in connection with the 2012 proposals. The first was, post-Lisbon, the necessity for and proportionality of the maintenance of a fragmented data protection regime given incorporation of the former PJCCM pillar in the main EU legal framework and the enhanced legal status of the EU Charter of Fundamental Rights (EUCFR)[16] by enacting two distinct supranational instruments with non-homogenous provisions.[17] The second

[11] *The Stockholm Programme - An Open and Secure Europe, Serving and Protecting Citizens*, OJ 2010 C115/1, paragraph 4.1.
[12] *Draft Internal Security Strategy for the European Union: Towards a European Security Model* Document 7120/10 which elucidated steps to be taken to translate the Stockholm agenda into concrete actions.
[13] Communication from the Commission to the European Parliament and the Council, *The EU Internal Security Strategy in Action: five steps towards a more secure Europe*, COM(2010) 673 final.
[14] Ibid. 3.
[15] Ibid.
[16] It is noted here that the UK and Poland secured a Protocol to the Lisbon Treaty opting out of the EUCFR. See O'Neill, chapter 2 of this book.
[17] This "twin track approach" has been criticised by the UK House of Commons Justice Committee *Opinion on the EU Data Protection Proposals*, *Third Report 2012-13* of 1 November 2012 HC 572, 3. See also the European Scrutiny

was the legitimacy of certain provisions contained in the then proposed directive with regard to policing etc. in light of the practical difficulty that presents when law enforcement professionals are required to distinguish between data subjects categorised as "suspects" and those who can be described as "associated third parties."[18] Individuals falling into the latter category who, through some form of personal or professional affiliation with the suspect, will become persons of interest to law enforcement authorities and stand to lose the enhanced protections offered by the then proposed regulation[19] in terms of the processing, sharing and retention of their personal data. This issue is explored through the lens of the directive as enacted, and is also further discussed by Blasi Casagran in chapter 6 of this book.

There is however a third issue, one that, at least superficially, appears unconnected with the 2012 proposals to reform the EU data protection regime. This is the potential for sharing of personal data for both internal and external security purposes when the respective imperatives of the ISS and the European Security Strategy (ESS) collide.[20] Fundamentally, the ISS is concerned with intra-member state co-operation on a supranational basis to combat the threat of terrorism and other significant criminal activity. Actions undertaken to implement specific ISS objectives are therefore governed by the terms of primary and secondary EU instruments and reviewable by the Court of Justice of the EU (CJEU). The ESS, on the other hand, has as its focus the formation of economic and political strategic partnerships with third countries via the Common Foreign and Security Policy (CFSP), in addition to a conflict resolution role under the European Security and Defence Policy, both of which, post-Lisbon, continue to proceed on the basis of intergovernmental, bi-lateral or multi-lateral co-operation. The adoption of legal acts in relation to the CFSP is

---

Committee, *Fifty-ninth Report of Session 2010–12*, Documents considered by the Committee on 14 March 2012, HC 428, paragraph 8.

[18] Proposal for a Directive - on the protection of individuals with regard to the processing of personal data, Article 5.

[19] The proposed regulation has now been enacted as Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L119/1.

[20] Council, *A Secure Europe and a Better World* 12.12.03, reviewed in *Report of the Implementation of the European Security Strategy: Providing Security in a Changing World*, 11.12.2008 S407/08.

expressly excluded by Article 24(1) Treaty on European Union (TEU), as is the jurisdiction of the CJEU from provisions relating to the CFSP, and any measures adopted on the basis of these provisions - excepting the Article 275 Treaty on the Functioning of the European Union (TFEU) right to review of decisions providing for restrictive measures against natural or legal persons adopted by the Council. It is against this backdrop that the extent of data subject rights in the context of the then proposed data protection directive and CFSP intergovernmental activity falls to be considered.

This chapter will initially examine, the necessity for, and proportionality of, a separate data protection instrument for internal security purposes. This will be undertaken by examining the nexus between the protection of personal data as a fundamental right and legitimising conditions for interference with that right at a supranational level. This will draw on the jurisprudence of the European Court of Human Rights (ECtHR), the CJEU and its previous incarnation, the European Court of Justice, (ECJ). The chapter will conclude by considering the overlapping and conflicting considerations for the protection of personal data posed by vestigial intergovernmental activity under the auspices of the CFSP. In doing so it will argue that the 2016 data protection framework should be extended to CFSP activities, thereby removing the general prohibition within Articles 24(1) TEU and 275 TFEU on the competence of the CJEU to review the compatibility of any measures adopted therein. This proposition proceeds on the premise that if Article 8(1) EUCFR is to truly confer fundamental rights, all citizens of the Union are entitled to have the extent of these determined before the CJEU whether the activities undertaken by the EU proceed on a supranational or intergovernmental basis.

Fundamental Rights and Implementation of the ISS

Whereas the commercially focused data protection Directive 95/46/EC was predicated on the desire to guarantee the free flow of information between member states to facilitate the economic single market,[21] action to enable data exchange for policing and security purposes emerged separately under the auspices of the post-Maastricht Justice and Home Affairs (JHA) pillar, which built on previous intergovernmental co-operation in that field. Article 67(1) TFEU now commits the Union to being an AFSJ with the central issue being, in the context of this chapter,

[21] Directive 95/46/EC, on the processing of personal data, Recital 3.

an area where fundamental rights are to be respected in tandem with the requirement to ensure a high level of security.[22] It is noted, at this point, for the sake of completeness, that Article 73 TFEU re-asserts the previous position that national security remains solely a matter for individual member states.

The proposed 2012 directive for PJCCM purposes was to be enacted on the basis of Article 16(2) TFEU which pertains to the adoption of rules legitimising the processing of personal data by EU institutions, bodies, offices, agencies and member states. Article 16 does not draw *per se* a distinction between mainstream processing and processing for law enforcement or related purposes, with there being no treaty prohibition on creating common rules underpinning the lawfulness or otherwise of all data processing activities undertaken within the EU. Indeed, the Krakow Declaration of April 2005, when debating the enactment of the earlier Framework Decision 2008/977/JHA on data processing for law enforcement purposes, foreshadowed the current debate, by declaring that the protective principles underpinning the mainstream Directive 95/46/EC should form the "common core of a comprehensive European data protection law,"[23] to ensure that the then JHA activities afforded data subjects a level of protection consistent with those available under the then EC pillar.

With the ISS providing the roadmap for implementation of AFSJ imperatives, Bigo has questioned what exactly it aims to deliver, asking "Is it security only or is it liberty, security and justice?"[24] Bigo's question has resonated with many academics, amongst them Guild and Carrera who have pointed out that the intended equilibrium between these competing objectives has yet to be achieved with justice subordinated to security.[25] Such positions lend credence to arguments against non-homogenous revision of the EU data protection regime post-Lisbon, given the repositioning of internal

[22] TFEU, Article 67(3).
[23] Conference of European Data Protection Authorities, Krakow, 25-26 April 2005. *http://europoljsb.consilium.europa.eu/media/51910/7ADC0308-5AA6-44C7-9E26-9E7FC6BC2C1B.pdf*.
[24] Professor Didier Bigo (then of King's College London) in written evidence to the UK House of Lords European Union Committee, *17th Report of Session 2010–12,The EU Internal Security Strategy*, HL Paper 149, paragraph 27.
[25] Professor Elspeth Guild and Sergio Carrera Centre for European Policy Studies in written evidence to the UK House of Lords European Union Committee, *17th Report of Session 2010–12, The EU Internal Security Strategy*, HL Paper 149, paragraph 30.

security activities within the supranational order, and the obvious propensity for non-coterminous instruments to perpetuate and create further imbalance between the rights enjoyed by different categories of data subjects. Perhaps by way of response to such perceptions the Commission's 2012 Communication, Safeguarding Privacy in a Connected World, reiterates that general data protection principles will apply to all PJCCM instruments and that minimum harmonisation criteria for limitations of the right of the data subject to be informed when law enforcement authorities "handle or access their data" will be established in tandem with rules to draw a clear distinction between different categories of data subjects.[26]

Whilst general data protection principles are not defined in the Communication, pre-Lisbon, the then ECJ resolved in *Connolly* v *Commission*[27] to receive the Strasbourg court's jurisprudence and absorb its *acquis* on the basis that the reasoning therein equated with the general principles of EU law, in light of *inter alia* various member states' constitutional and international obligations, including the ECHR which enjoyed special significance. Post-*Connolly*, the ECtHR returned the compliment in *Bosphorus Hava Yollari Turizm* v *Ireland*[28] by holding that in light of the (then) EC's protection of fundamental rights duly enacted EC instruments "can be considered to be, (and to have been at the relevant time) equivalent to that of the Convention."[29] This rapprochement has, in the opinion of then ECJ Advocate General (AG) Jacobs, limited the need for the Strasbourg court to routinely scrutinise judgments from EU courts to ensure Convention rights are being upheld.[30]

---

[26] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions *Safeguarding Privacy in a Connected World*, COM(2012) 9 final, paragraph 4.

[27] C-274/99 P *Connolly* v *Commission* [2001] 3 CMLR 58.

[28] *Bosphorus Hava Yollari Turizm* v *Ireland* Application No. 45036/98 (2006) 42 EHRR 1.

[29] Schorkopf, F., "The European Court of Human Rights' Judgment in the Case of *Bosphorus Hava Yollari Turizm* v *Ireland*," 6 *German Law Journal*, (2005), 1255-1264, 1261.

[30] Jacobs, F., "The European Convention on Human Rights, The EU Charter of Fundamental Rights and the European Court of Justice; The impact of European Union accession to the European Convention on Human Rights," in *The future of the European judicial system in a comparative perspective: 6th International ECLN-Colloquium/IACL round table, Berlin, 2-4 November 2005*, Pernice I. and Kokott J. and Sauders C. eds. (Nomos, 2005, 291-296, 292).

The decision in *Digital Rights Ireland,*[31] where the CJEU adopted the opinion of AG Cruz Villalon,[32] discusses the circumstances in which it is "constitutionally possible for the EU to impose a limitation on the exercise of fundamental rights"[33] through secondary legislation and member states transposition of same. The discussion centred on the Data Retention Directive 2006/24/EC[34] obligation on business entities to retain subscribers' electronic communications data for a statutory period of time, which could then be made available to the proper authorities upon request for the investigation and prosecution of "serious criminal activity." Cruz Villalon initially addressed the issue of the proportionality of the measure by way of reference to Article 5(4) TEU, where proportionality is required to be assessed conjunctively with the principle of subsidiarity, prior to considering the lawfulness of the limitation by reference to Article 52(1) EUCFR, where proportionality is assessed on the basis of legitimacy of the limitation. Finding that the objective and purpose of retention of subscribers data was valid in terms of Article 5(4) TEU, he considered its effect to be disproportionate on the grounds that it partially derogated "from the principles laid down in Directive 95/46/EC,"[35] and that "the intensity of the intervention…which through the implementation of the Directive… is imposed on member states.., the impact of which… by virtue of its 'creating effect' has on the member states' powers to regulate and guarantee the content of fundamental rights cannot… be underestimated."[36]

The discussion of Article 52(1) EUCFR also allied proportionality with the concept of subsidiarity, to the extent that the EU could not "content itself with assigning the task of defining and establishing those guarantees

---

[31] C-293/12 & C-594/12 *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Judgment of the Court (Grand Chamber) of 8 April 2014, [2014] All ER (D) 66 (Apr).

[32] Joined Cases C-293/12 and C-594/12 Opinion of Advocate General Cruz Villalón delivered on 12 December 2013 *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources*. [2013] ECR 2013 I-0000.

[33] Ibid. paragraph 1.

[34] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC, OJ 2006 L105/54.

[35] Joined Cases C-293/12 and C-594/12 Opinion of Advocate General Cruz Villalón, *Digital Rights Ireland Ltd,* paragraph 101.

[36] Ibid. paragraph 100.

to… the member states… called upon to adopt national measures."[37] In essence, Cruz Villalon considered, as did the CJEU, that it would only be constitutionally possible for the EU to impose specific limitations on the exercise of a fundamental right if it had first defined the limitations precisely in tandem with "a series of guarantees in the form of principles as a necessary and essential addition."[38] In the instant case, a more precise description of "serious crime" was given by way of example of such a failing as was the lack of guidance to member states on matters such as how denial of access to competent authorities may be achieved, and the procedure for ensuring such authorities deleted data when it was no longer of relevance to a specific enquiry. Accordingly, the pre-Lisbon Data Retention Directive was held to exceed the "limits imposed by the principle of proportionality"[39] demanded by Articles 7, 8 and 52(1) EUCFR.

In a series of Opinions,[40] the European Data Protection Supervisor (EDPS), commenting on both data protection and the emerging ISS, opined that a coherent and comprehensive approach to data subject rights is considered to be a pre-requisite for fair and lawful processing. Making specific reference to the then proposed directive, the EDPS concurs that the removal of the distinction between processing for domestic and supranational policing purposes imposed by Framework Decision 2008/977/JHA is a positive element. However he was of the view that this lonely virtue is negatived by the comparative weakness, without any "evident justification," of many other provisions.[41] He concluded that these many provisions do not achieve a "consistent and high level of data protection,"[42] which the Commission states in Recital 7 of the then proposed directive as being "crucial."[43]

---

[37] Ibid. paragraph 120.
[38] Ibid. paragraph 23.
[39] Rauhofer J. and Mac Sithigh D., "The Data Retention Directive Never Existed," (2014) *SCRIPTed*, 11:1: (2014) 118-127, 119.
[40] See for example *Opinion of the European Data Protection Supervisor of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of regions – A comprehensive approach on personal data protection in the European Union*, Opinion of 17 December 2010 on the Communication from the Commission EU Internal Security Strategy in Action: Five steps towards a more secure Europe.
[41] *Opinion of the European Data Protection Supervisor of 7 March 2012 on the data protection reform package*, paragraph 19.
[42] Ibid. paragraph 310.
[43] Ibid.

Thereafter, in a separate series of Opinions, the Article 29 Data Protection Working Party (DPWP) directly addressed adherence to the concepts of necessity and proportionality when legislating within the law enforcement sector for restrictive measures affecting data subjects' rights.[44] In doing so, the DPWP reminds member states that Article 52(3) EUCFR requires provisions of the EUCFR, which mirror those of the ECHR, to be afforded the same meaning and scope.[45] Whilst Article 8 ECHR makes no mention of personal data as a hypothecated subset within the overarching right to respect for private and family life, home and correspondence, the ECtHR has held that it may fall within the ambit of this broad-based right.[46] Citing the CJEU decision in *Schwarz* v *Stadt Bochum*,[47] DPWP Opinion 01/2014 notes that the court was of the view that Articles 7 ECHR (respect for private and family life), and 8(1) EUCFR (everyone has the right to the protection of personal data concerning him or her), are to be read together in cases where data protection and privacy issues coalesce.[48]

In *Schwarz* the CJEU held that the requirement for applicants' fingerprints to be stored on biometric passports as a condition of issue was a legitimate, necessary and proportionate measure to combat illegal immigration.[49] However, such a measure did have the potential to impact negatively on Articles 7 ECHR and 8 EUCFR. The judgment, drawing from earlier decisions of the CJEU/ECJ, (primarily *Volker und Markus Schecke and Eifert*,[50] *ASNEF and FECEMD*[51] and *S and Marper* v *United Kingdom*[52]), was at pains to point out that member states are required to take a narrow view of permitted derogations from the respective Article 7

[44] *Article 29 Data Protection Working Party Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211 adopted on 27 February 2014.
[45] Ibid. paragraph 2.2.
[46] *Malone* v *UK*, Application No. 8691/79 [1984] 7 EHRR 14.
[47] C-291/12 *Schwarz* v *Stadt Bochum* [2013] WLR (D) 386.
[48] *Article 29 Data Protection Working Party Opinion 01/2014*, paragraph 2.1.
[49] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States as amended, OJ 2004 L385/1, Article 1(2).
[50] C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I 11063, paragraph 52.
[51] C-468/10 and C-469/10 *ASNEF and FECEMD* [2011] ECR I 12181, paragraph 42.
[52] *S and Marper* v *United Kingdom* Application Nos. 30562/04 and 30555/04 [2008], ECHR 1581, paragraphs 68 and 84.

ECHR and Article 8 EUCFR rights and ensure specific guarantees in each case to effectively protect the data from misuse or abuse.

In this instance, the CJEU held that Article 1(2) of Regulation 2252/2004/EC only permitted storage of the data within an individual's passport,[53] and that in the absence of any other form of method of storage being stipulated in the regulation there could be no question of the data collected being used for any purpose unconnected with the primary aim of the provision, which was to prevent illegal entry to the EU. This part of the judgment stipulates that express rather than implied authority for reuse of data collected for a specific purpose must be present, and accords with Buttarelli's[54] view, that the wording of Article 8(1) EUCFR is suggestive of a palpable paradigm shift within which the post-Lisbon data protection regime must operate, i.e. one migrating from the previous obligation to protect the integrity of data[55] to the protection of the person to whom that data pertains.

With the similarity in content in Article 7 EUCFR and Article 8 ECHR, the judgments in *Digital Rights Ireland* and *Schwarz* amplify that legitimate interference for law enforcement activity with the fundamental right to data protection is to be adjudged by the precision with which any such limitations are specified in the relevant instrument and what measures have been put in place to protect the data subject from misuse or abuse of any information processed.

Prior to the *Digital Rights Ireland* and *Schwarz* judgments, the Commission had been the subject of criticism by the Article 29 DPWP for a perceived failure to uphold its self-defined guiding principles when framing the then proposed data protection directive. The DPWP highlighted and questioned the disparity between the varying levels of protection offered by the then proposed and mainstream data protection regulation and the directive, and in a series of opinions,[56] has consistently argued for the enactment of a

[53] C-291/12 *Schwarz*, paragraph 60.

[54] Speech at the Hearing of the European Economic and Social Committee, 9 February 2011 - Counter-Terrorism Policy and Data Protection, available at *https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-02-09_Counter_terrorism_EN.pdf* .

[55] *Durant* v *FSA* [2003] EWCA Civ 1746, paragraphs 27 and 45.

[56] *Article 29 Data Protection Working Party Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, 00379/13/EN WP 201, adopted 26 February 2013, *Opinion 08/2012*

unitary data protection regime where derogations for supranational policing etc. are detailed in a single instrument. If the status quo is to prevail, the EDPS and the DPWP make a number of specific recommendations. The salient ones are examined below in order to investigate whether the relevant articles, as originally constructed, are likely to achieve the normative and threshold requirement that all data subjects are entitled to fair and lawful processing of their personal data.[57] In doing so, and in light of the presumed comity achieved through the *Boshporus* decision, an issue which is examined by O'Neill in chapter 2, no distinction is drawn between the conditions for "justified interference" with the right under Article 8(2) of the ECHR and the terms of Article 52(1) EUCFR, where the phrase "lawful limitation" is used.

The data protection directive, Article 6

The obligation in terms of Article 6(1)[58] (Article 5 of the draft directive) is for data controllers to draw "as far as possible" a clear distinction between different categories of data subject. The five categories listed in the draft directive were indicative, not exhaustive, given they are presaged by the words "such as". They are suspects, persons with previous convictions for a criminal offence, victims or potential victims, third parties, including contacts or associates of suspects/convicted criminals and "others" who do not naturally fall within the previous categories. The DPWP recommended[59] that data subjects falling into the "others" category should only have their personal data processed if this proves necessary to assess the relevance of the data processed in relation to suspects/convicted criminals/victims or associates and that further use of the data for any other purpose is to be

providing further input on the data protection reform discussions, 01574/12/EN WP199, adopted 05 October 2012, and *Opinion 01/2012 on the data protection reform proposals*, 00530/12/EN WP 191, adopted 23 March 2012.

[57] Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ETS No 108 Strasbourg, 28 January 1981, Article 5(a).

[58] 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, OJ 2016 L119/89.

[59] *Article 29 Data Protection Working Party Opinion 01/2013*, paragraph 2.

forbidden.[60] This recommendation was on all fours with *Schwarz* and presages the further recommendation that the effect of each categorisation on data subject rights ought to be specified. These recommendations were broadly aligned with the decision in *Rotaru* v *Romania*,[61] which exemplified the requirement for (domestic) law to clearly specify categories of data subjects and the precision required in drafting such instruments[62] to meet the requirement of foreseeability when defining the circumstances in which personal data in each category can be lawfully processed, and stored by public authorities for the purposes of current and subsequent investigations. As the ECtHR in *Rotaru* put it: "the expression (in accordance with the law) not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question."[63] *Rotaru* also suggests that data surveillance[64] will only be justified where it is strictly necessary.[65] In *Uzun* v *Germany*[66] the ECtHR allied the concept of justified interference with a serious belief that the data subject had or was about to commit a serious criminal offence. However, *S and Marper* v *United Kingdom*[67] held that routine retention of personal data, there, the DNA profiles of the applicants, once a suspect had been acquitted or charges against them dropped, fell on the wrong side of the margin of appreciation afforded to signatory states when pursuing a legitimate aim.

The judgments above reflect the terms of Council of Europe (CoE) Recommendation (87) 15 E where the principles of limitation and

---

[60] It is also suggested in *Article 29 Data Protection Working Party Opinion 01/2013* at paragraph 2 that victims and associates be afforded additional limitations and safeguards, according to national law, although such measures are not identified.

[61] *Rotaru* v *Romania*, Application No. 28341/95, (2000) 8 BHRC 449 paragraph 57.

[62] *Malone* v *UK*, paragraph 87.

[63] *Rotaru* v *Romania*, paragraph 52.

[64] Data surveillance has been defined as "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection". Surveillance Studies Network: *A Report and the Surveillance Society for the UK Information Commissioner*, (2006), paragraph 3(1).

[65] See also *Kopp* v *Switzerland*, Application No. 23224/94, (1999) 27 EHRR 91, paragraph 55 and *Amann* v *Switzerland*, Application No. 27798/95, (2000) 30 EHRR 843, paragraph 50.

[66] *Uzun* v *Germany*, Application No. 35623/05, (2011) 53 EHRR 24, paragraph 80.

[67] *S and Marper* v *United Kingdom*, paragraph 125.

necessity are to be applied as the default rule to the collection of personal data for law enforcement purposes, and where the deletion of data is recommended when the data subject is of no further interest to a specific investigation.[68]

It is worth noting here that Article 12(1) of the until recently in force Council Decision establishing the European Police Office (the Europol Decision)[69] proceeded on the basis that the processing of personal data via the Europol Information System can only comprise "persons who, in accordance with … national law… are suspected of having committed or having taken part in a criminal offence… or who have been convicted of such an offence; or persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences…". If proceedings are dropped or if the suspect is acquitted the data is then to be deleted.

As Taylor has pointed out, "it is important to make the distinction between proportionality and the margin of appreciation," to the extent that the ECtHR has no locus, "unless the domestic [legal] system fails in some way to protect rights." Therefore "the Convention need not be applied uniformly in all states."[70] These assertions are undoubtedly correct and in the context of proportionality, the EU and member states have a dual responsibility to define any limitations in primary and secondary instruments with precision. However, in light of the discussion of the principles of limitation and necessity in *Digital Rights Ireland*, it is this author's opinion that the tension created by Article 5(4) TEU, where proportionality is required to be assessed conjunctively with the principle of subsidiarity, and Article 52(1) EUCFR, where proportionality is assessed on the basis of legitimacy of the limitation, may give the Strasbourg court cause to pause, and consider how the margin of appreciation is to be assessed should the EU finally accede to the ECHR.

---

[68] Council of Europe Recommendation (87) 15 E of the committee of ministers to member states regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987, Principle 2(1), Principle 2(2) and Principle 7.

[69] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office, OJ 2009 L121/37.

[70] Taylor, N., "Policing, privacy and proportionality," *European Human Rights Law Review* (2003) Supp Special issue: privacy 2003, 86-100, 95.

Article 6 does not retain the "others" category detailed in Article 5 of the proposed directive. The significance of this change may be limited given the categories of "contacts" and "associates" of the suspect remain and are not defined with any precision.

The processing of personal data of individuals falling into different Article 6 classifications will prove necessary on a practical and operational level. However, the varying level of protection offered to data subjects by the maintenance of EU agency-specific policing legal instruments, as discussed by Blasi Casagran in chapter 6, presents a further challenge. This challenge is the homogenous implementation of an EU-wide intelligence-led policing model to combat organised crime through the development of a European Criminal Intelligence Model (ECIM).[71]

The ECIM is predicated on member states and EU institutions observing a "common methodology for tackling serious and organised crime."[72] It is hard to envisage how a common methodology for processing and exchange of personal data is to be achieved, given, as discussed above, the margin of appreciation enjoyed by member states when implementing secondary legislation. Thus, any variability in the transposition of Article 6 of the data protection directive, and its subsequent domestic interpretation, has the potential to create further complexity and uncertainty as to the proper categorisation of third parties who it may transpire, be neither contacts or associates of the suspect, or fall within any other category listed in Article 6. For example, there will be uncertainty engendered where a person is considered to be merely a co-worker or family member in one member state but a contact or associate in another. Such a scenario could be ameliorated to a certain extent by amending Article 6 of the directive as enacted in line with the thrust of the DPWP's recommendation per the now defunct "others" category, so that the processing of personal data of individuals linked in some way to the suspect, but who are neither suspected of criminal activity or a convicted criminal, is subject to the enhanced rights and remedies contained in the data protection regulation.

[71] *Commission Communication to the Council and the European Parliament of 2 June 2005: developing a strategic concept on tackling organised crime*, COM(2005) 232 final.
[72] Ibid. Annex A, paragraph 2.

The draft data protection directive, Article 7

Article 7(1) (Article 6(2) of the draft directive) restates, almost word for word the terms of Principle 3(2) of the Council of Europe Recommendation (87) 15 E,[73] where it is mandated that a distinction is to be drawn, "as far as possible" between data derived from fact and that derived from personal assessment prior to processing. However, Article 6(2) of the draft directive failed to amplify what steps the data controller was required to take to meet this proviso and, in the absence of this, the EDPS recommended the words "as far as possible" were deleted.[74] This recommendation was not implemented in the revised Article 7. The proportionality of data surveillance of individuals who may or may not be suspects at the relevant time was addressed by the ECtHR in *Weber and Saravia* v *Germany*.[75] Holding, in contrast to the *S and Marper* v *UK* decision, that the requirement for (initial) surveillance to protect national security must be afforded a "fairly wide" margin of appreciation given the legitimacy of the aim, "adequate and effective guarantees against abuse" must be evidenced.[76] The proper assessment of the concepts of adequacy and effectiveness was expanded upon by ECtHR in *Khelili* v *Switzerland*,[77] where it was held that neither the processing nor long term retention of personal data implying criminal activity "founded on vague allegations not supported by fact"[78] was necessary in a democratic society. As argued above, Article 6 of the directive should be amended to mandate that the processing of personal data of those who are neither suspects or convicted criminals' ought to be subject to the rights and remedies contained in the data protection regulation. It follows that Article 7 should also be amended to define the circumstances and the basis on which a previous non-suspect may legitimately come to be viewed as a potential suspect based on personal assessment rather than fact. It is clear that this has not been provided by Article 7 of the directive which has been expanded only to require that "all reasonable steps" be taken to ensure

[73] Council of Europe Recommendation (87) 15 E of the committee of ministers to member states regulating the use of personal data in the police sector.
[74] *Opinion of the European Data Protection Supervisor of 7 March 2012*, paragraph 357.
[75] *Weber and Saravia* v *Germany*, Application No. 54934/00, (2008) 46 EHRR SE5.
[76] *S and Marper* v *UK*, paragraph 106.
[77] *Khelili* v *Switzerland*, Application No. 16188/07, 18 October 2011, unreported, (judgment available in French only).
[78] ECHR Information Note on the Court's Case Law No 145 October 2011, 17.

accuracy of, and as far as practicable" the "quality" of the personal data prior to transmission[79] or by the further requirement for a recipient to rectify or erase "incorrect" personal data upon notification.[80]

Accepting that time may be of the essence in many PJCCM operations the reality of intelligence-led policing means that initial suspicion will often be founded on personal opinion rather than evidential fact, a pragmatic approach would be to amend Article 7(3) by inclusion of a "sunset clause", which would ensure that, if no factual basis for suspicion emerges *viz á viz* a specific individual within a specified period of time,[81] any data gathered and processed in the interim, must be deleted by both the transmitting and receiving party. Such an approach would reflect the reality of the initial stages of any intelligence-led investigation of criminal activity and evidence adequate and effective guarantees against abuse as demanded by the Strasbourg court's judgments in *Khelili* and that of the CJEU in *Digital Rights Ireland.*

The data protection directive, Articles 36 and 37

Article 36(1) of the directive (ex. Article 34(1) of the draft directive) permits data transfers to third countries where the Commission had determined that an adequate, but not necessarily reciprocal, level of data protection exists. In the absence of such a declaration, the Commission can alternatively determine adequacy on a case-by-case basis. Where the Commission has yet to reach a decision, Article 37 (previously Article 35(1) of the draft directive) empowers member states to transfer data either where there are appropriate safeguards in place via a legal agreement or where the data controller after carrying out an assessment concludes that appropriate safeguards exist. In 2012 the EDPS was of the view that any assessment of adequacy undertaken by the data controller alone provides an insufficient safeguard and recommended that Article 35(1) of the proposed directive be deleted or "as a minimum" be amended to provide for prior authorisation by a national supervisory authority,[82] thereby bringing it into line with Article 23 of the Europol Decision and Article 42(5) of the then proposed data protection regulation. This proposal was

[79] Directive (EU) 2016/680, Article 7(2).
[80] Ibid. Article 7(3).
[81] Three months was noted to be acceptable in *Weber and Saravia* v *Germany*, paragraph 136.
[82] *Opinion of the European Data Protection Supervisor of 7 March 2012*, at paragraph 414 and paragraph 415.

not taken on board in the final drafting of the directive. Whilst a discussion of the proper definition of "adequate" protection is beyond the scope of this chapter, in the context of transborder data flows Poullet[83] had suggested that it should focus on the effectiveness of any controls exerted rather than their form. This view is also taken by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs which has argued that transfers should only proceed if appropriate safeguards are defined in a legally binding instrument and that the authorising party in each member state be required to fully document the necessity and justification for transfers for future scrutiny by national data protection supervisory authorities.[84]

There remains the potential for EU supranational ISS and intergovernmental CFSP security imperatives to collide and whatever safeguards it incorporates to evidence data processing by member states for internal security purposes which is both fair and lawful and EUCFR compliant. This is so in light of the tension created between the competing demands of Article 16(1) TFEU (the horizontal data protection provision) and Article 39 TEU which authorises, by way of derogation from Article 16 TFEU, the Council to adopt a decision, specifying the extent of data subjects rights in relation to activities undertaken by member states within the confines of the CFSP.

Whilst Article 16(1) TFEU adopts the wording of Article 8(1) EUCFR and applies to member states, institutions, EU bodies etc. when processing personal data relating to activities within the scope of Union law, Article 16(2) TFEU goes on to state that provisions adopted under its auspices are without prejudice to Article 39 TEU. As pointed out by Cremona,[85] Article 2(4) TFEU details (when delineating the extent of CFSP activities) that the

---

[83] Poullet, Y., "Transborder Data Flows and Extraterritoriality: The European Position," *Journal of International Commercial Law and Technology*, 2(3), (2007) 141-153, 148.

[84] *European Parliament Committee on Civil Liberties, Justice and Home Affairs Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM(2012) 10, 83.

[85] Cremona, M., "The Two (or Three) Treaty Solution: The New Treaty Structure of the EU," in *EU Law after Lisbon*, Biondi A. and Eeckhout P. and Ripley S. eds. (Oxford University Press, 2012, 47).

EU's competence to act is required to be in accordance with the provisions of the TEU. This leads her to consider the "significance" of the Council preferring the TEU over the TFEU as the instrument of choice for CFSP activities given that Article16 TFEU is of general application and horizontal effect as detailed at Title II TFEU.[86] In doing so, she underscores that Article 39 TEU places obligations on member states only. On one construction, it can therefore be proposed that EU institutions, bodies etc., when engaged in data processing for CFSP purposes, will not be bound by Article 16(1) TFEU. On the other, Cremona suggests that the exact wording of Article 39 TEU, which requires any Council decision adopted to be "in accordance with Article 16 TFEU," presupposes mandatory, rather than optional, compliance with its terms.[87]

The data protection directive; the CFSP and fundamental rights

Article 2(3)(a) of the data protection directive (Article 2(3)(a) of the draft directive) states the finalised instrument will not apply to the processing of personal data "in the course of an activity which falls outside the scope of Union law" whilst Article 2(3)(b) makes it clear that it will not apply to the data processing activities of Union institutions, bodies, offices and agencies. One such body, by way of example, is the European External Action Service (EEAS) which operates on the basis of Decision 2010/427/EU.[88] The EEAS is designated as a "functionally autonomous body of the Union"[89] tasked with assisting the High Representative of the Union for Foreign Affairs and Security Policy[90] who, in conjunction with member states, is required to implement CFSP initiatives "using national and Union resources."[91] Article 3 of this decision permits the EEAS to enter into service level agreements with, and to extend support and cooperation to, *inter alia* inter-institutional bodies of the Union and extend to these other institutions and bodies. Specifically, Article 3(4) obliges the EEAS to cooperate with the European Anti-Fraud Office (OLAF) in

[86] Ibid. 48.
[87] Ibid.
[88] Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service, OJ 2010 L201/30.
[89] Ibid. Recital 1.
[90] TEU, Article 27(3).
[91] Ibid. Article 26(3).

accordance with what is now Regulation (EU/ Euratom) 883/2013.[92] The new regulation requires member states to give the "necessary assistance to enable the staff of [OLAF] to fulfil their tasks effectively."[93] These tasks include cooperation with non-EEA countries and the transfer of personal data in accordance with Regulation (EC) 45/2001[94] which permits derogations from certain data subject right for, *inter alia*, the prevention, investigation, detection and prosecution of criminal offences.[95]

Article of 11(3) of the EEAS decision requires the EEAS to also comply with Regulation (EC) 45/2001, but states that "The High Representative shall decide on the implementing rules..." This intra-EU relationship alone provides a graphic and operative example of the Article 24(1) TEU caveats that the CFSP is subject to "specific rules and procedures" as unilaterally defined and implemented by the Council.

Thym's[96] examination of the constitutional and legal status of the CFSP postulates that the "specific rules and procedures" element of Article 24 TEU confers a *sui generis* legal personality[97] on CFSP actions through the "exercise of executive power based on 'legal intergovernmentalism'."[98] This proposition can be viewed in two ways. In the first instance, the concept of intergovernmentalism is well understood to proceed on agreement and to preserve the sovereignty of parties engaged in interstate cooperation and this is reflected in Article 73 TFEU which re-asserts the pre-Lisbon position that national security remains solely a matter for individual member states. Accordingly, common positions are reached through consensus or not at all. In such circumstance where no sovereignty

[92] Regulation (EU/EURATOM) 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ 2013 L248/1.
[93] Ibid. Article 7.3.
[94] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L8/1.
[95] Ibid. Article 20(1)(a).
[96] Thym, D., "The intergovernmental constitution of the EU's foreign, security and defence executive", *European Competition Law Review,* (2011) 7(3), 453-480, 454.
[97] Ibid. 454.
[98] Ibid. 472.

is ceded to a supranational organisation, the jurisdiction of the CJEU would *prima facie* be excluded. In this context, however, the *Kadi I*[99] judgment is of interest, holding, as it did, that all Union measures, even those implementing extra-EU obligations, must be compatible with fundamental rights.[100] As noted by Kokott and Sobotta,[101] the court reasoned that the "review of lawfulness would apply only to the Union act that gives effect to the (international) agreement at issue."[102] Thym also considers that, post-Lisbon, the CFSP, its institutions and agencies "are no exclave"[103] in relation to observance of fundamental rights. However, he notes the paucity of CFSP Council decisions specifying formal relationships with third countries, or how these operate enabling the EEAS, amongst others, to function as "Brussels-based executive institutions."[104]

It is questionable whether decisions as to "adequacy" of third party recipients' protection taken by member states in terms of Article 37 of the data protection directive would achieve the status of international agreement, as demanded by *Kadi I*.[105] These are national rather than Union "measures." However, this would not preclude review given the horizontal effect of Article 16(1) TFEU. On the other hand, decisions of adequacy taken by the Commission under Article 36(1) of the directive may be viewed as international agreements, given that such Commission mandated decisions are taken on a supranational rather than intergovernmental basis and are binding on member states. In addition, Article 51 EUCFR explicitly extends the provisions of the Charter to all acts of EU institutions and agencies, making no distinction between actors operating on a supranational and/or intergovernmental basis.

[99] Joined Cases C-402/05 P & C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* [2008] ECR 1 6351.
[100] Ibid. paragraph 281.
[101] Kokott J. and Sobotta, C., "The Kadi Case - Constitutional Core Values and International Law - Finding the Balance?" *The European Journal of International Law*, 23(4) (2012), 1015–1024.
[102] Ibid. 1016.
[103] Thym, "The intergovernmental constitution" 477.
[104] Ibid. 479.
[105] Joined Cases C-402/05 P & C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission*.

Conclusion

Given the demise of the PJCCM pillar and the supranationalisation of its former remit post-Lisbon there appears little objective justification for the 2012 data protection proposals leading to the maintenance of two separate regimes affording varying and uncertain levels of protection to data subjects - a matter further discussed by Blasi Casagran in chapter 6 of this book.

The Commission's 2005 communication on tackling organised crime[106] has been implemented through the ECIM requiring action at Union level to be underpinned by a common methodology per threat assessment.[107] As things stand, neither Article 6 or Article 7 of the directive could have been described as truly strategic or targeted in their approach. Thus the propensity for variance in their implementation between member states will be unlikely to lead to consistent decision making or taking between national policing etc. authorities when processing personal data.

As illustrated by the previous non-policing Data Protection Directive 95/46/EC,[108] legitimate and necessary derogations in the interests of national security, prevention, investigation, detection and prosecution of criminal offences etc. can sit naturally within a mainstream provision. However such derogations would require to be, in light of the CJEU's findings in *Digital Rights Ireland*, drafted with precision and clarity. The ruling in *Schwarz* further requires that the effect of any limitations on data subject rights is specified.

If it is accepted that the CFSP post-Lisbon continues to operate in the shadows of the Union, the interface between its vestigial inter-governmental remit and the reach of EU law can, at best, be described as tenuous, notwithstanding the ruling in *Kadi I*.[109] It would then follow, as discerned by Eckes,[110] that in the area of CFSP the EU's accession to the ECHR may represent the only viable route to a remedy for unjustified interference

[106] *Communication from the Commission - Developing a strategic concept on tackling organised crime*.
[107] Ibid. paragraph 9.
[108] Directive 95/46/EC, Article 13.
[109] Joined Cases C-402/05 P & C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission*.
[110] Eckes, C., "EU Accession to the ECHR: Between Autonomy and Adaptation," 76(2) *Modern Law Review* (2013), 254–285, 283.

with a fundamental right and, if this is so, potentially obviate any *casus omissus* in the evolving post-Lisbon EU data protection framework.

Certain EEAS activity can only proceed through reliance on supranational primary legislation (for example, the OLAF regulation) or secondary legislation (Article 37 of the directive). As a result the EEAS, tasked as it is, with implementing CFSP initiatives using national and Union resources - is to be considered *de facto* an intergovernmental "bureaucracy with supranational elements."[111] Data transfers to the EEAS, by virtue of such instruments, may allow data subjects to seek review of the legality of data transfers under the auspices of the supranational and/or the domestic legislation concerned before both domestic/EU and ultimately the Strasbourg court.

Bibliography

Amann v *Switzerland*, Application No. 27798/95 (2000) 30 EHRR 843.

Article 29 Data Protection Working Party Opinion 01/2012 on the data protection reform proposals, 00530/12/EN WP 191, adopted 23 March 2012.

Article 29 Data Protection Working Party 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, WP 211 adopted on 27 February 2014.

—. *Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, 00379/13/EN WP 201, adopted 26 February 2013.

—. *Opinion 08/2012 providing further input on the data protection reform discussions*, 01574/12/EN WP199, adopted 05 October 2012.

Bosphorus Hava Yollari Turizm v *Ireland*, Application No. 45036/98 (2006) 42 EHRR 1.

Commission Communication to the Council and the European Parliament of 2 June 2005*: developing a strategic concept on tackling organised crime*, COM(2005) 232 final.

Communication from the Commission to the European Parliament and the Council, *The European Economic and Social Committee and the*

[111] Peutter, U., "The Latest Attempt at Institutional Engineering: The Treaty of Lisbon and Deliberative Intergovernmentalism in EU Foreign and Security Policy Coordination" in *EU External Relations Law and Policy in the Post-Lisbon Era*, Cardwell P J. ed., (Asser Press, 2012, 32.)

Committee of the Regions Safeguarding Privacy in a Connected World, COM(2012) 9 Final.

—. *The EU Internal Security Strategy in Action: five steps towards a more secure Europe*, COM(2010) 673 final.

Conference of European Data Protection Authorities, Krakow, 25-26 April 2005. *http://europoljsb.consilium.europa.eu/media/51910/7ADC0308-5AA6-44C7-9E26-9E7FC6BC2C1B.pdf*.

Council, *A Secure Europe and a Better World*, 12.12.03.

Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service, OJ 2010 L201/30.

—. 2009/371/JHA of 6 April 2009 establishing the European Police Office, OJ 2009 L121/37.

Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ETS No 108 Strasbourg, 28 January 1981.

—. Recommendation (87) 15 E of the committee of ministers to member states regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L350/60.

Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States as amended, OJ 2004 L385/1.

Council; *Report on the Implementation of the European Security Strategy: Providing Security in a Changing World*, 11.12.2008 S407/08.

Cremona, M., "The Two (or Three) Treaty Solution: The New Treaty Structure of the EU," in *EU Law after Lisbon*, Biondi A. and Eeckhout P. and Ripley S. eds. (Oxford University Press, 2012, 47).

Case C-594/12 *Digital Rights Ireland Ltd* v *The Minister for Communications and others*, Opinion of the Advocate General Cruz Villalón delivered on the 12 December 2013, [2013] ECR I-0000.

C-293/12 & C-594/12 *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Judgment of the Court (Grand Chamber) of 8 April 2014, [2014] All ER (D) 66 (Apr).

—. C-291/12 *Schwarz* v *Stadt Bochum* [2013] WLR (D) 386.

—. C-468/10 and C-469/10 *ASNEF and FECEMD* [2011] ECR I 12181.

—. C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I 11063.

—. C-274/99 P *Connolly* v *Commission* [2001] 3 CMLR 58.
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, OJ 2016 L119/89.
—. 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC, OJ 2006 L105/54.
—. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L281/31.
Draft Internal Security Strategy for the European Union: Towards a European Security Model Document 7120/10.
Durant v *FSA* [2003] EWCA Civ 1746.
ECHR Information Note on the Court's Case Law No 145 October 2011.
Eckes, C., "EU Accession to the ECHR: Between Autonomy and Adaptation," 76(2) *Modern Law Review* (2013), 254–285.
European Parliament Committee on Civil Liberties, Justice and Home Affairs Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012)10.
Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ 2005 C53/1.
Hearing of the European Economic and Social Committee, 9 February 2011 - Counter-Terrorism Policy and Data Protection *https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-02-09_Counter_terrorism_EN.pdf*.
Jacobs, F., "The European Convention on Human Rights, The EU Charter of Fundamental Rights and the European Court of Justice; The impact of European Union accession to the European Convention on Human Rights," in *The future of the European judicial system in a*

comparative perspective: 6th International ECLN-Colloquium/IACL round table, Berlin, 2-4 November 2005, Pernice I. and Kokott J. and Sauders C. eds., Nomos, 2005, 291-296.

Joined Cases C-402/05 P & C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* [2008] ECR 1 6351.

Khelili v *Switzerland*, Application No. 16188/07 18 October 2011, unreported.

Kokott J., and Sobotta, C., "The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?" *The European Journal of International Law* 23(4) (2012), 1015–1024.

Kopp v *Switzerland*, Application No. 23224/94, (1999) 27 EHRR 91.

Malone v *UK*, Application No. 8691/79, [1984] 7 EHRR 14.

Opinion of the European Data Protection Supervisor of 7 March 2012 on the data protection reform package.

—. *14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of regions – A comprehensive approach on personal data protection in the European Union.*

—. *17 December 2010 on the Communication from the Commission EU Internal Security Strategy in Action: Five steps towards a more secure Europe*.

Peutter, U., "The Latest Attempt at Institutional Engineering: The Treaty of Lisbon and Deliberative Intergovernmentalism in EU Foreign and Security Policy Coordination" in *EU External Relations Law and Policy in the Post-Lisbon Era*, Cardwell P J. ed., (Asser Press, 2012, 17-34.)

Poullet, Y., "Transborder Data Flows and Extraterritoriality: The European Position," *Journal of International Commercial Law and Technology*, 2(3), (2007) 141-153.

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

—. a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

Rauhofer J. and Mac Sithigh D., "The Data Retention Directive Never Existed," (2014) *SCRIPTed*, 11:1: (2014) 118-127, 119.

Regulation (EU) 2016/679 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 and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L119/1.

—. (EU/EURATOM) 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ 2013 L248/1.

—. (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L8/1.

Rotaru v *Romania,* Application No. 28341/95, (2000) 8 BHRC 449.

S and Marper v *United Kingdom*, Application Nos. 30562/04 and 30555/04 [2008], ECHR 1581.

Schorkopf, F., "The European Court of Human Rights' Judgment in the Case of *Bosphorus Hava Yollari Turizm* v *Ireland*," 6 *German Law Journal*, (2005), 1255-1264, 1261.

Stockholm Programme - An Open and Secure Europe, Serving and Protecting Citizens Citizens, OJ 2010 C115/1.

Surveillance Studies Network: A Report and the Surveillance Society for the UK Information Commissioner, (2006).

Taylor, N., "Policing, privacy and proportionality," *European Human Rights Law Review* (2003) Supp Special issue: privacy 2003, 86-100.

Thym, D., "The intergovernmental constitution of the EU's foreign, security and defence executive", *European Competition Law Review,* (2011) 7(3) 453-480.

UK House of Commons Justice Committee *Opinion on the EU Data Protection Proposals, Third Report 2012-13* of 1 November 2012 HC 572, 3.

—. European Scrutiny Committee, *Fifty-ninth Report of Session 2010–12*, Documents considered by the Committee on 14 March 2012, HC 428.

UK House of Lords European Union Committee, 17th Report of Session 2010–12, The EU Internal Security Strategy, HL Paper 149.

Uzun v *Germany*, Application No. 35623/05, (2011) 53 EHRR 24.

Weber and Saravia v *Germany*, Application No. 54934/00, (2008) 46 EHRR SE5.

CHAPTER EIGHT

SEEING IS BELIEVING: POLICE PRACTITIONERS AS AN EPISTEMIC COMMUNITY

MO EGAN

Introduction

The developing "Area of Freedom, Security and Justice" places continued pressure on European Union (EU) agencies to shore up the available evidence base for policy development.[1] Specifically, the implementation of the EU Internal Security Strategy demonstrates how such evidence is incorporated within policy development at the EU level.[2] However, as acknowledged by Parkin, many of these EU policing agencies derive such evidence from member states' various data repositories.[3] Consequently, domestic organisations/agencies responsible for such data collection can influence EU level policy,[4] affirming Reiner's assertion that "all policing is inherently political."[5]

Against this background, this chapter examines the interaction of national police practitioners as "experts in their field," assessing the validity of

[1] Parkin, J., *EU Home Affairs Agencies and the Construction of EU Internal Security Strategy* (Brussels: CEPS Paper in Liberty and Security in Europe no 53, 2012).
[2] Council Conclusions on the creation and implementation of an EU policy cycle for organised and serious international crime, Doc. 15358/10.
[3] For specific discussion of the inter-relationship between Europol and national law enforcement see Blasi Casagran, Chapter 6.
[4] Parkin, J. *EU Home Affairs Agencies*.
[5] Reiner, R., *The Politics of the Police*, 3rd Ed, (Oxford: Oxford University Press, 2000), 49.

their knowledge as a foundation for such policy and increasingly, law making. Specifically, through an examination of the role of Scottish financial investigators this chapter will reveal the veneer of legitimacy afforded to police knowledge within the development of domestic law enforcement and evaluate epistemic claims. To demonstrate the precarious creation of this police knowledge this chapter will begin by explaining the research on which this chapter is based. Examining the qualitative and quantitative contributions of police knowledge to the development of policy and law within the financial investigation sphere, it sets out the role of the Financial Investigation Unit in Scottish policing. In doing so, it enables readers from other jurisdictions to consider where such expertise may be located within their law enforcement organisations. It is argued that the financial investigation community in Scotland can be conceptualised as an epistemic community. However, the impartiality of police knowledge must be called into question in light of its social construction through the subjective interpretation of normative orders. Indeed, this chapter concludes that the domestic context of police knowledge, as distinct from data, must not be lost as the EU Internal Security Strategy[6] develops, since transparency and accountability are fundamental components in the legitimate development of EU criminal justice policy.[7]

Foundation Research

The critical questions posed in this chapter, of police participation in the evolving structures of EU criminal justice policy, arose from an initial research project examining inter-agency cooperation across jurisdictions in the policing of money laundering.[8] More precisely, the project examined how the legislative framework designed to support the policing of money

[6] Council Document 5842/2/2010, Internal Security Strategy for the European Union: Towards a European Security Model. See also proposals for implementation in European Commission, (2010). Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final.

[7] European Commission. Communication from the Commission to the European Parliament and the Council. *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final.

[8] The project was jointly funded by the University of Abertay Dundee and the Scottish Institute for Policing Research 2009-2012.

laundering was operationalised by police officers in Scotland.[9] This involved semi-structured interviews of operational police officers and civilian staff with specialist experience in the field of financial investigation. The project offered an opportunity to engage practitioners in qualitative research. The research sample below (Table 1) illustrates the variety of local, national and regional officers and staff involved in the project. The interview schedules were designed around five academic debates that were established following a literature review. These included the concept of globalisation, the increasing emphasis on "the follow the money approach to crime control," the use of risk, the trend of promoting cooperation at EU level, and considering the mechanisms which influence police officers perception of "success" in policing. In the course of these interviews it was proclaimed "financial investigators are really enthusiastic, almost evangelical."[10] Undeniably, this was borne out in conversation with other officers as they emphasised the centrality of recovering the proceeds of crime to the disruption of future criminality. As one officer explained, "a prison sentence can be done by a lot of them standing on their heads, whereas if you hit them in the pocket, you're withdrawing their ability and means to start up where they left off when they come back out again...It's a two pronged attack really, you go in and deal with it conventionally and then you come back and sweep up the money."[11]

Table 1. Interview Sample

Police Force/ Agency	No of Participants	Females	Males	Police Officers	Civilian Staff	Other
Tayside	4	3	1	2	2	0
Lothian & Borders	4	0	4	3	1	0
Strathclyde	4	0	4	3	1	0
SCDEA*	5	0	5	5	0	0
Europol	1	0	1	1	0	0
Eurojust	1	0	1	0	0	1
Total	19	3	16	14	4	1

*Scottish Crime and Drug Enforcement Agency

[9] Egan, M., *Scottish based money laundering operations: Inter-agency cooperation across jurisdictions*, Doctoral Thesis, (Dundee: University of Abertay, 2013).
[10] Interview 12, Detective Constable, 9.
[11] Interview 4, Detective Constable, 1.

It is important to acknowledge that the police officers interviewed ranged in rank from Detective Constable to Detective Inspector. The significance of this observation is that "for the promotion process... the more of a politician you become,"[12] meaning the rank of the officer has implications in terms of the training each officer may have and their responsibilities within the organisation. This will impact on their reasons for participating in the research and perhaps the content of the interviews themselves, as officers seek to promote the virtues of financial investigation. All police officers interviewed were operational, and their service ranged from 14 to 30 years. A number of civilian financial investigators were interviewed and their experience ranged from 1 year to 13 years (although it should be noted that one of the members of police staff interviewed, who had been in post for one year, was an ex-police officer of 31 years' experience). Access to participants was gained through a "chain referral" process, characteristic of conducting research with sensitive organisations. [13] Participation was open to all officers and staff with experience or interaction with the policing of money laundering, subject to the way the information was disseminated within the particular forces/agencies, and availability on interview dates.

In the course of these interviews it became apparent that officers viewed their role as instrumental, not only in reactive policing activities consistently associated with law "enforcement," but also proactive policing activities. In that "[they] really are moving away from a kind of traditional investigation, towards right at the very beginning of an investigation saying 'what is the story with the money?'"[14] Reactive policing, on the one hand, refers to responding to events which may or may not be criminal, undertaking pertinent investigation, and collating evidence for prosecution. Proactive policing on the other hand, refers to attempting to pre-empt and prevent crime. In the context of financial investigation, an example of reactive policing activities would be preparing a financial profile to support a confiscation of assets on the basis that they are the proceeds of crime.[15] Proactive activities would include contributing financial intelligence to an ongoing operation for example

[12] Interview 1, Detective Constable, 28.
[13] Biernacki, P. Waldorf, D. "Snowball Sampling, Problems and Techniques of Chain Referral Sampling," *Sociological Methods & Research*, 10, no. 2 (1981), 141-163, 141.
[14] Interview 16, Detective Inspector, 3.
[15] Interview 8, Detective Sergeant, 1.

seeking to identify drug traffickers by "following the money."[16] Although, in some forces individual officers attempted to balance proactive and reactive responsibilities moment to moment, in other local forces the department divided proactive and reactive tasks between different teams within the department. It was apparent in all forces that their proactive involvement was considerably wider than preventative policing and encompassed promoting the persona of the Financial Investigation Unit internally and externally.[17] One particular officer was adamant that financial investigation is "the best kept secret in the police."[18] However, this chapter is not concerned with their desire to promote financial investigation *per se* but rather the knowledge created within the department and its dissemination.

Promoting Intelligence

The development of proactive policing is not specific to Scottish policing but reflects a broader trend towards intelligence led policing. Ratcliffe describes intelligence led policing as the use of intelligence to detect or disrupt criminal activity,[19] where the goal is said to be, to pre-empt the occurrence of crime, and to prevent it from taking place. The trend is thought, at least in the UK, to have been embedded in policing through the adoption of what is known as the National Intelligence Model (NIM). Originally designed by the then National Criminal Intelligence Service (a precursor to the National Crime Agency) in late 1990s, it provided a framework that could be used to manage information and intelligence.[20] Within the model, Flood and Gaspar argue that successful planning and resource allocation is predicated on "knowing the business,"[21] and that a central component of this is "rigorously evaluated intelligence."[22] However it is without doubt a difficult concept, as one civilian participant

[16] Interview 1, Detective Constable, 4.
[17] Interview 1, a Detective Constable referred to participating in training probationers and continuous professional development of more senior officers. In interview 18, a Detective Sergeant spoke of engagement with the media.
[18] Interview 14, Detective Inspector, 14.
[19] Ratcliffe, J., *Intelligence-Led Policing*, (Cullompton, UK: Willan Publishing, 2008), 72-73.
[20] NCIS, *The National Intelligence Model*, (London: NCIS, 2000).
[21] Flood, B. and Gospar, R., Stategic Aspects of the UK National Intelligence Model, Chapter 4 in ed. J. Ratcliffe, *Strategic Thinking in Intelligence*, 2nd Ed, (Sydney: The Federation Press, 2009), 53.
[22] Ibid. 55.

explained, "it's a real difficult thing to define and a real difficult thing to deal with... coming from so many different sources and all the sources are not reliable... it's their perspective of what they've seen."[23] In this context, intelligence refers to information that has been analysed by a police analyst. This product can be the result of a combination of sources from covert human intelligence and offender interviews, to crime patterns and police data sources.[24] Yet, an officer lamented "the days of Sherlock Holmes and his magnifying glass are long gone, if ever they were ever really here. We rely on the public telling us what's going on, that's an irrefutable fact as far as I'm concerned [because] the people coming into custody...you will get ones that sing like canaries but they are few and far between."[25] In making these remarks the participants highlighted the problematic nature of the availability and reliability of information enabling officers to tackle the complex problems of crime.

Ultimately, within the NIM, intelligence provides a foundation for decision making. However, to focus on the role of intelligence in the police organisation would provide little insight to the development of police knowledge. Since, as highlighted by Walsh in his analysis of the use of intelligence and intelligence analysis, questions have to be asked as to the extent to which intelligence agencies (both national security agencies and policing) have "provided full, frank and fearless assessments [of crime] to their governments, without undue pressure from them, to deliver a conclusion that matches existing policy prescriptions."[26] This is an interesting proposition to consider. Walsh acknowledges a power dynamic within the relationship between governments and their intelligence and policing agencies where the government is the dominant "partner." However, in the author's view this underestimates the ability of the agency to package the information, in combination with the limited scope for the government to challenge its validity. These organisations have privileged access to the creation and dissemination of this knowledge.

The Role of Financial Investigation in Scotland

It is important to provide an outline of the Financial Investigation Unit's (FIU) "routine" activities as they were at the time this research took

[23] Interview 3, Civilian Financial Investigator, 14.
[24] Ratcliffe, *Intelligence-Led Policing*, 4.
[25] Interview 1, Detective Constable, 12.
[26] Walsh, P., *Intelligence and Intelligence Analysis*, (London: Routledge, 2011), 204.

place.[27] This outline is necessary in order to understand the competing demands on the department, and how these impact upon the Unit's role in the collation and utilisation of information and their contribution to police knowledge. Accordingly, in 2009, when interviews took place, Tayside FIU was staffed by two police officers and two civilians. Here, Tayside FIU will be used as an illustration of the type of work undertaken by a typical FIU within the Scottish police.[28]

The daily routine began with checking the custody system that details everyone who is currently detained in the Tayside Police area. Each officer or Civilian Financial Investigator checked to see if anyone in custody was part of an ongoing policing operation. In a police operation several police departments came together to tackle particular individuals, or particular types of criminality, in a coordinated project. Such operations ran for a number of weeks or a number of years and indeed, there may be intervening circumstances which brought an operation to a premature close. For example, in drug trafficking operations where a large quantity of heroin was known to be changing hands, the police had to consider whether to seize the drugs, alerting the drug traffickers that they were under surveillance or, allowing the drugs to be distributed in the hope of tracing higher level criminals who were coordinating such transactions. Ultimately, if there was an individual of interest in custody, then this provided an opportunity for an officer (either from the FIU or a field intelligence officer) to interview the individual, to try and gain additional intelligence. Anyone who had been involved in drug trafficking, people trafficking, prostitution or any acquisitive crimes, was the subject of further examination.

[27] This description of the work if the FIU is based on the author's doctoral thesis. Egan, *Scottish based money laundering operations*, 89-95.

[28] Depending on the particular territorial unit the title of the department varied between Financial Investigation Unit and Financial Intelligence Unit. Financial Investigation Unit has been preferred in this chapter. This daily routine is composed following analysis of the interviews of the four participants from Tayside Police. Since these interviews took place there has been a number of significant changes within the Scottish police of particular significance is the amalgamation of the separate local forces into one, Police Scotland. (See Police and Fire Reform (Scotland) Act 2012. asp 8.) Still, within Police Scotland they have retained a local command structure and therefore these data remain broadly relevant.

In identifying these individuals, officers from the FIU were focusing on whether there was potential for asset confiscation. Thereafter, a credit check would be undertaken to try and build up a picture of the individual's financial situation. In doing so, a member of the FIU may have directly contacted financial institutions with which the individual had a relationship.[29] In addition, the Scottish Intelligence Database (SID) would also be checked for supplementary intelligence. One officer captured the frustrations of many with this relatively new database, as he explained although "we can now see intelligence from the whole of Scotland, it's such a laborious system to input and extract information from...It's so slow, I dare say because it's a national database...I'm not convinced that [local] forces are putting all their intelligence on it, and if they are, I think a lot of them are so protective of that intelligence they are putting it at a level that none of us can see."[30] Another officer highlighted the issue of what he called "operator error," explaining that "if you have an operator who doesn't link a name to the address then the chain breaks" resulting in a skewed picture of available intelligence with the potential to hinder the progress of an investigation.[31] Still, on the basis of the available strands of intelligence, officers fed into a policing operation, or contributed to reactive work, such as asset confiscation. Both proactive and reactive aspects often worked in tandem with one another. For example, a known criminal may have been the target of a police operation, and as part of that operation asset restraint and confiscation were considered. There were also a number of competing requests for assistance from the FIU by other departments or officers. For example, the FIU may have been approached to assist with trying to find a missing person. Accordingly, balancing the demands of proactive and reactive work within the department was acknowledged by officers and staff as being difficult.[32]

Significantly, the interviews coincided with major changes in the field of financial investigation. Firstly, the Scottish Government developed a

[29] For an examination of the relationship between the police and these private institutions see Egan, M., "The Role of the Regulated Sector in the UK Anti-Money Laundering Framework: Pushing the Boundaries of the Private Police", *Journal of Contemporary European Research,* 6(2) (2010), 272-288.
[30] Interview 1, Detective Constable, 5.
[31] Interview 6, Detective Constable, 8.
[32] Interview 1, 12.

strategy for tackling serious and organised crime in Scotland.[33] This identified that the pursuit of profit is central to serious organised criminals' activities. The Scottish Government's strategy specifically highlighted the intention to focus on disrupting crime through the improvement of seizure and confiscation, "ensuring Scotland is fully engaged with international intelligence sharing," and working with "regulatory bodies, including local authorities, to target the most harmful serious organised crime groups."[34] The strategy referred to the second significant influence of change, being the joint thematic inspection by Her Majesty's Inspectorate of Constabulary for Scotland and the Inspectorate of Prosecution in late 2009.[35] This inspection set out to examine how the Proceeds of Crime Act 2002 was being implemented by the Scottish police forces and the prosecution service.[36] This legislation provided the legal basis for the criminalisation of the proceeds of crime in the UK.[37] The inspection intended to review the process and systems used by the police and prosecution service, and identify and promote good practice in the use of the Proceeds of Crime Act 2002, hoping to make recommendations for improving service.[38]

During the interview process an officer spoke of their participation in the inspection stating they were "heavily involved with both parties."[39] In making this statement he demonstrated the wide sphere of engagement of the officers. On the one hand, it could be argued that officers were required to participate in the inspection. However, on the other hand, it could be argued it provided a forum for officers to express their views. Officers felt that the report captured many of the problems with mainstreaming financial investigation.[40] In particular, the lack of senior

[33] Scottish Government, *Letting Our Communities Flourish: A Strategy for Tackling Serious Organised Crime in Scotland*, The Serious Organised Crime Taskforce, Scottish Government, June 2009, [online] Available at: http://www.gov.scot/Publications/2009/06/01144911/0 (last accessed 24/7/17).
[34] Ibid, 10.
[35] HM Inspectorate of Constabulary for Scotland (HMICS) and the Inspectorate of Prosecution in Scotland (IPS), *Joint Thematic Report on the Proceeds of Crime Act 2002*, (2009).
[36] Ibid, 3.
[37] Proceeds of Crime Act 2002, c29. For example, s.92 Confiscation Orders, Scotland. There are additional provisions for each of the jurisdictions within the UK.
[38] HMICS and IPS, *Joint Thematic Report on the Proceeds of Crime Act 2002*, 3.
[39] Interview 14, Detective Inspector, 14.
[40] Interview 11, Detective Sergeant, 3.

officer representation within the financial investigation community was highlighted by officers and appeared in the resultant report.[41] They went on to explain that representation at the senior level was fundamental to successful change in an organisation dominated by hierarchical bureaucracy. It was reiterated in the course of this research that financial investigators "have a weak voice" within the organisation and that they had to tackle a lot of "structural inertia."[42] Still, the officers appeared to be determined to "push the voice and make it stronger."[43]

The Scottish Government committed to taking on board any recommendations made by the inspection. They incorporated appropriate changes into their over-arching strategy to tackle serious and organised crime demonstrating the concerns of officers filtering through to influence domestic policy.[44] This included investing money seized from criminals into expanding financial investigation.[45] It was acknowledged "it is a political decision essentially where the money gets spent."[46] These prospective changes were very much at the forefront of officers' minds and the basis of much speculation at the time of interview.

Still, financial investigation in and of itself is not new. The passage of the Proceeds of Crime Act 2002 raised the profile of policing powers in the UK in relation to asset restraint, confiscation and, of course, measures facilitating and enforcing anti-money laundering provisions, but these were building on an extensive body of existing law.[47] As early as 1961 moves were afoot at the international level to tackle the financial benefits of drug trafficking, and so, the focus on financial investigations percolated down through to domestic legislation.[48] Within the Scottish forces financial investigators have historically been located with the fraud squad, leading to an inevitable confusion as to the difference between fraud and financial investigation. The impetus for separating out financial investigation from fraud appears, from officers accounts, to have been the introduction

[41] Interview 1, Detective Constable, 1.
[42] Interview 11, Detective Sergeant, 3 and Interview 12, Detective Constable, 11.
[43] Interview 11, Detective Sergeant, 3.
[44] Scottish Government. (n31) 14.
[45] Scottish Government. (n31) 14.
[46] Interview 12, Detective Constable, 10.
[47] For example, the Drug Trafficking Offences Act 1986, c32. and the Criminal Justice (Scotland) Act 1987 c41.
[48] Single Convention on Narcotic Drugs 1961 as amended, Art 36(2). S24, Drug trafficking Offences Act 1986 and s23, Criminal Justice (Scotland) Act 1987.

of the Proceeds of Crime Act 1995.[49] Since then each force has gradually increased their commitment to financial investigation, through the dedication of officers and support staff.

Interviews took place prior to the addition of new personnel recruited as a result of the Scottish Government's strategy, and it must be acknowledged that it is likely that the addition of these new staff members will have changed the structure and capability of the three FIU's who received this additional funding.[50] Nevertheless, for the time being this illustration of the daily work of the Tayside FIU is broadly similar to that of the other forces. However, the division between proactive work and reactive work being allocated to dedicated teams/officers was more prominent in both Lothian and Borders Police and Strathclyde Police, which had more extensive resources. Again, it must be acknowledged that as the principal research took place over a period of three years (2009-2012), and with the intervention of the joint thematic inspection and reinvestment strategy, all three forces were undergoing an intensive period of change, with a vast increase in resources and personnel dedicated to mainstreaming financial investigation. This means that each force was at a different stage in addressing these intervening factors. Tayside was in the process of contemplating change at the time of interview, whereas Lothian and Borders and Strathclyde were in the process of implementing changes. Again, this makes it difficult to make direct comparisons between the forces' approaches to financial investigation. Moreover, the period over which this sustained investment took place was limited.[51] The money invested by the Scottish Government was for a period of two years, and therefore it remains to be seen whether the police officers and staff recruited to financial investigation at that time remained within the FIU, or were redeployed.[52] Nevertheless, in all forces the trend (at the time of interview) was the expansion and promotion of financial investigation. This trend facilitates the financial investigation community's claims to expertise.

[49] Interview 1, 3.
[50] See Cavanagh, B. *A review of reinvestment in financial investigation from the proceeds of crime.* Edinburgh: Justice Analytical Services Division, Scottish Government Social Research, 2011. (Last accessed on 24/7/17). Available at: http://www.scotland.gov.uk/Publications/2011/10/20092612/2.
[51] Ibid, para 1.
[52] Ibid.

Defining an Epistemic Community

This chapter is concerned with the components of the financial investigation community's expertise. Specifically, how the work of the FIU contributes to the creation of police knowledge and its subsequent dissemination. The creation and dissemination of police knowledge is of concern because claims to knowledge can be exercised to influence the policy and law.[53] Boswell argues exercising these claims to knowledge can serve a legitimising and substantiating function.[54] This means the knowledge can be drawn upon by an organisation to "bolster claims to resources or jurisdiction" or to justify policy preferences and marginalise competing interests.[55] Table 2 summarises the various categories of utilisation and dissemination of police knowledge identified by officers in the course of their interviews.

Table 2. Police knowledge on the paths to epistemic influence

Domestic	Regional	International
Promotion of financial investigation within law enforcement Collation/retention/ dissemination of intelligence and evidence (proactive and reactive components) Expert witness testimony/Statements of opinion Participation in legislative process Informal networks (e.g.	Contributions to EUROSTAT* Participation in Europol - Analysis Work Files - Threat Assessments** Responding to EU legislative proposals Participation in EU Commission Expert Groups *Drawn upon on European	Participation in Interpol Camden Asset Recovery Interagency Network Egmont Moneyval

[53] Boswell, C., *The Political Uses of Expert Knowledge: Immigration policy and Social Research*, (Cambridge: Cambridge University Press, 2013), 7.
[54] Ibid.
[55] Ibid.

Scottish Financial Investigators Practitioners Forum) Formal Networks (Scottish Asset Recovery Group) Performance Indicators Participation in research projects Media engagement	Commission Management Plan 2014 **Used as monitoring mechanisms of 'success' of Internal Security Strategy	

Communities who are able to make such claims to knowledge have been conceptualised as epistemic communities. Despite the rhetoric of their existence their definitive characteristics are a little more elusive, a perhaps ironic position given their propensity to claims of establishing knowledge within their varied scientific fields. Still, the concept of an epistemic community is fairly well established within the field of international relations. Haas, the first of the international relations scholars to explain the concept in the early 1990s, argued that knowledge-based experts (epistemic communities) play a role in "articulating the cause and effect relationships in complex problems, helping states to identify their interests."[56] More significantly, he argued that "control over knowledge and information is an important dimension of power and that the diffusion of new ideas and information can" determine the direction of international policy. [57] Attempting to identify such actors he claimed that these communities can be classified by the display of four traits. The first of these traits is narrated as a shared set of normative principled beliefs. The second trait being shared causal beliefs. The third trait shared notions of validity and the fourth, a common policy enterprise.[58]

Those within the financial investigation community displayed these different traits in their creation and dissemination of police knowledge. Here, police knowledge refers to intelligence, financial information,

[56] Haas, P., Introduction: epistemic communities and international policy coordination, *International Organization*, 46(1) (1992), 1-35.
[57] Ibid. 3.
[58] Ibid.

performance management data, and police officers' experience, that is in some respects self-substantiating. The precariousness of such epistemological claims based on experience is illustrated as one officer explained "[the police] are blinkered in that they have got intelligence that says [someone] is a bad guy."[59] He went on to demonstrate how this is reflected in the dissemination of that knowledge through the giving of expert witness testimony in that "if I'm asked a question by the Sheriff, I'll give him the truth as I know the truth," portraying the subjective nature of his police knowledge.[60] Still, the admissibility of such opinion evidence can be restricted if necessary in the Scottish courts by the judge exercising judicial discretion. In this way the accused can be protected should such evidence be, in the judge's view, prejudicial. This means that the impact of potentially subjective evidence can be limited.[61]

There are other ways that police officers participate in the creation of police knowledge that are perhaps less transparent. For example, as noted above, police knowledge includes data that is collated for the purposes of performance management. In Scotland, the performance of the police organisation was assessed at the time of the underpinning research by the Scottish Policing Performance Framework.[62] This framework involved assessing performance by recording performance indicators. Pertinent to financial investigation, in 2009 the framework required the recording of assets confiscated as a result of a Scottish Crime and Drug Enforcement Agency activity.[63] By 2010, this had changed to recording assets restrained as a result of Scottish Crime and Drug Enforcement Agency activity.[64] These measures are "a class of mythical numbers that are the product of government agencies" having resulted from consultation between the government and police representatives.[65] Throughout the interview process

[59] Interview 1, Detective Constable, 20.
[60] Ibid, 20.
[61] See Lord Sorn's remarks, *Hopes and Lavery* v *HMA Advocate*, 1960. J.C. 104 at 113. More generally, see Raitt, F., *Evidence: Principles Policy and Practice*, (Edinburgh: W.Green, 2013), Chapter 4 Expert and Opinion Evidence.
[62] Scottish Government, *Scottish Policing Performance Framework Annual Report 2012-2013*, (2013). See 2-3 for a summary of the history of the performance framework.
[63] Scottish Government, *Scottish Policing Performance Framework Annual Report 2009-2010*, (2010). 44.
[64] Scottish Government, *Scottish Policing Performance Framework Annual Report 2010-2011*, (2011). 74.
[65] Reuter, P. "The (continued) vitality of mythical numbers", *The Public Interest,* Spring, 75 (1984), 135-147, 136.

officers voiced their frustration with the recording of such statistics because they were of the view they did not reflect the reality of police work.[66] Yet, they still contended that they "try their best to influence them" and "make [their] targets work."[67]

Interviewees were very aware of the political impetus in police management decisions concerning the pursuit of such statistics and the potential problems. Illustrating the difficulties of political involvement in monitoring the performance of the police an officer explained "we could say we'll go after cocaine dealers and we'll quadruple [asset confiscation against] years before, but your street crime will go through the roof, so that is what we concentrate on, it's a balancing act all of the time...I think there are other ways to monitor how things are going rather than looking at facts and figures, but we're in that culture...I know the government demands these stats are kept, and it's very much a politically led thing, and the [senior officers] in Scotland have to fall into that." This raises concerns as to the potential influence of the Government on operational decisions particularly in areas of policing which create an illusion of quantifiable impact as is the case with financial investigation. Yet to critique the role of the Government alone in this regard would be to underestimate the role of the police organisation and individual officers within the development of criminal justice policy and practice.

Since the work of Haas there has been considerable exploration of the concept. In particular, Cross takes a great deal of time to review the literature on the existence and operation of epistemic communities, and identifies and reconsiders the characteristics of these communities.[68] Consequently, Cross's work can be drawn upon to construct a suitable framework in which to locate the concept of the epistemic community for the purposes of applying it to the financial investigation community. Cross attempts to address three specific issues within her literature review. Firstly, she argues epistemic communities are of growing importance in an increasingly globalised world as they are instrumental in translating knowledge into power. Secondly, she proposed that greater examination of the internal dynamics of epistemic communities is required to understand the strengths and weaknesses in these communities. She hypothesises that where greater internal cohesiveness is established this will lead to a more

[66] Interview 5, Detective Sergeant. 8-10. Interview 6, Detective Constable, 12.
[67] Interview 7, Detective Sergeant, 7-8.
[68] Cross, M., "Rethinking epistemic communities", *Review of International Studies*, 39(1) (2013), 137-160.

significant influence on policy outcomes. Thirdly, she argues that there is a need to reconceptualise the framework of epistemic communities more broadly.

Cross identifies a number of such communities and attempts to extrapolate their "epistemic" characteristics. These communities are wide ranging, including the global governance of safety standards within the field of shipping, air transportation, motor vehicle manufacturing, food production and pharmaceuticals, and in each of these fields it is possible to identify mechanisms of regulatory control that can be attributed to the influence of epistemic communities.[69] It is clear that the majority (if not all) of these studies are concerned with the dissemination of knowledge derived from the natural sciences. If this is the defining feature of the community then it would appear "police knowledge" cannot be accommodated within the theoretical framework of the epistemic community. However, it is argued here that the defining feature of the epistemic community is not the validity of the knowledge in question, but rather that community's claims to its validity, and their subsequent efforts to evangelise. This characteristic is demonstrated by the financial investigation community through their domestic, regional and international activities displayed in Table 2.

Haas' original four traits of an epistemic community are applicable to the police generally and the financial investigation community in particular. However, Adler argues that "the manner in which the world shapes and is shaped by human action and interaction depends on dynamic normative and epistemic interpretations of the material world," therefore it is pertinent to consider more deeply the specific influences on the creation of police knowledge.[70] The validity of that knowledge does not impact on the ability of the financial investigation community being viewed as an epistemic community in terms of the theoretical framework. Rather, the claim to that episteme is concerning since it achieves practical effect through exercising their influence on the substantiation of policy and law. It is easy to see the appeal of the concept of the epistemic community as providing a fairly commonsensical "rationalisation" of decision making. However, the difficulty lies in the relationship between the creation of

[69] Cross, ibid. cites Brathwaite, J. and Drahos, P., *Global Business Regulation*, (Cambridge: Cambridge University Press, 2000), 3-4, and Graz, J-C. and Nölke, A. eds. *Transnational Private Governance and Its Limits*, (New York: Routledge, 2008), 4.

[70] Adler, E. "Seizing the Middle Ground: Constructivism in World Politics", *European Journal of International Relations*, 3(3) (1997), 319-363, 322.

knowledge and its use in political enterprise. The legitimacy of knowledge is a central component in determining the acceptability of its use as an evidence base for the development of policy.

Exploring knowledge creation

There is a striking similarity in Haas' exposition of epistemic communities and Herbert's work examining subcultures of policing. Herbert's analysis proposes that police behaviour can be explained by unpacking the normative orders that influence it. He describes a normative order as "a set of rules and practices oriented around a central value."[71] This appears to be consistent with Haas' first characteristic of the epistemic community being a shared set of normative beliefs. Herbert argues that there are six such normative orders that are crucial to policing. These normative orders include law, bureaucracy, adventure/machismo, safety, competence and morality.[72] Law and bureaucracy are perhaps the most readily digestible as influences on police behaviour. In the context of financial investigation we have already seen some of those aspects. With the criminalisation of the proceeds of crime the legal framework to support officers in the investigating financial crime continues to expand.[73] However, demonstrating the subtle influence of their expertise being drawn into the legislative process an officer explained, "I was in contact with a Member of Parliament who sat on the committee that put the Proceeds of Crime Act through parliament...he was keeping us up to date...he would phone us and say "We're at our tea break and the Tories [Conservatives] have said such and such, what is your thought on it? About that section?" and you tell him you agree or don't agree and the reason."[74] This indicates that with such intimate participation in the development of domestic legislation, officers are simultaneously enforcers and creators of the rules.

Bureaucracy, as a guiding order of rules, is evident in the development of performance indicators seeking to monitor policing "success." However, again, they do not stand in isolation from the entrepreneurialism of the financial investigation community as they continue to try and influence both the creation of the measures of performance and the subsequent recording of them. Yet, it is the remaining normative orders that provide

[71] Herbert, S. "Police subculture reconsidered", *Criminology*, 36(2) (1998), 343-369, 343.
[72] Ibid.
[73] Proceeds of Crime Act 2002. c.29.
[74] Interview 6, Detective Constable, 2-3.

the greatest contribution to appreciating the social construction of police knowledge in the field of financial investigation, but they are also perhaps the most difficult to examine.

For example, one officer demonstrated the commitment to changing the culture of the organisation as he explained "I try to get through to a lot of folk that are working in my unit we have to see money getting taken off somebody rather than getting a prison sentence [as]making a difference."[75] However, this involved challenging officers' perceptions of competence. Fielding argues that competence should not be assessed with reference to articulated standards of performance, but rather by examining effective, skilful or good policing.[76] The difficulty for Financial Investigators is the relatively new approach to policing is not yet absorbed within the scope of this "competence." As officers spoke of demonstrating their success by "locking people up," "getting them the jail," counting the "kilos, cash and bodies," or "taking the money out their pockets," a tension can be identified between the traditional assessment of competence, and the advent of this new approach.[77] The individual officers' view of competence may impact upon the investigative choices that they make for example, whether to pursue drugs as they are distributed, or to focus on the money in the hope that it will lead to a "bigger player" or a "higher level criminal."[78] It is this aspect which has the potential to impact upon the development of police knowledge. Intelligence will be recorded, evidence procured, and this becomes theoretically an objective record of police action.

It may be that the desire for adventure amongst the police will inhibit the embedding of financial investigation, because the perception of the department is that it involves the "reading of pages and pages of bank statements," and that, given their propensity to machismo, officers would find this "torture."[79] Still, some officers appeared to find comfort in the "safety" aspects of the specialty as an officer explained "you're not exposed to violence...you're not dealing with criminals, you are dealing mostly with professionals in financial institutions."[80] Despite this

[75] Interview 5, Detective Sergeant, 10.
[76] Fielding, N., Competence and Culture in the Police, *Sociology*, 22(1) (1988), 45-64, 45.
[77] Interview 13, Detective Inspector, 4. Interview 16, Detective Inspector, 13.
[78] Interview 6, Detective Constable, 15. Interview 7, Detective Sergeant, 7.
[79] Interview 12, Detective Constable, 11.
[80] Interview 6, Detective Constable, 6.

acknowledgement of the "safer" aspects of financial investigation, it still appeared to be underpinned by the influence of "morality" being the last of Herbert's normative orders. This officer's categorisation of "criminals" as the "other" was not isolated, as various officers also referred to criminals as "bad guys" and "players."[81] In combination then, these normative orders will influence officers' interpretation of who and what contributes to the risk of crime.

It has been argued by Ericson that police officers produce and distribute knowledge for the management of risk.[82] However, Ericson claims that police officers offer distinctive knowledge about such risks, and it is this distinctive contribution to the "security quilt" that provides their legitimacy as an aspect of government.[83] Yet, the challenge to that legitimacy is the role of social construction in the creation of that knowledge. Moreover, that the components of social construction, (here exemplified by reference to Herbert's kaleidoscope of normative orders), introduce the potential for parochial differences between law enforcement in different jurisdictions. Moreover, the creation of knowledge within the police is bound up with the political entrepreneurialism of the policing institution as well as individual police practitioners. There are components of institutional and individual construction that influence the creation of this policing knowledge and the manner of dissemination. Promotion of these interests influence the types of behaviour that are labelled as crime and thereafter, those who are furnished with authority to identify, investigate, prosecute and punish the perpetrators of such crime.

Internal Security Strategy and National Law Enforcement

There has been an undeniable increase in the "inter-connectedness of states," that has resulted from contractions in space and time, as we travel through late modernity, where the walls between Westphalian sovereign states have crumbled.[84] From the rubble, competing interests have emerged in the control of crime, and international and regional structures

[81] Interview 1, Detective Constable, 1 and Interview 14 Detective Inspector, 16.
[82] Ericson, R., "The division of expert knowledge in policing and security," *BJS*. 45(2) (1994), 149-175, 151.
[83] Ibid. 153.
[84] Wallerstein, I., *World System Analysis: An Introduction*, (Durham, N.C: Duke University Press, 2004), cited in Drake, M., *Political Sociology for a Globalizing World*, (Cambridge: Polity Press, 2010), 18.

that provide the stage on which these interests can be promoted.[85] In the field of financial investigation, police officers have been able to capitalise on trends within the international, regional and domestic sphere, to secure extensions of police powers in the collation and utilisation of data. It is clear that with Directive on the Freezing and Confiscation of Proceeds of Crime,[86] and the proposed Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing,[87] financial investigation continues to be embedded in the formal legal structure designed to secure the internal security of EU citizens.

The European Union has emerged reborn time and time again like a phoenix. In its most recent incarnation following the adoption of the Lisbon Treaty, its jurisdiction in the area of freedom security and justice was bolstered. This was achieved by sweeping away the complexity of the third pillar structure, and expanding considerably the competence of the European Union in the development of criminal law measures. Historically, the European Union has demonstrated a reluctance to overstep the boundary between it supranational competence and the residual sovereignty of its membership, but times are changing.

Within the European Union, the institutions of the EU[88] and the EU agencies engaged in policing (broadly interpreted) of the area of freedom security and justice,[89] are capable of providing an additional layer of

[85] Ruggiero, V. "Global Markets and Crime," in ed. Beare, M., *Critical reflections on transnational organized crime, money laundering and corruption*, (Canada: University of Toronto Press, 2003), 172. Heron, T. (2008). "Globalization, Neoliberalism and the Exercise of Human Agency", *Int J Polit Cult Soc*, 20, 85-101, 85.

[86] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ 2014 L127/39.

[87] Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM(2016) 450.

[88] The three main institutions are the European Parliament, the European Commission and the Council of the European Union.

[89] These agencies are the European Asylum Support Office (EASO), European Institute for Gender Equality (EIGE), European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), European Network and Information Security Agency (ENISA), European Union Agency for Fundamental Rights (FRA), European Agency for the Management of Operational Cooperation at the External Borders

knowledge construction. In addition to these organisations, EUROSTAT provide comparable statistics on European countries. Their role was extended to the preparation of statistics on crime and criminal justice by the Hague programme in 2004, [90] and further strengthened by the Stockholm programme in 2009. The need for this renewed mandate was supported on the basis that "adequate, reliable and comparable statistics (both over time and between Member States and regions) are necessary... for evidence-based decisions on the need for action, on the implementation of decisions, and on the effectiveness of action."[91]

Now, drawing in the main from statistics recorded by the police in the member states, EUROSTAT acknowledges comparative problems. They are of the view that these statistics must be interpreted in light of the legal system from which they emanate, the point in time at which they may have been recorded (such as when reported to the police or where a suspect has been identified), the recording of multiple offences, and the categorisation of offences that are recorded. [92] These multifarious factors influence whether it is possible to draw comparisons between one jurisdiction and another. As demonstrated in Grant's chapter 7, although there are a multitude of measures that regulate the process of collation and retention of data, there remain gaps. Moreover, as the information becomes detached from its methodology the greater the likelihood the evidence becomes accepted wisdom. This can be seen throughout the European Commission's Directorate-General for Home Affairs Management Plan 2014 where there are various proclamations derived from EUROSTAT statistics, with a simple "(source: Eurostat)" acknowledgement.[93]

It is argued by Harding and Banach-Gutierrez that EU Criminal Justice Policy is "concerned with managing flows of people and activity, good

(FRONTEX), European Police College, The European Union's Judicial Cooperation Unit (EUROJUST) and The European Police Office (EUROPOL).

[90] Hague Programme – Strengthening Freedom, Freedom, Security and Justice in the European Union, OJ 2005 C53/01.

[91] Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ 2010 C115/21.

[92] EUROSTAT website (last accessed 22/3/14).
http://epp.eurostat.ec.europa.eu/portal/page/portal/crime/data/comparisons.

[93] Directorate-General for Home Affairs (2013), Management Plan 2014. European Commission.

and bad."[94] This remit is supported by the legal framework establishing and regulating the EU, but is given effect by the delivery of roadmaps. These roadmaps set out specific goals that the EU intends to deliver over a five year period.[95] This involves a matrix of inter-linked organisations that are furnished with powers and obligations to facilitate the achievement of these goals. It is argued that a fundamental component in development of policy goals is a robust evidence base. The robustness of this evidence based can be supported by epistemological claims that identify the ontology of crime problems. "Knowing" and "being" of crime problems become conflated in the production of police knowledge and subsequently, policies based on that knowledge. The problem becomes magnified, somewhat ironically, the more objective that knowledge claims to be.

Conclusion

It is clear that the financial investigation community in Scotland demonstrates the characteristics of Haas' epistemic community. They have actively contributed to both internal and external aspects of policy development.[96] Furthermore, they claim to have specialist knowledge in the field of financial investigation that is not present throughout the force, providing "the specific knowledge to the cop on the street."[97] They have taken every opportunity to voice their experience through participation in legislative drafting, required inspection and voluntary participation in research projects such as this. Reflecting on the summary of the dissemination of officers' knowledge, this chapter has only managed to explore some of their assertions. Still, the crucial argument in this chapter is that claims to expertise, and their dissemination of that expertise, are not problematic unless it becomes disassociated from its social construction. In this respect, Herbert's normative order can be drawn upon to try and examine more closely the construction of police knowledge within the financial investigation community. [98] Therefore, the concern, in terms of the implementation of the EU Internal Security Strategy, is that this disassociated police knowledge will become the foundation of the EU criminal policy. Still, considerably more work is required to fully explore

[94] Harding, C. and Banach-Gutierrez, J., "The emergent EU criminal policy: identifying the species," *E.L.Rev*. 37(6) (2012), 758-770, 760.
[95] Ibid.
[96] Haas, Introduction: epistemic communities and international policy coordination.
[97] Interview 6, Detective Constable. 5.
[98] Herbert, S., "Police subculture reconsidered", *Criminology*, 36(2) (1998), 343-369.

the implication of national variations of "normative orders" and they influence EU criminal policy.

Bibliography

Adler, E. "Seizing the Middle Ground: Constructivism in World Politics", *European Journal of International Relations*, 3(3) (1997): 319-363.

Biernacki, P. Waldorf, D. "Snowball Sampling, Problems and Techniques of Chain Referral Sampling," *Sociological Methods & Research*, 10(2) (1981): 141-163.

Boswell, C. *The Political Uses of Expert Knowledge: Immigration policy and Social Research*. Cambridge: Cambridge University Press, 2013.

Cavanagh, B. *A review of reinvestment in financial investigation from the proceeds of crime.* Edinburgh: Justice Analytical Services Division, Scottish Government Social Research, 2011. [online] (last accessed 24/7/17). Available at: http://www.scotland.gov.uk/Publications/2011/10/20092612/2.

Council Conclusions on the creation and implementation of an EU policy cycle for organised and serious international crime, Doc. 15358/10.

Council Document 5842/2/2010, Internal Security Strategy for the European Union: Towards a European Security Model. And also see proposals for implementation in European Commission, Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final.

Criminal Justice (Scotland) Act 1987 c41. (Scotland).

Cross, M. "Rethinking epistemic communities," *Review of International Studies*, 39(1) (2013): 137-160.

Directorate-General for Home Affairs (2013), Management Plan 2014. European Commission.

Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ 2014 L127/39.

Drake, M. *Political Sociology for a Globalizing World*. Cambridge: Polity Press, 2010.

Drug Trafficking Offences Act 1986, c32. (UK).

Egan, M. *Scottish based money laundering operations: Inter-agency cooperation across jurisdictions*. Doctoral Thesis, Dundee: University of Abertay, 2013.

—. "The Role of the Regulated Sector in the UK Anti-Money Laundering Framework: Pushing the Boundaries of the Private Police", *Journal of Contemporary European Research*. 6(2) (2010): 272-288.

Ericson, R. "The division of expert knowledge in policing and security," *BJS* 45(2) (1994): 149-175.

European Commission. *Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final.

EUROSTAT website http://epp.eurostat.ec.europa.eu/.

Fielding, N. "Competence and Culture in the Police", *Sociology*, 22(1) (1988): 45-64.

Flood, B., Gospar, R. "Strategic Aspects of the UK National Intelligence Model." In *Strategic Thinking in Intelligence*, ed. J. Ratcliffe, 2nd Ed. Sydney: The Federation Press, 2009.

Haas, P. "Introduction: epistemic communities and international policy coordination." *International Organization*, 46(1) (1992): 1-35.

Hague Programme – Strengthening Freedom, Freedom, Security and Justice in the European Union, OJ 2005 C53/01.

Harding, C. and Banach-Gutierrez, J. "The emergent EU criminal policy: identifying the species," *E.L.Rev.* 37(6) (2012): 758-770.

Herbert, S. "Police subculture reconsidered", *Criminology*, 36(2) (1998) 343-369.

Heron, T. "Globalization, Neoliberalism and the Exercise of Human Agency", *Int J Polit Cult Soc.* 20 (2008): 85-101.

HM Inspectorate of Constabulary for Scotland (HMICS) and the Inspectorate of Prosecution in Scotland (IPS). *Joint Thematic Report on the Proceeds of Crime Act 2002*, (2009).

Hopes and Lavery v *HMA Advocate*, 1960. J.C. 104 (Scotland).

Naylor, R. "Follow-the-money Methods in Crime Control Policy." In *Critical reflections on transnational organized crime, money laundering and corruption*, ed. Beare, M. Canada: University of Toronto Press, 2003.

Naylor, R.T. "Wash-out: A critique of follow-the-money methods in crime." *Crime, Law & Social Change*, 32(1) (1999): 1–57.

NCIS. *The National Intelligence Model*, London: NCIS, 2000.

Parkin, J. *EU Home Affairs Agencies and the Construction of EU Internal Security Strategy*. Brussels: CEPS Paper in Liberty and Security in Europe. No 53. 2012.

Police and Fire Reform (Scotland) Act 2012. asp 8. (Scotland)

Proceeds of Crime Act 2002, c29. (UK)

Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM(2016) 450.

Raitt, F. *Evidence: Principles Policy and Practice*. Edinburgh: W.Green, 2013.

Ratcliffe, J. *Intelligence-Led Policing*. Cullompton, UK: Willan Publishing, 2008.

Reiner, R. *The Politics of the Police*. 3rd Ed. Oxford: Oxford University Press, 2000.

Reuter, P. "The (continued) vitality of mythical numbers," *The Public Interest*. Spring 75 (1984): 135-147.

Ruggiero, V. "Global Markets and Crime," In *Critical reflections on transnational organized crime, money laundering and corruption*, ed. M. Beare. Canada: University of Toronto Press, 2003.

Scottish Government. *Scottish Policing Performance Framework Annual Report 2012-2013*. (2013).

—. *Scottish Policing Performance Framework Annual Report 2010-2011* (2011).

—. *Scottish Policing Performance Framework Annual Report 2009-2010*. (2010).

—. "*Letting Our Communities Flourish: A Strategy for Tackling Serious Organised Crime in Scotland*". The Serious Organised Crime Taskforce, Scottish Government, 2009, [online] (last accessed 24/7/17). Available at: http://www.scotland.gov.uk/Publications/2009/06/01144911/0.

Single Convention on Narcotic Drugs 1961. (UN)

Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ 2010 C115/21.

Walsh, P. *Intelligence and Intelligence Analysis*. London: Routledge, 2011.

ENVIRONMENT

CHAPTER NINE

SHIP-SOURCE POLLUTION AS AN ENVIRONMENTAL CRIME

ANGELA CARPENTER

Introduction

Ship-source pollution has long been recognised as a problem requiring international cooperation, whether at international, European Union (EU) or regional level. It has led to the development by the EU of an integrated maritime surveillance system. The EU builds its framework on regional and international treaty frameworks. These developments provide a model for further developments for both territorially based environmental crime, and transnational surveillance frameworks more generally, an issue examined by Skleparis in Chapter 4 in the context of border policing. In addition, as discussed by Blasi Casagran in Chapter 6, Europol will be expressly tasked with dealing with ship-source pollution under the Europol Regulation.[1]

This chapter examines a number of regimes established to protect the marine environment from intentional pollution. At the international level, it considers the development of the MARPOL Convention,[2] which aims to prevent pollution by oil, noxious liquids and garbage, for example, through the use of standards for ships and also zones where the discharge of wastes into the sea is prohibited. The chapter will examine the history of the MARPOL Convention, from its inception, through more recent

[1] Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, 5, Annex I.

[2] International Convention for the Prevention of Pollution from Ships 1973, (MARPOL) Misc.26 (1974), Cmnd 5748; 12 ILM 1319 (1973), and its 1978 Protocol.

changes. It will then consider the EU Directive on Port Reception Facilities for ship-generated waste and cargo residues,[3] which requires sea ports to provide facilities for ships to discharge waste as a way of reducing intentional inputs at sea. In support of that directive, the EU's European Maritime Safety Agency (EMSA) was established.[4] The role of EMSA as it relates to marine pollution from ships, particularly by oil, will be examined in this chapter. In due course the relationship between EMSA and Europol, post the implementation of the Europol Regulation will have to be examined, both from an academic and law enforcement practitioner perspective.

Oil pollution is one of the most easily detected pollutants at sea and a number of regimes have been established under international conventions to protect the marine environment from oil and other substances. For example, at a regional level, the 1992 Convention for the Protection of the Marine Environment of the North-East Atlantic (the OSPAR Convention[5]) building on the earlier Oslo[6] and Paris Conventions,[7] was established to prevent ships (and aircraft) from dumping waste into the marine environment. Under the OSPAR regime an assessment of the quality of the marine environment is required to identify the different types of waste being discharged into the seas around northern Europe.[8] Types of discharge include pollution from land-based sources,[9] from dumping or incineration of wastes,[10] from offshore sources[11] and from other sources not already the subject of measures set out by other international organisations or

[3] Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues, OJ 2000 L332/81.
[4] Regulation (EC) No 1406/2002 of the European Parliament and of the Council of 27 June 2002 establishing a European Maritime Safety Agency (Text with EEA relevance), OJ 2002 L208/1.
[5] Convention for the Protection of the Maritime Environment in the North East Atlantic (OSPAR), 1992, 2354 UNTS 67; 32 ILM 1069 (1993), in force 1998.
[6] Oslo Convention on the Prevention of Marine Pollution by Dumping from Ships and Aircraft, 11 ILM 262 (1972); UKTS 119 (1975), Cmns. 6228.
[7] Convention for the Prevention of Marine Pollution from Land-Based Sources (Paris Convention) 1974, 1546 UNTS 119; 13 ILM 352 (1974); UKTS 1978, No. 64.
[8] OSPAR Convention 1992, Article 6 and Annex IV.
[9] Ibid. Article 3 and Annex I.
[10] Ibid. Article 4 and Annex II.
[11] Ibid. Article 5 and Annex III.

conventions.[12] The EU, as a contracting party to the original Oslo and Paris Conventions, subsequently signed and ratified the provisions of the OSPAR convention for use within the EU.[13]

Identifying where ship-source pollution comes from is an important tool in trying to reduce levels of waste, and in potentially prosecuting the owners of ships which continue to dump substances such as oil at sea.[14] The United Nations Conference on Trade and Development (UNCTAD, 2012) sets out an overview of the international legal framework for dealing with pollution damage from tankers including both oil and chemical pollution.[15] In the case of oil, coastal states that are signatories to Conventions such as the 1992 Civil Liabilities Convention[16] and its amendments (CLC),[17] the 1992 Fund Convention[18] and its amendments, or the 2003 Supplementary Fund Protocol[19] can seek financial compensation for pollution damage caused by an oil spill, where pollution damage includes contamination resulting from the escape or discharge of oil from a ship. For pollution from a range of hazardous and noxious chemicals, compensation can be sought under the 1996 International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea (HNS Convention) and the 2010 HNS Protocol.[20]

---

[12] Ibid. Article 7.

[13] Council Decision 98/249/EC of 7 October 1997 on the conclusion of the Convention for the protection of the marine environment of the north-east Atlantic, OJ 1998 L104/1.

[14] Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L138/14.

[15] UN Conference on Trade and Development (2012).

[16] International Convention on Civil Liability for Oil Pollution Damage 1969, 973 UNTS 3; 9 ILM 45.

[17] Protocol of 1992 to amend the International Convention on Civil Liability for Oil Pollution Damage, 1969, B7 969: 88/C; 973 UNTS 3.

[18] International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage 1992 (1992 Fund Convention), 973 UNTS 3.

[19] Supplementary Fund Protocol establishing the International Oil Pollution Compensation Fund 2003 (the Supplementary IOPC Fund), Int'l Mar. Org., LEG/CONF.14/20.

[20] International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, 1996,

With the involvement of Europol in this crime area, under the express reference to ship-source pollution in the Europol regulation,[21] Eurojust, as the EU's investigating and prosecuting agency, will also have competence to act in this sphere, under Article 4.1 of the Eurojust Council Decision 2009, which provides that Eurojust shall have general competence in "the types of crime and offences in respect of which Europol is at all times competent to act." The chapter will therefore provide an overview of three regimes - covering three main EU member states' territorial waters, the Baltic Sea, the Mediterranean Sea and the North Sea - where aerial surveillance is used to detect oil pollution and, through the use of satellites (for example the European Space Agency's ENVISAT and the Canadian Space Agency's RADARSAT-1 and -2), and in co-operation with EMSA,[22] it may be possible to hindcast (back-track) oil pollution to a specific ship at sea. The chapter will then examine in more detail the regime covering the North Sea (together with the north-east Atlantic), the Bonn Agreement 1969,[23] and its subsequent amendments, as an example of those regional agreements.

Development of MARPOL

History

The MARPOL Convention arose from an international conference on marine pollution held in London in 1973. It was pre-dated by the 1954 International Convention for the Prevention of Pollution of the Sea by Oil (OILPOL 54) which was the result of a Conference organised by the United Kingdom (UK) government as a response to the threat of oil pollution from increasingly large oil tankers which used seawater to wash out tanks used to transport oil, discharging that mix of oil and water into

35 ILM 1415 (1996). For an overview of the HNS Convention see: http://www.hnsconvention.org/Pages/TheConvention.aspx.

[21] Proposal for a Europol Regulation, 5, Annex I.

[22] For details of how satellite images were used to monitor oil spills in European waters between April 2007 and January 2011 see European Maritime Safety Agency (2011). *CleanSeaNet First Generation Report: 16 April 2007 – 31 January 2011.* Available from: http://www.emsa.europa.eu/csn-menu/csn-background/items.html?cid=122&id=1309 (last accessed 3/7/17).

[23] Agreement for co-operation in dealing with pollution of the North Sea by Oil, Bonn, 1969. UKTS 77 (1975), Cmnd. 6056; 9 ILM 25 (1969).

the sea.[24] Subsequent incidents including the grounding, in 1967, of the *Torrey Canyon* on Seven Stones Reef off the Scilly Isles, UK, which spilt 80,000 tons of crude oil into the sea, highlighted the significant environmental threat posed by tanker accidents, and the limited measures available to try and prevent such accidents from occurring, or to handle the aftermath and determine liability for cleaning up pollution after such an event had occurred.[25]

The 1973 conference was organised by the Inter-Governmental Marine Consultation Organization, a United Nations (UN) Agency, which was subsequently renamed the International Maritime Organization (IMO) in 1982.[26] One of the main objectives of that conference was to "draft a comprehensive new convention that would completely eliminate the wilful and intentional discharge [of oil and other noxious or hazardous substances] into the seas" and to minimise "accidental spills from all types of ships."[27]

Resulting from the 1973 conference, the International Convention on the Prevention of Pollution from Ships (MARPOL 1973) was signed. It incorporated OILPOL in its Annex I, as well as a number of other measures relating to oil pollution. MARPOL also included annexes covering noxious liquid substances (Annex II), harmful substances in packaged form (Annex III), sewage (Annex IV), and garbage (Annex V). In 1997, Annex VI was added covering air pollution from ships.

The 1973 Convention, together with its Protocols of 1978 (thereafter MARPOL 73/78) and 1997, together with ongoing amendments, now make up the main international legal framework dealing with the prevention of pollution of the marine environment from ships, due to both operational and accidental activities. MARPOL 73/78 covers 99% of the world's merchant shipping by tonnage, so it has a substantial global effect.

---

[24] For an overview of OILPOL 54 and its subsequent replacement by MARPOL 73, see http://www.imo.org/OurWork/Environment/PollutionPrevention/OilPollution/Pages/Background.aspx (last accessed 3/7/17).

[25] Nanda, V. P., "The Torrey Canyon Disaster: Some Legal Aspects," *Denver Law Journal*, 44, (1967), 400-425.

[26] For more details on the history of the International Maritime Organization see http://www.imo.org/KnowledgeCentre/ReferencesAndArchives/Documents/The Origins of the IMO (MGH) April 2012.doc (last accessed 3/7/17).

[27] Pritchard, S.Z., *Oil Pollution Control*, (UK: Croom Helm Ltd., 1987).

Summary of MARPOL 73/78 Annexes

Each of MARPOL's annexes contains information on the substances it covers, the standards it sets for different vessel types, how signatory states are to apply the particular annex, and designation of "Special Areas" (SAs) where discharge standards are stricter than for other areas.[28] There is, in addition, a range of other requirements. The IMO also identifies Particularly Sensitive Sea Areas,[29] such as the well-known Australian Great Barrier Reef, but also areas of Western European Waters and the Baltic Sea, where even greater protective standards are in place than for the designated SAs.

The main elements of the MARPOL 73/78 Annexes are as set out below.[30]

Annex I – Oil entered into force in October 1983. It sets limits on the total quantity and speed at which oil can be discharged by a tanker at sea, with no discharges being permitted within 50 miles of the nearest land. Annex I, in the 2002 Consolidated Edition of MARPOL,[31] contains 9 chapters, 26 regulations and 9 appendices. It is therefore a substantial document. Regulations under Annex I include: a requirement for segregated ballast tanks;[32] that all new tankers ordered for construction after July 1996 should have double hulls;[33] a programme for phasing out or conversion of single hulled vessels, which pose the highest risk of oil spills if their hulls were breached;[34] and limits on oil tankers carrying different amounts of heavy grade crude oils.[35]

---

[28] A Summary of Special Areas under MARPOL Annexes I, II, IV, V and VI is available at:
http://www.imo.org/OurWork/Environment/PollutionPrevention/SpecialAreasUnderMARPOL/Pages/Default.aspx (last accessed 23/4/14).

[29] For information on Particularly Sensitive Sea Areas, see:
http://www.imo.org/OurWork/Environment/PollutionPrevention/PSSAs/Pages/Default.aspx (last accessed 26/2/14).

[30] For an overview of the various Annexes of MARPOL 73/78 see:
http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-%28MARPOL%29.aspx (last accessed 3/7/17).

[31] IMO (2002), MARPOL 73/78 Consolidated Edition 2002. The most recent Consolidation Edition of MARPOL 73/78 was published in 2011.

[32] MARPOL 73/78, Annex I, Regulation 13.

[33] Ibid. Regulation 19.

[34] Ibid. Regulation 20 (Regulation 13G under 1992 amendments).

[35] Ibid. Regulation 21 (Regulation 13H under 1992 amendments).

Annex I also identifies SAs which are given a higher level of protection than other areas due to their location, ecology or volumes of traffic. Under the 1973 Convention these SAs included the Mediterranean, the Baltic, close to the EU, the Black Sea, and further afield, the Red Sea areas, together with the "Gulfs" area and the Gulf of Aden. This protection was later extended to include the Antarctic area (1990), North West European waters (1997), the Oman Sea area of the Arabian Seas (2004) and Southern South African Waters (2006). Similar SAs exist for Annexes II (Noxious Liquid Substances), IV (sewage), V (garbage) and VI (air pollution and green-house gas emissions), although in a number of cases insufficient coastal states have confirmed that they provide adequate reception facilities for these materials, resulting in those SAs not yet being in effect.[36] However, all 27 EU member states (even those without maritime borders - Austria, Czech Republic, Hungary, Luxembourg and Slovakia) were signatories to Annexes I to V of MARPOL 73/78 at 7 April 2014, and only Austria, the Czech Republic and Hungary were not signatories to Annex VI.[37] No doubt the EU will be anxious to have these provisions in place at least for its member states' territorial waters.

Annex II – Noxious Liquid Substances (NLSs) - entered into force in October 1983. It set out discharge criteria and measures for a range of noxious liquid substances which, in 2004, were categorised as "X," "Y" and "Z" together with "Other Substances."[38] These categories are based on the evaluation of thousands of chemicals by the Evaluation of Hazardous Substances Working Group to produce a GESAMP[39] Hazard Profile. The categories are:

---

[36] See Special Areas under MARPOL, Note *. Available at: http://www.imo.org/OurWork/Environment/PollutionPrevention/SpecialAreasUnderMARPOL/Pages/Default.aspx (last accessed 3/7/14).

[37] For a full listing of signatories to IMO Conventions (at 21 June 2017), including the various Annexes of MARPOL 73/78, select the "Status of Conventions" excel spreadsheet link at: http://www.imo.org/About/Conventions/StatusOfConventions/Pages/Default.aspx (last accessed 3/7/17).

[38] Further information on Annex II and the carriage of chemicals by ships is available at: http://www.imo.org/OurWork/Environment/PollutionPrevention/ChemicalPollution/Pages/Default.aspx (last accessed 3/7/17).

[39] Group of Experts on the Scientific Aspects of Marine Environmental Protection, http://www.gesamp.org/.

- Category X – NLSs which, if discharged at sea, are deemed to present a major hazard to marine resources or human health. These are prohibited from being discharged;
- Category Y – NLSs apply where discharges present a hazard to marine resources, human health, or cause harm to amenities or other uses of the sea. Limits are set on quality and quantity of discharge of this category into the marine environment;
- Category Z – NLSs presents a minor hazard to marine resources or human health. Less stringent restrictions apply here than to Category Y discharges; and
- Other Substances, which fall outside Categories X, Y or Z. These are deemed to not present a risk to marine resources or human health, and can be discharged into the sea during normal ship operations.

Annex III – Harmful Substances in Packaged Form entered into force in July 1992. This annex includes detailed standards on packing, marking, labelling, and documentation required for ships which transport packaged goods. It categorises harmful substances in line with the International Maritime Dangerous Goods Code (IMDG Code),[40] or those which meet the criteria in the Appendix of Annex III. Those criteria include "bioacccumulated to a significant extent and known to produce a hazard to aquatic life or to human health," and "liable to produce tainting of seafood."[41]

Annex IV – Sewage entered into force in September 2003, with a revised annex adopted in April 2004, and entering into force in August 2005.[42] This annex sets out requirements to control the discharge of sewage into the sea, and includes regulations covering ships' equipment, and the provision of facilities in ports to receive sewage wastes. The Annex

[40] Further information on the IMDG Code is available at: http://www.imo.org/blast/mainframe.asp?topic_id=158#classes (last accessed 3/7/17).

[41] See for example IMO (2002) MARPOL 73/78 Consolidated Edition 2002, Appendix to Annex III, 343 and also the Hazard Profile developed by the Group of Experts on the Scientific Aspects of Marine Environmental Protection, http://www.gesamp.org/.

[42] Further information on Annex IV and the prevention of pollution by sewage from ships is available at: http://www.imo.org/OurWork/Environment/PollutionPrevention/Sewage/Pages/Default.aspx (last accessed 3/7/17).

applies to all new ships over 400 gross tonnage on international voyages, and carrying more than 15 people. Existing ships had until September 2008 to achieve the same standards. Only ships with approved sewage treatment plants, and where sewage wastes are disinfected and comminuted (where the solid matter is shredded or pulverised) can discharge sewage at sea between 3 and 12 nautical miles from land. Untreated sewage has to be discharged outside the 12 nautical mile limit, although a standard has been set for maximum rate of discharge from holding tanks, as it is assumed that natural bacterial processes will break down these wastes away from land. The Baltic Sea region was granted SA status in July 2011, with its entry into force being dependent on sufficient coastal states confirming they can provide adequate reception facilities for this waste.[43]

Annex V – Garbage was originally an optional annex, however sufficient ratifications were received for it to enter into force in December 1988. This Annex covers different types of garbage and how that garbage should be disposed of.[44] It sets standards similar to Annex IV with regard to the size of ship, and number of people on board. As with other annexes, it also sets strict limits in its SAs, which include the Antarctic area and the Wider Caribbean Region, an area of direct interest to some EU member states. Annex V covers all vessels, and includes a complete ban on the dumping of any type of plastic at sea. Plastic bottles can, for example, take around 450 years to dissolve at sea. It also sets limits for the disposal of food wastes, paper products, rags, glass, metal, bottles, packaging materials and other types of garbage at different distances from land.[45]

Annex VI – Air Pollution and Greenhouse Gas Emissions was introduced by way of a Protocol in 1997, which entered into force in May 2005.

---

[43] See Special Areas under MARPOL, Note 28. Available at: http://www.imo.org/OurWork/Environment/PollutionPrevention/SpecialAreasUnderMARPOL/Pages/Default.aspx (last accessed 3/7/17).

[44] See Simplified overview of the discharge provisions of Annex V as of 1 January 2013 at: http://www.imo.org/OurWork/Environment/PollutionPrevention/Garbage/Documents/Annex%20V%20discharge%20requirements%2007-2013.pdf (last accessed 3/7/17).

[45] Further information on Annex V and the prevention of pollution by garbage from ships is available at: http://www.imo.org/OurWork/Environment/PollutionPrevention/Garbage/Pages/Default.aspx (last accessed 3/7/17).

Annex VI was subsequently revised in October 2008.[46] This annex is particularly important in relation to issues of climate change/greenhouse gases and ozone depleting substances (for example chlorofluorocarbons (CFCs)). It sets out standards for the reduction of nitrogen oxides (NOx) emissions from the engines of various types of ships.[47] It also sets (a) limits on the sulphur content in ship's fuel to reduce sulphur oxides (SOx) emissions to air from ships of various types,[48] (b) limits on volatile organic compounds (VOCs) from tankers in ports and oil terminals,[49] and (c) standards for shipboard incinerators, and the incineration of ship-generated sewage sludge and sludge oil.[50] In this latter respect, there is some interaction with the provisions of Annexes IV (sewage) and I (oil) which broadly cover these waste types. In addition, it sets even stricter sulphur content on fuel limits within Sulphur Emission Control Areas (SECAs), which includes the Baltic Sea and other sea or port areas designated by the IMO. In July 2011 Annex IV was further updated with a new Chapter 4 entitled "Regulations on energy efficiency for ships," which had a mandatory requirement for all new ships to have an Energy Efficient Design Index (EEDI), and for all ships to have a Ship Energy Efficiency Management Plan (SEEMP). The aim of this measure is to reduce greenhouse gas emissions (GHGs) from ship operations for all ships.[51]

Port Reception Facilities (PRFs) under MARPOL 73/78

A key obligation of the governments of contracting parties to MARPOL 73/78 is to ensure that there is provision of reception facilities for ship-generated residues and garbage that cannot, under the various Annexes of the Convention, be discharged at sea.[52] Those facilities must meet "the

[46] Further information on Annex VI and air pollution and greenhouse gases, together with links to those specific topics, is available at: http://www.imo.org/OurWork/Environment/PollutionPrevention/AirPollution/Pages/Default.aspx (last accessed 3/7/17).
[47] MARPOL 73/78, Annex IV, Regulation 13.
[48] Ibid. Regulation 14.
[49] Ibid. Regulation 15.
[50] Ibid. Regulation 16.
[51] For more information on EEDI and SEEMP which are Technical and Operational Measures under Annex VI of MARPOL 73/78 see: http://www.imo.org/OurWork/Environment/PollutionPrevention/AirPollution/Pages/Technical-and-Operational-Measures.aspx (last accessed 3/7/17).
[52] The relevant regulations by MARPOL 73/78 Annex are: Annex I, Regulation 38; Annex II, Regulation 18; Annex III, Regulation 12; Annex V, Regulation 7; and Annex VI, Regulation 17.

operational needs of users," by providing facilities for "the types and quantities of waste from ships normally using the port."[53]

The provision of adequate reception facilities for waste was one of the topics considered at the third meeting of the IMO's Marine Environmental Protection Committee (MEPC III) in July 1975, when a working party was set up to look at the issue as it particularly related to oily wastes, in recognition of the fact that some signatory states faced difficulties in implementing the 1973 Convention.[54] More recently, the 54th MEPC meeting in March 2006 noted that only with adequate reception facilities could the policy of "zero tolerance of illegal discharges from ships" be effectively enforced.[55] Subsequently, the IMO, in 2009, produced a guide to good practice aimed at tackling the continuing problem of inadequate provision by ports for the disposal of waste.[56]

The European Commission, for its part, as early as 1993, identified a number of issues of concern relating to the marine environment.[57] Of particular concern, in relation to marine pollution and the need for legislation on PRFs, was the recognition that, while there was a need for parties to MARPOL 73/78 to "provide and maintain facilities in their ports for the discharge of waste" including oily waste,[58] there were wide variations between ports and this could "potentially [lead] to unlawful discharges at sea."[59]

---

[53] IMO, 1999, *MEPC 43rd Session*, Agenda Item 7, Inadequacy of Port Waste Reception Facilities Report, 2.

[54] Mikelis, N. *IMO's Action Plan on tackling the inadequacy of port reception facilities.* Presentation at the Ships' Waste: Time for action!, Brussels, October 14 2010, 4. Available online at: http://www.imo.org/.

[55] International Maritime Organization. *Marine Environment Protection Committee (MEPC), 54th Session: 20 to 24 March 2006. Port Reception Facilities Database.* (London: IMO, 2006). http://www.imo.org/.

[56] International Maritime Organization. *MEPC.1/Circ.671 of 20 July 2009. Guide to Good Practice for Port Reception Facility Providers and Users.* (London: IMO, 2009). http://www.imo.org/.

[57] European Commission. *Communication from the Commission – A Common Policy on Safe Seas*, COM(1993) 66 final.

[58] Ibid., paragraph 115, 61.

[59] Ibid.

An EU directive on Port Reception Facilities[60] etc. was subsequently signed in 2000, in order to ensure that adequate facilities are provided in the ports of EU member states. That directive is discussed below.

EU Directive on Port Reception Facilities

History of the Directive

The initial Proposal for a Council Directive on port reception facilities was submitted to the Commission in July 1998,[61] although an earlier version, the Draft Directive on Shore Reception Facilities,[62] had been under discussion for some time.[63] The Port Reception Facilities (PRF) Directive,[64] signed in November 2000 and published in December that year, entered into force in December 2002.

The PRF Directive was developed with the purpose of "reducing the discharges of ship-generated waste and cargo residues into the sea, especially illegal discharges" by means of an increased provision and uptake of waste disposal facilities at ports, "thereby enhancing the protection of the marine environment."[65] In line with the obligation under MARPOL 73/28, set out above, Article 4 of the directive required member states to ensure the availability of facilities "adequate to meet the needs of the ships normally using the port without causing undue delay,"[66] and capable of receiving the types and quantities of waste produced by those ships.[67]

---

[60] Directive 2000/59/EC of the European Parliament and Council of 27 November 2000 on port reception facilities for ship-generated wastes and cargo residues, OJ 2000 L332/81.
[61] Proposal for a Council Directive on port reception facilities for ship-generated waste and cargo residues, COM(1998) 452 final.
[62] Commission of the European Communities. Draft Directive on Shore Reception Facilities for Ship Generated Waste, Version 3 of December 1997 (no document reference – paper version of this document is held by the author).
[63] Carpenter A., "The EU Directive on Port Reception Facilities: A Case Study in the Development of an EU Environmental Directive," *European Environmental Law Review*, 15(12) (2006), 369-380. See also Tables 1 and 2 – Timetable of Events in the development of Directive 2000/59/EC and Comparison between versions of Directive on Port Reception Facilities, 377-379.
[64] Directive 2000/59/EC.
[65] Ibid. Article 1 Purpose.
[66] Ibid. Article 4, Port Reception Facilities Para. 1.
[67] Ibid. Article 4, Port Reception Facilities, Para 2.

The PRF Directive has been amended on a number of occasions, with consolidated versions published in 2002, 2007 and 2008.[68] Subsequent to its entry into force, the Commission has identified a number of weaknesses in the directive relating to a number of articles including: Article 2 Definitions (this as a result of the introduction of Annex VI to MARPOL 73/78 at an international law level); Article 4 Adequacy of Facilities; and Article 8 Cost Recovery Systems.[69] The various articles of the PRF Directive are discussed in more detail below.

Since 2005 the Commission, together with EMSA, has been evaluating the implementation of the PRF Directive.[70] A number of organisations have participated in that review, including consultants, and they have reported back to the Commission.[71] At the time of writing recommendations on policy options have been put forward to the European Commission but no decision has yet been made on the future of the directive.

The main requirements of the PRF Directive

Other than the Article 4 requirements discussed above, the directive has a number of articles aimed at improving provision, and also the uptake of facilities. These are:

---

[68] Directive 2002/84/EC of the European Parliament and of the Council of 5 November 2002 amending the Directives on maritime safety and the prevention of pollution from ships (Text with EEA relevance), OJ 2002 L324/53, Commission Directive 2007/71/EC of 13 December 2007 amending Annex II of Directive 2000/59/EC of the European Parliament and the Council on port reception facilities for ship-generated waste and cargo residues (Text with EEA relevance), OJ 2007 L329/33, Regulation (EC) No 1137/2008 of the European Parliament and of the Council of 22 October 2008 adapting a number of instruments subject to the procedure laid down in Article 251 of the Treaty to Council Decision 1999/468/EC, with regard to the regulatory procedure with scrutiny - Adaptation to the regulatory procedure with scrutiny - Part One, OJ 2008 L311/1.

[69] European Commission. *Task Specifications to award a Specific Contract under DG MOVE's Framework Contract TREN/A1/143-2007 regarding Impact Assessment and Evaluations etc. Review of the Port Reception Facilities for ship-generated waste and cargo residues Directive under Lot 2 (Transport).* Doc. Ref: Ares(2010)849538 – 23/11/2010, Annex 1.

[70] Ibid. Introduction, 2.

[71] See, for example, European Maritime and Safety Agency. *EMSA Study on the Delivery of Ship-generated Waste and Cargo Residues to Port Reception Facilities in EU Ports.* (2012). Reference No. EMSA/OP/06/2011. http://www.emsa.europa.eu/.

Article 5 – Waste reception and handling plans. Plans must be developed and maintained by ports, which should provide information on "the need for, and availability of, reception facilities ... for each individual port" or ports within a region.[72] The plan should take into account the requirements of other articles of the directive,[73] and full details of the plan being set out at Annex I.[74]

Article 6 – Notification. The master of a ship, with specific exclusions, must notify the port in advance of the ship's arrival,[75] of the amounts and types of waste on board to be discharged into the port's facilities.[76]

Article 7 – Delivery of ship-generated waste. The master of a ship must discharge all waste into the reception facilities before leaving port,[77] but may be permitted to travel to the next port of call if there is storage capacity on board, unless the next port of call is unknown, or there is some risk that the waste will be dumped at sea.[78] Cargo residues (for example, coal left in a bunker after the cargo has been offloaded), are covered under Article 10, which specifies that those residues be delivered to a port reception facility in accordance with MARPOL 73/78 and the fee for delivery should be paid by the user of the reception facility.[79]

Vessel inspections in EU member states' ports are conducted under the aegis of the 1982 Paris Memorandum of Understanding on Port State Control,[80] under which recognised organisations such as the Maritime and Coastguard Agency in the UK undertake inspections against a range of

[72] Directive 2000/59/EC, Article 5 – Waste reception and handling plans, Para. 2.
[73] Specifically Articles 4 (adequacy of facilities), 6 (notification), 7 (delivery of ship generated waste), 10 (delivery of cargo) and 12 (accompanying measures) are expressly referred to in Article 5 (waste reception and handling plans).
[74] Directive 2000/59/EC, Annex I – Requirements for waste reception and handling plans in ports.
[75] Ibid. Article 6 – Notification, Para 1.
[76] Ibid. Annex II, - Information to be notified before entry into the port.
[77] Ibid. Article 7 – Delivery of ship-generated waste, Para 1.
[78] Ibid. Article 7 – Delivery of ship-generated waste, Para 2.
[79] Ibid. Article 10 – Delivery of cargo residues.
[80] Paris Memorandum of Understanding on Port State Control in Implementing Agreements on Maritime Safety and Protection of the Maritime Environment, 221 ILM 1 (1982). The most recent version of the MOU, including its 36th Amendment adopted 23 May 2016 and effective 1 July 2016. https://www.parismou.org/system/files/Paris%20MoU%2C%20including%2039th%20amendment%20_rev%20final.pdf (last accessed 3/7/17).

international conventions and EU Directives (including the PRF Directive).[81]

Article 8 – Fees for ship generated waste. This article requires that the cost of facilities should be collected through a fee levied on ships using the port,[82] and these cost recovery systems should provide "no incentive for ships to discharge their waste into the sea."[83] However a number of different systems were in operation,[84] and this was an area identified as requiring work to ensure that fees were fair and transparent.[85] There was also a requirement for a subsequent Commission evaluation of the various payment systems used in different ports.[86] Fees for cargo residues are covered under Annex 10 which simply states that they will be paid by the user of the reception facility.[87]

The PRF Directive has a number of further important provisions. *Article 9 – Exemptions*, for example, sets out arrangements which can be made for ships travelling regular routes between ports, so that they need only use facilities in one port. *Article 11 – Enforcement* provides that ships should be inspected to ensure they comply with the provisions of Articles 7 (delivery of ship generated waste), and 10 (delivery of cargo).[88] It also set out the various criteria to be used in identifying ships for inspection.[89] *Article 13 – Penalties* requires member states to develop a "system of penalties for the breach of national provisions," at the national level, with those penalties needing to be "effective, proportionate and dissuasive."[90]

---

[81] For an overview of the Paris MOU and information on the International conventions and EU Directives against which ships in EU member state ports are inspected, together with the selection criteria to identify vessels for inspection, see Carpenter A., *International Protection of the Marine Environment.* In The Marine Environment: Ecology, Management and Conservation, ed. A.D. Nemeth (New York: Nova Science Publishers Inc., 2011), 51-86.
[82] Directive 2000/59/EC, Article 8 – Fees for ship-generated waste, Para 1.
[83] Ibid. Article 8 – Fees for ship-generated waste, Para 2.
[84] Carpenter, A and S.M. Macgill, "Charging for Port Reception Facilities in North Sea Ports: Putting Theory into Practice," *Marine Pollution Bulletin*, 42(2) (2001), 257-266.
[85] Directive 2000/59/EC, Article 8 – Fees for ship-generated waste, Para 3.
[86] Ibid. Article 8 – Fees for ship-generated waste, Para 4.
[87] Ibid. Article 10 – Delivery of cargo residues.
[88] Ibid. Article 11 – Enforcement, Para 1.
[89] Ibid. Article 11 – Enforcement, Para 2 and points (a) to (d).
[90] Ibid. Article 13 – Penalties.

Establishment and Role of European Maritime Safety Agency (EMSA)

EMSA was established as a result the sinking of the *MV Erika* in December 1999 in the Bay of Biscay, 30 miles off the coast of Brittany.[91] It was recognised that there was a need for uniform and effective measures to combat pollution from ships operating in EU waters. A proposal was put forward in 2000,[92] and EMSA was created in 2002.[93] As part of its remit, EMSA was tasked with providing objective, reliable and comparable information and data to enable EU member states to take steps to reduce the threat of both accidental and deliberate pollution.[94]

EMSA has an ongoing role for ensuring the adequate provision of PRFs, one of its Implementation Tasks.[95] This task supports the EU in meeting the requirements of both MARPOL 73/78, and any amendments over time to that Convention, and also the PRF Directive. In particular, it assists the European Commission and member states by "establishing an appropriate information and monitoring system to enable improved identification of ships which [fail to] deliver their waste according to the Directive."[96] That monitoring system forms part of the operational tasks of EMSA,[97] which cover activities in the areas of marine safety, maritime security and marine environmental protection. For the purposes of this chapter, the main operational tasks of the EMSA are:

---

[91] For an overview of the sinking of the *MV Erika* and the subsequent actions of the EU, see Carpenter, A., "The EU and Marine Environmental Policy: A Leader in Protecting the Marine Environment," *Journal of Contemporary European Research*, 8(2), (2012), 248-267, 260 *et seq*.

[92] European Commission: Communication from the Commission to the European Parliament and the Council on a second set of community measures on maritime safety following the sinking of the oil tanker Erika, COM(2000) 802 final, 96-116.

[93] Regulation (EC) No 1406/2002 of the European Parliament and of the Council of 27 June 2002 establishing a European Maritime Safety Agency, OJ 2002 L208/1.

[94] Ibid. Article 2, Task (f).

[95] Details of the implementation tasks of EMSA are available at http://www.emsa.europa.eu/implementation-tasks.html (last accessed 26/2/14).

[96] EMSA; *Port Waste Reception Facilities – Role of EMSA.* http://www.emsa.europa.eu/implementation-tasks/environment/port-waste-reception-facilities.html (last accessed 26/2/14).

[97] Details of all the operational tasks of EMSA are available at: http://www.emsa.europa.eu/operations.html (last accessed 3/7/17).

CleanSeaNet:[98] This is a European satellite-based oil spill and vessel detection service which enables member states to identify and potentially trace the source of oil pollution at sea, and also monitor accidental pollution resulting from emergencies;

SafeSeaNet:[99] This is a vessel traffic monitoring system covering European coastal waters which is able to track up to 12,000 ships every day, and which can assist in traffic management, search and rescue activities and tracking banned vessels. It can also aid in marine environmental protection by assisting member states in responding to incidents or accidents which cause pollution at sea; and

a *Pollution Response Service*;[100] under which EMSA has available, at various locations in the Baltic, Irish, Mediterranean, and North Seas, a number of stand-by oil spill response vessels. Those vessels can be used to respond to oil pollution at sea, each carrying specialised oil spill response equipment on board to deal with, for example, oil floating on the sea.

Overview of Regional Regimes

In addition to the role of the IMO through MARPOL 73/78, the EU through the PRF Directive (and any future iterations), and EMSA tasks, each of the EU's sea regions has in place a regional convention to which coastal states are signatories. These Conventions are outlined below.

The Baltic Sea

The Convention on the Protection of the Marine Environment of the Baltic Sea Area, 1992 (the Helsinki Convention)[101] entered into force in January 2000.[102] This superseded the 1974 Convention of the same name. The

[98] EMSA. *Satellite Oil Spill Monitoring (CleanSeaNet),* EMSA Operational Tasks. http://www.emsa.europa.eu/csn-menu.html (last accessed 3/7/17).
[99] EMSA. *Vessel traffic monitoring in EU waters (SafeSeaNet),* EMSA Operational Tasks. http://www.emsa.europa.eu/ssn-main.html (last accessed 3/7/17).
[100] EMSA. *Stand-by Oil Spill Response Vehicles.* EMSA Operational Tasks. http://www.emsa.europa.eu/oil-spill-response/oil-recovery-vessels.html (last accessed 3/7/17).
[101] Helsinki Convention 1992. http://www.helcom.fi/Documents/About%20us/Convention%20and%20commitments/Helsinki%20Convention/1992_Convention_1108.pdf (last accessed 3/7/17).
[102] Contracting Parties to the Helsinki Convention are Denmark, Estonia, the EU, Finland, Germany, Latvia, Lithuania, Poland, Russia and Sweden.

Helsinki Convention[103] seeks to protect all areas of the Baltic Sea from substances which can harm living resources and marine ecosystems. It covers pollutants entering the marine environment from both land and sea.[104] It includes articles relating to the prevention of pollution from ships,[105] and on co-operation in combating marine pollution.[106] While Annex IV[107] sets out how parties to the Convention will co-operate with the IMO in "the effective and harmonized implementation of rules adopted by the [IMO]"[108] and in applying the various Annexes of MARPOL 73/78.[109]

The Mediterranean Sea

The Convention for the Protection of the Mediterranean Sea against Pollution (Barcelona Convention) was signed in February 1976 and entered into force in February 1978. Subsequently, it was revised in Barcelona in June 1995 and became the Convention for the Protection of the Marine Environment and the Coastal Region of the Mediterranean which entered in force in 2014.[110] The European Community acceded to the original Convention in July 1977 under Council Decision 77/585/EEC[111] and to its various protocols under a number of other Council decisions.[112]

Pollution under the Barcelona Convention included "the introduction by man, directly or indirectly, of substances or energy into the marine

---

[103] http://www.helcom.fi/about-us/convention/ (last accessed 3/7/17).
[104] Helsinki Convention, Article 2 - Definitions, Paras 1-3.
[105] Ibid. Article 8 – Prevention of pollution from ships.
[106] Ibid. Article 14 – Co-operation in combating marine pollution.
[107] http://www.helcom.fi/about-us/convention/annexes/annex-iv/ (last accessed 3/7/17).
[108] Helsinki Convention. Annex IV – Prevention of Pollution from Ships, Regulation 1: Co-operation.
[109] Ibid. Annex IV – Prevention of Pollution from Ships, Regulation 4: Application of the Annexes of MARPOL 73/78.
[110] https://wedocs.unep.org/bitstream/handle/20.500.11822/663/bcp_eng.pdf?sequence=3&isAllowed=y (last accessed 3/7/17).
[111] Council Decision 77/585/EEC of 25 July 1977 concluding the Convention for the protection of the Mediterranean Sea against pollution and the Protocol for the prevention of the pollution of the Mediterranean Sea by dumping from ships and aircraft, OJ 1977 L240/1.
[112] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l28084 (last accessed 3/7/17).

environment resulting in ... harm to living resources [and] hazards to human health."[113] It provides for its contracting parties to enter bilateral or multilateral agreements to protect the marine environment against pollution,[114] and covers aspects including pollution from both ships,[115] pollution from land-based sources,[116] and cooperation in dealing with pollution emergencies.[117]

Unlike the Helsinki Convention, the Barcelona Convention makes no mention of either the IMO or of MARPOL 73/78. Nor does it make any reference to the provision of PRFs. It also differs in that many of the signatories to the Convention are North African or Eastern European countries, leading to a mix of EU and non-EU contracting parties.[118]

The North Sea

Within two years of the 1967 *Torrey Canyon* disaster, eight North Sea states[119] came together to establish the 1969 Agreement for cooperation in dealing with pollution of the North Sea by oil (the Bonn Agreement). That agreement was subsequently amended in 1983 to include other harmful substances, and again in 2001 to extend its coverage into Irish waters.[120] As with the Barcelona Convention, no mention is made within the Bonn Agreement text of the IMO, MARPOL 73/78 or to PRFs. The focus of the Bonn Agreement is toward minimising the likelihood of pollution

[113] Barcelona Convention, Article 2 – Definitions, Para (a).
[114] Ibid. Article 3 – General Provisions, Para 1.
[115] Ibid. Article 6 – Pollution from Ships.
[116] Ibid. Article 8 – Pollution from Land-Based Sources.
[117] Ibid. Article 9 – Cooperation in dealing with pollution emergencies.
[118] The EU Member State signatories to the Barcelona Convention are: Cyprus, Croatia, France, Greece, Italy, Malta, Slovenia and Spain, together with the EU in its own right. The remaining Mediterranean countries which are signatories are: Albania, Algeria, Croatia, Bosnia & Herzegovina, Egypt, Israel, Lebanon, Libya, Morocco, Montenegro, Monaco, Syria, Tunisia and Turkey.
[119] The original signatory states of the Bonn Agreement were Belgium, Denmark, France, Germany, the Netherlands, Norway, Sweden and the United Kingdom. The European Commission became a Contracting Party in 1983 and Ireland in 2001.
[120] For full text of the Bonn Agreement 1983 (Agreement for cooperation in dealing with pollution of the North Sea by oil and other harmful substances, 1983) together with its 2001 amendment to include Ireland (and also for specific details of geographical coverage).
http://www.bonnagreement.org/site/assets/files/3831/chapter29_text_of_the_bonn_agreement.pdf (last accessed 3/7/17).

occurring at sea and, where pollution does occur, in both identifying its source, and providing the means to clean up that pollution.

The Bonn Agreement requires its contracting parties to, for example, develop and carry out coordinated surveillance activities,[121] enforce "anti-pollution regulations,"[122] and offer mutual assistance in dealing with pollution.[123] Surveillance activities using aircraft, and more recently satellite imagery (including images available via the EMSA *CleanSeaNet*[124] service), have taken place for more than 25 years, to identify oil pollution from ships (and also oil drilling rigs), and more recently to identify the specific vessel from which such pollution has come. The surveillance activities of the Bonn Agreement are discussed in more detail below.

The Bonn Agreement

Despite a raft of international and regional measures including those discussed above, many types of waste including oil, garbage and plastics continue to be discharged into the sea globally. For example, despite SA status under MARPOL 73/78 being adopted for North-West European waters (including the North Sea) in September 1997 and in effect since August 1999, there continues to be a problem with ships (and oil rigs) discharging oil into the North Sea. In order to illustrate the situation in the North Sea, data from Bonn Agreement annual reports[125] has been used to produce the figures in this section.

Figure 1 illustrates that there has been an improvement in the region over the period 1986 to 2010. It looks at the number of hours of aerial surveillance conducted by all Bonn Agreement countries annually, the total number of slicks identified each year, and provides a ratio of slicks to flight hours.

---

[121] Bonn Agreement, Article 2.
[122] Ibid. Article 4(a).
[123] Ibid. Article 4(b).
[124] EMSA; Satellite Oil Spill Monitoring (CleanSeaNet).
[125] Bonn Agreement (Various years). *Bonn Agreement Aerial Surveillance Annual Reports* are available from the Bonn Agreement Secretariat. See also http://www.bonnagreement.org/en/html/surveillance;surveillance.html. (last accessed 26/2/14). Reports prior to 1988 are in paper format only.

Figure 1 – Flight hours, observed slicks and ratio of slicks to flight hours1986-2010.[126]

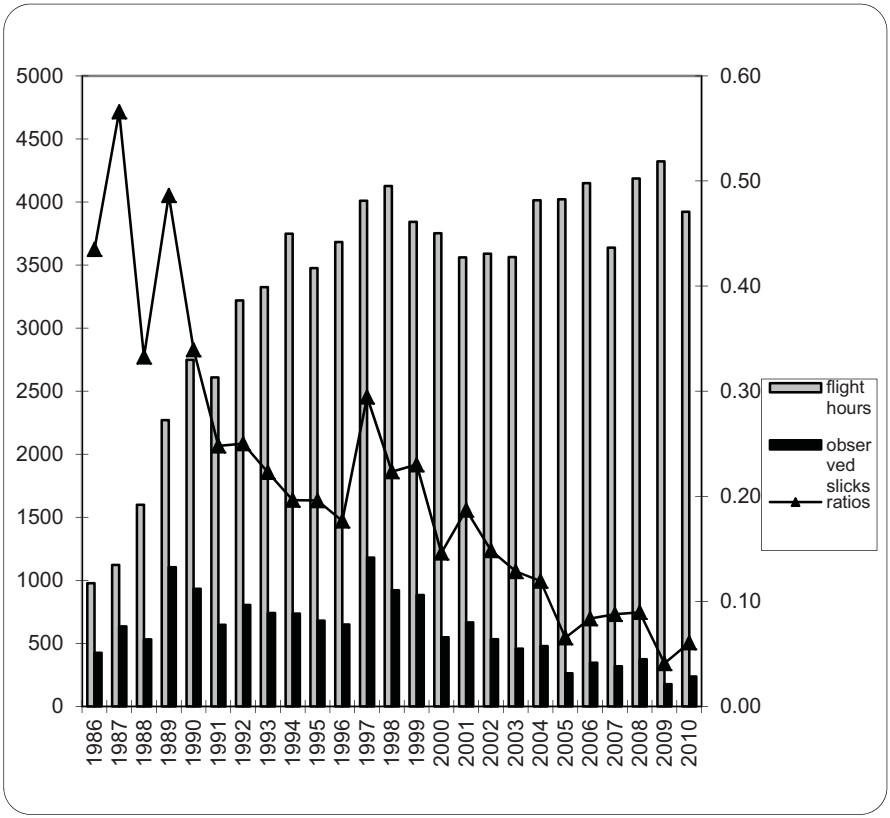


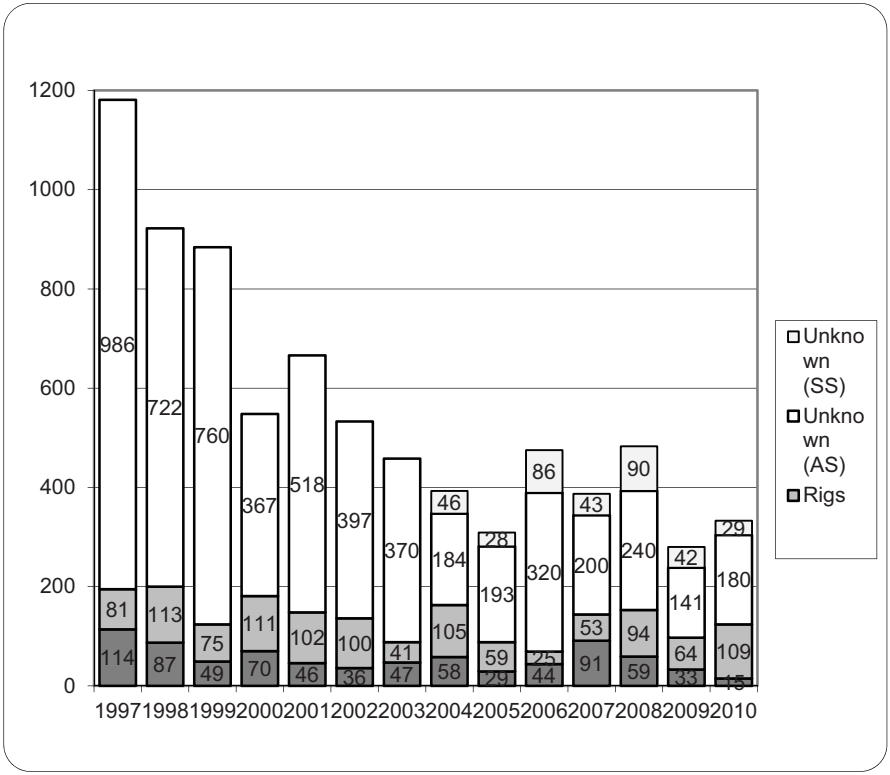
Figure 1 illustrates that there has been a decrease in the number slicks identified per flight hour. This can be viewed as an improving situation over time, particularly in light of increasing surveillance activities in recent years, and the introduction of satellite surveillance data since 2004.

[126] Figure 1 has been updated from Carpenter, A.; "The Bonn Agreement Aerial Surveillance programme: Trends in North Sea oil pollution 1986-2004," *Marine Pollution Bulletin*, 54(1) (2007), 149-163, Fig. 6. Bonn Agreement data 1986-2004 for all countries, 155. That figure has been extended to cover the period to 2010.

In the case of Bonn Agreement surveillance activities covering the North Sea, recent developments in the use of satellite imagery means that the likelihood of oil slicks being identified at sea has generally increased, but also that slicks can be identified during the hours of darkness. However, satellite surveillance data has only been available since 2004, so the data from 2004 onward can be considered to more accurately reflect the situation than the data up to 2003. Figure 2 identifies the number of slicks which can be attributed either to ships or oil rigs, together with those from unknown sources. From 2004 onwards that category is further broken down into slicks from unknown sources that have been identified as a result of aerial surveillance (AS) or from satellite imagery (SS).

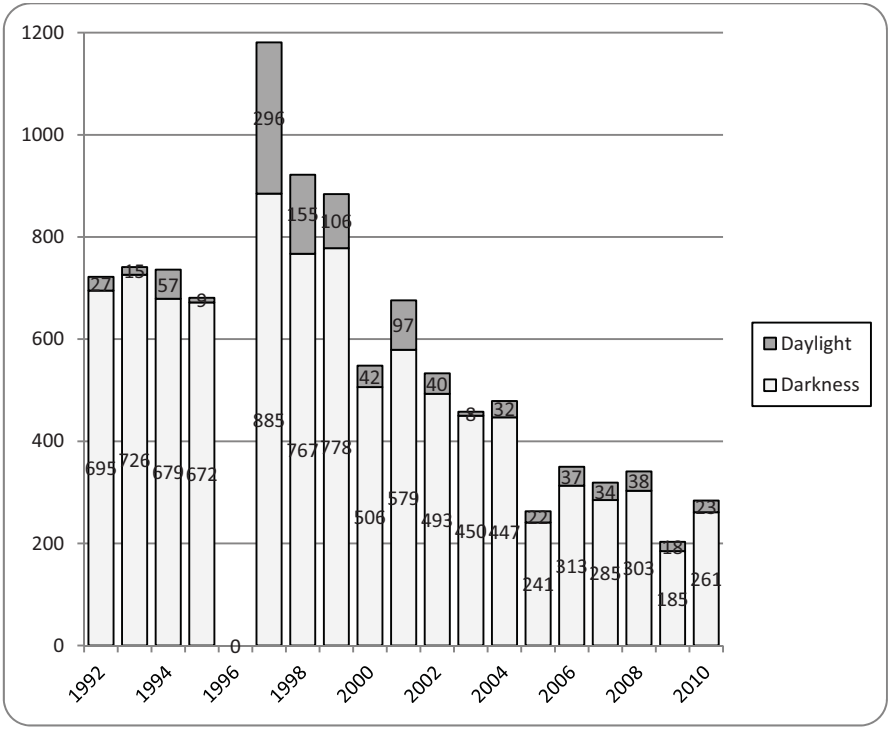
Figure 3 illustrates the number of slicks identified during the hours of daylight and in darkness for the period 1992 to 2010. It includes data from all flights conducted by Bonn Agreement states annually. It should be noted that the accuracy of the available data has improved over the last decade. From 2003 onwards the figures used for the number of oil spills detected are those where the detected spills have been confirmed as being mineral oil (prior to 2003 the figures are unconfirmed slicks which may include other types of oil). As a result, the use of confirmed slick data means that the data post-2003 can be considered to provide a more accurate picture of oil pollution trends in the North Sea region. In conjunction with the availability of satellite surveillance data from 2004, this provides an increasingly accurate picture of trends in oil pollution in the region over recent years.

Figure 2 – Number of observed oil spills by source 1997-2010.[127]



[127] Figure 2 has been updated from Carpenter; "The Bonn Agreement Aerial Surveillance programme", Fig. 1. Proportion of identified and unidentified polluters 1997-2004, 152. That figure has been extended to cover the period to 2010.

Figure 3 – Number of observed spills in daylight and darkness 1992 to 2010.[128]



Conclusions

Based on Bonn Agreement data, Figure 3 identifies that the total number of observed oil spills in the North Sea region has declined since a peak in 1997. In conjunction with Figures 1 and 2, this identifies that the ratio of slicks to flight hours has declined over a 25 year period (with the exception of a spike in 1997) and that an increasing proportion of oil slicks can be attributed to a specific source, which suggests that the overall

[128] Figure 3 has been updated from Carpenter; *The Bonn Agreement Aerial Surveillance programme*, Fig. 3. Breakdown of observed spills for all North Sea States 1992-2004, 153. That figure has been extended to cover the period to 2010. No data was available in 1996.

situation relating to oil pollution in that region has improved significantly over a quarter of a century.

However, the figures also illustrate that slicks continue to occur, despite legal measures such as MARPOL 73/78 and the establishment of SAs, the requirement for adequate provision of PRFs under the EU PRF Directive, and the increased possibility that vessels can be identified as being the source of oil pollution under EMSAs *CleanSeaNet* operational task and Bonn Agreement surveillance activities.

This chapter in particular highlights the range of activities taking place to prevent intentional oil pollution in the North Sea region, and more widely across EU maritime seas. It identifies that a number of measures are in place in relation to the North Sea but, despite that protection, ships continue to illegally discharge pollution in the region. Since many maritime areas are far less protected than the North Sea, it can be concluded that intentional pollution from ships will continue to be a problem. It is therefore vital that the work of the IMO globally, the EU and EMSA regionally, and the various regional conventions for specific seas, continues to try and minimise the problem. It will be interesting to see how the anticipated involvement of Europol pursuant to the Europol regulation, in this area will develop, and how Europol and Eurojust will interact with the EMSA and national law enforcement agencies when dealing with the issue of ship source pollution.

Bibliography

Agreement for co-operation in dealing with pollution of the North Sea by Oil, Bonn, 1969. UKTS 77 (1975), Cmnd. 6056; 9 ILM 25 (1969).

Bonn Agreement, *Bonn Agreement Aerial Surveillance Programme – Annual report on aerial surveillance for XXXX*. Bonn Agreement, London, (various years).

Carpenter, A. The EU and Marine Environmental Policy: A Leader in Protecting the Marine Environment," *Journal of Contemporary European Research*, 8(2) (2012): 248-267.

—. "International Protection of the Marine Environment." In *The Marine Environment: Ecology, Management and Conservation.* Ed. A.D. Nemeth. New York: Nova Science Publishers Inc., 2011.

—. "The Bonn Agreement Aerial Surveillance programme: Trends in North Sea oil pollution 1986-2004," *Marine Pollution Bulletin*, 54(1) (2007): 149-163.

—. "The EU Directive on Port Reception Facilities: A Case Study in the Development of an EU Environmental Directive," *European Environmental Law Review*, 15(12) (2006): 369-380.

Carpenter, A and Macgill, S M. "Charging for Port Reception Facilities in North Sea Ports: Putting Theory into Practice," *Marine Pollution Bulletin*, 42(2) (2001): 257-266.

Commission of the European Communities, 1997. *Draft Directive on Shore Reception Facilities for Ship Generated Waste, Version 3 of December 1997* (no document reference – paper version of this document is held by the author).

Convention for the Protection of the Maritime Environment in the North East Atlantic (OSPAR), 1992, 2354 UNTS 67; 32 ILM 1069 (1993).

Convention for the Prevention of Marine Pollution from Land-Based Sources (Paris Convention) 1974, 1546 UNTS 119; 13 ILM 352 (1974); UKTS 1978, No. 64.

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L138/14.

—. 98/249/EC of 7 October 1997 on the conclusion of the Convention for the protection of the marine environment of the north-east Atlantic, OJ 1998 L104/1.

—. 77/585/EEC of 25 July 1977 concluding the Convention for the protection of the Mediterranean Sea against pollution and the Protocol for the prevention of the pollution of the Mediterranean Sea by dumping from ships and aircraft, OJ 1977 L240/1.

Directive 2007/71/EC of 13 December 2007 amending Annex II of Directive 2000/59/EC of the European Parliament and the Council on port reception facilities for ship-generated waste and cargo residues (Text with EEA relevance), OJ 2007 L329/33.

—. 2002/84/EC of the European Parliament and of the Council of 5 November 2002 amending the Directives on maritime safety and the prevention of pollution from ships (Text with EEA relevance), OJ 2002 L324/53.

—. 2000/59/EC of the European Parliament and Council of 27 November 2000 on port reception facilities for ship-generated wastes and cargo residues, OJ 2000 L332/81.

European Commission. *Communication from the Commission – A Common Policy on Safe Seas*, COM(1993) 66 final.

—. *Task Specifications to award a Specific Contract under DG MOVE's Framework Contract TREN/A1/143-2007 regarding Impact Assessment*

and Evaluations etc. Review of the Port Reception Facilities for ship-generated waste and cargo residues Directive under Lot 2 (Transport). Doc. Ref: Ares(2010)849538 – 23/11/2010.

European Maritime and Safety Agency. *EMSA Study on the Delivery of Ship-generated Waste and Cargo Residues to Port Reception Facilities in EU Ports.* (2012). *Reference No. EMSA/OP/06/2011*. http://www.emsa.europa.eu/.

—. *CleanSeaNet First Generation Report: 16 April 2007 – 31 January 2011.* (2011). http://www.emsa.europa.eu/.

—. website: http://www.emsa.europa.eu/.

European Parliament, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA. COM(2013) 173 final.

International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (1992 Fund Convention), 973 UNTS 3.

—. on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, 1996, 35 ILM 1415 (1996).

—. for the Prevention of Pollution from Ships 1973, (MARPOL) Misc.26(1974), Cmnd 5748; 12 ILM 1319 (1973), and its 1978 Protocol.

—. on Civil Liability for Oil Pollution Damage 1969, 973 UNTS 3; 9 ILM4, 5, and its Protocol of 1992 to amend the International Convention on Civil Liability for Oil Pollution Damage, 1969, B7 969: 88/C; 973 UNTS 3.

International Maritime Organization (2009). *MEPC.1/Circ.671 of 20 July 2009. Guide to Good Practice for Port Reception Facility Providers and Users.* London: IMO. http://www.imo.org/.

—. *Marine Environment Protection Committee (MEPC), 54th Session: 20 to 24 March 2006. Port Reception Facilities Database.* London: IMO, 2006. http://www.imo.org/.

—. *MARPOL 73/78 Consolidated Edition 2002*. London: IMO, 2002.

—. *MEPC 43rd Session - Agenda Item 7. Inadequacy of Port Waste Reception Facilities Report*. Reference MEPC 43/7 of 31.03.99. London: IMO, 1999.

IMO website, http://www.imo.org/.

Mikelis, N. *IMO's Action Plan on tackling the inadequacy of port reception facilities.* Presentation at the Ships' Waste: Time for action!, Brussels, October 14 2010. http://www.imo.org/ .

Nanda, V.P. "The Torrey Canyon Disaster: Some Legal Aspects." *Denver Law Journal*, 44 (1967): 400-425.

Oslo Convention on the Prevention of Marine Pollution by Dumping from Ships and Aircraft, UKTS 119 (1975), Cmns. 6228; 11 ILM 262 (1972).

Pritchard, S.Z. *Oil Pollution Control.* UK: Croom Helm Ltd., 1987.

Proposal for a Council Directive on port reception facilities for ship-generated waste and cargo residues, COM(1998) 452 final.

Regulation (EC) No 1137/2008 of the European Parliament and of the Council of 22 October 2008 adapting a number of instruments subject to the procedure laid down in Article 251 of the Treaty to Council Decision 1999/468/EC, with regard to the regulatory procedure with scrutiny - Adaptation to the regulatory procedure with scrutiny - Part One, OJ 2008 L311/1.

—. 1406/2002 of the European Parliament and of the Council of 27 June 2002 establishing a European Maritime Safety Agency, OJ 2002 L208/1.

Paris Memorandum of Understanding on Port State Control in Implementing Agreements on Maritime Safety and Protection of the Maritime Environment, 221 ILM 1 (1982).

Supplementary Fund Protocol establishing the International Oil Pollution Compensation Fund 2003 (the Supplementary IOPC Fund) Int'l Mar. Org., LEG/CONF.14/20.

United Nations Conference on Trade and Development. *Liability and Compensation for Ship-Source Oil Pollution: An Overview of the International Legal Framework for Oil Pollution Damage from Tankers.* Studies in Transport Law and Policy – 2012 No. 1. New York and Geneva: United Nations, 2012. http://unctad.org/.

CONTRIBUTORS

Dr. Raphael Bossong, research associate at the German Institute for International and Security Affairs. His research interests span across the breath of transnational non-military security cooperation, with a special emphasis on the governance of counterterrorism, borders security and disaster management. His recent book publications include *Theorising EU Internal Security Cooperation* (with Mark Rhinard; 2016, Oxford University Press), *EU Borders and Shifting Internal Security* (with Helena Carrapico; 2016, Springer International) and *European Civil Security Governance* (with Hendrik Hegemann; 2015, Palgrave Macmillan).

Dr. Cristina Blasi Casagran, Public Law Department, Law Faculty, Autonomous University of Barcelona. She specialises in privacy and data protection law. Cristina has several publications on these matters, amongst which the book "Global Data Protection Law in the Field of Law Enforcement: An EU perspective" (Routledge, 2016) should be highlighted.

Dr. Angela Carpenter, Visiting Researcher, School of Earth and Environment, University of Leeds, UK. Angela is a geographer who specialises in security issues surrounding maritime ports and installations. Angela is also involved in non-security related port and maritime research, and is widely published in the areas of marine pollution and marine policy She has also edited a volume on *Oil Pollution in the North Sea* for the Springer-Verlag *Handbook of Environmental Chemistry* series and is co-editing a further volume on *Oil Pollution in the Mediterranean Sea.*

Dr. Robert S. Dewar, Cyber Defense Team, Centre for Security Studies, ETH Zurich, Switzerland. Roberts research interests cover cyber security and defence policy, security studies, the European Union and historical institutionalism. He has a number of publications in the area of cyber defence and security.

Dr. Mo Egan, Division of Law and Philosophy, University of Stirling, UK. Mo is a Scots lawyer researching in the field of justice and home affairs, focusing on financial crime, inter-agency cooperation and policing, in particular the interplay between state and non-state agencies in the delivery of criminal justice. She has a number of publications in this area, and in 2015 was appointed academic expert to the Law Society of Scotland Anti-money Laundering Panel.

Fiona Grant, Law Division, Abertay University, Dundee, UK. Fiona is a Scots lawyer whose teaching and research interests include information law and security and criminal law. She is a member of the University Association for Contemporary European studies collaborative research network on "Policing and European Studies". Her publications include *Legal Research Skills for Scots Lawyers*, with W Green.

Ken Swinton, Law Division, Abertay University, Dundee, UK. Ken is a Scottish qualified solicitor, legal academic and editor of a number of Scottish based law publications, to include the Scottish Law Gazette. He specialises in Financial Services law, and has co-edited an earlier volume with Cambridge Scholars edited *New Challenges for the EU Internal Security Strategy*.

Dr. Maria O'Neill, Law Division, Abertay University, Dundee, UK. Maria is an EU lawyer, who specialises in the EU's provisions on Police and Judicial Cooperation in Criminal Matters. She is the coordinator of the University Association for Contemporary European Studies collaborative research network on "Policing and European Studies". She has a number of publications in this area, to include a monograph on *The Evolving EU Counter-Terrorism Legal Framework*, with Routledge, and has co-edited an earlier volume with Cambridge Scholars edited *New Challenges for the EU Internal Security Strategy*.

Dr. Dimitris Skleparis, School of Social and Political Sciences, University of Glasgow, UK. Dimitris is an International Relations scholar who specialises in migration, refugee, and critical security studies. He has published in a range of international peer-reviewed journals, and has contributed to various edited books, research project reports, and research and policy briefs. He is currently a member of Yasar University UNESCO Chair on International Migration (2016-2020), and the Impact & Policy Officer of the Greek Politics Specialist Group (GPRG).