JCMS JOURNAL OF COMMON MARKET STUDIES
UACES
JCMS 2022 Volume 60. Number 5. pp. 1335–1355 DOI: 10.1111/jcms.13158

Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy

ANA PAULA BRANDÃO[1,2] and ISABEL CAMISÃO[2]
[1]University of Minho, Braga [2]University of Coimbra, Portugal and CICP - Research Centre in Political Science, Coimbra

Abstract

As EU security is an intergovernmental policy area, it has been assumed that the only relevant policy-shapers are member states. However, more recent analyses show that supranational actors, like the Commission, have developed strategies to enhance their role in this traditionally interstate realm. This article endorses this reasoning and intends to cast some light on these strategies. Building on Kingdon's concept of the policy entrepreneur and using EU's cybersecurity policy as an empirical case, we analyse the Commission's initiatives to draft a European response to cybercrime, in order to answer one central research question: how has the Commission managed to secure a prominent role in a highly salient security issue? The findings suggest that the Commission, acting as a policy entrepreneur, purposefully explored a market–security nexus in order to influence an otherwise intergovernmental security domain. Ultimately, the Commission was a much more relevant player than expected.

Keywords: European Commission; cybersecurity; cybercrime; policy entrepreneur; security policy

Introduction

Member states have been very reluctant to delegate power to EU supranational institutions in security matters. However, acting as a policy entrepreneur (Kingdon, 2003), the European Commission (henceforth Commission) adopted a comprehensive approach that captured the multidimensional nature of the new security challenges, such as cybercrime, firmly carving a way into the sensitive realm of security.

The literature on EU security has reflected this evolution. Initially framed by a fragmented external/internal matrix (based on a division of pillars that no longer exists), EU security studies have gradually moved towards a broad approach on security governance and actorness that acknowledges the salience of other actors (besides the USA) in advancing the EU security agenda (Brandão, 2016; Kostadinova, 2013; Riddervold, 2016; Smith, 2004). This article adopts this broad approach and aims to add empirical evidence to the existing scholarship on EU security governance by highlighting the Commission's entrepreneurship in the design of the EU cybersecurity policy. Theoretically, we draw on John Kingdon's 'policy entrepreneur' concept (1984, 2003) and on other literature that highlights the importance of institutional entrepreneurship as a driver of policy change (Crespy and Menz, 2015; Mintrom and Norman, 2009; Zahariadis, 2007), particularly in the EU context (Copeland and James, 2014; Rhinard, 2010). Using the EU's cybersecurity policy as the empirical case, we trace the Commission's initiatives to respond to cyberthreats and to cybercrime in particular, to answer one chief research question: how has the Commission managed to secure a prominent role in a highly salient security issue?

The article is organized as follows. Section 2 develops the theoretical framework, justifies the relevance of the empirical case and explains the methods used. Section 3 highlights the strategies of the Commission to enhance its role in a member state-dominated area and shows how its entrepreneurship has contributed to advance the cybersecurity agenda. Section 4 adds to the qualitative reading of data in section 3 by showcasing through content analysis the market–security nexus in relevant Commission's documents. Section 5 summarizes the main findings and highlights avenues for future research.

I. Theoretical Framework and Methodology

Framework

The concept of policy entrepreneur was first used by Kingdon (2003) to describe actors that are:

'willing to invest their resources – time, energy, reputation, and sometimes money – in the hope of a future return [which] might come to them in the form of policies of which they approve, satisfaction from participation, or even personal aggrandizement in the form of job security or career promotion' (Kingdon, 2003, pp. 122–123).

Kingdon's goal was to understand the three major process streams by which agendas were set and alternatives specified: problem recognition, policy formation (and refinement) and politics. Even though these streams evolve and operate largely independently of one another, it is their coupling that explains agenda and policy change. Policy entrepreneurs play a central role in coupling the streams, as they grab the policy windows to hook solutions to problems, proposals to political momentum and political events to policy problems (Copeland and James, 2014, p. 3; Kingdon, 2003, p. 182; Zahariadis, 2007, p. 5).

Policy entrepreneurs' incentives to prompt advocacy vary: they may be interested in the promotion of personal interests; they may simply like the game (being 'policy groupies'); or they may want to promote their own values, or affect the shape of the policy (Kingdon, 2003, p. 123). All these incentives could be relevant to explaining the entrepreneurship of the Commission (Rhinard, 2010, p. 41). The literature has shown that the Commission is a 'purposeful opportunist' (Cram, 1994) that actively seeks not only to preserve but also to expand its competences. Second, policy-making in the EU is a continuous negotiation game, in which the Commission's officials are actively engaged, using their privileged knowledge, expertise and information to their advantage. Third, under article 17 of the TEU, the Commission is in charge of promoting 'the general interest of the Union' and taking 'appropriate initiatives to that end'. This gives the Commission a 'special perspective and legitimacy', as it is the only EU institution that can claim to speak from a truly European point of view (Lindberg and Scheingold, 1970, p. 129) and this enables it to be activist; namely, through the continuous flow of proposals, communications, memoranda, studies, reports and other documents.

According to Kingdon (2003, p. 115), fixing attention on one problem rather than another is a central task of policy entrepreneurs. One of the Commission's key-tasks is agenda-setting (formal and informal), meaning that the institution has the ability to influence the attention that is given to a certain issue. In doing so, the Commission has also the

opportunity to frame the problem in a way that leads other stakeholders to see the institution's pet policy innovation as the ideal solution. Thus, the Commission engages in a process of 'strategic framing' directed to help building 'support coalitions, manipulate new and existing institutions, and link policy options to broader societal values' (Rhinard, 2010, p. 37). By inducing a sense that change is required, it paves the way to action (Crespy and Menz, 2015, p. 758; Mintrom and Norman, 2009, p. 651). Once an issue enters the agenda as a problem demanding a solution, policy entrepreneurs are expected to prompt the discussion of their proposals to solve the problem in different forums. The goal is to soften up the relevant stakeholders; that is, to get them used to the new ideas and to build acceptance for the new policy proposals (Kingdon, 2003, pp. 127–128). Success in placing its pet issues on the agenda and its ability to sustain support for these issues over time gives the Commission influence over policy outputs even if it does not hold the formal power to take decisions (Princen and Rhinard, 2006, p. 1119).

Methodology

Building on the above theoretical framework, we will explore the role and strategies of the Commission in designing and shaping the EU cybersecurity policy. The choice of the empirical case is justified by three interrelated reasons: First, in the 21st century, borderless threats such as cybercrime emerged as salient problems (Christou, 2016). This is understandable as we are dealing with criminal activities of potentially mass-scale and great geographical distance that represent a real menace to 'critical infrastructures, society, business and citizens' (European Commission, 2007). The EU, with its internet-mediated economy – particularly with the digital single market presented as the obvious stage in the road for the completion of the single market (SM)[1] – obviously became a chief target. However, member states initially underestimated the seriousness of the threat and the EU's initial response was more a piecemeal approach than a cohesive strategy.

Second, it is fair to assume that it is in the 'general interest of the Union' to take the appropriate initiatives to protect member states (and European citizens in general) from the new threats that became the flipside of a globalized and interconnected world. The fight against cybercrime thus is subsumed under a crucial security task:[2] protection. But in this case, as the Commission noted, it was protection of the EU's 'citizens, businesses and governments and their infrastructure from cyber-attacks' (European Commission, 2013, p. 2), therefore cutting across several EU policy areas.

Third, and directly related to the former, the inter-pillar and cross-pillar dimension of this new security challenge opened the ideal window of opportunity for the Commission to use its knowledge and expertise in the SM domain and its partnerships (particularly with the private sector) to its own advantage. If and how the Commission managed to seize the opportunity is, in our opinion, a relevant issue to study, as the findings could ultimately be a valid contribution to understanding how an actor, whose role in the security domain was initially negligible, has managed to get involved in a variety of security dimensions, even if the final decision remains an intergovernmental one.

[1]In this article the expressions 'internal market' and 'single market' are used interchangeably.
[2]The EU, as a security provider, performs four security tasks: prevention; assurance; compulsion; protection (Kirchner and Sperling, 2007).

Table 1: Classification of Concepts

Market	*Security*
Market	Cybercrime
Digital single market	Cyber resilience
Digital society	Crime
Online economy/digital economy	Cybercrime
Industry	Threat
Services	Risks
Products	Fraud
Businesses	Security
Growth	Safety
Jobs	Security network
Competitiveness	Malicious cyber activities
Economic profits/losses/costs	Cybersecurity incidents
Private sector	Cyber defence and cyber deterrence
Industry led	Public-private partnership/industrial capabilities

Source: Authors

Considering the abovementioned reasons, we start by identifying (section 3) the Commission's main actions to frame the cybercrime problem and its preferred solution: that of a comprehensive EU cybersecurity strategy. Our underlying assumption is that the Commission, acting as a policy entrepreneur, forged and took advantage of a *market–security nexus*, which allowed the institution to enter 'artfully' the security domain through its natural realm, the SM. In order to trace the Commission's actions, we have analysed EU cybersecurity (or related) official documents, namely proposals, communications on policy, strategies, studies, reports and speeches from the Commission and from other relevant stakeholders that interact with this institution in the EU policy cycle, particularly the European Council, the Council of the EU and the European Parliament. The analysis focuses on the period between 2000, when the draft of the action plan was launched, and 2016, when the network and information security (NIS) directive was adopted. However, earlier documents from the 1990s will also be introduced, either to give context or to illustrate how the Commission has from the start interlinked market and security issues.

We will then (section 4) examine the existence of a link between market and cybersecurity elements in the Commission's discourse through a direct content analysis of its communications. Using relevance sampling, the study includes policy and legislation documents authored by the Commission between 2000 and 2016.[3] The sample comprises 38 policy documents and six legislative documents, totalling 44 documents. Accordingly, there are documents that address digital aspects (security, economic and social) and others that are not digital specific but that have digital-related topics. The analysis is based on the content of the sample.

For the analysis we made use of Leximancer.[4] The text was scanned in two sentence text blocks to identify the main concepts in a sample (Leximancer, 2017). To assess the existence of a link between market and cybersecurity elements we devised a search

[3]See annex 1.
[4]Leximancer is a web-based platform that through statistical-based algorithms automatically analyses textual content.

parameter containing a taxonomy of both fields. The definition of the concepts to include in the search parameters was based on a predefined classification of market and cybersecurity elements (see Table 1):

II. Purposefully Exploring the Market–Security Nexus[5]

Unlike counter-terrorism, the evolving place of cybersecurity in the EU agenda (from its absence to its prioritization) was not dependent on single major attacks. Whereas terrorist attacks are exceptional, politically motivated, deadly, (publicly) visible and attracting high levels of media coverage, cyberattacks and crimes are daily occurrences, and in most cases they are not deadly and are not known by the public or reported by the media. Hence, to transform cybercrime from an issue to a problem was not easy to do. In this section, we show that the Commission's entrepreneurship has been decisive for cybercrime (and the solution, cybersecurity) agenda-setting and for the resultant adoption of the EU cybersecurity strategy.

Cybercrime: From A Neglected Issue to A Key Problem

An issue is considered a problem when it becomes evident that something has to be done about it. When the problem becomes pressing it creates an opportunity for advocates of a proposal to attach their solutions to it (Kingdon, 2003, p. 168). In fact, it is the degree to which the issue is considered a problem that explains the 'issue-attention' and that ultimately drives action (Camisão and Guimarães, 2017; Mintrom and Norman, 2009, p. 652).

The Commission's entrepreneurship in the domain of cybersecurity in general and cybercrime in particular was favoured by a combination of interrelated international and internal events. The end of the Cold War and the subsequent change in the security environment forced reluctant European leaders to add an international and internal security dimension to the new EU (the second and third pillars, respectively, were introduced by the Treaty of Maastricht). As a result, the idea of the EU as global security actor started to emerge. For its part, the growing use of the internet, that is evidence of the transition to the 'digital' society, favoured the securitization of cyber activities. In the late 1990s several international organizations undertook initiatives to fight cybercrime, pushing the cyber problem into the international agenda.[6] However, in the EU the issue remained very much in the hands of member state, a striking fact, particularly considering that, in the late 1980s and early 1990s, the completion of the SM and the construction of an economic and monetary union was at full steam. Early Commission's initiatives to fight cybercrime and forge a cybersecurity strategy (mainly studies and reports) reflected the emphasis on the market and were driven by two rationales: the regulation of the internet (against harmful use) and its economic benefits (to the internal market and information society

[5]Some of the data presented in this section was previously analysed, using a different theoretical framework, by Brandão (2016).

[6]The first international initiatives date from the 1990s and were associated with the G8 subgroup on hi-tech crime (1997), which, in cooperation with INTERPOL, created the 24/7 'network of contacts' (1997). Other international organizations and forums, such as the UN, which endorsed the world summit on the information society, ITU (International Communication Union), OECD (Organisation for Economic Co-operation and Development), NATO, the Council of Europe and the P8 Experts Group on Transnational Organized Crime (the Lyon group), also contributed to include the topic of cybersecurity and cybercrime in the international agenda.

technologies). The connection to SM-related matters greatly favoured the role of the Commission. Being the institution's realm par excellence, the single market potentiates several Commission resources, such as knowledge, expertise (content and process) and information (namely on other actors' preferences). It is also fertile ground for intra and extra EU coalitions, with the Commission often capitalizing on its support of transnational business interests. It is therefore expected that the Commission will take the lead and present proposals for deepening or reforming the SM. By calling attention to the market's cyber vulnerability that was precisely what the Commission did. Its purposeful activism in the area of cybersecurity can be traced back at least to its 1990 communication on personal data and information security,[7] where it proposed a system of protection at the Community level that was essential for the completion of the SM. However, its attempt to gain significant responsibilities in this domain was greatly reduced by the 1992 Council decision in the field of the security of information systems[8] to maintain network and information security policymaking under the control of the member states (Arnbak, 2014, p. 4). This initial setback did not stop the Commission, as the institution inscribed the goal to create an 'appropriate regulatory framework' and to 'protect privacy and ensure the security of information and communication systems' in its 1993 White Paper on growth, competitiveness and employment (European Commission, 1993, p. 24). Less than 3 years later, in 1996, the Commission approved a European Commission (1996a) and a European Commission (1996b). In the following year the Commission released an action plan for the safe use of the internet (which was adopted by the Council in 1999) and commissioned a study by the University of Würzburg on the legal issues of computer-related crimes. The latter is an example of the Commission's use of expertise (either coming from the Commission's services or resulting from its partnership with external experts) to its own advantage. The report concluded that 'computer crime has developed into a major threat of today's information society' (Sieber, 1998, p. 2) and that '[f]uture measures against computer crime must be *international* […] and 'should aim at *comprehensive* solutions' (Sieber, 1998, p. 4, emphasis in the original), coordinated by the Commission (Sieber, 1998, p. 239). The conclusions therefore fully backed the Commission's narrative. With these moves the Commission transformed the cyber issue into a common European problem, putting pressure on the need to find a solution, particularly considering the quantifiable perils that cybercrime represented for the digital economy.

But the Commission's arguments were not built exclusively on the measurable costs of cybercrime. In fact, the massive potential economic gains that would result from a cybercrime-free digital single market were also repeatedly stressed. In 1997 three commissioners – information technology and telecommunications, SM and the commissioner in charge of small businesses policy – issued a communication called 'European Initiative on Electronic Commerce' which emphasized the 'proven principles and benefits of the EU's Single Market to electronic commerce' (European Commission, 1997). In December 1999, 2 years later, the Commission launched the eEurope initiative prompted by two goals associated with the 'digitalised, competitive and mobile eEurope': to potentiate the benefits of information society technologies ('in work, education and leisure, in

[7]COM (90) 314 final, 13 September 1990. Information and network security was one of the three converging, but distinct, policy areas (the other two were electronic communications and cybercrime) that eventually were blended in together with the EU 2013 Cybersecurity Strategy (Fuster and Jasmontaite, 2020, p. 98).
[8]Council Decision 92/242/EEC, OJ L 123/19, 8 May 1992

government, industry and trade') and promote a socially inclusive information society (European Commission, 1999, 2000).

The idea that the new digital environment was opening up a window of opportunity that had to be grabbed then became part of the Commission's narrative: 'This is a crucial time and unique opportunity for the Union. […] Such chances are rare. They must be seized' (European Commission, 1999, p. 2). In most of the Commission's documents, the direct link between the success of the information society and Europe's growth, competitiveness and employment opportunities was recurrently (and purposefully) highlighted, particularly considering the far-reaching economic, social and legal implications of the information society (European Commission, 2000).

Thus, although building on a fairly technical dimension of the problem, the Commission managed to link its consequences to a core political aim enshrined in the treaties: Europe's growth and prosperity. This move served two purposes: it boosted the relevance of the issue and allowed the Commission to influence security matters through the emphasis on soft political and economic aspects. The course of action traced above shows that the Commission, acting as a policy entrepreneur, was actively engaged in a process of policy framing; namely, 'an interpretative construction of a policy problem that offers a rationale for change while also proscribing a course of action and a particular solution' (Rhinard, 2010, p. 37). According to Mark Rhinard (2010, p. 39), a policy frame should provide answers to three critical questions: 'What is at issue? What is to be done? What is the motive for action?' This was precisely what the Commission's framing did.

Indeed, the Commission's entrepreneurship appears to have contributed to the recognition of the problem by highlighting the many ramifications of the cybercrime issue at the security, economic and political. Bearing in mind its strategic goal of achieving a 'competitive, dynamic and knowledge-based economy', the Lisbon European Council in March 2000)invited the Council and the Commission to draw up an eEurope action plan. The action plan, adopted by the Feira European Council (June 2000), reaffirmed the need to improve cybersecurity and the fight against cybercrime.[9]

The Commission's entrepreneurship also contributed to the definition of the problem. Even though the EU has been active in the fight against cybercrime since 2000 (European Commission, 2000), initially there was no consistent *European* understanding of what the term 'cybercrime' should refer to, with implications for the interconnected notions of high-tech crime and cybersecurity (but also for cyber defence, cyber war, cyber warfare and cyber space). Cybersecurity ranged from being characterized as a matter of homeland security (Germany and the Netherlands), a defence problem (Latvia and Denmark) and a commerce and communications issue (Finland and Italy) (Ilves *et al*., 2016, p. 132). Additionally, the way that member states prioritized cyber threats also varied greatly. By 2013 only 13 member states had national cybersecurity strategies, which was indicative of the significant differences in terms of their 'preparedness, security, strategic culture and capacity to develop and implement national cyber-security strategies' (European Parliament, 2013).

The lack of a common perception and understanding of the new threat explains member states' initial undervaluation of this highly costly threat and the absence of a

[9]At international level the Commission contributed to the negotiation of the Council of Europe Budapest Convention on Cybercrime (2001).

coordinated EU strategy to deal with the problem. The Commission did not miss the opportunity to frame the issue. In January 2001[10] it released a communication aimed at creating a safer information society where it noted the absence of a unified definition of computer-related crime (European Commission, 2001a, 2001b, p. 12). In June the same year, the Commission adopted a communication on network and information security, which interlinked three policy areas: telecommunications and data protection, network and information security and cybercrime policies. Interestingly enough, security was presented as a commodity; that is, a product that could be bought and sold in the market (European Commission, 2001a, 2001b, p. 2; p. 18). Building on its previous communications, in 2007 the Commission issued a communication called 'Towards a general policy on the fight against cyber crime' where it recalled, amid other things, the importance of establishing a consensual definition of cybercrime and put forward its own definition[11]: 'criminal acts committed using electronic communications networks and information systems or against such networks and systems' (European Commission, 2007, p. 2). This document established that, in practice, cybercrime may be broken down into three categories of activities: traditional forms of crime (fraud or forgery, committed over electronic communication networks and information); the publication of illegal content over electronic media and crimes unique to electronic networks (such as attacks against information systems, denial of service and hacking) (European Commission, 2007, p. 2). As stated in a summary of legislation published in the EUR-lex page, with this Communication the Commission 'prepared the ground for a comprehensive policy to tackle [cybercrime]'.[12]

All in all, as the sequence of events presented above shows, the role of the Commission was instrumental in putting cybercrime on the European agenda and on highlighting the right solution – a comprehensive cybersecurity strategy – to the diagnosed problem. By taking advantage of the convergence between the international environment (and the EU emerging security actorness) and the internal EU agenda (internal market completion, information society and the European digital agenda[13]), the Commission created the right momentum to pave the way for new policy initiatives in this unexplored security domain. The motive for action was clear: to protect and take full advantage of one of the first (and one of the most relevant) European achievements, the SM.

Towards the Adoption of the EU Cybersecurity Strategy: The 'Softening up' Process

The role of policy entrepreneurs includes starting discussions of their proposals and push for their ideas in many different forums. They can publicize their goals, make speeches or hold hearings to create a climate that will allow them to introduce policy change (Kingdon, 2003, p. 130). Ever since the establishment of cybercrime as an EU problem,

[10]COM (2000) 890 final.
[11]However, the Commission acknowledged that harmonization of crime definitions and national penal laws in the field of cybercrime was a long-term objective, due to the complex nature of the phenomena.
[12]Summaries of EU legislation: Towards a General Policy on the fight against cybercrime: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560
[13]In May 2010, the Commission adopted 'A digital agenda for Europe' aiming to 'deliver sustainable economic and social benefits from a digital single market' (European Commission, 2010b, p. 3). The digital agenda was one of the seven flagship initiatives of the Europe 2020 strategy.

Table 2: Comprehensive Cybersecurity Approach

	Economy	*Internal Security*	*External Relations and CFSP/CSDP*
Goals	Growth, competitiveness and employment	Security of citizens and businesses, member states, infrastructures	International cooperation Cyber defence
Policy domains and issues	Internal market Liberalization of telecommunications markets Information society and digital Europe (Information Society Technologies dissemination, market liberalization, data protection, copyrights) Security industrial policy	Internal security (fight against organized crime, fraud, trafficking of human beings, child pornography, racism and xenophobia; counterterrorism and fight against radicalization) Criminal law Cybersecurity (securing network and information systems)	Third Countries: - USA (EU/US Working Group on Cyber-security and Cybercrime; - EU-US Initiative to Launch a Global Alliance against Child Sexual Abuse Online) International Organizations and international regimes: - Council of Europe (Convention on Cybercrime) - The International Criminal Police Organization (INTERPOL) - ITU (International Telecommunication Union) Global Cybersecurity Agenda - North Atlantic Treaty Organization (Technical Arrangement between the NATO Computer Incident Response Capability and the EU Computer Emergency Response Team (CERT-EU - International Multilateral Partnership against Cyber Threats (IMPACT) - London Action Plan - Virtual Global Task Force

Source: Authors Notes: CSDP, Common Security and Defence Policy.

the Commission has issued a regular stream of documents setting goals and assessing past achievements.

Between 2006 and 2012 it launched three studies (European Commission, 2007, 2011b, 2012a)[14] and issued four additional communications (European Commission, 2006, 2009, 2011a, 2012b)[15]on the subject. The first study, commissioned in 2006, identified the major trends of a 'changing environment', namely the growing number,

[14]A 2006 study to assess the impact of communication on cybercrime (Contract NoJLS/2006/A1/003); the 2011 'Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report'; the 2012 'Feasibility Study for a European Cybercrime Centre'; and the 2012 'Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft'.
[15]COM (2007) 267 final; COM (2009) 149 final; COM (2011) 163 final; COM (2012) 140 final.

sophistication and internationalization of cybercrimes; the involvement of organized crime groups in cybercrime and the stabilization of European prosecutions on the basis of cross-border law enforcement (European Commission, 2007). To address these challenges the Commission repeatedly stressed the urgent need to take action both at national and European level. In particular, it became clear that the cross-border dimension of cybercrime demanded a specific EU policy, perceived as a priority not only by the Commission but also by member states. With this goal in mind, the Commission established several guidelines: it improved operational law enforcement cooperation; it promoted better political cooperation and coordination between member states and political and legal cooperation with third countries; as well as awareness raising; training and research, and reinforced dialogue with industry and possible legislative action (European Commission, 2007).

The evolving threat environment, with a growing number of cyber incidents and crises affecting European countries, including the well-known incident in Estonia in 2007,[16] helped to validate the Commission's narrative. From the start, the Commission insisted on a comprehensive (see Table 2), multi-stakeholder, multilevel and multisectoral[17] approach to cybersecurity (Bendiek and Porter, 2013; Christou, 2018; Fuster and Jasmontaite, 2020) to fight cybercrime, which, in order to be effective would require proper coordination.

Strategically, the Commission took upon itself this coordinating role: the existing structures for cross-border operational cooperation were involved in the process (through meetings of law enforcement experts from member states, the EU Law Enforcement Agency - Europol, the EU Agency for Law Enforcement Training - CEPOL and the European Judicial Training Network - EJTN), a permanent EU contact point for information exchange was established and an EU cybercrime training platform was created (European Commission, 2007). The changes introduced by the Lisbon treaty (2009) gave a further push to the Commission's goal. Indeed, the legal personality of the EU, the abolition of the pillar structure and the transfer of cooperation on internal security to the Treaty on the Functioning of the European Union enabled intra and interinstitutional joint work (Directorate-General for Communications Networks, Content and Technology (DG CONNECT), Directorate-General for Justice and Home Affairs (DG HOME), European External Action Service) and the development of a single approach to cybersecurity (Dewar, 2017).

Gradually, other institutional stakeholders; namely the European Council and the Council, began to echo the Commission's narrative in their documents. The EU security strategies (European Council, 2008; European Commission, 2010a) included cyber threats among the key threats and challenges to European interests. In the 2011 internal security strategy report, both the fight against organized crime and the fight against cybercrime were identified as the two main challenges to be addressed in the following years (European Commission, 2011c).

[16]Other examples include major incidents in Georgia (2008), Stuxnet (2010),and other incidents such as the 2007 Storm Worm (that affected private computers in Europe and the USA), the external intrusion Center for Strategic and International Studies in British, French, German, Belgian government networks in 2007 and 2008 and the 50Hertz 2012. For a detailed list, see Center for Strategic and International Studies 'Significant Cyber Incidents since 2006' available at: Area not definedhttps://csis-website-prod.s3.amazonaws.com/s3fs-public/200727_Cyber_Attacks.pdf.

[17]'All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cybersecurity' (European Commission, 2013, p. 17).

The Commission also extended the softening up process to other stakeholders besides its EU institutional counterparts. As in other internal security domains, it advocated public–private cooperation (Christou, 2018); a strategy that normally adds leverage to the Commission's activism due to its past experience in dealing with the private sector,[18] which often acts as its ally. This partnership was particularly relevant in the cybersecurity domain, as cyberspace is largely owned and operated by the private sector; and non-governmental stakeholders tended to favour multi-stakeholder collaboration and co-operation as the best way to develop effective cybersecurity policies (Organisation for Economic Co-operation and Development [OECD], 2012, p. 9), meaning that they were likely to support the Commission's position. Accordingly, in February 2011 and March 2012 the first and second high-level public–private security roundtables were organized by the main European business association for security companies, the European Organisation for Security, in partnership with the Commission. Neelie Kroes's[19] speech on a European strategy for internet security (Kroes, 2012) was indicative of the Commission's market–security nexus and enticement of the private sector:

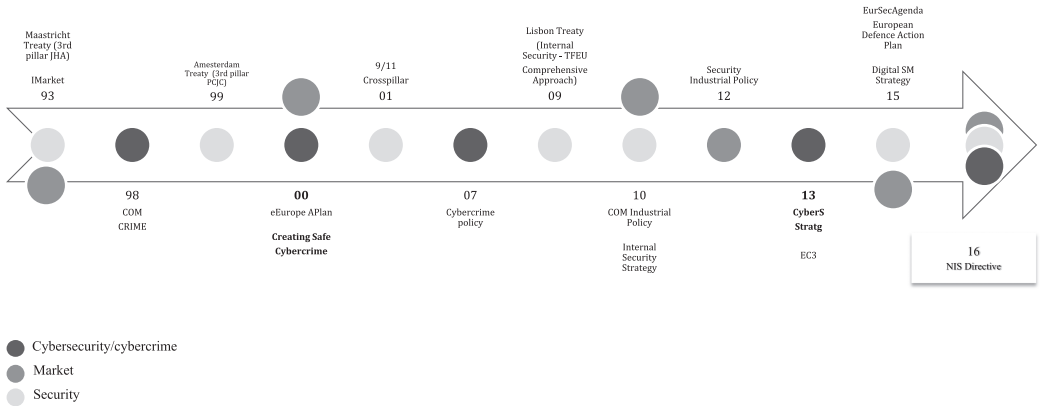
> Internet security is not a problem that's going to go away (…) [b]ut with an approach that is built on the Single Market, giving the right incentives to the private sector, investing in supply, and with an international outlook, then we can deliver not just a safer Internet for all, but also stimulate a vibrant and essential new EU industry.

The Result: The EU Cybersecurity Strategy and the Way Forward

In the beginning of 2013 the Commission and the High Representative issued a join communication on the EU's strategy for cybersecurity (European Commission and High Representative, 2013). This was the first EU's comprehensive policy document and it formally established cybersecurity 'as a new policy area' (Fuster and Jasmontaite, 2020, p. 98). Again, the link between security and market was made clear as it was noted that this 'will strongly support the good functioning of the internal market and boost the internal security of the EU' (European Commission and High Representative, 2013, p. 5). The EU cybersecurity strategy covered three main policies areas – SM, Justice and Home Affairs and foreign policy angles of cyberspace (including defence matters). It defined five strategic priority areas: achieving cyber resilience; drastically reducing cybercrime; developing a cyber defence policy and capabilities related to the common security and defence policy; developing the industrial and technological resources for cybersecurity; establishing a coherent international cyberspace policy for the EU and promoting core EU values. The first, achieving cyber resilience, called for new legislation. In fact, the strategy was accompanied by a legislative proposal from the Commission to strengthen the security of the EU's information systems: the NIS directive proposal.[20] Also in

[18]In fact, the importance of a public–private partnership in the cybersecurity domain had already been pointed out in the 2007 Communication: the Commission called for the definition of a 'strategy for cooperation between the public sector and private sector operators', including civil society organizations, the creation of the European security research and innovation forum and the organization of conferences for law enforcement experts and private sector representatives, especially internet service providers (European Commission, 2007).
[19]At the time, commissioner for the digital agenda.
[20]Truly, the NIS directive was not the Commission's first legislative proposal in the cybersecurity domain. See Regulation (EC) No 460/2004; Regulation (EU) No 580/2011; Directive (EU) No 40/2013.

FIGURE 1: The Market–Security Nexus Timeline (1993–2016).



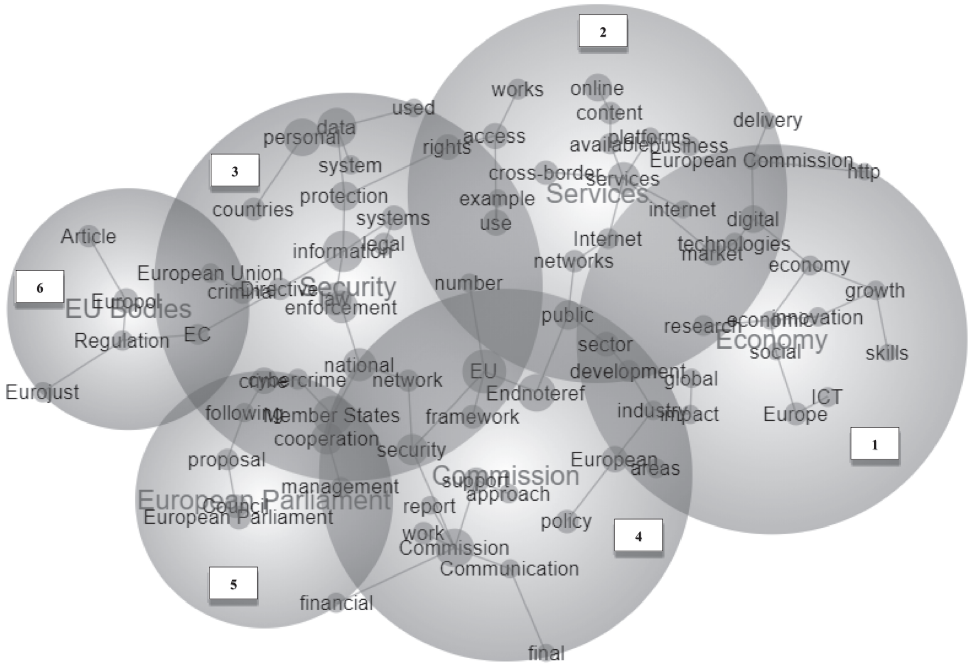
Source: Authors

2013, the European cybercrime centre proposed by the Commission in the previous year, was put in place.

The adoption of the EU cybersecurity strategy was not the end of the Commission's involvement in the EU response to cybercrime. The definition of cybersecurity[21] put forward in the joint communication was sufficiently (and, in our opinion, purposefully) 'elastic' (Fuster and Jasmontaite, 2020); to permit the Commission's continuing involvement in the issue. To prepare the new internal security strategy (European Council, 2010), the Commission consulted the main stakeholders, including the representatives of the private sector (the high-level conference on a renewed EU internal security strategy on 29 September 2014, as an embryonic form of an EU internal security consultative forum for the new EU Institute for Security Studies (EUISS)). On 6 May 2015 the Commission adopted a digital single market strategy, which included establishing a public–private partnership on cybersecurity in the area of technology and solutions for online network security in the course of 2016. Accordingly, in December 2015 the Commission launched a public consultation on the public–private partnership on cybersecurity and an EU internet forum with ministers and internet companies on the use of the internet for recruitment and radicalization. Also, the European Agenda on Security prioritized cybercrime alongside terrorism and organized crime 'as interlinked areas with a strong cross-border dimension' (European Commission, 2015, p. 13). In April 2016 the institution and the High Representative adopted a joint framework to counter hybrid threats such as cyberattacks, among others. Three months later, as envisaged in the digital single market strategy, a public–private partnership on cybersecurity was in place. Also, cybersecurity featured as one of the strategic priorities of the EU global strategy (European Council, 2016).

[21]'Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein' (European Commission and High Representative, 2013).

FIGURE 2: Concept Map generated by Leximancer from the Sample of the Commission's Communications (2000–16).



Source: Authors

Certainly, at present, there is no doubt that cybercrime is a major security threat to the EU and that fighting it should remain a key priority.[22] An overview of the main steps towards an EU cybersecurity policy shows the importance of the Commission's actions for this final outcome.

III. Showcasing the Market–Security Nexus: Documentary Evidence

This article builds on the core assumption that the Commission, acting as a policy entrepreneur, has purposefully explored the market–security nexus in order to obtain a relevant role in shaping a security policy area. Tracing the events that led to the adoption of the EU cybersecurity strategy and a qualitative reading of key documents issued between 2000 and 2016 appear to confirm our initial hypothesis (see Figure 1).

[22]Cybercrime has been an European Multidisciplinary Platform Against Criminal Threats (EMPACT) priority in 2011–13, 2014–17 and 2018–21 policy cycles. Several sources underline its expansion (scale, volume and speed) and sophistication (United Nations Office on Drugs and Crime, 2013; Center for Strategic and International Studies, 2018; Europol, 2019), which results in an estimated global annual loss between $445 and $600 billion (0,59% to 0,8% of global GDP) (Center for Strategic and International Studies, 2018, p. 7).

In this section, we use content analysis to double-check our first reading of the documents.

Conceptual Mapping

As explained in the methodological section of the article, for the content analysis we used Leximancer. In an automated analysis, Leximancer identifies the main concepts in a certain selection and aggregates them into themes. The analysis identified six main themes: the economy (1); services (2); security (3); Commission (4); European Parliament (5); EU bodies (6) (See Figure 2).

The results indicate that the Commission is greatly concerned with economic growth, which is linked with industry, the market and technological and skills development. The presence of the concept 'global' in the 'economy' theme suggests that the digital economy is perceived as a global reality. Intertwined with the 'economy' theme, the 'services' theme includes concepts such as services, cross-border, online, content, internet, networks, public, access, market and digital. This in turn shows the second concern of the Commission, which is the development of online cross-border services that are reliant on the internet and new technologies. Besides being connected to the 'economy', the 'services' theme is also connected with 'security'. This connection apparently indicates that services are necessary for the economy to thrive and that there are security threats to it. A closer look at the 'security' theme shows concepts such as information, crime, cybercrime, protection, systems, enforcement, legal and rights, among others. Thus, for the Commission security aspects and the protection of the cyber economy and digital services are linked to legal and law enforcements aspects.

The positioning of the 'European Parliament' theme implies that for the Commission[23] the institution is mainly relevant for regulatory and financial purposes. Lastly, the 'EU bodies' theme shows concepts such as Europol, Eurojust and regulation. Its graphic positioning suggests that, after the Commission, the main bodies to take part in the security of the cyber domain are Europol and Eurojust. At the intersection of the themes 'security', 'Commission' and 'European Parliament', are the concepts 'member states' and 'cooperation'. From this result we may conclude that for the Commission, cooperation with member states and the European Parliament is something to pursue.

In-depth Analysis

The results of the content analysis show that the communications from the Commission convey a clear correlation between market and cybersecurity. For the Commission, increasing levels of digital economy and activity (eBanking, eCommerce, eGovernment and eEnergy) potentiate an increase in cybercrime and cyberattacks; criminal organizations and states or state-sponsored agents seek to exploit the weaknesses of the system in order to obtain gains (COM and HR, 2013; COM 2013b, 2013d, 2014b, 2015a, 2015c[24]). The costs are also obvious for the institution: cybersecurity incidents (such as extortion, espionage and data attacks) are deemed to hinder economic growth and

[23]The Commission is connected to all themes, which is to be expected as the sample consists only of its communications.
[24]Due to the large number of documents analysed, we use COM (European Commission) and HR (High Representative) in the references of this section.

generate market distortions; they undermine the confidence of market agents and consumers, generate losses, reduce the attractiveness of digital economic models, hinder revenues and increase costs and may have negative consequences on creative processes. In short, they strongly endanger the SM. Indeed, the benefits of the cyber economy, or the economy boosted by the digital environment (such as efficiency and productivity gains and the liberation of resources) may be underexploited due to insecurity. High levels of cybersecurity are, thus, linked to economic growth, job creation, investment attraction, growth of companies, creativity and the emergence of new market and labour distribution models (COM, 2001, 2007a, 2007b, 2012b, 2012d; COM and HR, 2013; COM, 2013a, 2013b, 2013c, 2013d, 2015b, 2015c, 2016b, 2016f, 2016g).

Hence, it is clear in the Commission's narrative that online security, safety, freedom and trust are preconditions for a vibrant and competitive use of the cyberspace for economic purposes. The economy of the future is digital, interconnected and cross-border (COM, 2012b, 2013d; COM and HR, 2013). Consequently, the EU and its institutions are understood as key players in bridging the several stakeholders involved in the digital economy. In its approach the EU seeks to act in compliance with the Charter of Fundamental Rights of the European Union; namely, in what concerns the right to private life and communications, the protection of personal data, the freedom to conduct business, the right to property and the right to a remedy before a court, among others (COM, 2001, 2010c, 2013a, 2016j).

Dialogue and cooperation between actors such as states, organizations, academia, legal forces (national and international), companies and citizens are essential requirements to prevent, deter, detect and prosecute cyber incidents. This multi-stakeholder engagement builds the necessary economic, business and social drive to enhance security and increase resilience against threats. Countering cyber threats is a complex and costly affair and therefore the full commitment and the support of economic operators and users, national authorities and legal forces are indispensable to prevent in a cost-efficient manner the economic and human costs resulting from cyber aggression (COM, 2001, 2006, 2007b, 2007c, 2011c, 2012a, 2013a, 2013b, 2013c, 2013d; COM and HR, 2013; COM, 2014b, 2014c, 2015a, 2015c, 2016d, 2016j).

All in all, the results of the content analysis summarized above confirm that the Commission has intentionally played the market card to shape a comprehensive cybersecurity policy, based on shared tasks and responsibilities and cross (and inter) policy coordination. It is worthwhile noting that the 2017 cybersecurity package and, more recently, the Commission's communications on 5G (European Commission, 2020b) networks reaffirmed the market–security nexus: 'EU cyber preparedness is central to both the Digital Single Market and our Security and Defence Union' (European Commission and High Representative, 2017, p. 20). By the same token, the Commission's 2020 proposal for a recovery plan (European Commission, 2020a) foresees investment in cybersecurity explicitly related to the SM.[25]

[25]See sections 4.2 and 5.

IV. Concluding Remarks

Early studies on the EU security policy area focused on its intergovernmental character, emphasizing the role of member states, the ultimate 'decision-takers'. More recent works, however, acknowledge that, despite being formally left out from the final decision, supranational actors may be influential throughout the process of policy formation. A shift in the focus of analysis from decision-taking to decision-making allowed us to uncover a myriad of resources and strategies that supranational actors have learned to use to exert influence in avowedly intergovernmental fields.

In this article we have traced the Commission's main actions to respond to cyberthreats in general and to cybercrime in particular, from 2000 to 2016, to see how it managed to extend its role to a highly salient security issue, cybersecurity. The findings show that a strategic link between the SM (particularly its digital dimension) and cybersecurity was carefully created by the Commission. The institution made the case that cybercrime hinders the full potential of the SM, with significant economic losses for Europe as a whole. Also, the cross-border, multilevel and multisectoral nature of the cyberthreat demanded a comprehensive approach, which the Commission, acting as a policy entrepreneur, persistently endorsed and explored. The need for coordination between the internal security domain and other policy areas where the Commission has a legacy of presence and influence (in all phases of the EU policy cycle) – particularly the SM, the information society and digital Europe – opened up a window for supranational leadership that the Commission opportunistically took.

By engaging in a process of strategic framing that purposefully emphasized and explored this market–security nexus, the Commission was able to play a crucial role in problem recognition and definition and afterwards in the softening up process that led to policy formulation. Ultimately, this entrepreneurship granted the institution a more relevant role in the shaping of the EU's cybersecurity policy than previously anticipated.

Two notes on future research are due. In recent years the Commission's entrepreneurship in security matters has permeated several domains, ranging from internal security to external security and defence. How the Commission graduated from being a negligible actor to an influential player is an interesting agenda for research. Our findings on the Commission's opportunistic and entrepreneurial behaviour in the cybersecurity domain could give insights on how the institution has managed to secure a more pivotal role than expected in other security dimensions and, ultimately, in building an EU security governance system.

Another relevant line of research is a critical assessment of the implementation of the EU cybersecurity strategy. In terms of its effectiveness, the 2017 Commission assessment of the strategy concludes that its main objectives were 'only partially achieved' (European Commission, 2017, p. 57) and that the specific goal of 'drastically reducing cybercrime has not been achieved'. The latest internet organized crime threat assessment underlines 'the persistence and tenacity' of the phenomenon (Europol, 2019, p. 7) and the recent peak of cyberattacks during the ongoing Covid-19 pandemic showed the ingenuity and adaptability of cybercrime perpetrators, confirming that a generalized use of digital resources needs to be paired with reinforced cybersecurity measures.

[26]For a detailed assessment of gaps and challenges identified by the Commission, several EU bodies, the MS and other stakeholders, see European Commission, 2017.

However, apart from the evolving and complex nature of cyber threats, the EU faces numerous internal obstacles that hinder its coherence and effectiveness as a security provider in the digital area;[26] namely, the fragmentation of the legal framework (Fuster and Jasmontaite, 2020); the differences among member states in terms of their efficiency and commitment to the fight against cybercrime (Council of the EU, 2017); the lack of trust and cooperation among stakeholders (European Commission, 2017, p. 70); the big challenge of legislative framework implementation (European Commission, 2018, p. 10); the absence of a single database for electronic communications data across the EU; the limitations to cooperation with the private sector and the impediments to international cooperation (Europol and Eurojust, 2019); and the lack of institutional and policy cohesion. Curiously, some authors add an additional hurdle: the prevalence of the internal market rationale (Bendiek and Maat, 2019). Thus, one research question emerges: has the exploitation of the market–security nexus reached its limits?

Funding

This study was conducted at Research Center in Political Science (No. UIDB/CPO/00758/2020), University of Minho and University of Évora and was supported by the Portuguese Foundation for Science and Technology and the Portuguese Ministry of Education and Science through national funds.

The technical specificities of the concept map are: visible concepts 100 per cent; theme size; 45 per cent; rotation 86°.

Correspondence: Isabel Camisão, Department of History, European Studies, Archaeology and Arts, University of Coimbra, Largo da Porta Férrea, 3004-530 Coimbra, Portugal. Mobile: +351966489580.
email: isabelc@fl.uc.pt

References

Arnbak, A. (2014) 'Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy'. Available online at: https://www.ivir.nl/publicaties/download/1421.pdf. Last accessed 14 December 2020.

Brandão, A.P. (2016) "The European Commission and Security Governance: The Role of a Policy Shaper in the Fight against Cybercrime". In Building a European Digital Space – Proceedings of the 12th International Conference on Internet, Law & Politics (Barcelona: UOC), pp. 345–364.

Bendiek, A. and Maat, E. P. (2019) 'The EU's Regulatory Approach to Cybersecurity'. SWP Working Paper, No. 2 Available online at: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_2019_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf. Last accessed 14 December 2020.

Bendiek, A. and Porter, A.L. (2013) 'European Cyber Security Policy within a Global Multistakeholder Structure'. *European Foreign Affairs Review*, Vol. 18, No. 2, pp. 155–80.

Camisão, I. and Guimarães, M.H. (2017) 'The Commission, the Single Market and the Crisis: the Limits of Purposeful Opportunism'. *Journal of Common Market Studies*, Vol. 55, No 2, pp. 223–39.

Christou, G. (2016) *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Hampshire: Palgrave Macmillan).

Christou, G. (2018) 'The Challenges of Cybercrime Governance in the European Union'. *Journal of Cyber Policy*, Vol. 3, No. 3, pp. 355–75.

Copeland, P. and James, S. (2014) 'Policy Windows, Ambition and the Commission Entrepreneurship: Explaining the Relaunch of the European Union's Economic Reform Agenda'. *Journal of European Public Policy*, Vol. 21, No. 1, pp. 1–19.

Council of Europe (2001) 'Convention on Cybercrime (Budapest Convention)'. Available online at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. Last accessed 14 December 2020.

Council of the EU (2017) 'Final Report of the Seventh Round of Mutual Evaluations on "The Practical Implementation and Operation of the European Policies on Prevention and Combating Cybercrime" – Information to the Council (12711/17)'. Available online at: https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf. Last accessed 14 December 2020.

Cram, L. (1994) 'The European Commission as a Multi-organization: Social Policy and IT Policy in the EU'. *Journal of European Public Policy*, Vol. 1, No. 2, pp. 195–217.

Crespy, A. and Menz, G. (2015) 'Commission Entrepreneurship and the Debasing of Social Europe before and after the Crisis'. *JCMS*, Vol. 53, No. 4, pp. 753–68.

Center for Strategic and International Studies (2018) 'Economic Impact of Cybercrime – No Slowing Down'. Available online at: https://www.csis.org/analysis/economic-impact-cybercrime. Last accessed 14 December 2020.

Dewar, R.S. (2017) 'The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern'. In O'Neill, M. and Swinton, K. (eds) *Challenges and Critiques of the EU Internal Security Strategy: Rights, Power & Security* (Newcastle: Cambridge Scholars), pp. 113–48.

European Commission (1993) 'Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century – White Paper (COM/93/700)'. Available online at: http://aei.pitt.edu/1139/1/growth_wp_COM_93_700_Parts_A_B.pdf. Last accessed 14 December 2020.

European Commission (1996a) 'Green Paper on the protection of Minors and Human Dignity in the Context of New Electronic Services (COM/96/483 final)'. Available online at: https://op.europa.eu/en/publication-detail/-/publication/8593679e-0099-4616-9fd0-c3b4fe67c8b4/language-en

European Commission (1996b) 'Communication on Illegal and Harmful Content on the Internet, (COM/96/487 final)'. Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF

European Commission (1997) 'Press Release: Electronic Commerce: Commission Presents Framework for Future Action'. IP/97/313. Available online at: https://ec.europa.eu/commission/presscorner/detail/en/IP_97_313. Last accessed 14 December 2020.

European Commission (1999) 'eEurope: an Information Society for All. Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000 (COM/99/687 final)'. Available online at: http://aei.pitt.edu/3532/1/3532.pdf. Last accessed 14 December 2020.

European Commission (2000) '*Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (COM/2000/890)*'. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52000DC0890&from=EN

European Commission (2001a) 'Network and Information Security: Proposal for a European Policy Approach (COM/2001/298 final)'. Available online at: Area not definedhttps://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN. Last accessed 14 December 2020.

European Commission (2001b) 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (COM/2000/890 final)'. Available online at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:EN:HTML. Last accessed 14 December 2020.

European Commission (2006) 'Study Assess the Impact of Communication on Cybercrime (Contract NoJLS/2006/A1/003)'.

European Commission (2007) 'Towards a General Policy on the Fight against Cyber Crime (COM/2007/267)'. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0267&from=EN. Last accessed: 16 December 2020.

European Commission (2009) 'Protecting Europe from Large Scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (COM/2009/149 final)'. Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

European Commission (2010a) 'The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe (COM/2010/67)'. Available online at at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2. Last accessed 14 December 2020.

European Commission (2010b) 'A Digital Agenda for Europe (COM/2010/245 final)'. Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF. Last accessed 14 December 2020.

European Commission (2011a) '*Critical Information Infrastructure Protection Achievements and Next Steps: Towards Global Cyber-security' (COM/2011/163 final)'*. Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

European Commission (2011b) 'Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report'. Available online at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf

European Commission (2011c) 'First Annual Report on the Implementation of the EU Internal Security Strategy (COM/2011/790 final)'. Available online at: http://ec.europa.eu/dgs/home-affairs/news/intro/docs/20111125/1_en_act_part1_v6.pdf. Last accessed 14 December 2020.

European Commission (2012a) 'Feasibility study for a European Cybercrime Centre, 2012 Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft'. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf

European Commission (2012b) 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM/2012/140 final)'. Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF

European Commission (2013) 'Second Report on the Implementation of the EU Internal Security Strategy (COM/2013/179)'. Available online at: https://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-179-EN-F1-1.Pdf. Last accessed 14 December 2020.

European Commission (2015) 'The European Agenda on Security (COM/2015/185)'. Available online at: Area not definedhttp://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0185&from=EN. Last accessed 14 December 2020.

European Commission (2017) 'Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy'. Available online at: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF. Last accessed 14 December 2020.

European Commission (2018) *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building* (Luxembourg: Publications Office of the European Union).

European Commission (2020a) 'Europe's Moment: Repair and Prepare for the Next Generation (COM/2020/456 final).

European Commission (2020b) 'Secure 5G Deployment in the EU – Implementing the EU Toolbox (COM/2020/50)'. Available online at: https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission. Last accessed 14 December 2020.

European Commission and High Representative (2013) 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN/2013/1)'. Available online at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf. Last accessed 14 December 2020.

European Commission and High Representative (2017) 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU (JOIN/2017/450 final)'. Available online at: https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf. Last accessed 14 December 2020.

European Council (2008) 'Report on the Implementation of the European Security Strategy: Providing Security in a Changing World. Brussels European Council 11/12 December 2008'. Available online at: http://www.consilium.europa.eu/ueDocs/cms:Data/docs/pressdata/EN/reports/104630.pdf. Last accessed 14 December 2020.

European Council (2010) 'Presidency Conclusions Santa Maria da Feira European Council 19 and 20 June 2000'. Available online at: https://www.consilium.europa.eu/media/21027/santa-maria-da-feira-european-council-presidency-conclusions.pdf. Last accessed 14 December 2020.

European Council (2016) 'Shared Vision, Common Action: A Stronger Europe: a Global Strategy for the European Union's Foreign and Security Policy'. Available online at: https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf. Last accessed 14 December 2020.

European Parliament (2013) 'EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace. European Parliament Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))'. Available online at: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//EN. Last accessed 14 December 2020.

Europol (2019) 'Internet Organised Crime Threat Assessment (IOCTA) 2019'. Available online at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019. Last accessed 14 December 2020.

Europol and Eurojust (2019) 'Common Challenges in Combating Cybercrime as Identified by Eurojust and Europol'. Available online at: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF. Last accessed 14 December 2020.

Fuster, G.G. and Jasmontaite, L. (2020) 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights'. In Christen, M., Gordijn, B. and Loi, M. (eds) *The International Library of Ethics, Law and Technology* (Cham: Springer), pp. 97–115.

Ilves, L.K., Evans, T.J., Cilluffo, F.J. and Nadeau, A.A. (2016) 'European Union and NATO Global Cybersecurity Challenges A Way Forward'. *Prism*, Vol. 6, No. 2, pp. 127–41.

Kingdon, J.W. (2003) *Agendas, Alternatives and Public Policies* (2nd edition) (New York: Longman).

Kirchner, E. and Sperling, J. (2007) *EU Security Governance* (Manchester: Manchester University Press).

Kostadinova, V. (2013) 'The European Commission and the Configuration of Internal European Union Borders: Direct and Indirect Contribution'. *JCMS*, Vol. 51, No. 2, pp. 264–80.

Kroes, N. (2012) 'A European Strategy for Internet Security, Speech/12/204'. Available online at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_204. Last accessed 14 December 2020.
Leximancer (2017) *'Leximancer User Guide. Release 4.5.'*. Leximancer Pty Ltd. Available online at: http://doc.leximancer.com/doc/LeximancerManual.pdf Last accessed: 16 December 2020.
Lindberg, L.N and Scheingold, S.A (1970) *Europe's Would-Be Polity: Patterns of Change in the European Community* (New Jersey: Prentice-Hall).
Mintrom, M. and Norman, P. (2009) 'Policy Entrepreneurship and Policy Change'. *Policy Studies Journal*, Vol. 37, No. 4, pp. 649–67.
Organisation for Economic Co-operation and Development (OECD) (2012-11-16), 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy'. OECD Digital Economy Papers, No. 211,.
Princen, S. and Rhinard, M. (2006) 'Crashing and Creeping: Agenda-setting Dynamics in the European Union'. *Journal of European Public Policy*, Vol. 13, No. 7, pp. 1119–32.
Rhinard, M. (2010) *Framing Europe: The Policy Shaping Strategies of the European Commission* (Dordrecht: Martinus Nijhoff).
Riddervold, M. (2016) '(Not) in the Hands of the Member States: How the European Commission Influences EU Security and Defence Policies'. *JCMS*, Vol. 54, No. 2, pp. 353–69.
Sieber, U. (1998) 'Legal Aspects of Computer-related Crime in the Information Society Prepared for the European Commission (COM-CRIME-Study)'. Available online at: http://www.oas.org/juridico/english/COMCRIME%20Study.pdf. Last accessed 14 December 2020.
Smith, M.E. (2004) *Europe's Foreign and Security Policy: The Institutionalization of Cooperation* (Cambridge: Cambridge University Press).
United Nations Office on Drugs and Crime (2013) 'Comprehensive Study on Cybercrime'. Available online at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Last accessed 14 December 2020.
Zahariadis, N. (2007) 'Ambiguity and Choice in European Public Policy'. Paper presented at the biannual meeting of the European Union Studies Association, Montreal, Canada, May 17–19.

Annex 1

Sample of European Commission's official communications (2000–16)

Supporting Information

Additional supporting information may be found online in the Supporting Information section at the end of the article.

Supporting Information