XII Congreso de Ciencia Política de la Administración
Universidad del Pays Vasco, Spain
July 13-15, 2015

The European Commission and security governance: the role of a policy entrepreneur in the fight against cross-border threats[1]

Ana Paula Brandão[2]

CICP, University of Minho (Portugal)
abrandao@eeg.uminho.pt / apbrand@gmail.com

Abstract

The statecentric institutions demonstrate its limitations in a complex security environment characterized by multidimensional threats, and non-states actors, not only as threats sources but also as security suppliers. After the Cold War, the European Union assumed a role in responding to transboundary security problems that demand innovative forms of security governance. The transnational nature of cybercrime requires a common approach that is challenged by several issues: threat perception; definition of crimes and sanctions; coordinated management by multiple and separated authorities; public-private cooperation; balance between prevention and privacy; division of labour between the state, the main security provider, and the international organization, an emergent security actor. After decades of political and legislative initiative, the European Commission today extends its activism in the sensitive domain of security. The paper analyses the Commission as a policy entrepreneur in the fight against cybercrime. What are the main features of the Commission's approach to cross-border threats? Is that approach shaping a European security model? Is the Commission's role evolving from policy entrepreneur to policy manager? The main import of the paper is to think critically the contribution of the European Commission to the configuration of the EU security governance.

Keywords: Security Governance, European Commission, Cybercrime

The Monnet Project was a response to a Westphalian security concern – inter-state conflict- resorting to a post-Westphalian non-security means: supranational, incremental institutionalism. The European integration process has operated a 'silent revolution' in International Relations and has shown its dynamism in three essential aspects: deepening, enlargement and building a post-Westphalian polity. The internal dynamics facilitated, sometimes even enhanced, by the international environment, favoured the emergence of EU actorness: economic (in a first phase), international and, after the Cold War, security (ongoing process) actorness.

[1] Please, note that this is summary paper about an early version of a research topic in the framework of a collective project about EU security governance and transnational challenges. Please, do not quote.

[2] The author acknowledges financial support for the presentation of this paper from Fundação para a Ciência e a Tecnologia (FCT).

Ana Paula Brandão is Assistant Professor of International Relations at the University of Minho (Portugal) and integrated member of the CICP (Political Science Research Centre). She is auditor of National Defense, member of several Study Groups and speaker on European security at the IDN (National Defense Institute). She is member of the External Commission of the ICPOL – ISCPSI (Higher Institute of Police Sciences and Internal Security research unit). Her research interests focus on security studies (security theories, European security, Human Security) and European studies (CFSP/CSDP, EU Internal Security, EU actorness, EU political system).

In a context in which the EU's narrative has been fertile in identifying Europe's challenges in a globalised world[3], among which we find the transboundary security issues (Eriksson and Rhinard 2009), it is paramount to reflect upon the security governance of a post-Westphalian polity. The Union has been innovative in creating a *de facto* security community that overcame the European interstate conflict, and today it endeavours to address the multi-sector and transnational threats of a complex security environment:

> The threats facing Europe, no longer exclusively 'hard', but rather often 'soft', no longer respect the geopolitical borders of the nation-state and the EU. More importantly still, they traverse and resist the institutional 'borders' and arrangements traditionally designed to manage them (social agencies, informational authorities, police, etc.). The most significant effect of this shift is that the lives of citizens are no longer regulated at the physical borders. The border operations traditionally provided for by the nation-state (border controls and security guards, passport authorities, etc.) have in this way shifted outwards. At the same time, a growing number of European and international organizations have taken on increasingly dominant roles entirely detached from nation-state sovereignty, further contributing to the interrelatedness of non-national institutions and regions, and further weakening both the role and capacity of traditional sovereignty arrangements. (Burguess 2009, 315)[4]

Among those transnational security challenges is cybercrime understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (European Commission 2007, 2), covering different types of domestic but also cross-broader criminal activities. The EU is perceived as "a key target for cybercrime because of its advanced Internet infrastructure, rates of adoption and increasingly Internet-mediated economies and payment systems" (Europol 2011, 3). In spite of the difficulties[5] around the data about the phenomenon, several sources underline its expansion and sophistication:

> At the global level, law enforcement respondents to the Study perceive increasing levels of cybercrime, as both individual offenders and organized criminal groups exploit new opportunities, driven by profit and personal gain. (UNODC 2013, 6)
>
> Long gone are the days when cybercrime was tantamount to teenage miscreants causing mischief in their parents' basement. Today, as any commercial enterprise, cybercrime has evolved into a complex, highly organized hierarchy

[3] "Lecture by Javier Solana, Secretary General/High Representative for the Common Foreign and Security Policy, at the Inauguration of the Diplomatic Academy of the Ministry of Foreign Affairs of the Republic of Poland, on 'Global Challenges for the European Union's Common Foreign and Security Policy", Warsaw, 16 October 2002; "Press Conference at EU Informal Summit Hampton Court", 27 October 2005; European Commission, "Communication from the Commission to the European Council of June 2006 - Europe in the World — Some Practical Proposals for Greater Coherence, Effectiveness and Visibility " [COM (2006) 278], Brussels, 2006; "Speech by Javier Solana EU High Representative for the Common Foreign and Security Policy 'Europe's Answers to the Global Challenges' at the University of Copenhagen, 8 September 2006", Copenhagen, 2006; "Declaration on the Occasion of the 50th Anniversary of the Signature of the Treaties of Rome", Berlin, 25 March 2007; Commission of the European Communities, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of The Regions: The European Interest: Succeeding in the age of Globalisation: Contribution of the Commission to the October Meeting of Heads of State and Government" [COM (2007) 581], Brussels, 2007; "Comunicado de Imprensa da Presidência sobre o Conselho Europeu Informal [de Lisboa]", Lisboa, 19 de Outubro de 2007; Foreign Commonwealth Office, "Global Europe: Meeting the Economic and Security Challenges", 2007; "EU Declaration on Globalisation" (annex), "Brussels European Council - 13/14 December 2007 - Presidency Conclusions", Brussels, 2007.

[4] "The world faces traditional and non-traditional security fears. Many of our countries are targets of terrorism, which eight years on from Sept. 11, 2001, we must recognize is down, but by no means out. There are fragile states to contend with as well as the dangers of the proliferation of weapons of mass destruction, authoritarian regimes, and the threat of extremism. Globalization has also thrown up non-traditional security challenges with no respect for national frontiers. Global pandemics can spread faster; a lack of secure and sustainable energy could push us into a world-wide recession; and climate change, beyond its environmental consequences, could have serious geopolitical and social repercussions" (Durão Barroso. 2009. "Europe's Rising Global Role". Project Syndicate. [http://www.project-syndicate.org/commentary/barroso3]).

[5] "Because of the difficulties arising when trying to define and identify cybercrime, crossnationally comparative statistics on cybercrime are much rarer than for other crime types." (UN 2013).

> involving leaders, engineers, infantry, and hired money mules. Looking from the outside in, there's little to distinguish cybercrime organizations from any other business. (Fortinet 2013, 1)

> Cybercrime is bigger than the global black market in marijuana, cocaine and heroin combined ($288bn) and approaching the value of all global drug trafficking ($411bn) (2012 Norton)

The transnational dimension of cybercrime is well documented in the UNODC Study (2013):

> it is clear that the focus is on the misuse of ICT from a global perspective. More than half of responding countries, for example, reported that between 50 and 100 per cent of cybercrime acts encountered by the police involve a transnational element. Respondents referred to cybercrime as a 'global phenomenon' and noted that 'online communication invariably involves international or transnational dimensions.'

In Europe, the two most common cybercrimes acts are[6] "computer-related fraud and forgery", an increasing phenomenon with an emerging *modus operandi* of Crime as a Service (CaaS) (Europol 2013), and "computer-related production, distribution or possession of child pornography" (UNODC 2013, 26), also expected to increase (Europol 2013).

The studies on European security initially followed the fragmented (external/internal[7]) matrix formatted by the pillarised (second and third pillars) structure. This article adopts a broad approach of security governance and actorness, due to: the transnational dimension of the main security problems facing EU; the *formal* end of the pillar structure (Lisbon Treaty), with the precedent cross-pillar tendency catalysed by the 09/11 events; the European narrative that underlines a 'comprehensive approach' to security challenges.

The research on EU security governance generally do not consider the role of the European Commission. The security policy area is the realm of sovereign States, which explains the intergovernmental nature of European security cooperation expressed in the pillar structure from Maastricht to Lisbon Treaties: in the second and third pillars, the Council and the states were the protagonists as policy initiators, decision-makers and executors. The intergovernmental method is centred in the Council, leaving aside the European Commission as an exclusive legislative initiator. This explains the relative silence of Security Studies on the European Commission. In spite of the political and legal constraints, the Commission has been gradually incrementing its presence, particularly in internal security cooperation. The 'comprehensive approach', underlined by European Commission, enables that presence. It should be notice that Lisbon Treaty transferred the internal security matters to the Treaty on the Functioning of the European Union (although maintaining some specificities) which configures a positive move for the European Commission.

[6] The study identifies the following categories: Illegal data interference or system damage; Illegal access to a computer system; Illegal access, interception or acquisition of computer data; Computer-related copyright and trademark offences; Sending or controlling sending of SPAM; Computer-related fraud and forgery; Computer-related acts involving racism and xenophobia; Computer-related acts in support of terrorism offences; Breach of privacy or data protection measures; Computer-related identity offences; Computer-related solicitation or 'grooming' of children; Computer-related acts causing personal harm; Computer-related production, distribution or possession of child pornography.

[7] Second pillar/external security – CFSP and (after the Amesterdam Treaty) ESDP; internal security – Police and Judicial Cooperation in Criminal Matters.

The EU, the European Commission and security: from absence to presence

The economic specialisation of the European international organisation and the debacle of the European Defence Community Project, associated to the nature of the threat and the guarantee of the security needs by the USA and NATO during the Cold War, postponed the inclusion of the security agenda. Although this late inclusion by the Maastricht Treaty, one can say that the security issue has been ubiquitous in the European integration process.

Underlying the creation of the ECCS, there was a classic reactive security concern against a globalised European war and one preventive of a new inter-state conflict. The Monnet project built upon an institutionalised and gradual strategy aimed at guaranteeing the Franco-German peace (and thus European peace) through the integration of the coal and steel sectors in a post-Westphalian organisation. "European integration has always involved the use of economic cooperation to reduce political conflicts among EU member states" (Smith 2004, 7).

Countering the (realism) academic scepticism concerning the usefulness of the "community" concept in the world of *power politics*, national interest and anarchy, the European Union has proved it possible, even if at a regional scale, to fulfil "[T]he idea that actors can share values, norms, and symbols that provide a social identity, and engage in various interactions in myriad spheres that reflect long-term interest, diffuse reciprocity, and trust" (Adler and Barnett 1998, 3).

Countering the centuries of inter-state conflict, the European states have built a community in which there is "a real assurance that the members of that community will not fight each other physically, but will settle their disputes in some other way"[8]. Set on an institutional and societal transnational base[9] and having a structural common interest in keeping inter-state peace and security, the relations between Member-States have been characterised by mutual trust and predictability.

Internal pacification had a spill over effect on the external area. Different policies have contributed to international security and stability, especially, on the one hand, the enlargement policy that extends the security community to new States and supports the transition of candidate States and, on the other hand, the policy of cooperation for development which, as is the case with the United Nations, is based upon the link between security and development.

In a first phase, an implicit security actor was built, later evolving to the creation and consolidation of an expansive security community that favours the use of non-security means. The end of the Cold War, the implosion of the USSR, the decrease of American presence in Europe, the expansion of the security agenda, created the opportunity for the actor's evolution to a new stage. The weaknesses of its actions in neighbouring intra-state conflict situations (Balkans) and the concern with the transnational risks in an internally borderless market catalysed the clarification of the security actor thanks to the introduction of the Common Foreign and Security Policy (second pillar) and the

[8] Karl Deutsch, cit. by Adler and Barnett 1998, 6.

[9] Waever in Adler and Barnett 1998, 6.

police and judicial cooperation in criminal matters (third pillar[10]). This clarification was reinforced by the Amsterdam Treaty with the formalization of the actor's military component (ESDP) in the second pillar's framework, the specialisation of the third pillar and the externalisation of 'internal security' also within this pillar's framework.

The Maastricht Treaty inserted the security policy area based in a pillarised structure. Although under "a single institutional framework" which should "ensure the consistency and the continuity of the activities" (article C), the three pillars had relevant policy-making differences that affected the role of EU institutions, including the European Commission. Those differences were the result of the major distinction between communitarian (1st pillar) and intergovernmental (2nd and 3rd pillars) decision-making methods and policy instruments. It should be notice that this separation between the Community and intergovernmental instruments had been a trend since the times of EPC and due to a French insistence (Duke 2006).

Regarding the second pillar, the European Commission should be "fully associated with the work carried out in the common foreign and security policy fields" (article J.9) and shared with the Council the responsibility for ensuring the EC/EU external consistency (article C). The Commission direct and exclusive initiative power did not apply to this pillar: the institution representative of the common interest was only allowed to refer any question relating to the CFSP and to submit proposals to the Council (article J.8). The Commission's involvement in CFSP was mainly at the level of the external relations (coherence) and development issues. The nineties were marked by a cautious Commission and an internal problematic (competition and turf battles) relation among DG's (Duke 2006).

The growing relevance of the security aspects of CSFP, particularly after the Balkans crisis, and the creation of ESDP, including a civilian component, intensified another institutional rivalry – the Commission-Council struggles over competence in a pillarised structure. In spite of the above mentioned difficulties - the Maastricht inherited fragmentation, the intergovernmental method and the (intra and inter) institutional battles -, the Commission increased its presence through the use of Community instruments in support of CSFP decisions. Another expanding trend favoured its presence: the interpillar and crosspillar dimension of security problems. The most clear example of a demand for interpillar (1st and 2nd pillars) coordination was well patent in the security-development nexus narrative. The crosspillar (1st, 2nd and 3rd pillars) coordination became a priority after the 9/11.

The fight against transnational terrorism, enhanced by the materialization of the threat, inaugurated a new stage in the actor's construction, overcoming *de facto* the fragmented security approach: "The European Union will intensify its commitment against terrorism through a coordinated and inter-disciplinary approach that will incorporate all of the Union's policies" (European Council 2001). Although the focus of the European fight is placed on the police and judicial instruments, the

[10] In the Maastricht Treaty, the third pillar ("Justice and Home Affairs) concerned also cooperation in the domains of immigration and asylum.

complexity of the threat justified a cross-pillar approach underlined by the four axis - prevention, protection, pursuit, response - of the Counter-Terrorism Strategy (Europeam Council 2005). The coordination between the pillars concerning security previously required both by conflict prevention (1995) and by the cooperation externalisation in the 'internal security' realm (1999), reached a new level when it contemplated the three pillars simultaneously (cross-pillarisation).

The first document explaining the EU's "security doctrine" confirmed this comprehensive tendency: a holistic security concept, an interdependence of threats (threats dynamics/"threat multiplier"), the security nexus (internal/external, security/development, civilian/military). The European Security Strategy (European Council 2003) corroborates yet another relevant change in the actor's discourse:

> It stands for a discursive turn in the sense that the very theme of (external) security is no longer off-limits to the EU in the way it traditionally used to be. (…)' Whereas the EU previously pertained to security in a rather indirect manner and did so mainly through its structural essence by providing a unifying centre rather than appearing itself explicitly as a securitizing agent vis-à-vis the external environment, the new doctrine seems to be part of efforts that aim at bolstering the Union's actorness on the international scene. (Joenniemi 2007, 136)

In 2009, the Reform Treaty, similarly to previous treaties, ensured continuity, formalised *de facto* changes and introduced innovative elements. Reaffirming the objectives of making the European Union institutionally more efficient, closer to the citizen, more coherent in external action, it introduced a goal concerning global challenges (Portugal 2007).

In this reforming context, the European Security and Defence Policy (ESDP) and, particularly, the Police and Judicial Cooperation in Criminal Matters, stand out as the most dynamic areas of this last revision. Before analysing specific changes regarding internal security matters, three transversal changes that have implications in the (broad) security domain should be highlighted.

First, the Lisbon Treaty ends the dual (EC/EU) system in force since 1993 that penalized the Union's action capacity and its external recognition. Endowed with unique legal personality[11], it assumes the external representation, and it is capable of celebrating treaties and of participating in International Organisations. This means that, for the first time, CFSP/CSDP and PJCCM will evolve in the framework of an International Organisation under International Law. Beyond the legal meaning, Solana underlines the political importance of this change that facilitates the recognition, visibility and readability of the Union: "it would be easier for third countries to understand the EU without the complication of dealing with, and sometimes signing agreements with, different entities"[12].

Second, the Treaty overcomes, if only superficially, the Thatcherian pillar matrix, coming closer to the tree-like Delors matrix and consecrating *de jure* the tendency initiated by the *de facto* cross-pillarisation, namely in realms such as external relations, security and the environment

[11] "The Union shall have legal personality" (article 47 TEU).

[12] United Kingdom, Parliament. 2008. "European Union Committee 10th Report of Session 2007–08 The Treaty of Lisbon: an Impact Assessment Volume I: Report." [http://www.publications.parliament.uk/pa/ld200708/ldselect/ldeucom/62/62.pdf].

benefiting the actor's coherence and efficiency. The policies of the former second and third pillars were brought under the jurisdiction of a single entity; however, we can state that there subsists a disguised pillarisation, namely concerning the decision process, with implications in the realms of external action and security. In fact, the CFSP (and CSDP) maintains a separate legal character[13] that safeguards its intergovernmental nature. Concerning the Commission's right of initiative, it is restricted to the Union's High Representative for Foreign Affairs and Security Policy:

> Through its creation of a new HR (who partly represents the Commission), the Lisbon Treaty has elevated the Commission's voice in CFSP. However, whereas in the current EU Treaty, the Commission has the right to submit proposals to the Council (current EU treaty, Article 20, paragraph 1) and was "fully associated" with CFSP (current EU treaty, Article 18, paragraph 4), under the Lisbon Treaty it will lose this right – this now being associated solely with the High Representative. (Daghan 2008)

The CFSP's specificity also justifies the CSDP exclusion from the scope of article 352 of the TFEU (Wessels and Franziska 2008). Furthermore, it should be noted that, contrary to the simplification established by the Constitutional Treaty, the above mentioned domains are under the aegis of both treaties. So, concerning the security domain, the CFSP and the CSDP remain in the European Union Treaty (TEU), whilst the *PJCCM* is transferred to the Treaty on the Functioning of the European Union (TFEU)**.**

Finally, the creation of the posts of European Council President and High Representative intends to contribute to the inter-institutional and inter-policies coordination in a context of further continuity. The innovative formula associated to the European Union's institutional complexity and the absence of a clear division of competence could generate, at least in an initial learning by doing period, "role conflicts between the President of the European Council and the High Representative" (Quille 2008).

The issues pertaining to 'internal security', formerly under the aegis of the third pillar, were transferred to the TFEU and moved into title IV, dedicated to the "Area of Freedom, Security and Justice" (AFSJ)[14], constituting one of eleven areas of shared competence[15]. The "communitarisation" of the third pillar is considered one of the most innovative changes of the Treaty[16]: adoption of regulations, directives and decisions, according to the community method (co-decision and by

[13] "The common foreign and security policy is subject to specific rules and procedures. It shall be defined and implemented by the European Council and the Council acting unanimously, except where the Treaties provide otherwise. The adoption of legislative acts shall be excluded. The common foreign and security policy shall be put into effect by the High Representative of the Union for Foreign Affairs and Security Policy and by Member States, in accordance with the Treaties. The specific role of the European Parliament and of the Commission in this area is defined by the Treaties. The Court of Justice of the European Union shall not have jurisdiction with respect to these provisions, with the exception of its jurisdiction to monitor compliance with Article 40 of this Treaty and to review the legality of certain decisions as provided for by the second paragraph of Article 275 of the Treaty on the Functioning of the European Union." (article 24 TEU).

[14] Title V ("Area of freedom, security and justice") substitutes title VI of the TEC ("Visas, asylum, immigration and other policies related to free movement of persons"). Besides of chapters on "Policies on borders checks, asylum and immigration" (chapter 2) and "Judicial cooperation in civil matters" (chapter 3), it also includes chapters 4 (Judicial cooperation in criminal matters") and 5 (Police cooperation).

[15] Internal market; social policy, for the aspects defined in this Treaty; economic, social and territorial cohesion; agriculture and fisheries, excluding the conservation of marine biological resources; environment; consumer protection; transport; trans-European networks; energy; area of freedom, security and justice; common safety concerns in public health matters (article 4 TFEU).

[16] "(..) the powers of the Commission under Article 258 of the Treaty on the Functioning of the European Union shall not be applicable and the powers of the Court of Justice of the European Union under Title VI of the Treaty on European Union, in the version in force before the entry into force of the Treaty of Lisbon, shall remain the same, including where they have been accepted under Article 35(2) of the said Treaty on European Union" (article 10, Protocol No 36).

qualified majority, based on proposals from the Commission); control of the implementation of rules by the Commission and by the Court of Justice; EU representation by the Commission in international relations and negotiations. This change can be explained by the compensatory effect of the market opening that had already been at the origin of the formalisation of JHA cooperation by the Maastricht Treaty, which was intensified after 09/11.

It should be notes that we are facing a peculiar communitarisation, in which there are lingering clouds of intergovernmentalism: the right of initiative is not exclusive of the Commission, since a quarter of the Member States can put forward a legislative proposal (article 76 of the TFEU); there is an exemption to the judiciary control laid down in article 276 of the TFEU; the unanimous vote in the Council and the consultation procedure are applicable to certain matters[17]; "the strategic orientations of the legislative and operational programme" are defined by the European Council (article 68 of the TFEU); the opt-out possibility[18] and the "emergency brake" (article 82, no 3 of the TFEU) is introduced by the TFEU. The Lisbon Treaty, like the preceding ones, derives from a compromise between different perspectives on the European integration process, as well as from the historic tension between active solidarity and state sovereignty, which explains the "constructive ambiguity".

Bringing together issues concerning 'internal security' and immigration and asylum under the same title (title V TFEU), emulating the Maastricht model[19], this time in a community framework, confirms a (negative) securitizing movement only (formally) interrupted by the Amsterdam Treaty. This movement is reinforced by the security logic of the external borders, as demonstrated by two of the objectives set for these policies: "carrying out checks on persons and efficient monitoring of the crossing of external borders"; "the gradual introduction of an integrated management system for external borders" (article 77, no 1 of the TFEU)[20].

Aiming at reinforcing operational cooperation in the 'internal security' domain, the Internal Security Standing Committee (COSI) was set up within the Council, "in order to ensure that

[17] Operational police cooperation (n 3, article 87 TFUE), passports, identity cards, residence permit s(nº 3, article 77 TFUE), establish a European Public Prosecutor's Office (nº 1 , article 86 TFUE).

[18] See: Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice THE; Protocol (No 22) on the position of Denmark."While the Lisbon Treaty, for the vast majority of Member States, has the effect of 'homogenising' a communitarised Area of Freedom, Security and Justice, the position of the other Member States, is made only more anomalous" (Brendan 2008, 1).

[19] *See* Ana Paula Brandão. 2008. "Migração internacional na União Europeia: da politização à securitarização." *Lusíada* 6/8. 2007: 57-86.

[20] The Treaty formalizes a comprehensive concept of "integrated border security system", defined by the JHA Council in December 2006: "Frontex promotes a pan European model of Integrated Border Security, which consists not only of border controls but also other important elements. The first tier of the model is formed by exchange of information and cooperation between Member States, immigration and repatriation. The second tier is represented by border and customs control including surveillance, border checks and risk analysis. The third tier is linked with cooperation with border guards, customs and police authorities in neighbouring countries. The forth tier is connected with cooperation with third countries including common activities" (Frontex. "Origins". [http://www.frontex.europa.eu/origin_and_tasks/origin/]). External border security is historically related with internal market (see Commission of European Communities. 1988. "Completing the Internal Market: an Area without Internal Frontiers" (COM (88) 350); "Communication of the Commission to the Council on the Abolition of Controls of Persons at Intra-Community Borders" (COM (1988) 640 final, 1988). The Amesterdam Treaty attributed competences to EC (first pillar) regarding external border controls (article 62 and 66 TEC). In 2001, a 'European Border Police' proposal was presented by Germany, France, Italy, Spain and Belgium, and rejected by UK and other Member States. In 2002, the European Commission approved In 2003, the European Commission approved the communication "Towards integrated management of the external borders of the Member States of the European Union" [COM (2002) 233]. Frontex (Regulamentation (EC) nº 2004/2007) implemented " the concept of integrated border management" ("Frontex - Work Programme 2009". [http://www.frontex.europa.eu/gfx/frontex/files/justyna/programme_of_work_2009_final.pdf]).

operational cooperation on internal security is promoted and strengthened within the Union " (article 71 of the TFEU). This innovation was justified by the need to counter the efficiency and transparency deficit of operational cooperation, all the more urgent in the context of the anti-terrorist fight. Underlying the initial proposal of the new structure were the principle of clear separation between legislative and operational tasks[21] and the overcoming of the pillarisation of 'internal security'[22].

In the framework of the AFSJ multi-annual programme (Stockholm Programme), one of the priority tasks of the new organism has been the conception, follow-up and implementation of a global internal security strategy: "terrorism and organised crime, drug trafficking, corruption, traffic of human beings, people smuggling and arms trafficking, among others, keep on threatening the EU's internal security. The spread of cross-border criminality has become an urgent challenge demanding a clear and global response" (European Council 2010, 17). The Internal Security Strategy "took into account the External Security Strategy, due to "the existing inter-relation that exists between internal security and the external dimension of threats".

In sum, the post-Cold War (in)security environment created the opportunity for the EU presence on security matters. The post-post-Cold War created the opportunity for the implementation of a comprehensive and multidimensional security approach. The Lisbon Treaty confirmed the tendency towards the security actor's gradualist construction, associated to the prioritization of security issues on the European agenda. In spite of the persisting (external/internal security) policy and decision-making differentiation, those developments favour the increasing presence of European Commission on security policy. Based on the functional categorisation of this policy (Kirchner and Sperling 2007), it is possible to argue that the European Commission participates more actively in three of the four security tasks: prevention (inter/intra-state conflict prevention through the building of democratic institutions and the consolidation of civil society), assurance (peace-building), protection (internal security). The fight against cybercrime falls in the third security task: protection of EU's "citizens, businesses and governments and their infrastructure from cyber-attacks" (European Commission 2013, 2).

Security governance and cybercrime: the opportunity for European Commission entrepreneurship

The first international initiatives date to the nineties associated with the G8 Subgroup on Hi-Tech Crime that, in cooperation with INTERPOL, created the 24/7 'Network of Contacts'. Other IO's and

[21] See: Tom Bunyan. 2003. "The Creation of an EU Interior Ministry - for the Maintenance of Law and Order, Internal Security and External Borders." [http://www.statewatch.org/news/2003/apr/TBARTICLEpdf].

[22] "abolishing the pillars enables all the authorities concerned with "internal security" to be covered for the first time, not merely police forces but also those responsible for customs and civil protection. The abolition of the pillars in this way will be welcomed by all practitioners who stress that cooperation must cover a broader field than merely police aspects in order to ensure internal security. The consequences of the 11 September attacks have shown the importance of mobilising all services and of cooperation between disciplines" (Secretariat of the European Convention. 2003. "Cover Note - Area of Freedom, Security and Justice" (Document CONV 614/03). [http://www.statewatch.org/news/2003/mar/conv00614.en03.pdf].

international *fora* inserted the topic of cybersecurity and cybercrime in the international agenda such as OECD, International Telecommunications Union, World Summit on the Information Society, NATO and Council of Europe. In the fight against this threat, the international consensus underlies three vectors: awareness raising; public-private partnerships; cybercrime strategies integrated with a broad cybersecurity perspective (UNODC 2013).

The European Union has been active in the fight against cybercrime since 2001 (European Commission 2000)[23]. The EU security strategies (European Council 2008; European Council 2010) insert the cyber threats among the key threats and challenges to European interests: the European Security Strategy (EES) recognises the cyber-attacks as a "potential new economic, political and military weapon" (European Council 2008, 5); one of the five strategic objectives of the International Security Strategy is to enhance cybersecurity, grounded in three actions - build capacity in law enforcement and the judiciary (action 1), work with industry to empower and protect citizens (action 2), improve capability for dealing with cyber attacks (action 3) (European Commission 2010). In the 2011 Internal Security Strategy report, the fight against organised crime and cybercrime are identified as the two main challenges to be addressed in the following years (European Commission 2013).

This issue has represented a key priority for the Commission since 2007 (European Commission 2007). The Commission's entrepreneurial role in the fight against cybercrime is facilitated by four factors: the EU comprehensive security approach; the Commission's experience in Justice and Home Affairs/Area of Freedom, Security and Justice, including its external dimension (i.e. negotiation of cooperation and association agreements with third countries), particularly since 1999; its knowledge about the private sector (i.e. internal market, competition policy); the 'window of opportunity' of the "digital agenda for Europe"[24] and cybersecurity as a part of the Europe 2020 strategy.

Securitizing move for a EU policy

The cybercrime is considered a major security threat that the EU continues to face and the fight against it "remains a priority for the Commission and the Member States" (European Commission 2013, 9). It stands a danger for "whole society" considering the possibility of "mass-scale" and "great geographical distance" criminal activities that constitute "significant threats to critical infrastructures, society, business and citizens" (European Commission 2007). The words of the Commissioner for Home Affairs (herself also victim of large-scale cyber attack that severely affected

[23] See annex.

[24] See: "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/2010/0245 final); Commission Staff Working Document: Overview of progress on the 101 Digital Agenda actions and Digital Agenda Review package…, 2012; Commission Staff Working Document: "Digital Agenda for Europe - a good start and stakeholder feedback".

the Commission e-mailing system) are expressive: “I don't think I exaggerate when I say that this must be the golden age for cyber criminals” (Malmström 2011)

A study ordered by the Commission in 2006[25][26] identified the major trends of a “changing environment”: growing number, sophistication and internationalization of cybercrimes; involvement of organised crime groups in cybercrime; stabilization of European prosecutions on the basis of cross-border law enforcement (European Commission 2007). In order to cope with these challenges, the Commission sustains that “there is an urgent need to take action – at national as well as European level” (European Commission 2007): the cross-border dimension of cybercrime demands “a specific EU policy”, in particular, “recognised as a priority by the Member States and the Commission”, based in the following: “improved operational law enforcement cooperation; better political cooperation and coordination between Member States; political and legal cooperation with third countries; awareness raising; training; research; a reinforced dialogue with industry and possible legislative action” (European Commission 2007).

In sum, we identify five features of the Commission approach to cybercrime:

Comprehensive approach

The cybercrime affects different security reference objects (from governments to citizens). The fight against it requires a multi-stakeholder cooperation involving states, the private sector and international organisations. The European Union

The fight against cybercrime is connected with other EU policies and initiatives in the following areas: information society and Digital Agenda Europe (dissemination of ICT, liberalization of the telecommunications markets, data protection and copyrights) and cybersecurity (securing network and information systems from accidents and criminal activities); internal market; children rights; internal security, fight against organized crime, counterterrorism and fight against fraud; foreign policy (international cooperation)[27].

This specific policy adopts the usual means: legal instruments; operational cooperation among law enforcement and judicial authorities through European structures (Europol, Eurojust, CEPOL, EJNP), with particular focus on training; international cooperation (Council of Europe, G 8 Lyon-

[25] The Directorate-General Justice and Home Affairs was established by the Prodi Commission (its precedent was a Task Force for JHA). From to 1993 to 1995, JHA had been under the Commissioner with responsibility for Employment and Social Affairs; from 1995 to 1999, under the Commissioner with responsibility for Immigration, Home Affairs and Justice (and also relations with the Ombudsman, Financial Control, Fraud prevention). The first budget line for JHA was implemented in 1996. In July 2010, the DG became two separate directorates: DG for Home Affairs and DG for Justice. See Uçarer 2001.

[26] Study assess the impact of communication on cybercrime (Contract NoJLS/2006/A1/003).

[27] The European Cyber Security Strategy was elaborated by the European Commission and the High Representative.

Roma High-Tech Crime Group, IGF, ITU, Interpol, OECD, OSCE, UN, US); research (technologies to secure information)[28].

The European Cybersecurity Strategy, defined by the European Commission and the High Representative (2013), elucidates the principles - transparency, accountability and security – and strategic priorities of this EU policy: “achieving cyber resilience”; “drastically reducing cybercrime; developing cyberdefence policy and capabilities”; “develop the industrial and technological resources for cybersecurity”; “establish a coherent international cyberspace policy for the European Union and promote core EU values”.

For a common definition of cybercrime

The proposed definition -"criminal acts committed using electronic communications networks and information systems or against such networks and systems" - applies to three categories of activities: traditional forms of crime (fraud or forgery, committed over electronic communication networks and information; publication of illegal content over electronic media; crimes unique to electronic network (attacks against information systems, denial of service, hacking) (European Commission 2007, 2). The harmonization of crime definitions and national penal laws is considered a long term objective, due to complex nature of the phenomena.

Horizontal Coordination

The transnational dimension of cybercrime in accelerated development demands a coordinated European approach. According with the Commission, “[T]he lack, or underutilisation, of immediate structures for cross-border operational cooperation remains a major weakness in the area of Justice, Freedom and Security” (European Commission 2007): slowness and ineffectiveness of traditional mutual assistance; need to strengthen and clarify responsibilities of European structures. The Commission assumes the initiative of promoting this coordination through meetings of law enforcement experts from Member States, Europol, CEPOL and the EJTN, the establishment a permanent EU contact point for information exchange and the creation an EU cybercrime training platform (European Commission 2007).

Public-Private cooperation

As for internal security in general, the Commission clearly supports the cooperation between the public and private sectors: definition of a “strategy for cooperation between the public sector and private sector operators, including civil society organisations”; creation of the European Security Research and Innovation Forum; organisation of conferences for law enforcement experts and private sector representatives, especially Internet Service Providers (European Commission 2007)

[28] EU Seventh Research Framework Programme (FP 7): Information and Communication Technologies; Security

Normative dimension

The European Commission underlines that this EU policy will full respect the fundamental rights, "in particular those of freedom of expression, respect for private and family life and the protection of personal data" (European Commission 2007).

Final Remarks

The post-Cold War period demonstrates that the State is not the only referent object of security: it is not the only target of threats, nor the sole security provider. The different referent objects face multi-level and multi-sectorial threats. Therefore, it is required a combination of a diversity of actors, policies and tools to face complex threats and security challenges.

In a Cold War context, the EEC successfully faced the Westphalian challenge of inter-state conflict through non-security means and the post-Westphalian institutionalism. The change in the post-Cold War security environment favoured the explicitness of the security actorness of the European Union. In the post-Cold War, the European Union asserted itself as a comprehensive and multi-functional security actor.

In spite of this evolution (from absence to presence), security remains a sensitive issue under the realm of States, persisting the historical tensions between European solidarity and state sovereignty, common interest and national interests, collective declaration and unilateral action. But the complex nature of cybercrime, like other transboundary, multi-referent objects and multi-actors security issues, demands collective governance. The EU distances itself from intergovernmental security organizations in three crucial aspects: it is a polity; it has the competence and the means to fight a diversity of threats in the security spectrum; it is not restricted to the security domain, being able to use non-security tools to the advantage of that domain. These specificities represent an add value in the prevention and fight against complex threats.

The European Commission is a central institution in the EU governance system. However, the pillarised Maastricht structure limited the entrepreneurial role in security matters. In spite of that constraint, several factors facilitated a gradual presence of the Commission on the sensitive security area (although not comparable with its influence in other policies such as internal market and competition). In this context, the fight against cybercrime constitutes a 'window of opportunity' for European Commission to shape the internal security policy of a post-Westphalian actor.

Annex: The European Union and Cybercrime

Policy	Legislation	Structures
		2014 - Joint Cybercrime Action Taskforce (J-CAT)
Communication on Cyber security strategy JOIN(2013) 1 final	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems [replacing Council Framework Decision 2005/222/JHA]	2013 - European Cybercrime Centre (EC3) hosted by Europol - support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.
		Communication from the Commission to the Council and the European Parliament on Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM(2012) 140 final)
		Feasibility study for a European Cybercrime Centre
Communication from the Commission to the European Parliament, the Council, 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)		
	Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (accompanying impact assessment and its summary) (COM(2010) 517 final	2010 - the European Cybercrime Task Force (EUCTF) of Europol - representatives from Europol, Eurojust and the European Commission
	Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (accompanying impact assessment and its summary) (COM(2010) 251 final)	
	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (COM (2010) 520 final)	
Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" COM(2009) 149 final		
Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems (COM(2008) 448 final)		
Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime (COM(2007) 267 final)		

	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems	
	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 (consolidated version of November 2008)	2004 - European Network and Information Security Agency (ENISA) - an European Agency ENISA established to carry out very specific technical, scientific tasks in the field of Information Security, and to assist the European Commission in the technical preparatory work for updating and developing Community legislation in this field
Communication from the Commission to the Council, the European Parliament, the 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)		

Bibliography

Adler, Emanuel, and Michael Barnett, eds. 1998. *Security Communities*. Cambridge: Cambridge University Press.

Bendiek, Annegret. 2006. "Cross-Pillar Security Regime Building in the European Union: Effects of the European Security Strategy". *European Integration online Papers* 10 (9). Available at: http://eiop.or.at/eiop/texte/2006-009a.htm.

Brendan Donnelly. 2008. "Justice and Home Affairs in the Lisbon Treaty: A Constitutionalising Clarification?". *Eipascope* 2008 1: Available at: http://www.eipa.eu/files/repository/eipascope/20080509184107_SCOPE2008-1-4_BrendanDonnelly.pdf.22

Burguess, J. Peter. 2009. "There is No European Security, Only European Securities." *Cooperation and Conflict* 44: 309-328.

Council of the European Union. 2005. The European Union Counter-Terrorism Strategy [14469/4/05 REV 4]. Available at: [http://register.consilium.europa.eu/pdf/en/05/st14/st14469-re04.en05.pdf].

Daghan, Sophie. 2008. "The impact of the Lisbon Treaty on CFSP and ESDP*."* *European Security Review* (37). Available at: http://www.isis-europe.org/pdf/2008_artrel_150_esr37tol-mar08.pdf.

Donnelly, Brendan. 2008. "Justice and Home Affairs in the Lisbon Treaty: A Constitutionalising Clarification?". *Eipascope* (1): 19-23.
Available at: http://www.eipa.eu/files/repository/eipascope/20080509184107_SCOPE2008-1-4_BrendanDonnelly.pdf.

Duke, Simon. 2006. The Commission and the CSFP. EIPA Working Paper 2006/W/01. Avaialable at: http://www.eipa.eu/files/repository/product/20070815141210_CFSP_0601e.pdf.

European Commission. 2013. 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]. Available at: https://www.cepol.europa.eu/fileadmin/website/newsroom/newsitems/iss_second_report_com_2013_179_en.pdf.

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]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2.

European Commission. 2007. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: towards a general policy on the fight against cyber crime [COM (2007) 267]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

European Commission and High Representative. 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Joint 2013 1]. Available at:

European Council. 2010. The Stockholm Programme: an open and secure Europe serving and protecting citizens (2010/C 115/01). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF.

______. 2008. Report on The Implementation Of The European Security Strategy: Providing Security In A Changing World. Brussels European Council 11/12 December 2008. Available at: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf.

______. 2001. "Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001." [http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140.en.pdf].

Europol. 2013. SOCTA 2013 : EU Serious and Organised Crime Threat Assessment. Available at: https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

______. 2012. Europol Review 2011. https://www.europol.europa.eu/sites/default/files/publications/en_europolreview2011_0.pdf. Available at:

______. 2011. IOCTA: Threat Assessment [abridged]: Internet Facilitated Organised Crime. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf.

Fortinet 2013 Cybercrime Report. Available at: http://www.fortinet.com/sites/default/files/whitepapers/Cybercrime_Report.pdf.

Joenniemi, Pertti. 2007. "Towards a European Union of Post-security?" *Cooperation and Conflict* 42 (1): 127-148.

Kirchner, Emil, and James Sterling. 2007. *EU Security Governance*. Manchester: Manchester University Press.

Malmström, Cecilia. 2011. "It's time to take cyber criminals offline Hungarian Presidency Cyber Crime Conference in Budapest Brussels, 13 April 201" [SPEECH/11/260]. Available at: http://europa.eu/rapid/press-release_SPEECH-11-260_en.htm.

Norton 2012. 2012 Norton Cybercrime Report. Available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

Portugal. 2007. "Tratado de Lisboa - Portugal 2007." Available at: [http://www.eu2007.pt/NR/rdonlyres/4B70DC8C-B9EF-4352-A48B-4CF2F201DC31/0/20071228Brochuras_PM.pdf].

Quille, Gerrard. 2008. “The Lisbon Treaty and its Implications for CFSP/ESDP”. Brussels: European Parliament. Available at: http://www.statewatch.org/news/2008/feb/ep-esdp-lisbon-study.pdf.

Smith, Michael E. 2004. *Europe’s Foreign and Security Policy: The Institutionalization of Cooperation*. Cambridge: Cambridge University Press.

Uçarer, Emeke M. 2001. “Sidekick No More: the European Commission in Justice and Home Affairs.” *European Integration Online Papers* (EIoP) 5. Available at: http://aei.pitt.edu/2197/1/Ucarer.pdf

UNDOC 2013. Comprehensive Study on Cybercrime. Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Wessels, Wolfgang, and Bopp Franziska. 2008. “The Institutional Architecture of CFSP after the Lisbon Treaty – Constitutional Breakthrough or Challenges Ahead?” 2. Available at: http://www.libertysecurity.org/IMG/pdf_The_Institutional_Architecture_of_CFSP_after_the_Lisbon_Treaty.pdf.