Final version submitted to the Journal of Common Market Studies, 13/2/2017 and published 12/05/2017

The EU as a coherent (cyber)security actor?

Helena Carrapico and André Barrinha[1]

The last three decades have seen the development of the European Union (EU) as a security actor. The transnational character of the security threats and the challenges identified by the EU have led to the progressive integration between internal and external security concerns. These concerns have often led to calls for greater coherence within EU security policies. The literature, however, indicates that this need for coherence has, so far, not been systematically operationalised, leading to a fragmented security field. This article has two main aims: to devise a framework for the analysis of the EU's coherence as a security actor, and to apply it to the cybersecurity field. By focusing on EU cybersecurity policy, this article will explore whether the EU can be considered a coherent actor in this field or whether this policy is being implemented according to different and uncoordinated rationales.

Introduction

The European Union (EU) is an intricate security actor, covering an increasing number of areas and policies, ranging from the environment to cyberspace. A characteristic trait of this complexification has been the emphasis put by the EU on the merging of internal and external security and on the need to develop policies, actors and instruments that are coherent within this security context (Bossong and Rhinard, 2013). As acknowledged by former European

1 The authors would like to thank the reviewers for their excellent comments, as well as the interviewees who made this article possible. They would also like to thank the Aston Centre for Europe and the RIEF funding 2016/2017 from Canterbury Christ Church University (QR funding for Politics and International Relations) for supporting their fieldwork through financial support.

Commissioner for Justice, Freedom and Security, Jacques Barrot, "Justice and Home Affairs (JHA) policies have increasingly had an impact on international relations and play a vital role in the European Union's (EU) external policies. Conversely, many of Europe's internal policy goals depend on the effective use of external policy strategies" (2009, p. 11). More recently, the *EU Global Strategy* also refers to the need for further integration between internal and external security: "In security terms, terrorism, hybrid threats and organised crime know no borders. This calls for tighter institutional links between our external action and the internal area of freedom, security and justice" (2016, p.50). However, as the degree of complexity in the EU's security increases, questions should be asked regarding the coherence underlining the combination of what is now a large plethora of instruments, actors and policies. The EU may be becoming an increasingly complex security actor, but is it becoming a more coherent one, as it purports to be?

This is a particularly relevant question when considering cybersecurity (Wessel, 2015). Recognising that information technology has become the backbone of European societies (European Parliament and Council, 2016), the EU has made cybersecurity one of its main security priorities. Such prioritisation has reflected itself not only at the level of new initiatives being proposed, but also in the idea that in order for the EU to be an effective cybersecurity actor it needs to be fully coherent. Cybersecurity questions a number of important dichotomies (internal/external, public/private, civilian/military) while, simultaneously, blurring the geographical distinctions between national, European and global levels (Kirchner and Speling, 2007). As a security area, it provides an ideal ground to assess the coherence of the EU's security *actorness*. On this basis, the present article proposes to investigate whether the EU is becoming a more coherent security actor in cyberspace. Specifically, the article aims at contributing to two

main bodies of literature: one on coherence and one on cybersecurity. Where the first is concerned, the article offers an innovative case study that points out that numerous coherence problems observed in other areas of security have spilled over to cybersecurity. Discussing coherence in this policy context implies focusing on the policies and institutions that sustain the EU's cybersecurity approach and contrasting them against the underlying security understandings within which they are framed. Although cybersecurity as a unified domain is still a recent field of action for the EU (the EU's first strategy in this area only dates to 2013), the article argues that it is possible to trace a search for coherence in this field prior to that point. Regarding the contribution to cybersecurity, the article proposes to add to this literature by offering conceptual tools to assess the EU's activities in this field from a coherence-base perspective. This mapping exercise will allow for the progressive assessment of the EU's developments in this field, by matching its practices against its official rhetoric and policy objectives.

In terms of structure, the article is divided into three sections. The first one explores how the concept of coherence has gradually been integrated into EU security policies and presents an analytical framework, which focuses on the institutional practices and shared security understandings along two axes: vertical relations (between member states, European institutions and private actors) and horizontal relations (within member states, European institutions and private actors). The second section introduces the EU's rhetoric on the importance of cybersecurity and of achieving coherence in this policy area. The third section applies the analytical framework to cybersecurity and contrasts the EU's practices of coherence with its rhetoric. It suggests that significant obstacles to a fully coherent policy approach are still visible

both in terms of horizontal and vertical relations. The article concludes by offering a few normative reflections on the EU's coherence as a cybersecurity actor.

I. Conceptual Reflections on Coherence as a key Organisational Principle of the EU

Coherence has long been a topic of policy and academic discussion, reflecting the positioning of this concept at the heart of the construction of the European project (Pomorska and Vanhoonacker, 2016; Cremona, 2008). Since the 1990s, the focus of this literature has been on the association of coherence with efficiency and on how best to achieve it, namely through the identification of areas suffering from capability-expectations gaps (Hill, 1993). Although the concepts of coherence and consistency have been abundantly explored in the academic literature, in particular the legal one (Van Vooren, 2012; Cremona, 2008), this article has chosen not to embark on a definitional discussion, but rather adopt the conceptualisation used by the EU. The reason for this choice is determined by the purpose of this article, which is to explore whether the EU is becoming a more coherent cyber security actor, according to its own proposed coherence objectives. In the European Security literature, this coherence is debated along the lines of whether the Foreign and Security Policy and the Area of Freedom, Security and Justice can be seen as coherent, including coherence within each individual policy area (Trauner, 2011; Missiroli, 2001) and across the different security policy areas (Pawlak, 2009).

For the purposes of this article, and having the European Commission documents as a guiding reference, we propose to adopt a dual definition of coherence as institutional coordination and as shared understanding of security (2014; 2006). The institutional coordination focuses on two

elements: operational and political, i.e. the concrete practices of the actors involved in the cooperative efforts (or absence of) on the one hand, and the political obstacles and incentives framing those relations, on the other. For these relations to be solid and fully coherent, they should be based on similar views about security, threats and potential responses between those same actors, which corresponds to the second coherence dimension considered in this article.

As the external and internal dimensions of security became more relevant within the EU framework, so did the perception of their increased blurring (Davis Cross, 2013; Trauner and Carrapico, 2012; Bigo, 2000). The emergence of a post-Cold War security environment led to the replacement of nuclear deterrence with the prospect of new non-state security threats, such as organised crime and terrorism (Tickner, 1995). In Europe, new transnational solutions, better adapted to these emerging threats and coherently articulating the EU's security *actorness*, had to be devised. Although there had been references to coherence since the early 1970s (Juncos, 2013), it is in the post-Cold War context that the concept of coherence starts to permeate EU discourse in a clearer way.

This shift in security priorities reflects a larger trend in the development of the EU legal order, in which coherence has gradually become one of the main constitutional principles (Cremona, 2008). The Maastricht Treaty, for example, was explicit about this goal: "The Union shall in particular ensure the consistency of its external activities as a whole in the context of its external relations, security, economic and development policies" (Art. C). Since then, the importance of developing and strengthening a coherent approach to European security has continued to expand (Commission, 2014, 2006; European Council, 1999). As a recent example, the European Agenda on Security stressed that "EU internal security and global security are mutually dependent and

interlinked. The EU response must therefore be comprehensive and based on a coherent set of actions combining the internal and external dimensions" (Commission, 2015, p. 4). The *Joint Framework on countering hybrid threats: a European Union response*, presented in 2016, follows the same line when it promotes "a holistic approach that will enable the EU, in coordination with member States, to specifically counter threats of a hybrid nature by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors" (2016, p. 3). As mentioned above, the same logic has now been replicated in the recently launched Global Strategy (2016).

The concept of 'coherence' is, in our view, currently at the heart of the EU's security *actorness* and strategic vision and it has been used to further justify institutional reform. It is the case, for instance, of the creation of the High Representative for Foreign and Security Policy, aimed at increasing coherence between EU institutions (Juncos, 2013). However, and despite having attracted substantial policy and academic attention, this is a concept that remains rather fuzzy and problematic.

Incoherent coherence?

For the European Commission, coherence should be equated with 'better strategic planning', 'better delivery and impact' and 'better co-operation' (2006, pp. 6- 9). The European Security Strategy mentions that coherence is about "bringing together different instruments and capabilities', 'better coordination' and 'unity of command'" (2003, p. 13). Despite some degree of specification, however, the concept of coherence remains considerably vague. A good

example of this fuzziness is the EU's interchangeable use of coherence and consistency, as explored in Missiroli's work. In his view, the usage of different terms is significant as, legally, consistency is defined as the "absence of contradiction", whereas coherence implies "an added value" (2001, p. 4). Politically, however, as the author concludes, such distinction is less relevant as "[b]oth terms hint at the need for coordinated policies with the goal of ensuring that the EU acts unitarily" (2001, p.4). The expectation is that by acting in a coordinated fashion, the EU will be a stronger actor. Despite having taken some important steps in that direction in the last few years, there is still, we argue, an important gap between rhetoric and practices between the EU's aspired role as a unified security actor and the developments carried out for that purpose (Argomaniz, 2009).

As mentioned in the introduction, assessing the EU's coherence in this field entails looking at both its institutional coordination and the existence (or not) of shared views on security, threats and potential responses. In table 1, each of these conceptualisations is analysed along a horizontal and a vertical axis (Nuttall 2005). The horizontal one includes the elimination of contradictions in terms of policies, agency and instruments, at EU level, as well as between member states and private actors, whereas the vertical axis explores the coordination between actors from a multilevel perspective (Biscop and Andersson, 2008).

[please insert table 1 here]

Coherence as institutional coordination should be understood as the optimal alignment of procedures, policy outputs, instruments and actors, necessary to tackle security threats that are not bound by national borders (Brattberg and Rhinard, 2012). According to the academic

literature (Wessel, 2015; Trauner, 2011), there is considerable indication that the proposed increase in coherence has not yielded the expected results in terms of coordination, leading to a capability-expectations gap (Hill, 1993). On the one hand, the EU has made considerable progress in terms of promoting common policy outputs, implementing new procedures to develop common instruments and encouraging security actors to work together[2]. On the other hand, however, issues of inter-institution and inter-agency conflict, overlap and lack of communication are said to be particularly worrying[3].

Coherence as shared understanding of security threats, implies looking at how different actors both vertically and horizontally define security as a concept and identify both the threats and ideal policy responses to best address them. In this area, clear progress in member states' convergence towards a number of security-related concepts (Calderoni, 2010), such as 'transnational organised crime group', 'human trafficking' or 'terrorism' has been reported. Despite these developments, authors such as Trauner (2011), have pointed out discrepancies in terms of how European values are applied in the context of the convergence between internal and external security. Although the EU argues that it is highly committed to the upholding of democracy, rule of law and fundamental rights, it is not unusual to observe the EU cooperating

2 The streamlining of internal procedures has been accelerated through the elimination of the pillar system and the replacement of unanimity voting with qualified majority voting in Justice and Home Affairs (Treaty of Lisbon, 2009). In addition, integrated security approaches have been promoted through the co-production of joint instruments, such as the Cyber Security Strategy (2013).

3 Referring to Civilian Crisis Management and to the division of labour between the Commission and the Council, Howorth highlights that the CSDP "missions embarked on to date have all revealed serious problems of inter-agency rivalry" (2007, p. 132).

with countries that do not share the same respect for these values[4]. If we focus specifically on the issue of convergence towards common threat understandings at national level, considerable differences have also been identified among national definitions (Calderoni, 2010).

The first section of this article proposed a conceptual mapping to analyse the level of coherence in EU security. The following section will now provide a detailed insight into the case study of cybersecurity, not only by exploring the origins and development of this policy field, but especially by focusing on the rhetoric of a policy field that is considered to represent one of the main successes in security coherence (European Commission, 2014). The mapping of the EU's rhetorical construction of its cyber security policy will then serve as a comparative basis for the third section and draw conclusions regarding the level of coherence of the area.

II. EU Cybersecurity as a Coherent Policy Field?

Cybersecurity is a broad term that covers occurrences and risks of different nature, from cybercrime and cyber-attacks to critical infrastructure and personal data protection (Klimburg and Tirmaa-Klaar, 2011). An indirect concern of the EU since the early 1990s (Porcedda, 2011), the origins of this policy can be found in the area of information and computer security, which later expanded to a comprehensive cybersecurity policy encompassing not only cybercrime but also critical information infrastructure protection and more recently cyber defence. According to the 1993 *White Paper on Growth, Competitiveness and Employment* and the 1994 Bangemann

4 For instance, the EU external border agency, FRONTEX, has coordinated operations where the EU intercepted suspected illegal migrants and handed them over to third countries, including to authoritarian regimes such as Qaddafi's Libya (Frontex, 2007).

report, information and communication technologies were seen as essential to the continued development of economies and the completion of the single market (European Commission; European Council). Both these documents already contained the idea that information and communication technologies would only benefit the economy if they were coherently articulated and integrated with older sectors of activity. The EU's interest for cybersecurity thus started off as an economic concern, which was related to the advancement of the Single Market, and whose association to a coherent economic policy appears from an early stage.

The addition of a security rationale to the already existing economic one occurred towards the end of the 1990s, driven by the international community's interest for computer- related crime (Commission, 2001). The development of this security rationale also reflected itself within the EU's rhetoric, which was by then particularly worried about illegal and harmful content on the Internet, as well as rapidly growing high-technology crime (Council, 1997). From the late 1990s to the mid- 2000s, a flurry of non- legally binding instruments and initiatives emerged in this area, aimed at fostering member state awareness and shared concern. Examples of such instruments include the introduction of the term high tech crime in Council conclusions for the first time in 1999 (Council, 1999); the *eEurope 2002* action plan, which focused on fostering a more secure Internet in order to create the most dynamic knowledge- based economy in the world (Council, 2000); and the 2000 Commission Communication on improving the security of Information Infrastructures and combating computer-related Crime (Mendez, 2005). Similarly to the international shift, the idea of coherence also moved in the direction of increased cooperation at EU level.

Notwithstanding the above-mentioned evolution, cybersecurity did not become a top security

priority until the mid-2000s (even the 2003 European Security Strategy was notably silent on the topic). The change emerged with the growing realisation that information systems and technologies were vulnerable to external attacks, particularly of a terrorist nature (European Commission, 2004). This shift led to two main outcomes: 1) the move from non- legally binding to legally binding instruments, as was the case of the 2005 Council Framework Decision on *Attacks against Information Systems*; and 2) the further reinforcement of the idea of coherence as a necessary element of efficiency and as a desirable result best achieved by the EU level. Both outcomes were connected by the perception that organised crime and terrorism represented a clear threat to the achievement of a safer information society, which was being put at risk by the existence of gaps and differences, and indeed gaps, between member states' laws. The national level was presented as being insufficiently equipped to adequately answer to these increasingly transnational threats and a common approach, characterised by approximation and developed at EU level was, instead, introduced as a necessary response (Council, 2005).

Since then, there has been a clear effort to consolidate the EU's activities in the field, namely by raising public awareness, by investing in a comprehensive and coherent strategy and corresponding instruments, such as the recently approved NIS Directive. As the second part of this section will demonstrate, the EU's consolidation efforts have been focused on the three main pillars of this policy's institutional architecture: cybercrime, critical information infrastructure protection (CIIP) and, to a lesser extent, cyber defence.

Consolidating a coherent EU cybersecurity policy

There has been a concerted attempt within the EU to promote coherence throughout the field.

The publication of the 2013 EU Cyber Security Strategy (EU-CSS) is particularly representative of the push towards increased coherence, as it resulted from a combined effort between then Home Commissioner Cecilia Malmström, High-Representative Catherine Ashton and DG Connect Commissioner Neelie Kroes, with the input of DG JUST (Fahey, 2014). The EU-CSS rests on three main action pillars – critical information infrastructure protection, cybercrime, and cyber defence (European Commission and HREU, 2013). The creation of the strategy aimed at improving the coordination between these three dimensions, which gradually came to be included in the area of cybersecurity but were still regarded as fairly separate (Christou, 2016). Critical information infrastructures correspond to physical and information technology facilities or services that are essential to society (health services, water and energy networks, telecommunications, banking), which, if disrupted, could seriously affect the wellbeing of citizens (Dunn Cavelty and Kristensen, 2008). Cybercrime refers to a large set of different criminal activities where computers and information systems constitute either the primary tool of the attack or their main target (Commission, 2007). Finally, cyber defence covers the safeguarding of the communication and information systems at the basis of national defence mechanisms (European Commission and HREU, 2013).

As previously mentioned, coherence in the EU's security approach can be divided into two broad categories: 1) Institutional cooperation and 2) Shared understanding of security. Where the first is concerned, considerable rhetorical emphasis is being put on the development of a common approach to cybersecurity based on the enhancement of cooperation among actors, instruments and policies (European Commission and HREU, 2013). Institutional cooperation is understood as being particularly important given that the European governance of cybersecurity is rather

decentralised, with relevant bodies to be found in the public and private sectors. In addition to national cybersecurity authorities and international bodies such as the Council of Europe, the main actors in cybersecurity include: DG Migration and Home Affairs (cybercrime), the European Cybercrime Centre (EC3) (cybercrime), the European External Action Service (cyber defence), the European Defence Agency (EDA) (cyber defence), DG for Communications Networks, Content and Technology (network and information security), the European Network and Information Security Agency (ENISA) (network and information security) and Computer Emergency Response Teams (CERTs) (cybercrime).

Cooperation with the private sector is also understood as essential, as companies are considered to have a better insight into the practices of cybercrime (either as victims or as producers of anti-cybercrime products), and critical information infrastructures are often in the hands of the private sector (European Commission and HREU, 2013). In order to reinforce the need for intra-actor coherence, a Cooperation Group has been proposed by the Directive on security of network and information systems (NIS Directive) that entered into force in August 2016 (Directive (EU) 2016/1148). Similar trends can be observed regarding instruments and policies. Considerable emphasis has been put on harmonising member states' capabilities and infrastructures, and on ensuring a minimum level of requirements among private sector actors to allow cooperation to take place from a technical point of view (Directive (EU) 2016/1148). There is also a clear interest in ensuring that cybersecurity is being mainstreamed into larger policy areas, namely EU external relations and Common Foreign Security Policy (European Commission and HREU, 2013). Cybersecurity has recently been framed as a priority area in the EU Global Strategy (2016).

Coherence as shared understanding of security is directly connected with the perceived need for a EU-wide approach to cybersecurity: "attacks against private or government IT systems in EU member States have given [cybersecurity] a new dimension, as a potential new economic, political and military weapon" (Council, 2008, p. 5). This need for a more common approach implies the encouragement of a holistic effort by all stakeholders, including international partners, the private sector and civil society (European Commission and HREU, 2013). There is the clear perception that cyber insecurity cannot be controlled directly by state institutions and therefore requires the full collaboration of the different sectors of society. Security is understood in this context as collaborative, preventive and resilient. Furthermore, it is also an understanding of security that is intimately tied with the promotion of EU values and principles: "Cyber security can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values" (European Commission and HREU, 2013, p.4). This issue has been rather salient with regard to the post-Snowden relations between the EU and the United States where divergences between both – particularly regarding privacy and data protection – have been visible regarding the fundamental norms that underpin governance in cyberspace (Bendiek, 2014; Christou, 2016).

III. From Rhetoric to Practices

Following this analysis of the EU's cybersecurity rhetoric, this article will now more thoroughly assess whether the EU can be considered a coherent actor in this field. The analysis will proceed by first exploring the differences between rhetoric and practices within the horizontal axis (inter-

institutional relations at the different EU, national and private levels), and then within the vertical axis (relations between member states and the EU, and between these actors and the private sector).

[please insert table 2 here]

Horizontal Relations

Europe, the EU included, has been witnessing a shift towards a greater awareness of the importance of cybersecurity and the need to mainstream it into all areas. Interviews conducted with EU and national officials in Brussels have confirmed the growing centrality of cybersecurity in policy discussions. The EU Global Strategy was unambiguous about it: "The EU will be a forward-looking cyber player, protecting our critical assets and values in the digital world" (2016, p.42). However, the interviews also revealed that despite these important steps, much remains to be done to achieve coherence in this area. As a security field, and when compared with other major cybersecurity players, the EU's actorness in cyberspace is still rather limited (Christou, 2016) and it faces multiple challenges, including inter-institutional coordination and other factors that limit its operational capacity, such as financial investment and human resources. When making the distinction between operational institutional cooperation and political cooperation, the former is presented as less problematic and having progressed quicker whereas the latter seems to have remained a more sensitive area (interview, CERT EU, 2016). Let us look at the different levels of the horizontal analysis to better unpack these differences.

As mentioned above, cybersecurity is now a policy priority for EU institutions (Kroes 2012b, p. 3). Present and future measures in the European security field will prioritise cyberspace, as made clear in the EU-CSS (2013), in the December 2013 European Council Conclusions, the *European Agenda on Security* (2015), the *Joint Framework on countering hybrid threats: a European Union response* (2016) and the *EU Global Strategy* (2016). In fact, the EU institutional architecture has developed considerably since 2004, with the creation of specialised agencies, such as ENISA and Europol's EC3, as well as coordination mechanisms such as the Horizontal Working Party on Cyber Issues, specifically created to offer additional coordination between member states. The latter has succeeded the Friends of the Presidency Group on Cyber Issues and is responsible for bringing a large range of cyber related topics to the attention of COREPER and the Council in order to ensure coherence between areas as different as criminal justice in cyberspace and cyberdiplomacy (Council, 2016). There is now a much clearer idea of who the key stakeholders in the field are and where the need for greater coherence lies (interview, German Permanent Representation, 2016). The NIS Directive (European Parliament and Council, 2016) appears to further contribute to this by bringing together the European Commission, member states and ENISA as members of the new Cooperation Group, which has been created to offer strategic guidance and facilitate cooperation between member states on information security.

Bendiek refers to this progress when she mentions that "this cooperation finds expression in the joint meetings of the Political and Security Committee (PSC) and the Committee on Operational Cooperation on Internal Security (COSI), as well as in the joint sessions of the Parliamentary Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Committee on Foreign

Affairs (AFET)" (2012, p. 20). It is also embodied in the mutual representation of ENISA in the EC3 board and vice-versa. The two agencies signed a cooperation agreement in 2014 that contributed to a higher level of coordination between them. More recently, they have been developing a common taxonomy for practitioners to refer to cyber incidents, a common format for relevant information and a mechanism for information exchange (ENISA, 2015b). EEAS representatives also sit on the board of EC3. In fact, interviews conducted by the authors in 2015 and 2016 reveal an emerging 'cybersecurity community' across EU institutions that is based upon a culture of communication, coordination and the acknowledgment of limited resources (interview, EEAS, 2015; interview, Commission, 2016).

The attempt to increase coordination has not, however, always resulted in coherent inter-institutional work. On the contrary, the EU's approach to cyberspace continues to be fragmented, (Klimburg and Tirmaa-Klaar, 2011; Christou, 2016), and possesses characteristics of an emerging policy field with a "lack of clearly delineated areas of responsibility and accountability among the different institutions" (Bendiek, 2012, p. 12). There are coordination problems between, but also within institutions, which are related to the historical evolution of the different cybersecurity areas, as well as the perception that each area still experiences different separate challenges. It is not unusual to find projects whose objectives clash with those of other institutions (interview, European Parliament, 2016). Furthermore, states, via the Council, seem to be more reluctant than other institutions (such as the European Parliament) to enhance EU powers in this area (interview, CERT EU, 2016).

As a consequence, the allocated resources are often extremely low when compared with other security areas and other parts of the world. For instance, in 2013 the Pentagon requested USD 3.2 billion worth of funding be allocated to cybersecurity (Comninos, 2013). Comparatively, the EU's network and information security agency, ENISA, has an annual budget of €11 million (ENISA, 2016), the European Cybercrime Centre, EC3, had an initial budget of €7 million (BBC News, 2013), and until recently the European External Action Service (EEAS) had only four people working on cybersecurity (Renard, 2014b, p. 14).

Regarding the level of coherence at the national level, the problems are similar, although more acute. Cybersecurity is regarded, on the one hand, as a sensitive area where the sharing of information does not come naturally to all member states, and on the other hand as an emerging area which is new to many countries (an idea consensually shared by all the stakeholders interviewed in Brussels for this article). Whereas member states such as France, Germany, the Netherlands and Italy would like to go further than the current EU cybersecurity framework, other countries prefer forms of sub- regional cooperation. One such example is the Visegrad countries plus Austria, who created the Central European Cyber Security Platform (CSCSP) that promotes cooperation between their respective CERTs and Computer Security and Incident Response Teams (CSIRTs) (interview, CERT EU, 2016). The problem of differing priorities does not lie only in political preferences but also in security capabilities, including the necessary institutional framework to exchange information with other countries and the capacity to conduct cybercrime and cyber defence operations. Where the first is concerned, there is still no agreement regarding the most appropriate model for the collection and sharing of information between member states (interview, European Parliament, 2016). There is also the issue that

national authorities have different models of cybersecurity coordination at national level, which further complicates the choice of a model for information exchange (Christou, 2016; Guitton, 2013). Furthermore, not all countries are ready to make the financial commitment that is involved in creating the necessary infrastructure and as a result tend to not prioritise cybersecurity (interview, European Parliament, 2016). This difference in capabilities and prioritisation is particularly visible in the number of existing national cybersecurity strategies among EU member states, which in 2016 was still limited to 23 (ENISA, 2016). The NIS Directive recognises these discrepancies between member states, suggesting that this "results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union" (European Parliament and Council, 2016, p. 2).

Regarding the level of private actors, we can also identify similar coherence problems. As mentioned previously, the private sector plays a central role in this security area: it acts as an agenda setter – as it raises awareness of specific trends – and as a partner to EU institutions and member states (interview, European Parliament, 2016). The fulfilment of this role also implies a considerable amount of intra-sector cooperation. In particular, ENISA feels that it is extremely important for different sectors of the economy to collaborate on the development and adoption of security standards in order to better protect consumers, the Digital Single Market and the industries themselves from cyber-attacks (2015a). However, there is indication that the level of coordination among companies and levels of cybersecurity maturity vary considerably depending on the sector of activity. Whereas the financial sector is more open to cooperation, the telecommunications one is more hesitant (interview, Commission, 2016). The hesitation can in

part be explained by the fear that information exchange could result in the eroding of a competitive edge (interview, European Parliament, 2016; Giacomello, 2014).

Vertical Relations

When asked about the coherence between the EU, national and private actors levels, most of the interviewees agreed that we have witnessed an increase in coherence, linked to the Europeanisation of national approaches to cybersecurity. The Europeanisation has become visible in the greater awareness of cybersecurity issues and in gradual development of cybersecurity standards. This trend is particularly linked to three main elements: 1) the perception that cybercrime is increasing; 2) the response to the massive usage of the Internet and digital services; 3) the reaction to international cyber-attacks and their impact on countries such as Estonia and The Netherlands (interview, German Permanent Representation, 2016). Despite growing Europeanisation, cybersecurity in Europe "remains almost exclusively a national prerogative" (Renard, 2014a, p. 13). This point is particularly relevant, given the EU's claim, as seen above, that cybersecurity is too complex and too transnational in nature to be left to member states. In 2012, officials from the European Commission publicly criticised the low level of preparedness of a considerable number of member states (Nielsen, 2012). The problems of coordination that were described above among member states also reflect themselves in the cooperation between member states and EU institutions. Brussels often has difficulty convincing member states of the importance of furthering integration in this area, often resorting to projects 'á la carte' where national participation is voluntary as is the case of EDA projects. The problem, however, is not stemming only from the national level. The Network and Information Directive is a specific example which could lead to coordination problems and a lack of coherence,

particularly regarding the division between network information infrastructure bodies and law enforcement ones, as EC3 plays a very limited role in the directive (Parliament and Council, 2016: 9).

In terms of cooperation between private and public actors, similar problems emerge. Although public private partnerships (PPPs) are widespread in this sector, their level of cooperation varies considerably and there is often a degree of uncertainty regarding what the partners can offer each other (interview conducted in Brussels, 2016). One of the problems, long identified, but not yet solved, is the existence of diverging interests where the private sector privileges efficiency and profit, and the public sector prioritises security (Dunn Cavelty, 2009). According to Bossong and Wagner (2016), this divergence in interests reflects itself well in the large multitude of ill-defined forms of public-private cooperation in the area of cybersecurity. These authors show through a comparative study of many PPPs in this area that these forms of cooperation often remain at the rhetorical level because they have little to offer to the private side. As an example, an ENISA report from 2015 revealed that the main PPP led by this agency, the European Public Private Partnership for Resilience (E3PR), failed to produce meaningful results because of multiple conflicts of interests relating to the costs of mandatory security measures and of data confidentiality (2015c)[5]. This divergence eventually affects the level of trust between partners, which is essential for information sharing regarding the disclosure of cyber-attacks at national level. Finally, PPPs also have the problem of being too narrow and not taking into account the level of integration of specific markets (Dunn Cavelty, 2009): a PPP focusing on the protection

5 In addition to E3PR, other PPP-related initiatives can also be found in the NIS Public- private Platform, which was proposed in the EU Cybersecurity Strategy of 2013. More recently, a contractual Public- private Partnership (cPPP) has also been signed in this area in July 2016 with the aim of structuring and coordinating digital security industries in the EU.

of electric grids might not consider the security of third party companies, which the electric grid relies on to produce energy.

Overall, we could argue that there is a contradiction within the EU's vertical axis of cybersecurity: on the one hand, it clearly highlights the limits of national approaches, both due to the transnational character of the threats and to the heterogeneous approach to the field, and, on the other hand, it promotes, in its strategy, "a decentralized organization, where cybersecurity governance remains in the MS, while the EU supports capacity building, ensures consistency across MS, and facilitates coordination and outreach" (Ramunno, 2014, p.1).

Conclusion

Our understanding of European security in 2016 is certainly less assertive than a decade ago, when authors such as Allen G. Sens argued that "[t]he EU will increasingly become the institutional centre of gravity for security policy deliberation, coordination and action by European governments" (2007, p. 25). However, even if such favourable view of the EU's security actorness is far from being accomplished, one cannot deny that in areas, such as cybersecurity the EU is gradually becoming an important actor (Christou, 2016; Wessel, 2015). If to this we add the increasingly complexity of issues the EU needs to deal with (from border management to counter-terrorism), it becomes clear that a coherent EU might be necessary to tackle the multiple security issues that affect its citizens and members states.

The mapping presented above allows for a structured approach to the issue of coherence in EU security, focusing both on the vertical relations between the EU, its member states and private

actors, and on the horizontal relations between its multiple institutions and agencies. Focusing on the specific case of cybersecurity, it was possible to conclude in this preliminary study, that the EU has an explicit ambition to be a coherent security actor. However, both the architecture put in place under the EU-CSS and the resistance from member states to allow the EU to have a more stringent control over their cyber activities, limit the EU's coherence in the field. That said, both the rising political importance given to cybersecurity and the progressive consolidation of what is still a rather recent field of activity, means there are signs the EU might move towards a more coherent actorness in the field.

We should, however, conclude this article on a cautionary note. When discussing the coherence of the EU as a security actor, there are a few normative assumptions that are, by default, associated with it. First, and foremost, the idea that it is better for the EU to act as a unitary actor, as that will mean a more 'effective' EU. This is an assumption that is far from self-evident, at least in the realm of foreign policy, where the EU "has often achieved unanimity at the expense of effectiveness". Furthermore, "a policy can be effective without necessarily being consistent (as the 'carrot-and stick' metaphor and the good cop-bad cop' example epitomise)" (Missiroli, 2001, p. 5). Second, there is also the notion that a more coherent Union is, in the security field, a more integrated union where different policy areas coincide to offer the best possible toolkit of action. In such a case, security threats are presented in a spectrum where continuity, rather than difference, occupies central stage, but that ultimately, might encourage an exaggeration of connections between them" (Anderson, 2007, p. 43). Finally, the idea that a more effective EU is 'a good thing' due to the values it portrays, as visible in the European Security Strategy: "An active and capable European Union would make an impact on a global scale. In doing so, it would contribute to an effective multilateral system leading to a fairer, safer and more united

world" (2003, p. 14). That might not always be the case. As alerted by Bendiek, "regulative strategies such as the planned EU strategy on cybersecurity cannot be measured only by their efficiency. Instead, they also have to fulfil the fundamental criteria of democratic governance: transparency, rule of law, accountability and participation." (Bendiek, 2012, p. 26). Particularly in the field of cybersecurity, where decision-making "is characterised by a lack of transparency and accountability" (Bendiek, 2012, p. 24), it is fundamental that we understand that a coherent actor must also be coherent with the values it defends.

References

Anderson, M. (2007) 'The Changing Politics of European Security' in Ganzle, S. and Senz, A. G. (eds.) *The Changing Politics of European Security. Europe Alone?* (London: Palgrave), pp. 31-46.

Argomaniz, J. (2009) 'When the EU Is the "Norm-taker":The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms'. *Journal of European Integration*, Vol. 31, No.1, pp. 119–137.

Barrot, J. (2009) 'Overview of the role of JHA policies in improving global security by fighting organised crime and terrorism'. In von Wogan, K. (ed.) *The Path to European Defence. New Roads* (New Horizons. London: John Harper Publishing), pp. 11-13.

Bendiek, A. (2012) 'European Cyber Security Policy', *SWP Research Paper* No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paper-detail/article/european_cyber_security_policy.html Accessed 22 August 2014

Bendiek, A. (2014) 'Tests of Partnership', SWP Research Paper No5. Available at http://www.gmfus.org/ archives/tests-of-partnership-transatlantic-cooperation-in-cyber-security-internet-governance-and-data-protection/
Accessed 20 November 2016.

Bigo D. (2000) 'When two become one'. In Kelstrup, M. and Williams, M. C. (eds), *International Relation Theory and the politics of European Integration, Power, Security and Community* (London, Routledge), pp. 171-205

Biscop, S. and Andersson, J. (2008) *The EU and the European Security Strategy: Forging a Global Europe* (Abingdon, Oxon: Routledge).

Bossong, R. and Rhinard, M. (2013) 'The EU Internal Security Strategy: Towards a More Coherent Approach to EU Security?'. *Studia Diplomatica*, Vol. LXVI, No. 2, pp. 45- 58.

Bossong, R. and B. Wagner (2016) 'A Typology of Cybersecurity and Public- Private Partnerships in the Context of the EU', Crie, Law and Social Change. Doi:10.1007/s10611-016-9653-3.

Brattberg, E. and Rhinard, M. (2012) 'The EU as a global counter-terrorism actor in the making'. *European Security*, Vol. 21, No. 4, pp. 557-577.

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

Comninos, A. (2013) 'A Cyber Security agenda for civil society: what is at stake?', APC Issue Papers, April, Available at http://www.apc.org/en/pubs/cyber-security-agenda-civil-society-what-stake

Council of the European Union (2016) *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. Brussels. Available at https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union Accessed 09 August 2016.

Council of the European Union (2016) Establishment of a Horizontal Working Party on Cyber Issues- Terms of Reference. 17 October 2016. No 11913/2/16.

Council of the European Union (2005) 'Council Framework Decision on Attacks against Information Systems'. *Official Journal of the European Union. L 69/67. 16/03/2005.*

Council of the European Union (2003) *A Secure Europe in a Better World*. Brussels. Available at https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf Accessed 14 August 2014.

Council of the European Union (1997) 'Action Plan to Combat Organised Crime'. *Official Journal of the European Communities*. 15 August 1997. No C 251/1.

Cremona, M. (2008) 'Coherence through Law: What Difference will the Treaty of Lisbon make' *Hamburg Review of Social Sciences*, Vol. 3, No. 1, pp. 11- 36.

Dunn Cavelty, M. and Sutter, M. (2009) 'Public- private Partnerships are no Silver Bullet: an expanded governance model for critical infrastructure protection'. *International Journal of Critical Infrastructure Protection*, Vol. 2, pp. 179- 187.

Dunn-Cavelty, M. and Kristensen, K. S. (2008) *Securing 'the Homeland': Critical Infrastructure, Risk and (in)Security* (London, Routledge).

ENISA (2015a) *Information Security and Privacy Standards for SMEs*. December. The Hague.

ENISA (2015b) *Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement*. December. The Hague.

ENISA (2015c) *E3PR 2009- 2013 Future of NIS Public Private Cooperation*. The Hague.

European Commission (2014) *Communication from the Commission to the European Parliament and the Council on The Final Implementation Report of the EU Internal Security Strategy 2010-2014.* 20 of June. COM (2014) 365 final.

European Commission (2006) *Communication from the Commission to the European Council of June 2006: Europe in the World- Some Practical Proposals for Greater Coherence, Effectiveness and Visibility*. 8 June. COM (2006) 278 final.

European Commission (2004) *Communication from the Commission to the Council and the European Parliament: critical infrastructure protection in the fight against terrorism*. 20 October, COM (2004) 702 final.

European Commission (2001) *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer- related Crime*. 26 January, COM(2000)890 final.

European Commission and European External Action Service (2016) *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats: a European Union response*. 6 April, JOIN(2016) 18 final.

European Council (1999) *Tampere Council Conclusions*, 15- 16 October, Tampere.

European Council (2008) *Report on the Implementation of the European Security Strategy- Providing Security in a Changing World*. 11 December, S407/08.

European Parliament and Council (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, 19 September 2016, L 194/1.

European Parliament and Council (2013) *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*. Official Journal of the European Union, 18 June 2013, L 165/41.

European Parliament and Council (2004) *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.*

European Union External Action Service (2016) 'Ongoing Missions and Operations', *European Union External Action Service webpage*, Available at http://www.eeas.europa.eu/csdp/missions-and-operations/index_en.htm. Accessed 1 May 2016.

Fahey, E. (2014) **'**EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security'. *European Journal of Risk Regulation*, Vol. 5, No. 1, pp. 46-60.

Giacomello, G. (2014) 'Introduction: security in cyberspace'. In Giacomello, G. (Ed.) *Security in Cyberspace- targeting Nations, Infrastructures, Individuals* (London: Bloomsbury).

Guitton, C. (2013) 'Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?'. *European Security*, Vol. 22, No. 1, pp. 21- 35.

Hill, C. (1993) 'The Capability–Expectations Gap, or Conceptualizing Europe's International Role'. *Journal of Common Market Studies*, Vol. 31, No. 3, pp. 305–28.

Juncos, A. (2013) *EU Foreign and Security Policy in Bosnia: the Politics of Coherence and Effectiveness* (Manchester: Manchester University Press).

Missiroli, A. (2001) 'Introduction'. In Missiroli, A. (ed.), *Coherence for European Security Policy: Debates-Cases-Assessments*. Occasional Paper No. 27, Institute for Security Studies, Western European Union, Paris.

Monar, J. (2014) 'The EU's growing role in the external AFSJ domain: factors, framework and forms of action'. Cambridge Review of International Affairs, Vol. 27, No. 1, pp. 147-166

Nielsen, N. (2012) 'EU Cyber-security legislation on the horizon', *EU Observer*. Available at http://euobserver.com/justice/116239 Accessed 22 August 2014.

Nuttall, S. (2005) 'Coherence and Consistency'. In Hill, C. and Smith, M. (eds.) *International Relations and The European Union* (Oxford: Oxford University Press), pp. 91 - 112.

Pawlak, P. (2009) 'The External Dimension of the Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-pillarization?'. *Journal of European Integration* 31, No. 1, pp. 25–44.

Pomorska, K. and Vanhoonacker, S. (2016) 'Europe as a Global Actor: Searching for a New Strategic Approach'. *Journal of Common Market Studies*. DOI: 10.1111.

Ramunno, G. (2014) 'EU Cyberdefence strategy'. *European Union Military Committee*, Vol. 6, May 2014.

Renard, T. (2014a) *Partners in Crime? The EU, its Strategic Partners and International Organised Crime*. ESPO Working Paper No. 5, European Strategic Partnership Observatory.

Renard, T. (2014b) *The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security*, ESPO Working Paper No. 7. Available at http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf

Sens, Allen G. (2007) 'The Challenging Politics of European Security'. In S. Ganzle and A. G. Senz (eds.) *The Changing Politics of European Security. Europe Alone?* (London: Palgrave), pp. 1-28.

Tickner, A. (1995) 'Re-visioning Security'. In K. Booth and S. Smith (Eds.) *International Relations Today* (Cambridge, Oxford: Polity Press).

Trauner, F. and H. Carrapico (2012) 'The External Dimension of Justice and Home Affairs after the Lisbon Treaty: analyzing the dynamics of expansion and diversification'. *Foreign Affairs Review*, Vol. 17 (special issue), pp. 1- 18.

Trauner, F. (2011) 'The Internal- external security nexus: more coherence under Lisbon?', *Occasional Paper* No. 89, Paris: European Union Institute for Security Studies.

Van Vooren, B. (2012) *EU External Relations Law and the European Neighbourhood Policy- A Paradigm for Coherence*. London: Routledge.

Wessel, R. A. (2015) ‘Towards EU Cybersecurity Law: Regulating a New Policy Field’, in N. Tsagourias and R. Buchan (Eds.), Research Handbook on International Law and Cyber Space, Edward Elgar Publishing, pp. 403-425.

Table 1 - Coherence in the security field

	Horizontal Axis	Vertical Axis
Institutional coordination/integration	Are member states' security institutions/ bodies coordinating policies and instruments efficiently at national level? Are EU institutions coordinating initiatives efficiently at European level? Is there coordination between private companies in the area of security?	Are member states and EU institutions coordinating effectively across security policies? Are European institutions gaining competences in the area of security? Is the private sector, as an emerging actor in European security, coordinating effectively with member states and EU institutions?
Shared understandings Threats, approaches, responses	Has there been an approximation or harmonization of national understandings of specific security threats? Do member states prioritise a European response to security issues? Do European institutions share the same understanding of security threats? Are threat responses framed within a similar conceptual framework? Does the private sector project a shared understanding of security threats?	Are member states' understandings of security threats similar to those of EU institutions? Do EU documents reflect national security understandings? Do member states apply at national level the security threat definitions used in EU documents? Does the private sector share the same understandings of security threats as the State sector?

Table 2 - Coherence in the cybersecurity field

	Horizontal Axis	Vertical Axis
Institutional cooperation	Growing culture of coordination between EU institutions, visible through increase in number of official documents referring to the need for closer coordination and through representation of EU bodies in management boards (namely EC3, ENISA and CERT EU). However, increased rhetorical coordination has not produced evidence of coordinated practices. Coherence is hindered by limited financial resources, low staff numbers and confusing division of labour. Lack of evidence of greater coordination among private actors through efficient self- regulation and the setting of benchmarks.	There are clear problems of coordination between the EU level and the national one due to different levels of preparedness of member states. Cybersecurity governance remains the responsibility of member states. Fragmentation of the European approach through the creation of sub-regional partnerships. ENISA and EC3 are gaining new competences in the area of cybersecurity and their influence in shaping national policies has also increased. There is evidence of the willingness of the private sector to collaborate in cybersecurity governance, but results have so far been limited.
Shared understandings Threats, approaches, responses	Growing rhetoric on shared cybersecurity threats both at the EU and at national level through the production of official documents. However, member states' commitment to a shared understanding of cybersecurity is not always clear. Lack of evidence regarding whether the private sector shares the same understanding of cyber threats. Prevention and preparedness practices show that not all companies share the same understanding of risk.	member states have added responsibilities, given the central role they assume in Europe's cybersecurity architecture, but they, overall share the same threats and concerns. They do not, however, share the same responses, due to different levels of cybersecurity development and lack of trust. Only part of the private sector shares the EU and national concerns as responses continue to diverge considerably.