EUSA, Boston 2015

Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy

Robert Dewar, University of Glasgow

Abstract

Cyberspace offers unique opportunities for communication and commerce, but also a wide range of security threats both to individuals and nation states. These threats create specific security challenges. This paper will examine the impact of the Treaty of Lisbon on the EU's response to those challenges. Prior to the coming into force of the Lisbon Treaty in 2009 EU cybersecurity policy was highly fragmented. Responsibility was split between the three Pillars of the European political system: the Communities, justice and home affairs and the common foreign and security policy (CFSP). By abolishing the Pillar system the Lisbon Treaty enabled the EU to develop a single, unified, strategic approach to cybersecurity issues. The 2013 Cybersecurity Strategy was a direct result of this newly-established capacity for coherence. However, the key area of competence relating to the CFSP was left largely undefined in the Lisbon Treaty, limiting the EU's capacity to respond to external cyber-threats. This paper will evaluate how the new legal personality of the Union and the abolition of the Pillar system affected both internal and external cybersecurity policy by examining one of the Treaty's most significant "loose ends": CFSP. It will argue that cybersecurity and external cyber-defence serve as a microcosm of a much wider problem of unresolved and undefined competences. While the Lisbon Treaty facilitated a coherent internal strategy, clarification of EU competence regarding the CFSP was left largely unresolved, a fact demonstrated by the nature of cybersecurity challenges. By examining the EU's cybersecurity policy and strategy this paper will further argue that the EU's approach can be seen as an exemplar of the successes and challenges of post-Lisbon European politics.

Introduction

The Treaty of Lisbon has had a profound impact on EU policy development and implementation. It amended the Amsterdam and Maastricht Treaties and repackaged them as the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). These Treaties now form the basis of all legislative acts of the EU and its structure and established the Union as a single legal entity. In this new structure the European Parliament was elevated to a position of co-decision with the Council of the European Union, a permanent office of President of the European Council was founded and the European Council itself

formalised as an official institution of the EU. In addition the pillar system of policy development and implementation was abolished, enabling previously disparate agencies and Commission Directorates General (DGs) to work together.

This major institutional change had equally profound impacts on key areas of EU policy. The new European External Action Service (EEAS) now acts as an unofficial if de facto foreign service, acting on behalf of the High Representative of the Union for Foreign Affairs and Security Policy, developing the EU's role as an international actor in both security and peaceful pursuits. The streamlining of competencies in the new TEU and TFEU clarified the levels of action for the EU in fields as diverse as sports policy, agriculture, the internal market, marine resources and the environment. One area where the Treaty of Lisbon has had a considerable impact is cybersecurity, in particular the manner in which the European Commission and its DGs approach that policy field.

The security challenges arising through an increased use of the online sphere in civilian, commercial and government life are many and varied. They touch on almost all aspects of the EU's policy portfolio including criminal justice, the common foreign and security policy (CFSP) and protection of personal data and critical infrastructure. The Treaty of Lisbon had three key impacts on EU policy in this field. First, it abolished the pillar system instituted in the Maastricht Treaty. Under this institutional architecture the various elements cybersecurity were handled by Commission DGs, institutions and agencies operating independently of one another, creating great inefficiency and duplication. The abolition of the pillar structure enabled entities dealing with foreign affairs and internal market security, previously separated under

the pillar system, to work together to develop a truly unified, holistic approach to cybersecurity.

The Treaty of Lisbon also clarified areas of competence, for example in cyber-crime. It provided DG HOME with the right of enforcement of key pieces of hard and soft legislation. Finally, in establishing the EEAS and confirming the EDA as an EU agency (Howorth, 2013, pp. 13–15), the Treaty enabled the EU to address the internationality inherent in cybersecurity challenges.

Cybersecurity policy can therefore showcase the best that the Treaty of Lisbon has to offer: its capacity for efficiency and coherence; its enabling of joint-working between previously separated agencies and institutional departments; and a holistic strategy unattainable under the pre-Lisbon pillar system. However, all is not perfect. While the Treaty of Lisbon enabled international cybersecurity issues and defence to be incorporated into a single strategic approach, the general competence of the new EU in foreign and security affairs remains unresolved. There is a disconnect between the existence of competence and the use of competence (Craig, 2010, p. 184). The EU is undertaking military missions around the world under the aegis of the CFSP, establishing itself as an important international actor. Yet EU officials themselves insist that the EU has no competence in foreign or military affairs. For cybersecurity issues, particularly in relation to cyber-defence and the combatting of alleged state-sponsored or sanctioned cyber-incidents, this disconnect is particularly problematic. Given the inherently international nature of cybersecurity threats and the impact of those threats on the EU's commercial viability, the EU cannot be seen to lack a concerted response. Yet its own officials argue that it has no competence to provide such a response. Cybersecurity therefore highlights a significant

weakness in the Treaty of Lisbon: unclarified competences in CFSP. By using the EU's cybersecurity policy as an exemplar of both the strengths and the weakness of the Treaty of Lisbon, this paper will therefore argue that cybersecurity and the policy of the EU in that field serve as a microcosm of a much wider problem of unresolved and undefined competences.

The paper will proceed in three sections. The first will examine the situation in EU cybersecurity policy prior to the entry into force of the Treaty of Lisbon. The policy development of the EU in the field of cybersecurity will be examined and situated in context with the nature of cybersecurity itself in order to demonstrate the fragmentation of the Union's approach in this field. This examination will utilise available academic literature as well as the acquis[1] pertinent to EU cybersecurity policy. It will also draw on a series of elite interviews undertaken at the EU's institutions and agencies. Subjects for interview were selected by identifying the agencies and Commission DGs most relevant to the EU's cybersecurity policy, its development and implementation. Interviews themselves were carried out in Brussels during the summer of 2014. A second section will examine the state of EU cybersecurity policy after 2009, once the Treaty of Lisbon had entered into force, examining the key changes that Treaty caused in that policy area. The third and final section will examine the CFSP, to highlight the unresolved nature of EU competence in this field, through the lens of EU cybersecurity policy. The paper will employ an historical institutionalist approach, using the data collected and historiography of the acquis relating to cybersecurity to map out the EU's approach and demonstrate the impact of institutional variables on a policy area over time, but also use that policy area to demonstrate the strengths and weaknesses of a

[1] The body of principles, measures, legislation and agreements making up to totality of instruments available to the EU (European Union, n.d.).

particular institutional change (in this case the treaty of Lisbon) at a particular point in time.

This paper also aims to address a gap in research. A strong body of literature has been produced examining both cybersecurity and the Treaty of Lisbon, but has treated these topics separately. In cybersecurity, work has been carried out examining the nature and existence of cyber warfare (Dinniss, 2012; Junio, 2013; Liff, 2012; McGraw, 2013; Rid, 2013) as well as conceptual and data-oriented discussions of the overhyping the threat landscape (Dunn Cavelty, 2012a, 2010; Guitton, 2013; Hansen and Nissenbaum, 2009; Valeriano and Maness, 2014). The impact of both internal (Deibert, 2009; Hayden, 2014) and external (Schmitt, 2012) state and criminal activity (Buono, 2012) has also been discussed. Academic examinations of the impact of the Treaty of Lisbon on particular policy areas such as sports (Weatherill, 2014) and the environment (Lee, 2008; Vedder, 2010) has been equally extensive. Comparatively little has been produced on European Union cybersecurity policy specifically, however. Two internal documents commissioned by the European Parliament have provided a state-of-the-art of the EU's policy (Cornish, 2009; Klimburg and Tiirmaa-Klaar, 2011), but the pace of change in the field has dated these evaluations. This paper, in conjunction with two works forthcoming in 2014 (Christou, 2014; Dewar, 2014a) will develop research in this field.

Cybersecurity in the European Union: The Pre-Lisbon Situation

Prior to 2009 and the coming into force of the Treaty of Lisbon, EU policy development and implementation was divided into three policy areas or pillars,

instituted by the Treaty of Maastricht (Bache et al., 2011, p. 161; Bretherton and Vogler, 2006, p. 14). The first pillar was that of the Communities. It comprised, inter alia, social and economic policy, as well as the management of the internal market and agriculture. Foreign, defence and security policy comprised the second pillar and the third pillar focussed on police and judicial co-operation.

This pillar structure was designed to formally separate economic and social dimensions of policy from more highly politicised areas (Bretherton and Vogler, 2006, p. 6) such as foreign policy and criminal justice. A consequence of this was that not only were policy areas divided amongst these pillars, but they were also subject to different decision making procedures. Pillar 1's institutional functioning was denoted by the "community method", whereby the European Commission held the monopoly of policy initiative and decisions were made by the Council using qualified majority voting. Pillars 2 and 3 by contrast involved intergovernmental processes, whereby the Commission shared the right of initiative with Member States or had this right confined to specific areas of activity. Decisions were made by the Council of the EU, generally acting unanimously (European Union, n.d.).

For cybersecurity policy, such a division of responsibilities, remits and decision-making procedures caused significant difficulties in part due to the nature of cybersecurity itself. This is a field which has come under intense scrutiny in the last decade, but still remains largely undefined and unclarified as a concept (Kruger, 2012). The security challenges generated by an increased use of information and communications technologies (ICT) are many and varied. Criminal activities range from the use of viruses, malware and Trojan horses to illegally access secure networks (Dunn Cavelty, 2012a, p. 8), to copyright infringement and digital piracy

(Tikk et al., 2010, p. 100). Organised criminal networks employ social engineering techniques such as phishing to carry out identity thefts or corporate espionage (Johnson, 2011, p. 23). "Hacktivist" groups access government or official websites and networks to damage or deface them in an effort to engage in a form of social protest (Jordan and Taylor, 2004, p. 3). All sides in a regional conflict can use the internet to gain a political advantage though the distribution of, for example, graphic images of conflict casualties, an activity dubbed "cyber-cortical warfare" (Conway, 2005). Government security services can strategically place routers and filters in order to enable or hinder access to certain data (Deibert, 2009, p. 325; Zimmer, 2004, p. 4) or potentially weaponise these tools for military purposes (Rid and McBurney, 2012, p. 6). This last example raised the political profile of cybersecurity to national security levels and increased academic and political discussions on the concept of cyber-war (Barrett, 2013; Junio, 2013; Rid, 2013).

What all these potential security threats share are the same basic methodologies to enable unauthorised access to data or networks. The skills and techniques used to infiltrate a system, carry out a data theft, dedicated denial of service (DDoS)[2] attack or hacktivism are the same, regardless of the target. What those who are targeted need to know are the aims and identities of the perpetrators[3]. Once this information is known, the correct agencies and policy procedures can be put in place to address the incident and prosecute the perpetrators.

The problem for cybersecurity policy and action in the EU is that the aims of criminals or other actors operating in cyberspace cross pillar boundaries resulting in

[2] A DDoS attack involves automating requests for access to a website so that the servers hosting the website are flooded with such ac cess requests. This overloads the server causing it to fail or crash (Dunn Cavelty, 2012b, p. 33)
[3] The so-called "attribution problem" (Gaycken, 2011, pp. 80–86)

the various DGs of the European Commission developing policy solutions to particular elements of cybersecurity simultaneously, depending on the nature of the incident they were to address. The theft of large quantities of digital data is clearly a criminal matter, subject to the policies and procedures of the judiciary and investigation by the police (Pillar 3). However, if the data stolen is corporate banking records, access codes to stock exchanges or large numbers of customer online log-in details, this necessarily has a significant impact on EU economic policy, potentially eroding trust in – and thereby use of – the internal market. Consequently, Directive 2002/58/EC was passed in 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (a.k.a., the Directive on privacy and electronic communications). This was amended in 2009 by Directive 2009/136/EC. Both of these were developed in the Communities pillar, Pillar 1.

A further example is online child exploitation. Protection of children in their online activity is a social policy matter, which would normally come under the aegis of Pillar 1. However, the abuse of children and investigation of international paedophile networks is a criminal matter and so was addressed by Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (amended and replaced in 2011 by Directive 2011/92 of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography). These were developed under Pillar 3 – Justice and Home Affairs.

The result of this separation of responsibilities and remits was the development of an extensive acquis relevant to cybersecurity. In addition to the legislation cited above, the Commission published a Communication on a "European Programme for Critical

Infrastructure Protection (EPCIP)"(European Commission, 2006a) in 2006. This set out the horizontal framework for the protection of critical infrastructures in the EU (European Commission, 2012). The Trust and Security chapter of the Digital Agenda for Europe (European Commission, 2010a) launched several actions addressing security and resilience. The relevant sections of the Stockholm Programme/Action Plan (European Commission, 2010b) and the EU Internal Security Strategy (ISS) (European Commission, 2010c) underline the Commission's commitment to building a digital environment which enables the economic and social potential of the EU's digital space to be achieved.

This extensive acquis was further complicated by the establishment of specific agencies to address key elements of the EU's cybersecurity response. The European Network and Security Agency (ENISA) was established in 2004. It describes itself as an "advice broker" (ENISA, 2005), a conduit for information between actors, sharing best practice, running simulation exercises (ENISA, 2010) and assisting Member States in achieving NIS goals set out in the EU acquis. The Computer Emergency Response Team for the EU (CERT-EU) works closely with CERTs in other member states and private sector partners to detect and respond to cybersecurity incidents (Interview 7). Leading the investigation and combatting of cyber-crime was Europol's high-tech crime office, which would become the European Cybercrime Centre (EC3) in 2013 (Europol, 2013a, 2013b).

Given the similarity of remits and commonality of purpose between the various DGs, agencies, institutions and offices involved in cybersecurity policy, one would anticipate there being a great deal of joint working and cross-pillar co-operation similar to that which occurred in certain elements of foreign policy (Bretherton and

Vogler, 2006, p. 32; Stetter, 2004, p. 721). Two attempts were made in 2001 and 2006 to generate a unified approach to cybersecurity policy for the EU (Dewar, 2014a, pp. 1–2). These were the Commission Proposal on Network and Information Security (NIS) (European Commission, 2001) and the Strategy for a Secure Information Society (European Commission, 2006b). These attempts were not fully successful however, nor truly all-encompassing as they focussed on crime and citizen protection, with little or no mention of CFSP issues. While institutionalising a concentration on cyber-crime, public and private sector awareness and resilience of critical and digital infrastructure, the NIS Proposal mentioned national security issues – CFSP Pillar 2 matters – only in the sense of disaster prevention, critical infrastructure protection and crisis management. The Strategy for a Secure Information Society made no mention of defence or national security issues. The reasons for this were that was that the 2006 Strategy was developed under the aegis of Pillar 1 at a time when the EU was engaged in an identity crisis following the rejection of the Constitutional Treaty, the precursor to the Treaty of Lisbon. Member states were wary of the potential for the proposed Constitution to confer elements of state-hood on the EU (Bache et al., 2011, p. 212) and degrade the individual member states' national sovereignty in defence matters, part of the intergovernmental remit of Pillar 2. Consequently any "high politics" element of cybersecurity was absented from attempts to generate a holistic strategy.

The pillar structure of the EU and the silo-mentality it generated, under which functionaries operated separately from each other, therefore prevented a truly holistic approach to cybersecurity being developed. This illustrates wider institutional problems in the EU pre-Lisbon for the coherence of policy solutions (Bretherton and Vogler, 2006, p. 32). CFSP matters were not present in the 2001 and 2006

documents because of division of competences and concerns regarding the degradation of national sovereignty. Separate polices and strategies with similar remits – online data and child protection – were being developed independently in separate Commission DGs, necessarily leading to duplication and inefficiencies. The development within the framework of the pillar structure of such a multiplicity of instruments to address the various challenges led to a fragmentation of the EU's response to cybersecurity (Klimburg and Tiirmaa-Klaar, 2011, p. 29) across the institutions, agencies and DGs, a fragmentation symptomatic of the inefficiencies of the EU prior to 2009. For cybersecurity policy, that fragmentation was so extensive that Cornish (2009, p. 29) goes so far as to argue that, in 2009, it was difficult to identify an EU agency or body which did not have an interest or involvement in some element of cybersecurity policy or operation.

All this changed following the coming into force of the Treaty of Lisbon in 2009. That Treaty initiated a range of extensive institutional changes within the EU, radically reshaping its political and institutional structure.

EU Cybersecurity Policy post-Lisbon: A New Institutional Architecture

In an effort to create a more effective and efficient institutional structure, the Treaty of Lisbon initiated a number of radical changes in the way the EU was constructed. In repackaging the Treaties of Amsterdam and Maastricht into the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), the aim was ensure coherence and comprehensibility as well as increase effectiveness in policy development and implementation across the array of policy areas in which the EU is involved (Dinan, 2010, p. 154; Verdun, 2013, p. 1131). The

European Parliament was placed on an equal footing with the Council of the EU by it being granted co-decision powers on legislation. The European Council was established as a formal institution and the Union itself was established as a single, legal entity. In the field of foreign and security policy, the High Representative of the Union for Foreign Affairs and Security Policy was to be assisted by a new European External Action Service (EEAS) in the fulfilment of common foreign and security policy (CFSP) and common security and defence policy (CDSP) goals. Additionally, the European Defence Agency (EDA) was confirmed as a formal EU body (Howorth, 2013, p. 13).

If nothing else, the specific mention of "computer crime" in Article 69(b) of the Treaty of Lisbon itself highlights the importance placed on cybersecurity in the EU (European Union, 2007, p. 65). It is a field of crucial significance to the stability and viability of the internal market to due to the nature of the security challenges involved. In terms of practical solutions to those challenges, the most significant impact of the Treaty of Lisbon on cybersecurity policy was the abolition of the pillar structure. As discussed in the previous section, this structure separated a number of policy areas affected by the same cybersecurity challenges. With its removal, for the first time functionaries from agencies and Commission DGs operating across what used to be the distinct areas of the Communities, foreign and security policy and judicial co-operation were able to work together (Interview 1, Interview 3, Interview 5).

In the field of cyber-crime, for example, DG HOME, previously under the judicial co-operation pillar, was able to work under pillar 1 policy development processes. This provided two important new capabilities. DG HOME, and thereby the Commission

itself, was given the right of initiative of policy in the growing field of cyber-crime (interview 3). The EC3 at Europol had developed from a high-tech crime centre to an established pan-European hub in its own right. It has a multiplier effect, able to direct, pool and co-ordinate the resources across all the member states, removing the requirement for individual capacity building (Interview 6). Before 2009, however, the Commission did not have the ability to generate policy or legislative suggestions to support the EC3 in its activities. With the entry into force of the Treaty of Lisbon, the Commission could now do so. Secondly, the Commission now has the power of enforcement (Interview 3). It could ensure that all elements of the relevant cyber-crime acquis were implemented by all member states, and potentially launch infringement procedures were this implementation not undertaken. These two features highlight a dramatic increase in the capacity of the EU to act in the field of cyber-crime and by extension internal cybersecurity issues.

The capacity to work under what used to be different pillars was not restricted to cyber-crime, however. In a move not possible prior to the Treaty of Lisbon, representatives from Commission DGs HOME and CONNECT and the new External Action Service come together to develop a single strategy document encompassing all elements of EU cybersecurity acquis. At the time this was unique, for it represented the first time all three former pillars were present in the development of a single policy (Interview 1). DG CONNECT (the former DG INFSO) prior to 2009 fell under Pillar 1. The EEAS is the new agency responsible for managing and developing the common foreign and security policy – the former Pillar 2. DG HOME previously fell under the heading of Pillar 3. The new, streamlined EU resulting from the Treaty of Lisbon enabled this unprecedented level of joint working not just between overlapping policy areas but between the institutional departments

themselves. This is particularly evident in cybersecurity as the result of this joint working was the first truly holistic approach to policy produced by the Union: the Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace (European Commission, 2013).

A new, holistic approach to European Union cybersecurity policy

Released in 2013, the Cybersecurity Strategy drew together the various elements of the extensive acquis pertinent to cybersecurity which previously had been developed independently and with significant overlap (Dewar, 2014a, p. 14). The new Strategy elucidates five key objectives: achieving cyber-resilience; reducing cyber-crime; developing cyber-defence policies and capabilities; developing industrial and technological resources for cybersecurity and establishing a coherent international policy for EU cybersecurity based on promoting EU values. Throughout the exploration of these objectives, the key goals of the various policies and strategies making up the previous acquis are evident. Co-operation between stakeholders to develop multilateral solutions and accept joint responsibility was promoted, as established in the Internal Security Strategy of 2010 (European Commission, 2013, p. 4, 2010c). The EU and its digital space were to be promoted as a safe place to live and conduct business, a key tenet of the Stockholm Programme (European Commission, 2013, p. 2, 2010b) and digital illiteracy was to be combatted to ensure universal benefit of the economic potential of cyberspace, as set out in the Digital Agenda (European Commission, 2013, p. 4, 2010a). What the Cybersecurity Strategy did was to draw the elements together and enable the EU to move forward with a single strategic vision, something not possible under the previous institutional architecture.

Continuing established policies of fighting cyber-crime and ensuring resilience of critical and digital infrastructure in an holistic framework was not the sole innovation of the new Cybersecurity Strategy, however. In what is perhaps the most significant development for EU cybersecurity policy, the Strategy also, for the first time, includes specific action points for cyber-defence under the aegis of the CFSP (European Commission, 2013, p. 11). This is the first time cybersecurity capabilities are mentioned in the context of defence and national security capacities, and not just crisis management or disaster relief. It demonstrates the seriousness placed on cybersecurity by the EU and reflects the political mood at the time due to a series of high-profile incidents which involved allegations of state involvement (Interview 3; Zanders, 2009, p. 2). The DDoS incidents in Estonia in 2007and Georgia in 2008 as well as the discovery of the Stuxnet virus in 2010 raised international cybersecurity to the national security level. Furthermore, due to this area previously coming under the jealously guarded mandate of the Pillar 2 (CFSP), such an inclusion demonstrates the capacity of the new, post-Lisbon EU architecture to generate truly holistic policies. The new Strategy firmly established a unified position for the EU on cybersecurity. It established clear goals including reducing cyber-crime, ensuring the resilience of the internal market and European information space, promoting EU values internationally, establishing the EU as an international actor in the field and developing cyber-defence capabilities. What is clear from these goals, and the action points included to achieve them, is the presence in one strategy of aspects of policy covered under the former pillars. The collation of these measures and goals would not have been possible without the Treaty of Lisbon ending – or rather, streamlining – the institutional framework and architecture of the pre-2009 EU.

However, while the Cybersecurity Strategy and its holistic approach demonstrate the best that the changes brought in by the Treaty of Lisbon has to offer, it is not complete. The inclusion of strategic goals for cyber-defence within the CFSP showcase that the pillar structure of policy development has been removed. Such an inclusion would have been unheard of prior to 2009. This inclusion, though, belies an underlying ontological weakness in the new institutional architecture: competence in the CFSP. While the EU sought to establish itself as an actor in the international sphere in the particular field of cybersecurity post-Lisbon (European Commission, 2013, p. 5), it could be argued that its scope as an actor – what it can actually do – is much more limited in this area when compared to criminal justice matters or the resilience of the internal market.

Cybersecurity and the Common Foreign and Security Policy

A common refrain for EU officials in relation to external cybersecurity and cyber-defence is that the EU has no mandate or competence to act in this capacity (Interview 3). The EU cannot engage in defence measures, nor does it wish to do so (Interview 3). Furthermore, the TEU and the TFEU are explicit in acknowledging NATO's role in this capacity (European Union, 2009, p. 278). Despite some scholars arguing that the EU is steadily developing such capacities through the externalities of the CSDP aspects of CFSP (Toje, 2011, p. 44), institutionally, the EU is not pursuing such an agenda due to its restricted competences. As a result, the development of cyber-defence capabilities as extolled in the 2013 Strategy is one which is restricted to the co-ordination of current Member State resources, building relations with NATO and promoting the sharing of information (Interview 4). A recent progress review of the Cybersecurity Strategy action points highlights that, while much work has already

been successfully carried out in four of its five key objectives, work in the area of cyber-defence is either still "ongoing" or relates to meetings undertaken, some informal, to encourage co-operation and dialogue (European Commission, 2014, pp. 15–17).

The situation regarding the EU's capacity in cybersecurity issues relating to the CFSP is actually more complex than this for two reasons. First, the matter of EU competence in external affairs is not as clear cut as some scholars and EU functionaries are claiming. The problem is not simply that the EU has no competence to act militarily or proactively in "high politics" security matters. That competence has not been clearly defined in spite of the Treaty of Lisbon's goal of streamlining competence, coherence and comprehensibility. This has created a disconnect between, on the one hand, the existence of competence as outlined in Article 5(3)-(4) TEU (European Union, 2012, p. 18) and the practical application of that competence (Craig, 2010, p. 184). Second, the nature of cybersecurity challenges necessitates a global, international perspective to resolution given the inherent transnational nature of those challenges and the rise in allegations of state-sponsored or sanctioned cyber incidents.

A Question of Competence

Following the coming into force of the Treaty of Lisbon, Article 2(4) of the new TFEU stipulates the nature of exclusive, shared and supporting competence in matters such as the customs union and marine resources (exclusive), the internal market and environmental policy (shared) and sports policy (supporting) (European Union, 2009, pp. 50–51). The area of the CFSP, by contrast, remains largely unclarified

(Craig, 2010, p. 182). It is still treated as a separate area of competence, but not labelled as such (Laursen, 2010, p. 10).

Under the terms of Article 24 TEU and Article 2(4) TFEU the Union's competence in foreign and security affairs shall "cover all areas of foreign policy and all questions relating to the Union's security, including the progressive framing of a common defence policy that might lead to a common defence" (European Union, 2012, p. 30). However, Article 24(1) TEU goes on to place a series of restrictions on the Union's capacity to act in that field. The Union is not able to adopt legislative acts pertaining to areas of CFSP policy. While the Parliament has, post-Lisbon, been elevated to a position of co-decision with the Council, in CFSP matters that role is restricted to consultation and recommendation under Article 36 TEU (European Union, 2012, pp. 35–36). Furthermore, distinct rules of decision-making and policy implementation remain (Dinan, 2010, p. 155), echoing elements of the pre-Lisbon architecture in that the European Council and Council of the EU dominate (Craig, 2010, p. 182). CFSP is even specifically exempted from Article 352 TFEU, the so-called "flexibility" clause (Craig, 2010, p. 183). Article 352(1) TFEU states that if action by the Union is necessary to attain a Treaty objective, but the necessary powers are not set out in the Treaties, the Council of the EU can act unanimously to "adopt appropriate measures" (European Union, 2009, p. 196). However, Article 352(4) specifically states that Article 352 itself cannot be used for attaining CFSP objectives (European Union, 2009, p. 196).

The result is that the CFSP is "*a specific policy area with a separate set of legal rules and treaty basis, a specific budget line, distinct set of institutions and equipments [sic], as well as a staff with competencies, know-how and experiences"* (Rieker,

2009, p. 704). CFSP matters therefore remain a de facto pillar of EU policy, considered separately (Wouters et al., 2008, p. 161) to other areas of competence in the EU's Treaties, the basis of the Union's operation, and also to other areas of the EU's mandate for action such as agriculture, tourism, sport and energy. It is deliberately left out of the definitions of the types of competence and their concomitant subject areas. One official (Interview 2) described the combination of this absence with the series of restrictions placed on the EU's institutions a making the Commission and EEAS a "toothless tiger" as it has no right of initiative or enforcement of policy or action. Furthermore, the Court of Justice of the EU has no jurisdiction over CFSP matters (European Union, 2012, p. 30) [4], further reducing the Union's capacity to compel member states to adhere to policy decisions. In cybersecurity policy, this can be contrasted with internal measures. The Commission's DG HOME, as examined above, now has the right of enforcement in certain key policy areas relevant to cybersecurity (Interview 3).

On the face of things, such a situation regarding competence should severely restrict the EU in the international arena. The EU is, however, an important actor in international politics, illustrating a disconnect between the existence of competence and the application or use of competence. While the EU has no competence to take decisive foreign or defence policy action, the Union has in effect become a 'normative power` in foreign policy (Dinan, 2010, p. 545; Manners, 2002, p. 29). This is particularly problematic for cybersecurity policy, given the rise in state-sponsored international cyber-incidents.

[4] Except in issues brought by an individual person where an act directly affects them (see Article 263 TFEU). However, as indicated above, the EU cannot adopt legislative acts relating to the CFSP.

The Existence of Competence v. The Use of Competence: The EU as a normative power

As an international actor the EU has been described as an economic giant but a political pygmy (Dinan, 2010, p. 545), calling into question the extent to which the EU is a successful actor in international global politics. The Union has a great deal of influence in the development of economic policy in its 28 member states and in global commerce. Historically, however, some scholars have argued that this economic power has not translated into international influence (Dinan, 2010, p. 545). The power-politics involved in developing state-like apparatus and nomenclature led to the failure of the Constitutional Treaty in 2003: member states did not want the EU to develop into a super-state, with more supranational power and sovereignty being granted to Brussels. A consequence of this is precisely the vague, ill-defined and complex nature of the EU's competence in foreign and international security policy following the coming into force of the Treaty of Lisbon.

Yet, the EU is an actor in international politics and security. It is one of the members of the Quartet for the Middle East peace process. Military forces under the EU banner have been deployed to Libya, Somalia and the Democratic Republic of Congo (EEAS, 2014a). In the EUPOL Afghanistan police mission, the Union assisted in civilian reconstruction and police and justice reform (Gross, 2012, p. 109). The Union has also been active in counter-terrorism (Zwolski, 2012, p. 993) and border control as recently as the ongoing Libyan conflict (EEAS, 2014b). With specific regard to cybersecurity and cyber-defence, the EU action is relatively recent (Interview 4), due to the relative youth of the EU's military capacity due to the perception of the EU as a civil, socio-economic organisation. The EDA's main tasks

in cybersecurity and cyber-defence focus on supporting members states in their own actions, as well as ensuring a pooling of resources to avoid duplication. In a similar way that ENISA operates as an advice broker, the EDA ensures that best practice and information is shared amongst the member states, but only insofar as that information is able to be shared. However, this is also a key role for the EDA across the full range of its activities. Information-sharing and efficiency building are not restricted solely to cybersecurity or cyber-defence matters. This highlights a particular aspect of the EU in CFSP in general: its presence as a normative actor.

Where the EU can operate internationally is in the projection of its normative influence. In the specific examples of the CFSP/CSDP operations, the norms and patterns of behaviour and action include humanitarian action, peacekeeping and peacebuilding. The principles behind these operations are not hard security solutions to the challenges faced. While military force is deployed, it is in specific, restricted circumstances relating to humanitarian and peacekeeping missions. The EDA describes itself as an agency specialising in providing support and co-ordination to military assets in efforts to increase efficiency, but not as a military arm in itself. This softer approach reflects principles established historically in the "Petersberg tasks" which define the type of military action the EU can undertake (EEAS, n.d.). The original declaration was expanded by the Treaty of Lisbon to include not just humanitarian, peacekeeping and peace-making tasks, but also disarmament, military advice and assistance and post-conflict stabilisation (EEAS, n.d.; Western European Union, 1992).

These operations demonstrate that the EU is an actor, if a somewhat *sui generis* actor (Bretherton and Vogler, 2006, p. 35). It operates on principles of assistance

and peacekeeping, so-called “soft power” norms. It has military resources to deploy but these are not deployed in active, deliberate combat situations in the same way that NATO forces were deployed in Libya in 2011. While these operations demonstrate that the EU is an international security actor, there are identifiable characteristics to its approach which affect the capacity of the EU as an actor, characteristics which are brought into sharp relief by the nature of international cybersecurity challenges. These challenges are not restricted to one policy area. However, they are also not restricted to one geographical area. Illegal botnets operating in EU Member States may be made up of zombie computers based all over the world, operated from central servers based in, for example, South East Asia. The anonymising effects of cyberspace enable perpetrators to carry out security breaches while making it, if not impossible to identify them, costly to do so in time and resources and makes it difficult to establish judicial jurisdiction. This has particular attractions for international criminal networks in seeking to evade identification and prosecution. Accurately locating and identifying perpetrators – the so-called “attribution problem” (McGee et al., 2013; Schmitt, 2013, pp. 29–31; Tsagourias, 2012, p. 242) – is one of the biggest challenges in addressing cybersecurity incidents and tackling cyber-crime.

In terms of tackling cyber-crime the problem of attribution is a labour-intensive but technical exercise. According to officials at the EC3, Europol acts in concert with an extensive network of law enforcement, public and private partners and technicians to identify and tackle international criminal networks utilising the Internet (Interview 6). However, when the investigation of cybersecurity incidents points not to criminal networks but to nation states, attribution of incidents poses serious problems for the EU. In recent years a series of high profile network and information security

breaches have raised the profile of cybersecurity on the political agenda due to strong allegations of state involvement (Interview 3). Estonia '07, Georgia '08 and Stuxnet have all involved alleged state involvement (Dinniss, 2012, pp. 176,289–291). The issue for the EU in these cases is not just that the accurate attribution of these incidents to particular nation states is problematic, but that these incidents can, in certain circumstances of international law, constitute an armed attack (Dewar, 2014b, p. 10). While the TFEU contains a "mutual assistance" clause, the lack of clearly defined competence in CFSP and deferral to NATO in matters military, coupled with the retention of a de facto foreign policy pillar with separate decision-making procedures, means the EU has little capacity to act once state involvement is suspected in a cybersecurity incident, beyond its role in resource co-ordination.

Under Article 42 TEU civilian and military resources are to be made available to the Union "for the implementation of the CSFP" (European Union, 2012, p. 39). By extension, the computer network resources of the member states in the area of military or cyber-defence capabilities can therefore be called upon. However, Paragraph 4 of Article 42 stipulates that the use of such action can only be proposed by the High Representative and deployment is subject to unanimous agreement in the Council (European Union, 2012, p. 39). Coupled with the established norms of soft power, this places a severe restriction on the capacity of the EU to act in the cyber domain, despite clear threats to the internal market and commercial viability of the EU's digital space. While botnets used for criminal activities such as the theft of data, identity details or money can be investigated and taken down through joint working between member states and other international partners, botnets apparently used by state-sponsored or sanctioned entities pose different political problems. If a national government is identified as being behind a botnet attack, EU law

enforcement agencies and their extensive resources are not involved in any responsive action. The incident is escalated to the level of CFSP discussion and therefore subject to more restricted modes of joint working. The EEAS and EDA are heavily involved in developing diplomatic and practical tools to address these issues, but are once again hamstrung by the limitations of competence expressed in the Treaty of Lisbon, limitations caused by a lack of clarity in the CFSP and the entrenchment of that policy area as a separate pillar.

The result therefore, is not just a disconnect between the existence of competence and the use of competence. There is also a disconnect between the drive for efficiency and coherence in the Treaty of Lisbon, demonstrated to good effect in internal cybersecurity matters, and the elements of EU policy left out of that efficiency drive: the CFSP and external cybersecurity issues involving alleged state action. The EU's competence in the field of CFSP is, according to its own functionaries, very restricted (Interview 3, Interview 8). The EU is developing as an international security actor, but of a very particular kind. The lack of clear CFSP competence post-Lisbon and the precise nature of the EU's capacity as an actor can be illustrated through its cybersecurity policy. It remains restricted to projecting its particular normative stance, one found in the 2013 Cybersecurity Strategy itself: protection of fundamental human rights and promotion of core EU values, in short a projection of soft power (European Commission, 2013, pp. 3–5).

Conclusion

In reforming the treaties on which the EU is founded the Treaty of Lisbon aimed for simplicity (Christiansen and Dobbels, 2013, p. 1164). It was intended to tackle

perceived deficiencies in effectiveness, efficiency and democratic accountability. It sought to streamline processes and responsibilities and achieved, in many respects, a more coherent and comprehensible European Union.

Although these goals were not directed at any specific policy area, they can be most clearly recognised in the field of cybersecurity. By abolishing the old pillar system, which lead to duplication of policy development and a highly convoluted and fragmented approach to cybersecurity, offices that were not able to work together were now able to do so under the new institutional structure of the EU (Interview 3). As a result, a single strategic approach was developed which encompassed the areas of the common market, critical physical and digital infrastructure, internal security and defence. Cybersecurity policy therefore demonstrates the achievements of the Treaty of Lisbon in its streamlining goals. Decision-making has been made more coherent, duplication has been reduced and a more holistic, unified approach to a single policy area has been developed.

However, this process has been only partially successful. In the area of the CFSP, the competence of the EU remains unclarified. In terms of cybersecurity and, more specifically, cyber-defence, this lack of clarity restricts the capacity of the EU to develop more active responses to security challenges, on a par with its successful efforts in law enforcement, data protection, civil education and system harmonisation, areas where the EU's competence is more clearly defined. Due to different rules of action and decision-making to other areas, the CFSP remains a de facto separate pillar. It therefore creates a grey area of policy, which translates into an institutionalised complexity of responsibilities and action, particularly with regard to those cybersecurity challenges incorporating allegation of state involvement. .

This means that the Union's cyber-defence capabilities are curtailed by institutionalised weaknesses unresolved by the changes brought in by the Treaty of Lisbon, despite the goals of simplification and coherence. Although the Union has a strong presence on the international arena, that presence is limited to particular normative values, namely peacekeeping, peace-making and humanitarian activities.

Cybersecurity as a policy area for the EU therefore demonstrates the best and worst of what the Treaty of Lisbon has to offer. It shows how the new institutional structure of the EU has the capacity to carry out more streamlined policy development and activity, but only in specific circumstances, demonstrating where the inherent ontological weaknesses of the Treaty lie: the clarification of the EU's status and capacity as an international actor.

It has only been five years since the coming into force of the Treaty of Lisbon and, although examples of its best features are evident in the 2013 Cybersecurity Strategy, the continued development of the EU as an international actor provides exciting opportunities for further examples of the institutional changes introduced by that treaty as well as further opportunities for academic research.

References

Interviews

Interview 1 – Official from the EEAS, 10 June 2014, Brussels
Interview 2 – Official from the European Union, 17 June 2014, Brussels
Interview 3 – Official from the European Commission, 19 June 2014, Brussels
Interview 4 – Official from the European Defence Agency, 11 June 2014, Brussels
Interview 5 – Member of the European Parliament, 8 July 2014, Brussels
Interview 6 – Official from the EC3, Europol, 23 May 2014, The Hague
Interview 7 – Official from the European Union, 17 June 2014, Brussels
Interview 8 – Official from ENISA, 16 May 2014, Heraklion, Crete

Bibliography

Bache, I., George, S., Bulmer, S., 2011. Politics in the European Union. OUP.
Barrett, E.T., 2013. Warfare in a New Domain: The Ethics of Military Cyber-Operations. J. Mil. Ethics 12, 4–17. doi:10.1080/15027570.2013.782633
Bretherton, C., Vogler, J., 2006. The European Union as a global actor. Routledge.
Buono, L., 2012. Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3). New J. Eur. Crim. Law 3.
Christiansen, T., Dobbels, M., 2013. Delegated Powers and Inter-Institutional Relations in the EU after Lisbon: A Normative Assessment. West Eur. Polit. 36, 1159–1177. doi:10.1080/01402382.2013.826023
Christou, G., 2014. Cyber Security in the European Union: Resilience and Adaptability in an Age of Governance (forthcoming 2014). Palgrave Macmillan, Houndmills, Basingstoke.
Conway, M., 2005. Cybercortical Warfare: Hizbollah's Internet Strategy, in: Oates, S., Owen, D., Gibson, R. (Eds.), The Internet and Politics; Citizens, Voters and Activists. Routledge.
Cornish, P., 2009. Cyber Security and Politically, Socially and Religiously motivated Cyber Attacks (Study), Directorate General External Policies of the Union. European Parliament.
Craig, P., 2010. The Lisbon Treaty: law, politics, and treaty reform. OUP.
Deibert, R.J., 2009. The geopolitics of internet control: Censorship, sovereignty, and cyberspace, in: Chadwick, A., Howard, P.N. (Eds.), Routledge Handbook of Internet Politics. Routledge, London, pp. 323–336.
Dewar, R., 2014a. The European Union and Cybersecurity : A Historiography of An Emerging Actor's Response to a Global Security Concern, in: O'Neill, M., Swinton, K. (Eds.), Challenges and Critiques of the EU Internal Security Strategy: Rights, Power and Security (forthcoming 2014). Cambridge Scholars.
Dewar, R., 2014b. The "Triptych of Cyber Security": A Classification of Active Cyber Defence, in: Prangetto, P., Maybaum, M., Stinissen, J. (Eds.), 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 7–22.
Dinan, D., 2010. Ever closer union: an introduction to European integration, 4th ed. Rienner, Boulder, Colorado.
Dinniss, H.H., 2012. Cyber Warfare and the Laws of War, 1st ed. CUP.
Dunn Cavelty, M., 2010. Die Militarisierung des Cyberspace. Neue Zür. Ztg.

Dunn Cavelty, M., 2012a. The Militarisation of Cyber Security as a Source of Global Tension, in: Möckli, D., Wenger, A. (Eds.), Strategic Trends Analysis. Center for Security Studies, Zurich, Switzerland.
Dunn Cavelty, M., 2012b. Cyber-security, in: Collins, A. (Ed.), Contemporary Security Studies. OUP.
EEAS, 2014a. Operations and Missions [WWW Document]. Oper. Missions. URL http://www.eeas.europa.eu/csdp/missions-and-operations/index_en.htm
EEAS, 2014b. EUBAM Libya [WWW Document]. EUBAM Libya. URL http://eeas.europa.eu/csdp/missions-and-operations/eubam-libya/index_en.htm
EEAS, n.d. About CSDP - The Petersberg Tasks [WWW Document]. URL http://www.eeas.europa.eu/csdp/about-csdp/petersberg/index_en.htm
ENISA, 2005. Activities — ENISA [WWW Document]. URL http://www.enisa.europa.eu/about-enisa/activities (accessed 8.12.13).
ENISA, 2010. Cyber Europe [WWW Document]. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe (accessed 8.16.13).
European Commission, 2001. COM (2001) 298 Final Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach (Communication). European Commission.
European Commission, 2006a. COM (2006) 786 final Communication from the Commission on a European Programme for Critical Infrastructure Protection (Communication). European Commission.
European Commission, 2006b. COM (2006) 251 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A Strategy for a Secure Information Society – “Dialogue, partnership and empowerment.”
European Commission, 2010a. COM (2010) 245 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 (Communication). European Commission.
European Commission, 2010b. COM (2010) 171 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the - Delivering an area of freedom, security and justice for Europe’s citizens Action Plan Implementing the Stockholm Programme (Communication). European Commission.
European Commission, 2010c. COM (2010) 673 Final Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (Communication). European Commission.
European Commission, 2012. European policy and legislative documents relevant for cybersecurity.
European Commission, 2013. JOIN (2013) 1 Final Joint Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Communication). European Commission.

European Commission, 2014. Table on the Implementation of the “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace” (JOIN2013) 1).
European Union, 2007. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community.
European Union, 2009. Treaty on the Functioning of the European Union.
European Union, 2012. Treaty on European Union.
European Union, n.d. Community acquis [WWW Document]. URL http://europa.eu/legislation_summaries/glossary/community_acquis_en.htm (accessed 8.15.12a).
European Union, n.d. Community and Intergovernmental Methods [WWW Document]. URL http://europa.eu/legislation_summaries/glossary/community_intergovernmental_methods_en.htm (accessed 8.15.12b).
Europol, 2013a. Mandate [WWW Document]. URL https://www.europol.europa.eu/content/page/mandate-119
Europol, 2013b. A Collective EU Response to Cybercrime [WWW Document]. URL https://www.europol.europa.eu/ec3 (accessed 2.1.13).
Gaycken, S., 2011. Cyberwar: Das Internet als Kriegsschauplatz. Open Source Press, Munich, Germany.
Gross, E., 2012. The EU in Afghanistan, in: Whitman, R.G., Wolff, S. (Eds.), The European Union as a Global Conflict Manager. Routledge, pp. 107–119.
Guitton, C., 2013. Cyber insecurity as a national threat: overreaction from Germany, France and the UK? Eur. Secur. 0, 1–15. doi:10.1080/09662839.2012.749864
Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. Int. Stud. Q. 53, 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x
Hayden, M., 2014. Beyond Snowden. World Aff. 176, 13–23.
Howorth, J., 2013. European security institutions 1945-2010: the weaknesses and strengths of “Brusselsization”, in: Biscop, S., Whitman, R.G. (Eds.), The Routledge Handbook of European Security. pp. 5–17.
Johnson, C., 2011. Anti-Social Networking: Crowdsourcing and the CyberDefence of National Critical Infrastructures.
Jordan, T., Taylor, P.A., 2004. Hacktivism and Cyberwars: Rebels with a Cause? Psychology Press.
Junio, T.J., 2013. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. J. Strateg. Stud. 36, 125–133. doi:10.1080/01402390.2012.739561
Klimburg, A., Tiirmaa-Klaar, H., 2011. Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU. European Parliament.
Kruger, D., 2012. Radically Simplifying Cybersecurity.
Laursen, F., 2010. The EU as an International Political and Security Actor after the Treaty of Lisbon: An Academic Perspective, in: Jean Monnet Conference on the Lisbon Treaty, May.
Lee, M., 2008. The environmental implications of the Lisbon Treaty. Environ. Law Rev. 10, 131–138.
Liff, A.P., 2012. Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War. J. Strateg. Stud. 35, 401–428. doi:10.1080/01402390.2012.663252
Manners, I., 2002. Normative power Europe: a contradiction in terms? JCMS 40, 235–258.

McGee, S., Sabett, R.V., Shah, A., 2013. Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense. J. Bus. Technol. Law 8, 1.
McGraw, G., 2013. Cyber War is Inevitable (Unless We Build Security In). J. Strateg. Stud. 36, 109–119. doi:10.1080/01402390.2012.742013
Rid, T., 2013. Cyber War Will Not Take Place. Hurst, London.
Rid, T., McBurney, P., 2012. Cyber-Weapons. RUSI J. 157, 6–13.
Rieker, P., 2009. The EU — A Capable Security Actor? Developing Administrative Capabilities. J. Eur. Integr. 31, 703–719. doi:10.1080/07036330903274599
Schmitt, M.N., 2012. Classification of Cyber Conflict. J. Confl. Secur. Law 17, 245–260. doi:10.1093/jcsl/krs018
Schmitt, M.N. (Ed.), 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. CUP.
Stetter, S., 2004. Cross-pillar politics: functional unity and institutional fragmentation of EU foreign policies. J. Eur. Public Policy 11, 720–739. doi:10.1080/1350176042000248115
Tikk, E., Kaska, K., Vihul, L., 2010. International cyber incidents: Legal considerations. Cooperative Cyber Defence of Excellence (CCD COE).
Toje, A., 2011. The European Union as a small power. JCMS J. Common Mark. Stud. 49, 43–60.
Tsagourias, N., 2012. Cyber attacks, self-defence and the problem of attribution. J. Confl. Secur. Law 17, 229–244.
Valeriano, B., Maness, R., 2014. The dynamics of cyber conflict between rival antagonists, 2001–11 (in press). J. Peace Res.
Vedder, H., 2010. The Treaty of Lisbon and European environmental law and policy. J. Environ. Law eqq001.
Verdun, A., 2013. Decision-Making before and after Lisbon: The Impact of Changes in Decision-Making Rules. West Eur. Polit. 36, 1128–1142. doi:10.1080/01402382.2013.826021
Weatherill, S., 2014. EU Sports Law: The Effect of the Lisbon Treaty, in: European Sports Law, ASSER International Sports Law Series. T.M.C. Asser Press, pp. 507–525.
Western European Union, 1992. The Petersberg Declaration.
Wouters, J., Coppens, D., Meester, B.D., 2008. The European Union's External Relations after the Lisbon Treaty, in: Griller, U.-P.D.S., Ziller, U.-P.D.J. (Eds.), The Lisbon Treaty, Schriftenreihe Der Österreichischen Gesellschaft Für Europaforschung (ECSA Austria) / European Community Studies Association of Austria Publication Series. Springer Vienna, pp. 143–203.
Zanders, J.-P., 2009. Cyber Security: What Role for CFSP? (Institute Report No. IESUE/SEM(09)04). European Union Institute for Security Studies.
Zimmer, M., 2004. The tensions of securing cyberspace: The Internet, state power and The National Strategy to Secure Cyberspace. First Monday Online 9.
Zwolski, K., 2012. The EU and a holistic security approach after Lisbon: competing norms and the power of the dominant discourse. J. Eur. Public Policy 19, 988–1005. doi:10.1080/13501763.2012.662057