European Union Cyber Security:

A Viable Solution?

María Björt Guðbrandsdóttir

Lokaverkefni til BA-gráðu í stjórnmálafræði

Félagsvísindasvið

Febrúar 2015

HÁSKÓLI ÍSLANDS

European Union Cyber Security:
A Viable Solution?

María Björt Guðbrandsdóttir

Lokaverkefni til BA-gráðu í stjórnmálafræði

Leiðbeinandi: Alyson Bailes

Stjórnmálafræðideild

Félagsvísindasvið Háskóla Íslands

Febrúar 2015

100987-2609

Reykjavík, Ísland 2015

Abstract

The aim of this thesis is to evaluate the European Union Cyber Security, the many aspescts of it, and if the Cyber Security Strategy has provided for a viable solution to cyber-crime by achieving the right balance between privacy and security. The thesis provides for an overview of the legal framework regarding cyber security in the European Union and the institutions and institutional remedies set up to combat cyber-crime. New developments emerged in the European Union in 2013, as it has anounced its 2020 strategy, it also set 'a Digital Agenda' for Europe. The European Union has thus put forth a strategy to battle cyber-crime in the European Union and with doing so it has created a legal framework Member States must enter into force, and act on when cases of cyber-crime being committed arise.

The findings of this thesis suggests that the European Union has made strong advances to protect its citizens while simultaneously providing security. Although its current legal framework is still unclear on some issues regarding jurisdiction, information sharing and uneven preparedness among Member States, the fundamental right to personal data has been established and cyber-crime has been defined as a criminal offence in the European Union.

Útdráttur

Megin markmið þessarar ritgerðar er að leggja mat á Net Öryggi Evrópusambandsins, hina mörgu þætti þess, og ef Net Öryggis áætlun Evrópusambandsins sé í raun hagkvæm lausn gegn afbrotum á netinu og nái þar að skapa jafnvægi á milli þess að vernda öryggi einstaklinga og brjóta ekki gegn réttindi einstaklinga til persónuverndar. Ritgerðin gefur yfirlit yfir helstu laga ákvæði Evrópusambandsins til net öryggis, stofnanir Evrópusambandsins og þau úrræði sem stofnanirnar hafa gegn afbrotum á netinu. Ný þróun átti sér stað árið 2013, þegar Evrópusambandið tilkynnti 2020 stefnu sína, og setti þar með fram "Stafræna Stefnu" fyrir Evrópusambandið. Evrópusambandið hefur með því sett fram stefnu með það markmið að berjast gegn afbrotum á netinu og einnig sett á fót lagaramma sem meðlimir Evrópusambandsins verða að innleiða og fara eftir í þeim tilfellum sem upp koma afbrot á netinu.

Niðurstöður þessarar ritgerðar benda á að Evrópusambandið hafa tekið stór skerf til verndar ríkisborgara, og þar með veitt þeim aukið netöryggi. Þó lagarammi Evrópusambandsins varðandi netöryggi sé á köflum óskýr varðandi lögsögu, vinnslu persónuupplýsinga og misjafnan viðbúnað meðlima ríkja til að bregðast við net afbrotum, þá hafa grundvallarréttindi um persónuupplýsingar verið staðfest og afbrot á netinu verið skilgreint sem afbrot af Evrópusambandinu.

Table of Contents

1 Introduction

Information technology (IT) has infiltrated every niche of society.[1] IT is everywhere, in telecommunications, commercial and financial systems, government, food production; that is, in virtually every aspect of 21st century global civilization. We depend on interconnected cyber systems to operate, systems that have helped advance medicine, streamline everyday commerce, and much much more.[2]

We have also become familiar with the down-side of the information revolution, namely cyber-crimes. We fear threats such as identity theft, financial fraud, and the cataclysmic meltdown of the information infrastructure and everything that depends on it.[3] It is for these reasons that keeping these systems safe from threat has become one of the most pressing problems we face.[4]

As society has become more dependent on information technology, and it has become part of everyday life, we are now able to realise the dire consequences a cyber-attack could have. For this reason, government officials, technology specialists, policy analysts and industry leaders - as well as the general public, ourselves - have all become more concerned about cyber security and the challenges it presents.[5]

For the purpose of this thesis the focus will be directed towards criminal activity, namely cyber-crime inside and between governmental jurisdictions. The world took notice when Stuxnet was discovered, a malware that had catastrophic effects on the Iranian nuclear programme.[6] The malware operated by affecting the rate at which nuclear centrifuges spun. In order to produce uranium suitable for use in a nuclear bomb (or nuclear power plant), the centrifuges must run at a constant rate. Stuxnet caused the centrifuges to run at a highly variable rate, while falsely reporting to the operators that everything was in working order. To this day nobody knows who built this malware, but it is the first known case of a major attack on a government's infrastructure.[7]

There is no proof of the real source of the Stuxnet virus, although many speculations have pointed to its being developed by the Israelis with American assistance. Whatever its source, the Stuxnet virus's significance is that it shows what damage a software attack can inflict on

[1] Berkowitz and Hahn (2003). http://www.issues.org/19.3/berkowitz.htm
[2]Paul Rosenzweig. http://www.thegreatcourses.com/tgc/courses/course_detail.aspx?cid=9523
[3] Berkowitz and Hahn (2003). http://www.issues.org/19.3/berkowitz.htm
[4] Paul Rosenzweig. http://www.thegreatcourses.com/tgc/courses/course_detail.aspx?cid=9523
[5] Berkowitz and Hahn (2003). http://www.issues.org/19.3/berkowitz.htm
[6] Rosenzweig. http://www.hoover.org/publications/defining-ideas/article/102401
[7] Rosenzweig. http://www.hoover.org/publications/defining-ideas/article/102401

the “real” world, our world, society. Stuxnet is proof that cyber war can be real, both within and between nations.[8]

Cyber security is a novelty, and it is still in its very early stages. Today there are few specific organisations that battle cyber-crime, and governments have for the most part set up a program within their law enforcement agencies to tackle this problem.

This thesis has two research questions:

1. Is the current approach and system for tackling cyber-crime effective? and
2. Does the current framework achieve the right balance between security on the one side, and human rights and freedoms (including privacy) on the other?

The cyber security activities of the European Union (EU) will be used as a case study to answer the above questions. The EU provides for an excellent case study, as it has already managed to develop consensus and transparency among its Member States on various aspects of cyber-policy and related standards. It has also made reforms in Data Protection, an important factor in cyber security, and shows the EU´s commitment to further security to its citizens in the field of cyber security.

Such trans-national cooperation needs to be at the forefront when discussing the battle against cyber-crime, in order to establish a common ground where governments can battle this threat head on and together.

[8] Rosenzweig. http://www.hoover.org/publications/defining-ideas/article/102401

2 Theoretical Framework

When writing about security the first question must be, is it possible to achieve international security in the world we live in? There is disagreement amongst security specialists about whether the main focus of enquiry should be individual, national, international or global security.[9] Cyber security touches on each of these aspects of security, and can be addressed on a regional or global as well as domestic level.

When it comes to cyber security the answer to the above question is most likely No, but the aim should be to provide the best security we can to protect our society and the individuals who build it. In a media release on September 3rd 2013, Interpol's Secretary General Ronald K. Noble told the Underground Economy 2013 conference that the only way to protect cyberspace against criminal abuse is through a global network of partners.[10]

Noble's strategy of a global network of partners is much aligned with Constructivist theory. The notion that international relations are not only affected by power politics, but also by ideas, is shared by constructivist theorists. In their view the fundamental structures of international politics are social rather than strictly material. If we manage to change the nature of social interaction among governments, it can bring a fundamental shift towards greater cyber security.

The theory of Liberal Institutionalism argues that international institutions are an inherent part of achieving cooperation and stability. Institutions can provide information, make commitments more credible, establish focal points for coordination, and overall provide a platform for governments to reach a common goal – in the present case, a more secure cyberspace.[11]

There are many more specific security theories, all addressing different aspects and indicating different strategies for national security. As cyber security is a national security issue as well as being a global issue, the emphasis must be put on common security achieved through a consensus on policy, action and burden-sharing. The belief in the possibility of pursuing changes in the international system – although contrary to traditional Realism - is shared among most modern scholars, who point to new trends already taking place in world politics. Some go as far as to argue that the process of globalization has accelerated to the point where clear outlines of a global society are now evident,[12] reflecting the emergence of a global economic system, communication, and culture.

---

[9] Baylis, Smith and Owens (2011). pp. 233
[10] Interpol press release.
http://www.interpol.int/en%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%C5%B8%20%20%20%20%20%20%20%20/News-and-media/News-media-releases/2013/PR101
[11] Baylis, Smith and Owen (2011). pp. 237.
[12] Baylis, Smith and Owens (2011). pp. 240

3 Towards an EU Cyber Security Strategy

The goal of the EU cyber security strategy is to protect Europe's society, its citizens, infrastructure and economies from cyber disruptions. The protection covers all phases from prevention to preparedness and response. This goal requires delivering the correct levels of speed and reach capabilities, through an end-to-end comprehensive approach supported by efficient governance for implementation and management, leveraging appropriate tools, leading to the consolidation of present initiatives and competences and the de-fragmentation of the market.[13]

Network and information systems (NIS) threats have a cross-border nature, and if these threats are not detected and dealt with appropriately it can lead to each State having to guard its own territory while ignoring the interdependence between existing network and information systems. For the appropriate management of NIS incidents, Member States should ensure that NIS risks can be well managed in the cross-border context by cooperation through information sharing.[14]

The importance of this cross-border element explains why enforcing standards at European level does not infringe the subsidiarity principle of the EU. Regulatory obligations are required to create a cohesion in cyber security measures, and minimize legislative irregularities within and between nations. The first attempt at a cyber security policy in the EU resulted in a purely voluntary approach where only a few Member States tackling cyber security were left to their own means and effort. The only way to ensure cooperation among all Member States is to set a required minimum level of capabilities and make it an obligation for Member States to fulfil.

Action at EU level is aimed to improve the effectiveness of existing national policies and/or to promote their development. It has however become clear that NIS policy actions are directly correlated with the effective protection of fundamental rights, in particular the right to the protection of personal data and privacy. European citizens are increasingly entrusting their data to complex information systems they do not understand, by choice or necessity, without perhaps being fully able to assess the threats involved. When these NIS incidents occur, individuals are not be able to take suitable steps in most cases, nor is it certain that Member States involved can be able to address these incidents and assist its citizens. When there is not

[13] European Organisation for Security (2011). Steps towards implementing a European cyber-security strategy. pp 17: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf
[14] European Organisation for Security (2011). Steps towards implementing a European cyber-security strategy. pp 17: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf

a EU-wide NIS coordination in place to facilitate individuals and even Member States in addressing the issue at hand, it undermines the effective protection of fundamental rights in the EU.[15]

3.1 European Cyber Security: Introduction

Security risks are not constrained by borders, neither within nor outside the EU. Cyber-crime does not allow itself to be contained within one jurisdiction, under one authority, or by national borders. Cyberspace is a globally interconnected network, and cyber-crime travels freely.[16] For that reason, among others, to secure cyberspace and create an international order, cooperation is needed among states.

The question of why states cooperate has been an on-going issue for scholars of international politics.[17] Globalization is said to reduce the capacity of individual states to govern effectively in key policy areas, while new sites of authority seem to be emerging, in particular in the field of security.

As the EU became a leading international economic actor, its relatively weak political presence on the world stage became more apparent. The EU at its foundation was not designed to be a defence organisation, but an economic cooperation initiative, "building a stronger Europe" in the aftermath of WWII. Since the establishment of the EU it has, however, touched on aspects of security, dealing most notably with the 'softer' aspects i.e. economic, financial and social security. Following the end of the Cold War, and subsequent conflicts in the Balkans, it became clear that the EU needed to assume its share of responsibilities for conflict prevention and crisis management.[18] During the Cold War the European Commission was widely regarded as the central focus of civilian power, and its role developed slowly in the delivery of external policies.[19]

In the period of 1991-1999, leading up to the Maastricht Treaty, the nature of European political cooperation was reformulated with the introduction of a Common Foreign and Security Policy (CFSP). The Common Security and Defence Policy (CSDP) is a vital component of the CFSP, and it has its own objective: the progressive framing of a common Union defence policy. The CSDP gives the Union the power to carry out military, civilian and

[15] European Organisation for Security (2011). Steps towards implementing a European cyber-security strategy. pp 33: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf
[16] Neelie Kroes (2013) *Towards a coherent international cyberspace policy for the EU.*
[17] Rosamond (2000). pp. 166
[18] European External Action Service: About CSDP: http://eeas.europa.eu/csdp/about-csdp/index_en.htm
[19] Deighton, Anne (2002). pp. 722 http://onlinelibrary.wiley.com/doi/10.1111/1468-5965.00395/pdf

conflict prevention actions under its own flag without having to rely on other power institutions, such as the United Nations.[20]

The EU adopted its first comprehensive security strategy in 2003, labelled "A Secure Europe in a Better World." This was the first step towards a coherent security strategy for Europe, a new turning-point in the development of EU's self-awareness and its practical cooperation in the field of security.[21]

The EU's new broad awareness of its capacities and responsibilities as a security actor and has thus taken steps towards creating a cyberspace policy for the EU, as is evident by the "Digital Agenda", and Directive 2013/40/EU on attacks against information systems, putting forward regulations regarding cyber-crime.

The EU´s cyber security strategy stretches across the fields of the internal market, justice and home affairs, and CFSP insofar as there are foreign policy angles to cyberspace issues. The Strategy sets four main goals for the EU's international cyberspace policy. First is Freedom and openness, where the strategy outlines the vision and principles on applying the EU's core values and fundamental rights in cyberspace. Secondly, the laws, norms and EU's core values should apply as much in cyberspace as in the physical world. Thirdly, developing cyber security capacity building will engage the EU with international partners and organisations. Fourth and lastly, the goal should be to foster international cooperation in cyberspace issues to preserve an open, free and secure cyberspace. This is a global challenge and the EU sets to address it together with international partners and organisations. With such documents and other practical steps the EU has made moves towards a coherent cyber security policy for Europe; but to better understand its approach and direction, the EU framework for action now needs to be examined in more detail.

3.2 European Foundations: the Council of Europe Convention.

Among regional cooperation in cyber security it is worth mentioning the efforts made by the Council of Europe, and the adoption of the Convention on Cyber-Crime and its additional Protocol, opened for signatures in 2001 and entered into force 1st of July 2004.[22] The Council of Europe Convention is the first and so far the only multilateral legal instrument to deal with cyber-crime, and it provides a basic framework for the establishment by contracting states of

[20] Kaczorowska (2011). Pp. 118
[21] Dinan (2005). Pp. 559
[22] Council of Europe Convention on Cyber Crime (2001).
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

domestic substantive and procedural law aimed at combating all types of computer related crimes.[23] In 1999 the EU – which at that time had no mandate to establish a similar legal framework on the issue itself - expressed its perspective at the Convention of Cyber-Crime in a common position, calling for Member States to support its preparation. In fact, several EU Member States contributed to the drafting, with the Stockholm programme entering into force in 2010, and its focus on internal security issues,[24] the EU not only called upon Member States to ratify the Council of Europe Convention but also stated that in the EU's view this instrument should become the legal framework of reference for fighting cyber-crime at global level.[25] The Convention has indeed provided the base of subsequent EU legislation on the matter, which was the groundwork for the Council Framework Decision on Attacks against Information Systems of 2005.[26]

3.3 EU Policy: The Role of Institutions

The EU´s Institutions and Treaties have had a strong impact on the development and process of cyber security policy making and implementation within the EU. Cyber security is an indisputable cross-border phenomenon and cross-sectorial by nature. Therefore, any policy related to cyber security can only be transversal, which makes the approach to the subject complex.

3.3.1 The Institutions

Given its executive authority in the Union, the European Commission (The Commission) has been a leading force in the creation of a cyber security policy in the Union. The Commission is the institutional body which represents the interests of the EU through common action and the exercise of supranational powers, especially within the EU's own territory.[27] It exercises many functions, of which the most important one is to promote the general interests of the Union and take appropriate measures to that end. The Commission is in all the guardian of Treaties, initiator of EU legislation, the executive arm of the EU, and the representative of its collective identity in the international arena.[28] As in all democratic institutions, power is divided, and so it is in the Union. For a legislative proposal to become Union law, the Commission proposes new law, and

[23] Pocar, Fausto (2004). Pp 30: http://link.springer.com/article/10.1023%2FB%3ACRIM.0000037565.32355.10
[24] European Council (2010). The Stockhom Programme http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:01:EN:HTML
[25] International Telecomunication Union. *Understanding cybercrime: Phenomena, challenges and legal response (2012) pp. 135 http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*
[26] Porcedda, Maria Grazia (2012). Pp. 4
[27] European Union: European Commission „How it works" : http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm
[28] Kaczorowska (2011). Pp. 143

then it must be adopted by the Council of European Union (the Council) and the European Parliament (Parliament). It is then the duty of the Commission to follow up and ensure that the laws are properly applied and implemented by the Member States. These three institutional bodies of the Union produce the policies and laws that apply throughout the Union.[29]

The Commission, along with its legislative power, also has substantial power over the Union's budget and allocation of funds. With the Council and Parliament, the Commission sets the long-term spending priorities for the Union in the EU Financial Network. It also has an impact on the annual budget for approval by Parliament and the Council, as well as supervising how EU funds are spent, by agencies and national and regional authorities. The Commission manages funding for EU policies such as cyber-crime, which weighs heavily against any protests against the Commission's Cyber Security initiatives.

The most important aspect of the Commission's power with regards to the development of Cyber Security is its role as "Guardian of Treaties", and its power to enforce EU law. If the Commission believes a national government is failing to apply correctly EU law, the Commission has the authority to first send an official letter asking the Member State to correct the problem; after which, as a last resort the Commission can refer the issue to the European Court of Justice (ECJ). The ECJ, after receiving a request from the Commission, can impose penalties and its decisions are final and binding on all Member States.[30] The Commission's role as the enforcer of EU law is extremely important in the light of Cyber Security initiatives. The main reported problem in directives combatting cyber-crime has been that there are gaps in implementation and enforcement across the EU, notably in terms of national capabilities and coordination in case of incidents spanning across borders.[31]

Union law has direct effect and supremacy over national law. In the context of the EU, direct effect means that some provisions of EU law may give rise to rights that individuals (natural and legal persons) can enforce before natural courts. These rights flow directly from EU law and are entirely independent of national law. Individuals can rely on directly effective provisions of EU law in the absence of, or against national provisions. In order for a provision to have direct effect, it must be clear, precise, and unconditional, and it must confer rights upon individuals. The application can therefore not depend upon the adoption of further implementing measures, either at national or EU level.[32] The founding Treaties and their

[29] European Union: Institutions and Other bodies: http://europa.eu/about-eu/institutions-bodies/index_en.htm
[30] European Union: European Commission „How it works" : http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm
[31] European Commission (2013). Cyber Security Strategy of the European Union: An Open and Secure Cyberspace. pp. 5: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[32] Kaczorowska (2011). Pp. 305

amendments do not rule on the issue of priority between national and Union law. The Treaty of Lisbon, does however, confirm that in accordance of case law of the European Court of Justice, the Treaties and law adopted by the Union have primacy over Member States, without mentioning it directly.[33]

Although the power of the Commission as an executive branch of the EU has played a vital role in the development of cyber security measures in the Union, none of it would have been possible without the creation and development of the "Area of Freedom, Security and Justice" (AFSJ). The AFSJ was created to ensure the protection of EU citizens, and it covers policy areas such as judicial and police cooperation in criminal matters. While drawing on the previous work of Pillar Three, the AFSJ was launched at the same time as the "Three Pillar" structure of the EU was abolished, with the entry into force of the Lisbon Treaty on December 1st in 2009. With the Treaty of Lisbon, it opened the way for the AFSJ to be brought within the scope of EU law, and legislative proposals to be adopted when appropriate under ordinary legislative procedure. The AFSJ also introduces institutional changes to the power structure of the Union. National Parliaments have a time limit for their examination of legislative proposals, the Commission can bring proceedings for failure to fulfil an obligation against Member States that do not comply with the provisions concerning the AFSJ, and further bodies and agencies have been set up to help oversee policies in a number of important areas of the AFSJ. [34]

The Union has with its Treaties, legislation, and directives, set up bodies and agencies within the Union for cooperation in the field of Cyber Security: a special division of EUROPOL, European Union Agency for Network and Information Security (ENISA) and the European Forum for Member States (EFMS).

3.3.1.1 Cyber Security Institutions

The EU has two main forums for cooperation and information sharing regarding cyber security, ENISA and the EFMS. The EFMS was established in 2009 as a follow up to the policy initiative on Critical Information Infrastructure Protection (CIIP) adopted by the Commission.[35] It was set up in cooperation between the Commission and ENISA, and builds on national approaches to CIIP. The EFMS is used to foster common understanding of cyber

[33] Kaczorowska (2011). Pp. 341-342
[34] European Parliament. An Area of Freedom, Security and Justice: General Aspects. http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_5.12.1.html
[35] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 98: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

security issues and strategies to deal with them,[36] providing a platform for representatives from national public authorities to present and review public policy matters relevant to CIIP. The EFMS is not involved in technical and operational issues, but these informal discussions may rather complement and give further support for formal decision-making processes.[37]

There are limitations to EFMS, Member States tend not to share important information on incidents, risks, and threats within the EFMS. As the EFMS is only a forum for Member States to communicate and cooperate in the area of cyber security, it has no power to make it a requirement for its Member States to have minimum capabilities in place, or even enforce it.

ENISA provides support and advice to the Commission and Member States with the goal to improve the overall level of NIS in the EU. However, ENISA has no institutional powers and cannot intervene to fix NIS problems. It is an independent institution set up for an independent advisory role. An external evaluation of ENISA in 2007 concluded that the added value of ENISA is lies in its ability to provide an independent platform to assess problems and put forth solutions regarding NIS.[38]

EUROPOL´s EC3 (European Cyber Crime Centre) division specialises in cyber-crime and was established to tackle three main areas of cyber-crime: that committed by organised groups to generate large criminal profits such as online fraud; that which causes serious harm to the victims, such as online child sexual exploitation; and that which affects critical infrastructure and information systems in the EU.[39] The EC3 is intended to pull together European cyber-crime expertise to support Member States in capacity building, providing support to Member States' cyber-crime investigations, and to become a voice of the European cyber-crime investigators across law enforcement.[40]

EU legislation requires that relevant data should be made available to the competent specialized Union agencies and bodies, such as EUROPOL. The EC3 division needs information to gain a more complete picture of the problem of cyber-crime and NIS at EU level and thus contribute to formulating a more effective response. Member States should submit information on the modus operandi of the offenders to EUROPOL and its EC3 crime centre for the purpose of conducting threat assessments and strategic analyses of cyber-crime

[36] Purser, Dr. Steve. (2011). http://www.mediacom.public.lu/cybersecurity/LUX_Cybersecurity_23_11_11.pdf
[37] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 97: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf
[38] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 28: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf
[39] Europol. European Cybercrime Centre. https://www.europol.europa.eu/ec3
[40] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 67: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

in accordance with Council Decision 2009/371/JHA of 6th of April 2009 establishing Europol.[41]

These three institutions provide a platform for cooperation in the field of cyber security and enhance information sharing about NIS risks and threats, although it does not provide an authority enforcing cooperation and information sharing. None of these institutions has the legal competence to provide for action and sanctions against Member States, when they fail to cooperate.

ENISA and Europol's EC3 Centre are the main institutions providing support for Computer Emergency Response Team's (CERT´s) and information sharing amongst Member States. Although information sharing is required, the level of information sharing through ENISA and EC3 is not at the appropriate level as some Member States are lacking in cyber security resilience. ENISA´s new regulation gives it the scope to closely cooperate with EUROPOL in supporting the fight against cyber-crime, but ultimately EUROPOL is the agency that coordinates law enforcement efforts in combatting cyber-crime.[42]

The EU has set up institutions to respond to cyber-crime, and each has their mandate and institutional respond. However, it all begins with the treaties which give the institutions their framework and mandate to respond to cyber-crime.

3.3.2 The Lisbon Treaty

With the entry into force of the Treaty of Lisbon in December 2009, the EU has begun a new chapter in its existence. Under the new Treaty the EU is designed to be more democratic, providing a very high level of protection of human rights to its citizens, and giving its Institutions the power necessary to meet the 21st century challenges head on, speedily and efficiently. [43]

The Treaty of Lisbon changed the functioning of the EU significantly and for the first time provided the EU with a solid framework in the field of cyber-crime. Article 82, along with Article 86 of the Treaty on the Functioning of the European Union, provides the EU with a mandate for harmonizing criminal law legislation. Article 82, paragraph 1, states that:

"Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation

[41] European Parliament (2013). Directive 2013/40/EU On attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJL 218/8. pp. 3
[42] ENISA (2013). Cybersecurity cooperation: Defnding the digital frontline . pp. 11. http://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline
[43] Kaczorowska (2011). Pp. 3

of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83."[44]

Article 83 of the Treaty on the Functioning of the European Union is most relevant with regard to cyber-crime as it authorizes the EU to establish minimum rules concerning the definition of criminal offences and sanctions in relations to serious crime with a cross-border dimension.[45] Article 83, paragraph 1, states that:

"The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.

These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. It shall act unanimously after obtaining the consent of the European Parliament."[46]

The term "Computer Crime" is used in Article 38, and as the term is broader than cyber-crime it authorizes the EU to regulate both areas and make more advances towards a cyber-crime policy.[47]

Given that the EU is an intergovernmental institution, and not a supranational government, a cyber-crime policy has taken time to emerge. Slowly, with institutional changes, shifts in security strategies around the world, and recent events in global security, cyber security has gained acknowledgement as an important area for strategy in states, international organizations, and other settings such as business and citizens' networks.

In August, 2013, Directive 2013/40/EU came into effect, replacing Council Framework Decision 2005/222/JHA. This Directive is the first comprehensive policy document on cyber security produced by the Union. It covers the internal market, justice and home affairs, and

---

[44] Consolidated Version Of The Treaty On The Functioning Of The European Union (2010). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF

[45] International Telecomunication Union. *Understanding cybercrime: Phenomena, challenges and legal response (2012) pp. 128 http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

[46] Consolidated Version Of The Treaty On The Functioning Of The European Union (2010). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF

[47] International Telecomunication Union. *Understanding cybercrime: Phenomena, challenges and legal response (2012) pp. 129 http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

foreign policy aspects of cyberspace issues. This directive is part of the "Digital Agenda" set up by the EU for 2020, and is set up to offer clear priorities for the EU's international cyberspace policy. The new policy has four key objectives: first, to outline the vision and principles for applying the EU's core values and fundamental rights in cyberspace. Secondly, to secure the application of laws, norms and EU core values so that they apply equally in cyberspace as in the physical world. Thirdly, to develop cyber security capacity-building, the EU will engage with international partners and organisations. Fourthly, to foster international cooperation in cyberspace issues, with the goal of preserving an open, free and secure cyberspace.[48]

3.4 Cyber Security in the European Union: Legal Framework

The EU´s first approach to cyber-security hinged on the relevance to the development of the internal market. The White Paper on Growth was published 5th of December in 1993, acknowledging the delay of the EU in developing a profitable e-market vis-à-vis the United States and encouraged to remove all obstacle hindering its pursuit, i.e. creating favourable conditions for the development and strengthening of cyber security. [49]

The EU made its first step towards cyber security more specifically in 1996, when it addressed risks related to the internet in a communication from the Commission to the Council, dealing with illegal and harmful content on the internet.[50] The EU highlighted the importance of cooperation between Member States to combat illegal content online. The next step came in 1999, when the European Parliament and the Council adopted an action plan on promoting safe use of the internet and combating illegal and harmful content on global networks. The plan focused on self-regulation rather than criminalization, thereby falling short of address security breaches as a crime.

In 2001 the Commission published a communication titled "*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer related Crime*". In this communication the Commission analysed and addressed the problem of cyber-crime and pointed out for the first time the need for effective action to deal with threats to information systems. In addition, the Commission also published a communication on "*Network and Information Security*", which analysed the problems in network security and

[48] European External Action Service: EU Cyber Security Strategy. http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm
[49] Porcedda, Maria Grazia (2012). p. 10; Commission of the European Communities, *Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century. White paper*, COM(93) 700, 5 December 1993.
[50] International Telecomunication Union. *Understanding cybercrime: Phenomena, challenges and legal response (2012) pp. 129 http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

drafted a strategic outline for action. Both communications advocated the need for approximation of substantive criminal law within the EU. Harmonization of substantive criminal law within the EU in the fight against cyber-crime was now fully recognized as a key element and further development was needed.[51]

3.4.1 Council Framework Decision 2005/222/JHA: on attacks against information systems

In 2005 the Commission adopted a framework Decision on attacks against information systems. It was the first law explicitly harmonizing the criminalization of malicious conduct online.[52]The objective of the framework decision was to improve cooperation between judicial and other competent authorities, including the police and other specialized law enforcement services of the Member States, through approximating rules on criminal law in Member States in the area of attacks against information systems. It concentrated on the harmonization of substantive criminal law provisions designed to protect critical infrastructure elements. The decision highlighted the gaps and differences in the legal frameworks of the Member States and effective police and judicial cooperation in the area against information systems.

In Article 1 of the Framework Decision, an 'information system' is defined as any device or related devices performing automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purpose of their operation, use, protection and maintenance. The Directive also defines, 'computer data', and 'legal persons'.[53]

The Directive has been implemented in different ways in the Member States. In some states the wording of the national law is close to that used in the Directive, but in other a more general and indirect method has been used. One result is that the legal concepts and expressions used are not easily comparable.[54]

Article 2 of the Framework Decision, on Illegal Access to Information Systems, states that Member States shall take the necessary measures to ensure that intentional access without right to the whole or any part of an information system is punishable as a criminal act.[55]

---

[51] International Telecomunication Union. *Understanding cybercrime: Phenomena, challenges and legal response (2012) pp. 130 http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*
[52] Porcedda, Maria Grazia (2012). Pp 21.
[53] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[54] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 3
[55] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67

Member states are obliged to incorporate provisions in their national legislation to ensure that intentional access to an information system without permission is punishable as a criminal offence. Paragraph 1 of Article 2, however, allows Member States the option to criminalize such conduct only for cases 'which are not minor'. Such room for divergence of interpretation and the option for a state not to criminalize certain acts poses a serious risk to the objective of approximating Member States' rules on criminal law in the area of cyber security.[56]

Article 3 of the Framework Decision, on Illegal System Interference, states that each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system is punishable as a criminal offence when committed without right, at least in cases which are not minor.[57] This provision of the Directive aims at protecting the integrity of information systems. The concept of 'minor case' must refer to cases where the system interference as such is of minor importance or where the integrity of the information system is only interfered with to a minor degree. Six Member States opted to implement the 'minor clause' of the Directive; in doing so they also claimed that their national models cover such circumstances of 'minor cases'. [58]

In Article 4 of the Framework Decision, on Illegal Data Interference, each Member State shall take the necessary measures to ensure that the intentional deletion, damaging deteriorating, alteration, suppression or rendering inaccessible computer data on an information system is punishable as a criminal offence, when accessed without permission, at least in cases which are not minor.[59]

Many Member States have opted to implement Article 3 and 4 in a single provision. The final sentence of this Article allows Member States the option to criminalise such conduct only 'for cases which are minor'. The option has been used by three Member States, which claim that their national law covers such incidents. Again, their national law varies and it is therefore hard to make an overall comparison.[60]

Article 5 of the Framework Decision, on Instigation, aiding and abetting and attempt, it states that each Member States shall ensure that instigation of, aiding and abetting as well as

[56] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp.4
[57] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[58] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 5-6
[59] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[60] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 6

the attempt to commit, an offence is punishable as a criminal offence.[61] The Member States have the option of deciding not to apply the obligation to ensure that any attempt to commit the offence of illegal access to information systems is punishable. Only two Member States have opted to not apply the obligation to ensure any attempt of access to information system is punishable as a criminal offence.[62]

In Articles 6 to 7 in the Framework Decision, Penalties and instances of aggravating circumstances are explained. Article 6 of the Directive ensures that Member States take necessary measures to ensure that offences referred to in Article 2, 3, 4 and 5 are punishable by effective, proportional and dissuasive criminal penalties. This means that the offences referred to in Articles 3 and 4 are punishable by a maximum of at least between one and three years of imprisonment.[63]

Article 7 of the Directive, allows for a higher maximum punishment in cases of 'aggravating circumstances'. In such cases, the offences referred to in Articles 3 and 4 are punishable by criminal penalties of at least between two and five years of imprisonment when committed within a framework of a criminal organisation.[64]

Generally speaking, EU Member States have made sure that the offences referred to in Articles 2-5 of the Directive are punishable by reasonably effective criminal penalties. However, the situation regarding the obligation to take into account 'aggravating circumstances' for an offence committed within a framework of a criminal organization is more varied. Member states have either chosen to make no reference to criminal organizations, or still need to make adjustment to their laws in order to fully comply with the Directive.[65]

In Articles 8 and 9, the Framework Directive elaborates further on the liability of legal persons and penalties for legal persons. Member states shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person. Member states must also ensure that a legal person can be held liable where the lack of supervision or control by a legal person referred to in paragraph one of Article 8, of the Directive.[66]

---

[61] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[62] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 7
[63] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[64] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[65] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 7
[66] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67

Under Article 9, Member States must take the necessary measures to ensure that a legal person held liable pursuant to Article 8, is punishable as a criminal offence. Punishments shall include criminal or non-criminal fines and may include other penalties further described in Article 9, paragraph 1.[67]

Member states have for the most part fulfilled their obligation and taken necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2-5. However, four Member States did either not fulfilled their obligation to enact relevant rules on the liability of legal persons, or claimed that their rules on civil liability covered all cases described in Article 8. Member states who enacted measures correctly implementing Article 8 also fulfilled their obligation and took the necessary measures to ensure that a legal person held liable pursuant to Article 8 shall be punishable by effective, proportionate and dissuasive penalties.[68]

Article 10 of the Council framework, on jurisdiction, states that each Member State shall establish its jurisdiction with regards to the offences referred to in Articles 2-5, where the offences have been committed within its territory, by one of its nationals, or for the benefit of a legal person that has its head office in the territory of a Member State. When a Member State does not surrender or extradite its own nationals, it shall take the necessary measures to establish jurisdiction over and to prosecute the offences referred to in Articles 2-5, in appropriate cases.[69]

Different methods have been implemented for legislating on jurisdiction across Member States, and this makes comparison more difficult. Paragraph 5 of the Council Framework provides an option for Member States not to apply, or to apply only in specific cases or circumstances, the jurisdiction rules set out in paragraphs 1(b) and 1(c). A total of 9 Member States have used the option provided for in paragraph 5, using either option 1(b) in the case of an offence by one of its nationals, or 1(c) for the benefit of a legal person that has its head office in the territory of that Member State.[70]

3.4.1.1 Implementation

By 1st of June 2008 the Commission had received notifications or replies to the reminder about implementation of the Framework Decision from 23 Member States. No replies were

[67] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[68] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 8
[69] European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[70] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 9

received from Malta, Poland, Slovakia and Spain, In addition to missing replies, the answers received from Ireland, Greece, and the United Kingdom did not allow for any assessment of the implementation, since they reported that implementation had been delayed.[71]

The European Commission Impact Assessment Board published an Opinion in 2009, where it identified three key issues that required further action. The first was the enhanced penalisation of and approximation of criminal laws against cyber-crime as an effective measure to combat cyber-crime. The level of penalties in some Member States indicated that they considered the crimes insufficiently serious to warrant rapid enforcement or the use of certain investigative techniques and tools. Ways should be found to clarify and guarantee the necessary level of commitment among the Member States to implement the voluntary measures. The second issue was to gain a clearer understanding about the appropriate level of action. The Member States which had not experienced large-scale attacks were lacking in incentives and experience to upgrade their legislation on their own. The third and final issue was the need to strengthen the joint analysis in support of a joint approach to setting the level of penalties for large-scale attacks. Further clarification was needed to support the choice of minimum level of the maximum penalty of 5 years.[72]

3.4.2 Digital Agenda For Europe

Security threats were highlighted by recent attacks across Europe following the adoption of the Framework Decision. The emergence of a large scale simultaneous attacks against information systems in Estonia (2007) and Lithuania (2008), and increased criminal use of botnets, grabbed our attention. These attacks highlighted problems that were not so clearly in focus when the Framework decision was adopted, and in response the Commission had to consider further action aiming at better solutions for cyber security.[73]

In its Report of 2008 to the Council on Framework Decision implementation,[74] the Commission pointed to a possible future need for specific criminalization of certain activities that facilitate criminal use of botnets, and tougher minimum penalties for offences committed in the form of massive and particularly dangerous attacks against information systems.[75]

[71] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 2-3
[72] European Commission (2009). Impact Assessment on: Proposal to amend Framework Decision 2005/222/JHA on attacks against information systems. pp. 2
[73] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems.pp. 10
[74] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems.
[75] European Commission (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems. pp. 10

Since then, the EU has continued to work to fill the gaps in its current framework on cyber security. The Commission was not convinced that the current voluntary approach was enough to provide sufficient protection against network and information security incidents and risks across the EU, or to keep up with the fast changing landscape of cyber threats. Accordingly, on the 12th of August 2013, Directive 2013/40/EU of the European Parliament and of the Council, on attacks against information systems replacing Council Framework Decision 2005/222/JHQ, came into force. The new regulation is designed to fill in the gaps and shortcomings of the previous Framework Decision, and set the groundwork for a coherent EU Cyber Security Policy.

The new Directive sets minimum levels of national capabilities by requiring each Member State to establish a competent authority for NIS, set up CERTs, and also adopt national NIS strategies and national NIS cooperation plans.[76] It further requires the disclosure and sharing of information between these national authorities, supported by ENISA and the new Europol Cyber-crime centre, known as the Network and Information Security Directive. The aim is for the EU to effectively prevent and respond to cyber threats and attacks.[77]

3.4.2.1 Directive 2013/40/EU

-of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

The European Parliament has recently approved a Directive by 541 votes to 91, which has replaced and updated Framework Decision 2005/222/JHA.[78] The new Directive addresses the three key issues reported earlier from Framework Decision 2005/222/JHA. The objective of Directive 2013/40/EU is to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions.

The new Directive covers areas previously left out in Directive 2005/222/JHA. Illegal interception of information systems is introduced as a new offence in Article 6. Member States shall take the necessary measures to ensure that intercepting private transmission of computer data, to, from, or within an information system, is punishable as a criminal offence.

Requirements for penalization of the use of tools, such as malicious software, for committing offences are laid out in Article 7. The Member States shall take the necessary

[76] Wong (2013). *Data Security Breaches and Privacy in Europe.* pp. 40
[77] Wong (2013). *Data Security Breaches and Privacy in Europe.* pp. 40
[78] Wong (2013). *Data Security Breaches and Privacy in Europe.* pp. 31

measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, is punishable as a criminal offence, when used to commit any offences laid out in articles 3 to 6.

Articles 13, Exchange of Information, and article 14, Monitoring and Statistics, lay's out new measures to improve European criminal police cooperation, by strengthening the existing structure of 24/7 contact points, including an obligation to answer an urgent request within 8 hours and also the obligation to collect basic statistical data on cybercrimes.

Furthermore, in Article 9, the Directive states that Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by a maximum term of imprisonment of at least two years, which is an increase from Directive 2005/222/JHA where the maximum penalties was between one and three years' imprisonment. As well as raising the minimum penalty, instigation, aiding, abetting and attempting of those offences have become penalized as well, as laid out in Article 8.

The Directive also raises the level of criminal penalties for offences committed within the framework of a criminal organization, where the maximum penalty is at least five years, and it also adds new aggravating circumstances. First there is the case when a significant number of information systems have been affected through the use of a tool - maximum penalty at least three years; second case, when causing serious damage - at least five years; and finally in cases when committed against a critical infrastructure information system, where the maximum penalty is at least five years.[79]

The EU has made progress with the new Directive, and fixed some of its predecessor's loopholes in the Framework. It is however important to discuss the other aspect of Cyber Security, Data Protection and Privacy, the element cyber security is set to protect.

3.5 Data Protection and Privacy

The rapid technological change and globalization have transformed the way in which an ever increasing volume of personal data is collected, accessed, used and transferred. Your whole life can now be uploaded to your icloud, account, storing all your photos, documents, music, contacts and personal information and social accounts. This has become part of life for many of Europe's 250 million internet users. Individuals have the right to enjoy effective control over their personal information and that right is protected in Article 7 of the Charter of

[79] European Commission (2013). Questions and Answers: Directive on attacks against information systems : http://europa.eu/rapid/press-release_MEMO-13-661_en.htm

Fundamental Rights of the European Union, and the right to data protection enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, and needs to be protected accordingly.[80]

3.5.1 Data Protection: Directive 95/46/EC

The EU´s milestone in Data Protection was Directive 95/46/EC of the European Parliament and of the Council of 24th of October 1995, on the protection of individuals with regard to the processing of personal data and in the free movement of such data. It was designed with the aim of protecting fundamental rights and freedoms of citizens and in particular their right to privacy with respect to the processing of personal data.[81] The Directive applied to data processed by automated means (e.g. a computer database of customers) and data contained or intended to be a part of non-automated filing systems (traditional paper files). It did not apply to the processing of data in the case of a natural person in the course of personal or household activities, or in the course of an activity which falls outside of the scope of EU law, such as operations concerning public security, defense or state security. Under the Directive, personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be accurate, and where necessary, be kept up to date.[82]

The Data Protection Directive harmonises Member States national law with the aim to protect the fundamental right to privacy with respect to the processing of personal data, and provide for the free flow of personal data between Member States.[83] In the years since the Data Protection Directive was established, the Member States have reacted to new advances in technology in different ways and thus contradicting the purpose of the Directive, to harmonize Data Protection Law in the EU and amongst its Member States.[84]

A lot has changed in the way we process data and protect it. Recent events such as Wikileaks and Edward Snowden highlight the need for protection of personal data, and also the need of reform of current legislation. It is an understatement saying that the 1995 Data Protection Directive is out dated, but the Commission has since 2009 been preparing the

---

[80] European Commission (2012). Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. Pp. 2

[81] European Parliament (1995). Directive 95/46/ on the protection of individuals with regard to the processing of personal data and on the free movement of such data. pp. 8
: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF

[82] European Parliament (1995). Directive 95/46/ on the protection of individuals with regard to the processing of personal data and on the free movement of such data. pp. 8
: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF

[83] Irion and Luchetta (2013). Pp. 15

[84] European Commission (2013.) The EU´s Data Protection rules and Cyber Security Strategy: two sides of the same coin. Press Release SPEECH/13/436. Pp 3.
: http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm

reform of the EU´s data protection act. These reforms include the EU engaging in dialogue with stakeholders, launching public consultation on data protection, and exploring options for a more consistent application of EU data protection rules across all EU Member States.[85]

3.6 Processing of Data by Authorities: Directive 2008/977/JHA

The Directive applies to all processing made by any public authority for the prevention, investigation, detection or prosecution of criminal offences. The Directive provides a distinction between different categories of data subjects, lays down rules on the different degrees of accuracy and reliability of personal data, profiling and the processing of sensitive data.[86]

The processing of data by police and judicial authorities in criminal matters relevant to their investigation is currently principally covered by Framework Decision 2008/977/JHA. The Commission has no power to enforce its rules, and that has led to uneven implementation as each Member State has implemented the regulation as they seemed appropriate.

The scope of the Framework Decision is limited to cross-border processing activities, causing the processing of personal data that has not been made the subject of exchanges and is therefore currently not covered by EU rules governing such processing and protecting the fundamental right to data protection. This creates uncertainty for police authorities and whether data processing is to be purely domestic or cross border.[87]

The entry into force of the Lisbon Treaty, and the introduction of a new legal basis allows the establishment of a comprehensive data protection framework ensuring a high level of protection for individuals' data whilst accommodating the specific nature of the field of police and judicial cooperation in criminal matters. This allows the revised EU data protection framework to cover both cross-border and domestic processing of personal data, which will reduce differences between the legislation in Member States for a stronger protection of personal data overall. [88]

The Directive is faced with two main problems, attributing jurisdiction when data is processed and providers are established in several locations. Also, the lack of mechanisms to

[85] European Commission (2012). Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. Pp. 3
[86] Porcedda, Maria Grazia (2012). Pp 64.
[87] European Commission (2012). Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. Pp. 10
[88] European Commission (2012). Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. Pp. 9

prevent third states from breaching EU data protection standards when accessing data in relation to EU citizens, whether upon transfer of data, or forced access.[89]

3.6.1 Data Retention: Directive 2006/24/EC

Telecommunication data are extremely valuable for police and judicial authorities for their investigations, prosecution of crime, and protection to citizens. EU law calls for telecommunications service and network providers to retain certain categories of data for a specific period of time and to make them available to law enforcement where needed.[90] This Directive aims at harmonizing Member States provisions concerning the obligations of providers to retain certain data in order to ensure its availability for law enforcement.[91]

Telecommunication service providers or operators store their clients´ personal data for the purposes of transmitting communications, invoices, and interconnection payments, marketing and certain other value-added services. Due to the value of these data in preventing danger and investigating criminal activity, the EU has sought to ensure that they are made available to law enforcement authorities.[92]

The Directive on Data Retention requires operators to retain certain categories of data for a period between six months and two years and to make them available on request to law enforcement authorities for the purposes of investigating, detecting, and prosecuting serious crime and terrorism.[93]

The Directive leaves it up to Member States to define a catalogue of serious crime for the investigation, detection, and prosecution of which the retained data can be accessed by the competent authorities. With Member States being able to categorize what is a serious crime results in uneven legal requirements under which the data can be accessed across the EU.[94]

On 12th of December 2013, the Advocate General of the European Court of Justice, Mr. Cruz Villalón, sent out an opinion stating the Data Retention Directive is incompatible with the Charter of Fundamental Rights. He however proposes, that the effects of the finding of invalidity should be suspended in order to enable the EU legislature to adopt the measures

[89] Porcedda, Maria Grazia (2012). Pp 65.
[90] European Commission: Data Retention: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm
[91] Irions and Luchetta (2013). Pp. 18
[92]European Commission: Data Retention: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm
[93]European Commission: Data Retention: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm
[94] Irion and Luchetta (2013). Online Personal Data Processing and EU Data Protection Reform. Pp. 22

necessary to remedy the invalidity found to exist.[95] This shows the determination of the EU and a united front of its institutions to pave the way for a cyber security policy for Europe.

3.6.2 Reform of Data Protection and Privacy in the EU

In January 2012 the Commission proposed a major reform of the EU legal framework on the protection of personal data.[96] The new proposals will aim at strengthening individual rights and tackle challenges of globalisation and new technologies, something that has been greatly lacking in recent years. The two major themes of the new directive are the protection and free flow of personal data.[97]

The proposal for reform will first and foremost focus on strengthening individual's rights to data protection and building their trust in the digital environment. The reform will furthermore simplify the legal environment for businesses and the public sector substantially. The EU is expecting this to stimulate the development of the digital economy across the EU´s Single Market and beyond. Finally, the reform is set to enhance trust among law enforcement authorities in order to facilitate exchanges of data between them and cooperation in the fight against cyber-crime whilst ensuring a high level of protection for individuals.[98]

EU citizens are increasingly more aware of risks related to Cyber Security, and frequently increasing number of individuals are worried about the possibility of themselves becoming a victim of cyber-crime.[99]The EU is no less ambitious in its quest to build a comprehensive and harmonized Data Protection policy, than it has been regarding cyber-crime. It is imperative to the Commission that the reform design of Data Protection and Privacy policy of the EU is drafted in a way that renders the fight against cyber-crime 'winnable'. This proposes some difficulties in regards to privacy in the digital age and raises the question as to what extent the EU is willing to go to protect its citizens against cyber-crime.

[95] Court of Justice od the European Union (2013). Press Release No 157/13. Pp 1. http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf
[96] European Commission: Data Protection: http://ec.europa.eu/justice/data-protection/
[97] European Commission: Data Protection: http://ec.europa.eu/justice/data-protection/
[98] European Commission (2012). Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. Pp. 12
[99] European Commission (2013.) The EU´s Data Protection rules and Cyber Security Strategy: two sides of the same coin. Press Release SPEECH/13/436. Pp 4.
: http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm

4 Assessing the cyber risks

The legal framework of the EU in combatting cyber-crime provides an overview of the tools the EU has at its disposal in combatting cyber-crime. It is also important to evaluate the risks and threats the EU faces every day and how do the legal frameworks measure up against these risks? The cyber security challenge facing the EU can be described overall as an insufficient level of protection against NIS incidents, risks and threats across the Union, its Member States and institutions. The lack of security in place risks undermining the proper functioning of the internal market. The Commission conducted and published an Impact Assessment of cyber security in the EU in early 2013.[100] This assessment highlighted the five key problem areas of cyber security for the safe functioning of the Union.[101]

Internal Market disruptions[102] are caused by NIS incidents originating in a country, and if not appropriately contained, spreading quickly to other countries and thereby undermining the functioning of the internal market. Cross-border services can become unavailable and large-scale companies such as eBay or PayPal have either experienced web-based attacks that have made all or parts of their websites unavailable for periods of time. Any interference in the functioning of the internal market affects e-commerce and the free flow of capital and goods in the EU.[103]

NIS Incidents[104], can only be dealt with through cooperation among Member States. As previously mentioned, the lack of available information on NIS incidents can be due to various reasons, but these incidents are most commonly a result from human errors or malicious attacks. The human factor is of the utmost importance, as individuals often do not follow security regulations and it can cause a security breach. Such NIS incidents are triggered by negligence or distraction, e.g. by people using infected USB sticks, opening unsolicited emails, revealing passwords etc.[105]

---

[100] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 12: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[101] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 12: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[102] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 12: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[103] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 12: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[104] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 13: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[105] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 12: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

Malicious Malware and malicious attacks has been increasing at a steady pace. Web-based attacks increased by 36% between 2010 and 2011, and the total number of attacks by 81%. Malware can mutate as it spreads, and the attackers are able to generate an almost unique version of their malware for each potential victim, which makes the detection of malicious malware ever more challenging. There is strong reason to believe that only a fraction of incidents which discovered, are disclosed. The lack of information on incidents hampers the capability to react and to take the appropriate measures.[106]

Economic interconnectedness, as NIS attacks tend to affect economic actors alike,[107] they spread quickly through the economic system affecting private, public, small and large scale organizations.[108] Public administrations, businesses and consumers are dependent on the usage of ICT, e.g. online services everyday. Given the critical role of networks and information systems, the possibility of an attack or system failure would spread to all corners of society. Businesses and other organisations can be seriously affected if the networks and information systems who run their operations are compromised. If Google´s server or Apple´s icloud became unavailable or targeted by a cyber attack it would hurt individuals and businesses alike.[109]

However, there are particular sectors which are more vulnerable and others.[110] The problems described above do affect all parts of society and the economy in the EU, but a number of sectors, infrastructures and service providers are extremely vulnerable due to their high dependence on correctly functioning network and information systems, and also their essential role in providing key support services for society and the economy. Hospitals, police authorities, social welfare systems, governmental systems, banking systems, these are all systems that rely on a fully functioning and protected infrastructure.[111]

With out affirmative action at EU level, consumer confidence could be undermined in the internal market, and could spread across Member States. The number of NIS incidents and

---

[106] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 15: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[107] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 15: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[108] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 15: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[109] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 16: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[110] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 17: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[111] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 16: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

their consequences could continue to increase, causing negative effects on the use of online public and private services, consumers' trust in the online economy, and the integrity of the internal market.[112]

A second consequence would be insufficient business investment in NIS. Businesses are lacking in risk management as there is no consensus to do so, no incentive which could lead to adaptation of appropriate NIS measures. Security is closely intertwined with the economy, it is an externality which can lead to a market failure and render society completely crippled and can spread to other economic systems affecting the world.

Third and lastly, failure in this field could create a lack of credibility for Europe in the international scene and thereby affecting commerce. The opportunity would be lost to coordinate activities at a global level and to achieve higher efficiency in addressing the problems. Furthermore, higher EU credibility in NIS could boost economic potential and support as such in the internal market.[113]

4.1 Cause and Effect

The main problem drivers for the disruption of the internal market through NIS threats to the EU are first and foremost to be found in the preparedness of Member States, their response to security incidents, and insufficient sharing of information on incidents, risks and threats.

Member states are at very different levels of capabilities which hinders Member States from trusting their counterparts, and trust is an important factor when it comes to cooperation and information-sharing. Only 11[114] Member States have a level of preparedness that is in accordance with the targets pursued by the Commission since 2009 (CIIP Action Plan and CIIP Communication of 2011).[115]

Public sector players dealing with NIS in the EU has expanded and now include a variety of ministries, agencies and National Regulatory Authorities. The profusion of existing bodies, each with different mandates, makes it difficult for Member States to identify the correct body to reach out to. Not all Member States have operational CERT's in place to handle and monitor NIS threats. This uneven level of preparedness stops Member States from fully

[112] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 16: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[113] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 16: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[114] Denmark, Finland, the Netherlands, Sweden, the United Kingdom, Austria, Belgium, Germany, Luxembourg, France and Ireland.

[115] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 24: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

cooperating with other European states, as was confirmed by a study undertaken by ENISA in 2012.[116]

Not all Member States have in place a detailed plan, providing protocols for communications and coordinated action in crisis situations. Most security breaches go unnoticed and unreported due to the reluctance of companies to share the information of fear of reputational damages or liability. What would happen if Google or Apple admitted to their services being at risk? The insufficient sharing of information on threats and risks results in underwhelming preparedness, and the insufficient sharing of incidents results in underwhelming response. The lack of reliable data and information on NIS threats and incidents make it difficult for governments and institutions to conduct effective policy-making and to respond to incidents affecting networks timely. [117]

[116] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 24: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

[117] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 25: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

5 The EU and Cyber Security: An Evaluation

After reviewing the institutional framework of the EU and the groundwork that has built the cyber security and data protection policy of the Union, there are still questions to be answered. Firstly, is the current system effective in reaching its security objectives, and secondly does it achieve the right balance? To answer these questions, it is necessary to review the overall level of protection against NIS incidents and threats, as well as the protection of data, by efforts of the EU.

The goal of the EU cyber security strategy is to protect Europe's society, its citizens, infrastructure and economies from cyber disruptions. The protection covers all phases from prevention to preparedness and response. This goal requires delivering the correct levels of speed and reach capabilities, through an end-to-end comprehensive approach supported by efficient governance for implementation and management, leveraging appropriate tools, leading to the consolidation of present initiatives and competences and the de-fragmentation of the market.[118]

As already stressed, NIS threats have a cross-border nature, and a lack of intervention at EU level would lead to a situation where each Member State is left to guard its own territory while ignoring the interdependence between existing network and information systems. An appropriate degree of coordination among Member States should ensure that NIS risks can be well managed in the cross-border context in which they also arise.

The importance of this cross-border element explains why enforcing standards at European level does not infringe the subsidiarity principle. Regulatory obligations are required to create a level playing field and close some legislative loopholes within and between nations. As discussed above, an initial purely voluntary approach resulted in cooperation only taking place amongst few Member States. In order to ensure cooperation encompassing all Member States it proved necessary to make sure that all of them have the required minimum level of capabilities.

Action at EU level is designed to improve the effectiveness of existing national policies and/or to facilitate their development. However, it is clear that concerted and collaborative NIS policy actions can also have a strong impact on the effective protection of fundamental rights, in particular the right to the privacy and protection of personal data. European citizens are increasingly entrusting their data to complex information systems, by choice or necessity,

[118] European Organisation for Security (2011). Steps towards implementing a European cyber-security strategy. pp 17: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf

without perhaps being able to correctly assess the related data protection risks. When incidents affecting individuals occur, they may not be able to take suitable steps, nor is it certain that the Member State involved would be able to effectively address incidents with a cross-border dimension.[119]

5.1 Is it effective?

When evaluating the effectiveness of EU framework, the focus is put on cyber-crime and institutional remedies against it. Cyber-crime raises several challenges for the EU effectively combatting it. The first concern is the complexity of ICT and how frequently unfamiliar it is to the traditional EU institutional and legal framework. As the ICT is a rapidly growing and changing sector, operators must constantly retain so that they are prepared for new risks and threats. Most cyber-crime occurs in a virtual environment, such as mobile phones or the internet, which frequently clashes with Member States jurisdiction and sovereignty.

Four arguments can be highlighted to evaluate the effectiveness of the EU´s preparedness against cyber-crime. *Firstly*, the framework of the EU´s cyber security measures approximates criminal law of Member States in the area of attacks against information systems by establishing minimum rules concerning cyber-crime. This aspect the EU has fulfilled effectively as the Framework Directive 2013/40/EU is explicit in its legislation regarding definitions, penalties and jurisdiction. The new Framework Directive takes a tougher stance on cyber-crime and provides for more severe penalties, something that was lacking in the previous framework. As the EU has provided for a clearer and more effective framework for cyber-crime, it has improved cooperation between competent authorities of the Member States as well as the competent specialised Union agencies such as Europol, ENISA and the EFMS. Without the harmonization of criminal law regarding cyber-crime, definitions, jurisdiction and penalties, the EU´s fight against cyber-crime would not prove to be effective at a Union level.

Secondly, the collection of statistical evidence is mandatory for Member States, which contributes to a better understanding of the problem and thus leads to better policies. Although the Framework Directive encourages information sharing, the implementation of information sharing remains a voluntary approach and is left up to the Member States to implement. The lack of a framework and infrastructure for sharing trusted information, based

[119] European Organisation for Security (2011). Steps towards implementing a European cyber-security strategy. pp 33: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf

on common confidentiality requirements, will also hinder exchanges at EU level. This will increase the gap between the high-performing and less-performing Member States.[120] It can be considered unlikely that all Member States will reach comparable levels of national capabilities and preparedness as a result of voluntary initiatives. As a consequence, and in the absence of a minimum level of national capabilities in all Member States, there is no guarantee that cooperation involving all Member States will take place. The EU has not provided for an effective framework regarding the collection and sharing of information, as it states in the new Framework Directive. The EU needs to take a clearer and tougher stance on information sharing and not only require cooperation of Member States but enforce it to build an effective pan-European cyber security network. A solution to create a more effective information sharing measure is introducing security requirements for public administration and key private players, which would create a strong incentive for those players to manage and share security risks effectively.

Thirdly, the EU explicitly criminalizes the use of botnets. As the development in cyber-crime has been towards increasingly dangerous and malicious large-scale attacks against information systems, it seems only appropriate that the EU step up to this development with a more effective framework against it. The new framework directive has criminalised the creation and use of botnets, and therefor Member States can now punish creators as well as users of botnets. This has provided the EU with an effective Framework for preventing a serious attack on information systems, as botnets are a growing concern globally.

Fourthly, cyber attacks linked to organised crime are a growing menace, and the EU has made it clear that a more severe penalties should be provided for by Member States when an attack against information systems is committed by a criminal organisation, and or conducted on a large scale and thus affecting a significant number of information systems. The Framework Directive addresses the fact that large-scale attacks are essentially the same type of crime on a bigger scale, and marks the difference in terms of gravity and penalty. This is an essential move towards further criminalisation of cyber-crime.

These four arguments show that the EU is effective in the continuous fight against cyber-crime as it had provided Member States with a framework and penalties for the on-going cyber threats facing the Union. Although the EU´s framework provided Member States with

[120] European Commission (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union. pp. 54: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

harmonization of criminal law for cyber-crime, it is still lacking in information sharing regarding NIS risks and threats for preventative measures.

5.2 The Right Balance?

The question of achieving the right balance refers to the challenge of combining privacy and security. The Directive 2013/40/EU on attacks against information systems states that it respects human rights and fundamental freedoms, and observes the principles recognized by the Charter of Fundamental Rights of the EU and the European Convention for the Protection of Human Rights and fundamental freedoms, including the protection of personal data and the right to privacy among others. The EU cyber security strategy seeks to ensure full respect for these rights and principles and must be implemented accordingly.[121]

The protection of personal data is a fundamental right in accordance with article 16(1) of the Treaty on the Functioning of the European Union and Article 8 of the Charter on Fundamental Rights of the European Union. Therefore, any processing of personal data should fully comply with the relevant Union law on data protection. In the case of illegal data interference, Member States shall take the necessary measures to ensure that deleting, damaging, deteriorating, altering or supressing computer data on an information system, or rendering such data inaccessible intentionally and without right, is punishable as a criminal offence.[122]

The EU data protection and privacy frameworks are a combination of different instruments, Data Protection Directive, Processing of Personal Data by Authorities, and the Data Retention Directive. These three Directives all focus on Data Protection and Privacy, but vary in capacity, focusing on protecting data and providing data to competent authorities, which leads up to three arguments for the evaluation of data privacy rights in the EU.

First line of argument of evaluating the right balance of privacy right in the EU, is that the EU has made Data Protection a fundamental right, and thereby providing Europe's citizens with a legal right to data protection that can be enforced before a national court. This provides a framework of protection against third parties/ states stealing and manipulating private data, and therefore it can be said that the EU has achieved it goal of providing its citizens with protection of privacy.

[121] European Parliament (2013). Directive 2013/40/EU On attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJL 218/8. pp. 5
[122] European Parliament (2013). Directive 2013/40/EU On attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJL 218/8. pp. 4.

Secondly, although data protection is a fundamental EU right, there are still cases where data retention is applicable by law. This is provided for by the Data Retention Framework, giving operators the legal framework to save private data from six months up to two years. This provides for the other side of the coin, privacy vs. security. It is agreed upon that data retention is a fundamental act in the fight against cyber-crime and the data collected can be extremely valuable in prosecuting cyber-criminals. The Directive sets out clear objectives and frameworks regarding data retention, but has failed however in providing for explicit circumstances where Member States may retain data. The Directive has left it up to Member States to decide for themselves in each case what is considered a serious crime to allow for data retention. Without clear and objective rules regarding cases when data retention is legal, Member States have very different requirements for when they can legally retain data and this has caused an uneven implementation of the data retention and privacy rights now vary between Member States.

Thirdly, the collection of data and providing them to the competent authorities is a necessary measure in the preventative measure against crime. The idea for data transfer among Member States and competent authorities, seems to be against the notion of data protection and privacy. But to achieve security, there will always be some form of breach of privacy for citizens. The EU has tried to set up a clear and objective framework regarding processing of data by authorities, but it has not fully reached the achieved balance. What the Framework is lacking, is a clear set of rules regarding what is a serious enough crime for authorities to collect data on individuals. Having each Member States decide this objective themselves results in uneven rules regarding the collection and sharing of data across Europe.

6 Conclusion

The EU has made great advances in securing its cyberspace and protecting the privacy of its citizens. The most notable constant in the process it is the importance of EU institutions advocating for cooperation and further advances in harmonising the cyber security framework of Member States. As the EU has slowly recognised the dangers of cyber-crime, and is ready to face new security challenges, Constructivist theory reminds us of the importance of common perceptions and a sense of community.

Liberal Institutionalism has shown us just how important institutions and the rules they make can be for bringing Member States together in a cooperative, and coherent approach to transnational threats. The Commission has been an undeniable force of motivation and fuelled cooperation across Europe to build a coherent cyber security policy.

The EU has recognised the importance of cyber security, and is now on the face of a very suitable institution to solve the problem of cyber-crime in theory and practice. The EU´s very close integration allows for common perceptions, and it also has the competence to make detailed regulations for the Single Market which affects non-state actors as well as governments. Furthermore, the EU has a unique stance and experience in areas which are of great importance for cyber security, such as industrial policy, harmonization of standards, research and development, health and safety, and of course consumer protection, as well as high standards on protection of human rights including data protection and privacy.

To answer the research questions, the EU has so far not been affective in battling cyber-crime, as its original Frame Work Directive from 2005 left some loopholes, i.e. criminalising the creation and use of botnets. The new Directive, which came into force in 2013, is designed to fill in the legal loopholes of the previous framework and has so far proven to be a more effective regulation, and therefore it can be argued that the EU has put forward an effective framework to combat cyber-crime. Now, regarding the second question on achieving the right balance of privacy vs. security, the EU has built frameworks that protect citizens right of data protection of privacy, sets limits to data retention and data sharing, and also a framework for data sharing to competent authorities. The EU is has achieved an ‘acceptable’ balance of privacy vs. security, although it cannot be considered the right balance as the regulation regarding sharing of information is still too unclear and cases of serious crime allowing data retention is too vague and creates loopholes to infringe upon citizens’ rights of data protection.

However, although the EU has made great advances in building a greater cyber security policy in Europe, and has great advantages in its institutional framework to do so compared to other organizations, it has still failed to make a clear Framework which forces Member States to achieve an even level of preparedness against cyber-crime and a coherent framework for data retention and sharing of data among competent authorities. This conclusion is due to the fact that the newest Framework Decision 2013/40/EU is relatively new and Member States have until 2015 to complete the implementation process of EU law. It is therefore hard to place judgement if the previous problems from Directive 2005/222/JHA will also be present this time around. The previous Frameworks failure mainly had to do with uneven level of preparedness and Member States were not sharing information regarding NIS risks and threats. Only the few Member States which had the highest levels of preparedness worked together to fight cyber-crime and left the more under-developed Member States to fend for themselves.

It can now be concluded that the EU is in a very strong position to complete the creation of a viable solution to combat cyber-crime. There are some shortcomings in its policy regulations, but as the EU is open to further cooperation and cohesion of cyber security it can only be viewed as step in the right direction.

Bibliography

Baylis, John., Smith, S., and Owens, P. (2008). The Globalisation of World Politics: An introduction to International Relations. Oxford University Press, USA; 5 edition

Berkowitz, Bruce., Hahn, Robert W. (2003). *Cybersecurity: Who´s Watching the Store?* [online] Available at: http://www.issues.org/19.3/berkowitz.htm [Accessed 26th of September]

Council of Europe. (2001). Convention on Cyber Crime CETS No.: 185 [online] Available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG [Accessed 26th of September]

Court of Justice od the European Union (2013). Press Release No 157/13. [online] Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf [Accessed 17th January 2014]

Deighton, Anne (2002). The European Security and Defence Policy. [online] Available at: http://onlinelibrary.wiley.com/doi/10.1111/1468-5965.00395/pdf [Accessed 14th of November 2013]

Dinan, Desmond. (2005). *Ever Closer Union: An Introduction to European Integration.* Nugent, Neill., Paterson, William E. (General Editors). Palgrave Mcmillan: 5th Edition

ENISA. (2012). EU Cyber Cooperation. the Digital Frontline. [online] Available at: https://www.enisa.europa.eu/media/key-documents/eu-cyber-cooperation-the-digital-frontline/at_download/fullReport. [Accessed 30th of November 2013]

ENISA. (2013). Cybersecurity cooperation: Defnding the digital frontline. [online] Available at: http://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline [Accessed 10 th of November 2013]

European Commission. (1993). *Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century. White Paper.* COM (93) 700, 5 December 1993. [online] Available at: http://europa.eu/documentation/official-docs/white-papers/pdf/growth_wp_com_93_700_parts_a_b.pdf [Accessed 20th of November 2013]

European Commission. (2009). Impact Assessment on: Proposal to amend Framework Decision 2005/222/JHA on attacks against information systems. [online] Available at: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2010/sec_2010_1124_en.pdf [Accessed 25th of October 2013].

European Commission. (2008).Report from the Commission to the Council. Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against information systems.
[online] Available at: http://db.eurocrim.org/db/en/doc/1023.pdf
[Accessed 27th October 2013].

European Commission. (2012). Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century.
[online] Available at:
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF
[Accessed 10th of January 2014]

European Commission. (2013). Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace.
[online] Available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[Accessed 27th October 2013].

European Commission. (2013). Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union.
[online] Available at: http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_impact_ass_en.pdf
[Accessed 5th of October]

European Commission. (2013). Questions and Answers: Directive on attacks against information systems.
[online] Available at: http://europa.eu/rapid/press-release_MEMO-13-661_en.htm
[Accessed 29th of October]

European Commission. Data Retention.
[online] Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm
[Accessed 5th of January 2014]

European Commission (2013.) The EU´s Data Protection Rules and Cyber Security Strategy: two sides of the same coin. Press Release SPEECH/13/436,
: http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm

European Council (2005). Framework Decision 2005/222/JHA, 2005. On attacks against information systems. OJ L69/67
[online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF
[Accessed 29th of September]

European External Action Service. About CSDP
[online] Available at: http://eeas.europa.eu/csdp/about-csdp/index_en.htm
[Accessed 28h of November 2013]

European External Action Service. EU Cyber Security Strategy.
[online] Available at: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm

European External Action Service (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). The European Commission.
[online] Available at: http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_comm_en.pdf

[Accessed 20th of November 2013]

European Organisation for Security (2011). Steps towards implementing a European cyber-security strategy.
[online] Available at: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf
[Accessed 25th of November 2013]

European Parliament (1995). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
[Accessed 20th of November 2013]

European Parliament (2004). Regluation No 460/2004 establishing the European Network and Information Security Agency.
[online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
[Accessed 20th October 2013].

European Parliament. An Area of Freedom, Security and Justice: General Aspects.
[online] Available at:
http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_5.12.1.html
[Accessed 20th October 2013].

European Parliament (2010). Proposal for a Directive of the European Parliament and of the Council. On attacks against information systems and repealing Council Framework Decision 2005/222/JHA.
[online] Available at:
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_en.pdf
[Accessed 20th October 2013].

European Parliament (2010). Directive of the European Parliament and of the Council. On attacks against information systems and repealing Council Framework Decision 2005/222/JHA.
[online] Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_en.pdf
[Accessed 1st November 2013].

European Parliament (2013). Directive 2013/40/EU On attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJL 218/8
[online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

European Union. „How it works": *European Commission.*
[online] Available at: http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm
[Accessed 20th November 2013]

European Union. EU Institutions and Other bodies.
[online] Available at: http://europa.eu/about-eu/institutions-bodies/index_en.htm
[Accessed 20th November 2013]

Europol. European Cybercrime Centre.
[online] Available at: https://www.europol.europa.eu/ec3
[Accessed 18th November 2013]

International Telecommunication Union. *Understanding cybercrime: Phenomena, challenges and legal response (2012).*
[online] Available at: http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
[Accessed 4th October 2013.]

Interpol Press Release (2013). *Partnerships key to protecting cyberspace, Head of Interpol*
[online] Available at: http://www.interpol.int/en%20%20%20%20%20%20%20%20%20%20%20%20%20%20%C5%B8%20%20%20%20%20%20%20%20/News-and-media/News-media-releases/2013/PR101
[Accessed 1st October 2013].

Irion and Luchetta (2013). Online Personal Data Processing and EU Data Protection Reform: Report of the CEPS Digital Reform. *CEPS Digital Forum.*
[online] Available at: http://www.ceps.eu/ceps/dld/7928/pdf
[Accessed 4th of January 2014]

Kaczorowska, Alina (2011). European Union Law. Routledge: 2nd Edition.

Kroes, Neelie. (2013).Global Cyber Security Conference in Brussels. *Towards a coherent international cyberspace policy for the EU.*
[online] Available at: http://europa.eu/rapid/press-release_SPEECH-13-82_en.htm
[Accessed 3rd October 2013].

Pocar, Fausto (2004). European Journal on Criminal Policy and Research: *New Challenges for International Rules Against Cyber-Crime.* Volume 10, Issue 1.
[online] Available at:
http://link.springer.com/article/10.1023%2FB%3ACRIM.0000037565.32355.10
[Accessed 5th October 2013]

Porcedda, Maria Grazia. (2012). Data Protection and The Prevention of Cybercrime: The EU as an area of security? *European University Institute: Working Paper.*
[online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2169340
[Accessed 5th October 2013]

Purser, Dr. Steve. (2011). Cybersecurity: The European Perspective.
[online] Available at:
http://www.mediacom.public.lu/cybersecurity/LUX_Cybersecurity_23_11_11.pdf
[Accessed 5th December 2013]

Rosamond, Ben. (2000). *Theories of European Integration.* Nugent, Neill., Paterson, William E. (General Editors). Palgrave Mcmillan: 1st Edition

Rosenzweig, Paul. *Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare.*
[online] Available at:
http://www.thegreatcourses.com/tgc/courses/course_detail.aspx?cid=9523
[Accessed 16th of September 2013]

Rosenzweig, Paul. (2011). From Worms to Cyberwar. *Defining Ideas: A Hoover Institution Journal.* 9th September 2011.
[online] Available at: http://www.hoover.org/publications/defining-ideas/article/102401
[Accessed 20th September 2013]

Wong, Rebecca (2013). Springer Briefs in Cybersecurity: *Data Security Breaches and Privacy in Europe.*
[online] Available at: http://download.springer.com/static/pdf/808/bok%253A978-1-4471-5586-7.pdf?auth66=1384353826_99afa658829b8e9da57882fc994eef77&ext=.pdf
[Accessed 10th October 2013]