June 23, 2013

Bachelor Thesis

EU Foreign Policy and Russian Cybercrime

Comparing the Cyberspace Governance Systems of the EU and Russia

Stefan Sennekamp (s1129341)

B.Sc. European Studies

School of Management and Governance

Examination Committee

Dr. M.R.R. Ossewaarde
Claudio Matera

UNIVERSITEIT TWENTE.

Abstract

This paper discusses Russian cybercrime and cyberspace governance systems in the European Union and in Russia. In this context, the main research question deals with the difference between the EU and the Russian cyberspace governance systems. Previous research rarely incorporates the issue of cybercrime into the framework of international relations and often lacks the explicit distinction between cybercrime and cyberwarfare as two separate issues. This paper approaches the research question by comparatively analyzing the European and the Russian cyberspace governance systems in terms of criminalization, investigation and prosecution, and international cooperation in order to assess the differences therein. This is done by evaluating the European and the Russian systems regarding institutional and legal arrangements, national and sub-national differences, as well as international cooperation. Subsequently the findings are related to the theories of liberalism and pragmatic liberalism. The paper finally answers the research question and identifies resulting problems for the construction of a potential future cybercrime agreement between the EU and Russia so as to show implications and recommendations for respective future EU policies as well as to give suggestions for further research.

List of abbreviations

ANSSI	-	Agence Nationale de la Sécurité des Systèmes d'Information
AWF	-	Analysis Work Files
BKA	-	Bundeskriminalamt
BMI	-	Bundesministerium des Innern
BSI	-	Bundesamt für Sicherheit in der Informationstechnik
CERT	-	Computer Emergency Response Team
CFSP	-	Common Foreign and Security Policy
CoE	-	Council of Europe
COSSI	-	Centre opérationnel pour les systèmes et sécurité de l"information
CSDP	-	Common Security and Defense Policy
EC3	-	European Cybercrime Centre
ENISA	-	European Network and Information Security Agency
EU	-	European Union
HTCC	-	High-Tech Crime Center
ICROS	-	Internet Crime Reporting Online System
ICT	-	Information and Communication Technology
IFOREX	-	Internet Forensic Expertise
ISP	-	Internet Service Provider
JIT	-	Joint Investigation Teams
NATO	-	North Atlantic Treaty Organization
NCAZ	-	Nationales Cyber-Abwehrzentrum
NIS	-	Network and Information Security
OCLCTIC	-	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication
SME	-	Small and Medium-sized Enterprise
UN	-	United Nations
USA	-	United States of America

Table of Contents

1. Introduction

'Russia is also trying to build a modern nation-state which relies on hard power. By contrast, the EU is a post-modern entity which wields a vast soft power of attractiveness, but which lacks strong sanctioning mechanisms. No wonder it is often hard to find common language.' (Rehn, 2008)

- Olli Rehn in his speech 'EU-Russia relations: the way forward?' in 2008

The statement by Olli Rehn describes the core of the problem faced by European foreign policy towards cooperation with Russia, namely the difference between the European political climate based on soft power and democracy and the Russian one based on hard power and rather authoritative politics. One key element of EU-Russia relations concerns the threats posed by Russian cybercrime and its implications for the European society with information technology at its core. This paper shall analyze the differences between the Russian and the EU cyberspace governance systems.

Given the fact that modern information systems like the internet play a key role in the European society, the protection and governance of cyberspace are essential in promoting and preserving the principles and values of the European Union. As the Eurobarometer Survey of 2012 (European Commission, 2012b) indicates, about one third of Europeans do not trust online banking or purchasing and more than 10 % of internet users have already experienced online fraud. For these and other reasons, the fight against cybercrime gains increasing importance in European foreign and security policy. The European Commission (2013a) recently released its 'Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace' including key principles, strategic priorities and actions, as well as important roles and responsibilities. This strategy highlights the particular importance of an internationally secure cyberspace calling for an international cyberspace policy for the European Union. However, the transnational character of cybercrime creates global networks, which make the EU highly dependent on foreign cyberspace governance. One of the most important countries in this context is Russia with the Russian-speaking cybercrime market constituting to about one third of the global market (Kuzmin, 2012). These problems and challenges endanger the EU cyberspace and come along with a seemingly uncooperative Russian government, which has been shown by the Russian refusal to sign the Council of Europe Convention on Cybercrime (Council of Europe, 2001).

Past failure to combat cybercrime in Europe has shown that the transnational character of cyberspace is too much of a burden for national or European legal and protection systems due to

their increased dependency on foreign cyberspace governance. Next to that, the scientific literature seems to lack the necessary incorporation of cybercrime into international relations theory or as Choucri and Goldsmith (2012) put it 'there is an enormous disconnect between the cyber realities of today and the theories of the twentieth century, which continue to guide national policy and international relations' (p. 75). However, liberalism acknowledges that the increasing development of transnational relations and the increasing amount of transnational actors seize the sovereignty of modern nation states. While international relations scholars usually stress the positive effects of interdependence among states (Eriksson & Giacomello, 2006), Nye (2003) emphasized the costs of interdependence as sensitivity and vulnerability. The sub-theory pragmatic liberalism presents a basic framework for the inclusion of cybercrime into the broader context of international relations. The main force behind cyberspace evolvement in this theory is assumed to be focused international cooperation. Furthermore, pragmatic liberalists point to the importance of civil society actors and the view that information as well as information security are collective goods to be preserved through international efforts (McEvoy Manjikian, 2010). For the purpose of this paper, these theories will be applied to the central elements of cyberspace governance in the EU and Russia allowing conclusions about the differences between the two cyberspace governance systems. The main focus of this paper will thus be the following research question:

To what extent do the cyberspace governance systems of the European Union and the Russian Federation differ?

The dependent variable will be named 'the differences between the EU and the Russian cyberspace governance systems'. The evaluation of the independent variables, namely 'institutional and legal arrangements regarding cybercrime', 'national and sub-national differences', and 'existing patterns of cooperation' will allow conclusions on the former. The Council of Europe Convention on Cybercrime aims at three main aspects: law harmonization in the area of cybercrime, provision of investigation and prosecution mechanisms, and the establishment of a regime of international cooperation (Council of Europe, 2001). In line with the Convention, these three aspects form the basis for the following sub-research questions, which will be answered in the analysis section.

(1) *To what extent does cybercrime criminalization in the European Union and in the Russian Federation differ?*
(2) *To what extent do cybercrime investigation and prosecution mechanisms in the European Union and in the Russian Federation differ?*
(3) *To what extent does the degree of international cooperation regarding cybercrime in the European Union and in the Russian Federation differ?*

The sub-questions cover the most significant aspects of cyberspace governance and thus will facilitate an answer to the main research question.

The following section will outline the theoretical framework including a definition of cybercrime and the most important issues covered in the EU Cyberstrategy. Next, the transnationality of cyberspace will be contrasted with the national character of legal systems. The concept of liberalism with the sub-point of pragmatic liberalism will be applied to cybercrime in order to bring the theoretical framework to a conclusion. The methodology of the paper will then be explained so as to elaborate on the research question and the sub-questions as well as on the data collection and data analysis methods. Furthermore, the utility of the paper beyond answering the research question will be explained in the methodology. The analysis section will answer the sub-questions by focusing on the independent variables. Institutional and legal arrangement regarding cybercrime will be evaluated as well as respective differences on the national and sub-national level. Furthermore existing patterns of cooperation will be assessed. This will enable an evaluation of the Russian and European performance regarding criminalization, investigation and prosecution, and international cooperation in relation to cybercrime. Thus, it will provide answers to the sub-research questions. Finally, the last section will give an answer to the main research question and identify problems for the construction of a potential cybercrime agreement between the EU and Russia. Moreover, it will show further implications for the EU allowing recommendations on future cybercrime policies regarding cybercrime and give incentives for further research.

2. Theorizing cyberspace governance systems

This chapter will constitute the theoretical framework of the paper and theorize the issue of cybercrime as well as the notion of cyberspace governance according to a liberalist and pragmatic liberalist view. To begin with, the term ‘cybercrime’ will be defined so as to give a clear picture of what is at stake when talking about cybercrime. This will be followed by a section about the Cybersecurity Strategy of the European Union in order to characterize the EU plan for cyberspace governance. After that the transnationality of cybercrime will be contrasted with the nationality of legal systems in order to clarify which problems are caused by this contrast. This will be followed by a description of cyberspace governance according to liberalism and subsequently according to pragmatic liberalism in order to identify important issues and to give an overview of the scientific literature on the topic. Finally, a conclusion will be given so as to summarize the theoretical background of cyberspace governance

.

2.1 Defining cybercrime

For the purpose of this paper it is important to clearly define the term 'cybercrime' in order to clarify its meaning and scope, which will be done in this section.

According to the Cybersecurity strategy of the European Union, Cybercrime is defined as the following:

> *'Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).'* (European Commission, 2013a)

Looking at the definition of cybercrime, it is important to draw a clear line between which issues are covered under cybercrime and which issues can be seen as cyberwarfare. This differentiation is extremely difficult for several reasons. One of the main problems is the difficulty to trace back where an attack came from, because a 'hacker' from one country could theoretically use a computer or IP address in a second country for an attack on a third country. While Liff (2012, p. 404) limits cyberwarfare to computer network attacks 'with direct political and/or military objectives […] and computer network defense', cybercrime mostly has an economic dimension. There is a constant debate among scholars about what to include and what not to (Barkham, 2001). This paper will refer to cybercrime as acts being predominantly motivated by economic gains including forgery and counterfeiting, dissemination of child pornography or the like, fraud, as well as spread of malware and the like.

2.2 Cybersecurity strategy of the European Union

This section will describe the official plan for EU cyberspace governance in order to define the core values and issues the EU tries to promote and realize.

In February 2013, the European Commission released its 'Cybersecurity Strategy for the European Union – An Open, Safe, and Secure Cyberspace' (2013a) including a European vision on cyberspace, responsibilities, necessary actions to be taken, as well as general principles for cybersecurity. This can be seen as the basic plan for cyberspace governance in the European Union including the following points:

To begin with, the proposed core values include the protection of fundamental rights, freedom of expression, personal data protection, and privacy. Furthermore, universal accessibility, efficient

multi-stakeholder governance, as well as the need for a shared responsibility between all relevant actors on different levels of governance are highlighted.

Five strategic priorities are included in the Commission´s vision on cyberspace. First of all, cyber resilience shall be promoted by developing defense and prevention capabilities and cooperation between public authorities and the private sector. The establishment of institutions such as ENISA or CERTs and proposed legislation including risk assessments by key players like ISP´s as well as risk awareness-raising especially for end users shall help guaranteeing reliable and robust networks. Second, a drastic reduction of cybercrime is aimed at by effective legislation, increased operational capability for responding to cybercrime, and enhanced coordination at the EU level. 'Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defense Policy (CSDP)' is the third priority including a focus on 'detection, response and recovery from sophisticated cyberthreats' as well as enhancing synergies between civilian and military protection approaches. Fourth, the development of industrial and technological resources for cybersecurity includes increased promotion of a single market for related products as well as fostering of research and development investments and innovation. Finally, a coherent international cyberspace policy for the European Union shall be established and EU core values shall be promoted. For this purpose, cyberspace issues shall be included in EU external relations and the CFSP.

Acknowledging the borderlessness of cybercrime, highlighted roles and responsibilities include the coordination between NIS competent authorities/CERTs , law enforcement and defense on national, EU, and international level as well as 'EU support in case of a major cyber incident or attack'.

2.3 The transnationality of cybercrime and the nationality of legal systems

Cyberspace is transnational in nature and thus conflicts with the nationality of legal systems. This conflict will be elaborated in the following paragraph.

As Levin and Ilkina (2012) acknowledge, the international nature of cyberspace poses a great challenge to cybersecurity since relevant computers are mostly located in different countries and are thus subject to differing national legal systems. For this reason, states try to enter into international agreements bearing potential for conflicts caused by differing interests. However, the national nature of law in general causes international law to lack enforcement powers, which calls for independent agreements between different states and their law enforcement bodies. Furthermore, the transnationality of emerging actors in cyberspace like social movements or transnational corporations should be kept in mind when constructing such agreements. Some liberal theorists even describe sovereignty as a burden rather than an advantage in this context (Eriksson & Giacomello,

2006). These points create many challenges to be kept in mind for policy makers in governing cyberspace.

2.4 Liberalism

International relations theory generally lacks the inclusion of cybercrime into its field of science. However, liberalism presents a basic framework for this inclusion. On these grounds, this chapter aims to apply liberalism to the field of cyberspace governance.

In his book 'Liberalism and International Relations Theory' (1992), Moravcsik presents three core assumptions about liberal international relations theory with the first one concerning important social actors and their motivations. These actors can be individuals or groups acting according to their own independent interests with the aim to promote social and political order through interaction and improve individual welfare. The pluralist nature of society leads to a multi-interest society with conflicts between competing private goals, thus trying to prevent a concentration and abuse of social and political power. In terms of cyberspace governance, this could for instance mean a conflict between privacy and security trying to prevent issues like censorship and the like. According to Moravcsik, this has three implications for international politics: The core determinants of politics are in society itself, institutions have to channel private interests towards wealth and security in order to promote progress, and liberalism facilitates evolutionary social progress through conflicts. Moreover, liberal international relations theory assumes that some segment of domestic society and its interest is represented in all governments, creating a link between state and society. In this context, a pure tyranny would represent only one person´s interest whereas a democracy would ideally represent all citizens, which makes it interesting to see what interests are represented in EU governance and in Russian governance. Finally, the behavior of states and thus the extent of international cooperation and conflict is said to reflect the nature and configuration of state preferences, which again arouses interest in identifying preferences involved in cyberspace governance. Where converging preferences promote cooperation, diverging interests are rather a source of conflict. Liberals put state purpose at the core of international relations with changing relationships to the domestic and international society shaping it (Moravcsik, 1992). Eriksson and Giacomello (2006) highlight four points to keep in mind within liberal international relations theory: the plurality of international actors, domestic political factors and their influence on international state behavior, the importance of international institutions in establishing rules of behavior, and the broader agenda of international studies focusing on multiple issue areas. This has several implications for the issue of cyberspace and cybercrime as liberalism, for instance, calls attention to emerging new actors like online groups and the resulting transnationality challenging the sovereignty of states as well as to the importance of international cooperation in regulating cyberspace. In

addition to that, domestic political factors, e.g. law harmonization and civil society involvement could become interesting in assessing the difference between the two cyberspace governance systems. Moreover, norm and institution building on an international level constitute a key feature of liberal theory (Eriksson & Giacomello, 2006). Nye (2004) even extents this view by arguing that soft power in the digital age is more important than ever before. However, he highlights the dangers of ICT in relation to propaganda and terror. It will thus be worthwhile to reflect on the difference between the alleged soft power in the EU and the Russian system based on hard power. Having given a general introduction into the foundation of liberalism, the view will now be extended to the sub-theory of pragmatic liberalism and subsequently be applied to cybercrime.

2.4.1 Pragmatic liberalism

In this chapter, the basic field of liberalism will be extended to its sub-theory pragmatic liberalism and subsequently applied to cyberspace governance in order to create an enhanced theoretical background for the analysis.

Pragmatic liberalism in general applies to all forms of organized human efforts including the industry, trade, school, and sciences. In his book 'Pragmatic Liberalism' (1990, p. 3), Anderson describes its most distinctive, feature as 'the proposition that the performance of the diverse functional associations that make up our society is a matter of public concern and that participation in them is a form of public responsibility and an act of citizenship'. This means that human interactions, among them ICT, acquire a political aspect and thus create a link between the private and the public. Moreover, pragmatic liberalism not only puts a focus on the public responsibility of private associations, but also on how the state regulates and coordinates the larger public life of the society (Anderson, 1990). This view has several implications for cyberspace governance seen through the pragmatic lens of liberalism. The main force behind cyberspace evolvement is considered to be focused international cooperation including regulation to enable its functionality. The old world structures thereby become less important as regulation mainly happens trough international governmental regimes and professional as well as social organizations. This highlights the importance of international cooperation, civil society, and private companies in cyberspace governance. Cyberspace is considered to be both of public and private nature having a certain degree of nationality and borders requiring defense. More general, it can be seen as 'economic and political territory subject to international regulation' (McEvoy Manjikian, 2010, p. 389). With regard to citizenship, McEvoy Manjikian describes the term of 'netizens' as internet citizens assimilating community norms and behavior with the goal to preserve collective goods. These norms can be of local, national, or international character creating on the one hand a national identity with tiered citizenship and on the other hand a digitized identity or 'digital body' including intellectual property,

personal data etc., which calls for legal protection mechanisms. Civil society actors thus gain increasingly in importance for cyberspace governance. Finally, information in the field of pragmatic liberalism is seen as a collective good along with information security necessitating national and international rules and norms concerning its quality and availability. (McEvoy Manjikian, 2010, pp. 392-393)

2.5 Conclusion

This chapter has theorized the issue of cybercrime as well as the notion of cyberspace governance in a liberalist and pragmatic liberalist perspective. The term 'cybercrime' was defined and an overview of the basic EU plan for cyberspace governance was given. Moreover, the transnationality of cybercrime was contrasted to the national nature of law, which has been said to cause problems regarding enforcement powers of international law and thus to necessitate international agreements. Liberal international relations theory has highlighted the dispute between privacy and security in multi-interest societies as well as the importance of institutions in governing cyberspace. Moreover, the importance of international cooperation as well as of domestic political factors in assessing the difference between cyberspace governance systems was stressed along with the increasing relevance of soft power. Pragmatic liberalism has refined the issue raised by liberalism and has again underlined the significance of international cooperation, civil society, and private companies in cyberspace governance.

3. Methodology

This part of the paper will give an overview of the chosen research design. In more detail, it will describe how the analysis of relevant data is aimed to answer the main research question.

The research will follow a comparative case study design, in which the difference between the European and the Russian cyberspace governance systems will be elaborated. In the following, the data collection method including the case selection and relevant data and information will be described. This will be followed by a detailed description of the data analysis method, which includes explanations of the dependent variable being 'the difference between the EU and the Russian cyberspace governance systems' and the independent variables 'institutional and legal arrangements concerning cybercrime', 'differences on national and sub-national level', and 'existing patterns of cooperation'. Finally, the utility of the paper beyond answering the research question will be explained and a conclusion on the methodological framework will be given.

3.1 Data collection method

Having introduced the methodology chapter, the data collection method will now be explained. To begin with, the case selection for the analysis of national and sub-national differences will be developed so as to facilitate a fruitful analysis. After that, the data and information necessary for the analysis will be explained in detail and will also be supplemented by a detailed list in the Appendix.

Case selection: The main part of the analysis will focus on the EU and Russia in general. However, especially for the attribute of national/sub-national differences certain countries have to be chosen. Three factors were chosen for the case selection: the date a country ratified the Council of Europe Convention on Cybercrime, a country´s relative power in EU politics, and a country´s economy. Based on these factors three countries have been chosen for detailed examination. France ratified the convention in 2006 and performs on a medium to high level when it comes to power and economy. Germany ratified the convention rather late in 2009 and is a strong actor in European politics with a strong economy. And finally, Estonia has been subject to the 2007 cyberattacks by Russia (Aaviksoo, 2010), ratified the convention early in 2003 and is rather weak when it comes to power and economy. Needless to say, a choice of three cases out of 27 potential cases brings a risk of error, but a broader selection of cases would extend the scope of this research. This shall be tackled by, first of all, including key actors like Germany into the sample, and secondly, by carefully foreseeing if any extreme cases could bias the results.

Data and information: Two approaches highlighted by Babbie (2011) will be used for the data collection - content analysis and existing data research. The data and information necessary will exclusively be of secondary nature and mainly qualitative. Legislative texts, reports, as well as websites and documents of EU and Russian institutions will give an insight into legal and institutional arrangements, including criminalization of cybercrime and existing prosecution and investigation mechanisms or institutions. In contrast to that, national policy reports, scientific articles, and reports like the ENISA Country Reports or RAND Europe Reports will be necessary to elaborate on national and sub-national differences. Additionally, scientific articles, international agreements, and governmental websites will be used to assess existing patterns of cooperation. This data will be reviewed in order to first evaluate the European and the Russian cyberspace governance systems in terms of criminalization, investigation and prosecution, and international cooperation as well as the difference between these performances in order to answer the sub-research questions. This will provide an assessment of the difference between the overall cyberspace governance systems in the countries. A detailed list of the data and information used in the analysis will be given in the Appendix (Appendix A-D). This list will also indicate which data and information was used in which section.

3.2 Data analysis method

Following the explanation of the data collection method, this section will state the relevant aspects of the data analysis method beginning with the general research design. This will be followed by an extensive explanation of the variables in order to introduce their most crucial aspects. Finally, the utility of the paper beyond answering the research question will be described so as to explain how the paper can help future EU policies regarding the construction of a cybercrime agreement with Russia.

The data will be analyzed on a comparative basis, meaning the European and Russian performances on the relevant aspects of the variables will be compared in order to facilitate an assessment of the independent variables. This will give information on the dependent variable. In this context, not all actors, opinions, and information can be weighed equally. This will require careful consideration on how to assess the variables as it bears the potential for bias. In the following, the variables will be explained more in detail.

Variables: The dependent variable of this thesis will naturally constitute the main part of the research question, namely the 'difference between the EU and the Russian cyberspace governance systems'. The independent variables will by contrast be the main cause or determinant influencing the former and will be explained in detail in the following:

(1) *Respective institutional and legal arrangements concerning cybercrime:* These arrangements include measures taken regarding the criminalization of cybercrime, its investigation and prosecution, as well as related issues like the existence of anti-cybercrime institutions or the like. This variable will give an insight into which instruments already exist in Russia and the EU.

(2) *Differences on national and sub-national level:* Do national (EU) or sub-national (Russia) policies, institutions etc. exist? On what aspects and how do they differ? Do they influence or hinder supranational (EU) or national (Russia) prosecution or investigation mechanisms? This variable will evaluate the current level of harmonization.

(3) *Existing patterns of cooperation:* Are the parties subject to any relevant international agreements? Can patterns of cooperation on a national or sub-national level be observed? Are the individual countries subject to relevant agreements? This variable will analyze the current state of international cooperation and willingness to cooperate.

Utility beyond answering the research question: Beyond answering the research question this paper aims to show implications of the difference between the two cyberspace governance systems for future EU policies concerning the construction of a potential cybercrime agreement with Russia. This

section will explain how the analysis of the systems will facilitate this by identifying key interests at stake in cyberspace governance.

The general concept of liberalism assumes the behavior of states and, resulting from that, the extent of international cooperation or conflict to be reflecting the nature and configuration of state preferences (Moravcsik, 1992). Thus, from looking at previous state behavior in constructing or entering international agreements as well as from the way states govern their cyberspace one can to a huge degree tell how state preferences are shaped and which interests or obstacles are involved. For the case of Russia this means that state preferences are 'Kremlin preferences', because - as 'Freedom House' evaluated - the Kremlin is the sole actor in Russian politics. The civil society in Russia does not have the necessary power to influence Russian foreign policy and non-governmental organizations or independent media rarely exist (Orttung, 2012). In contrast to that, non-state actors are highly involved on the input and output side in EU decision-making processes. This involvement next to other mechanisms includes consultation of civil society actors or funding of e.g. non-governmental organizations, which leads to a partial reflection of their interests in EU policies (Voltolini, 2012, pp. 17-19). This means that a careful examination of the existing three attributes can show relevant obstacles and interests at stake in the following way. A close look on the legal and institutional arrangements will reflect the interests involved in the criminalization, investigation, and prosecution mechanisms regarding cybercrime and what costs would potentially be involved in entering an agreement. Furthermore, the evaluation of national differences regarding cybercrime governance in Europe and possibly of sub-national differences in Russia will reflect EU member state interests and Russian regional interests. Finally, the assessment of existing patterns of cooperation and especially the behavior in constructing previous agreements as well as past reasons not to enter an agreement will give an insight into the EU´s and Russia´s willingness to cooperate and potential reasons not to cooperate. Following this argumentation the analysis of the independent variables can help future EU policies regarding the construction of a potential cybercrime agreement by identifying interests preventing or decelerating international cooperation and consequently setting the focus on issues to be kept in mind for an agreement. Furthermore, the analysis will facilitate an assessment of how extensive such an agreement could become and of which aspects would hinder cooperation.

3.3 Conclusion

This chapter has given an extensive overview of how the comparative analysis of the EU and the Russian cyberspace governance systems can result in answers to the main research question. It has presented the data collection method including the case selection and an outline of relevant data and information. Moreover, it has shown how the data is going to be analyzed. For this purpose, the research design and the variables have been presented. Finally, the utility of the paper beyond

answering the research question has been elaborated. In the following section, the analytical part will start with legal and institutional arrangements in the EU and Russia, followed by national and sub-national differences regarding criminalization as well as investigation and prosecution mechanisms. The countries Estonia, France, and Germany will serve as cases for the European Union. Afterwards, existing patterns of cooperation between the EU and Russia as well as cooperation between these two and external countries will be analyzed. The findings will facilitate answers to the sub-questions by analyzing the EU´s and Russia´s performance in terms of criminalization, investigation and prosecution, as well as international cooperation and be judged against the theory. In the concluding part, the overall distance between the European and Russian cyberspace governance systems will then be assessed in order to answer the main research question. Next to that, recommendations resulting from the findings and theories as well as incentives for further research will be given.

4. Analyzing the EU and Russian cyberspace governance systems

This section will constitute the main analytical part of the paper. Beginning with the analysis of the three independent variables, the EU´s and Russia´s performance on institutional and legal arrangements will be evaluated first. This will include the criminalization as well as the investigation and prosecution of cybercrime. Secondly, national (EU) and sub-national (Russia) differences will be evaluated regarding the same three aspects. Estonia, France, and Germany will serve as cases for the EU being followed by a short conclusion on the differences in the EU. After the evaluation of sub-national differences in Russia, existing patterns of cooperation regarding cybercrime between EU member states and Russia, between the EU and external parties, between Russia and external parties, as well as between the EU and Russia will be assessed. This will conclude the analysis of the independent variables - the distance between the European and the Russian cyberspace governance systems regarding criminalization, investigation and prosecution, and international cooperation will be evaluated in order to answer the sub-research questions. Finally, the findings will be applied to the theory and current debates.

4.1 Analyzing the independent variables

In order to provide an answer to the sub-research questions the independent variables will be analyzed first. This will be done by analyzing institutional and legal arrangements regarding the criminalization as well as investigation and prosecution of cybercrime in the EU and Russia. This will be followed by an analysis of national and sub-national differences in relation to the same aspects as well as by an analysis of existing patterns of cooperation on cybercrime involving the EU and Russia.

The findings from these sub-sections will have important implications for answering the sub-research questions.

4.1.1 Institutional and legal arrangements regarding cyberspace governance

This section will give an analysis of criminalization, as well as investigation and prosecution mechanisms in the European Union and the Russian Federation.

4.1.1.1 Institutional and legal arrangements regarding cyberspace governance in the European Union

With regard to criminalization of cybercrime three acts are important in the European Union. The first one is the *'2005 Framework Decision on Attacks Against Information Systems'.* Broadly speaking, it tries to incorporate the main parts of the Council of Europe Convention on Cybercrime into European law with the aim to 'improve cooperation between judicial and other competent authorities, via approximation of different Member state criminal law concerning what is now known as cybercrime' (Robinson, et al., 2012, p. 28). Articles 2, 3, and 4 of the framework decision define three central criminal offences that shall be subject to approximation and improved cooperation: illegal access to information systems (Art. 2), illegal system interference (Art. 3), and illegal data interference (Art. 4) (Council of the European Union, 2005). In a 2008 report assessing the current state of implementation in the member states, the Commission saw the degree of implementation as being 'relatively good' whereby seven member states 'had yet to communicate any implementing measures' (European Commission, 2008). This shortcoming by the respective member states led to the second important act, namely a new '*draft Directive on attacks against information systems*' repealing Framework Decision 2005/222/JHA (Robinson, et al., 2012, p. 29). The new proposal expands the former framework decision by aiming at closer harmonization of cybercrime definitions and penalties as well as including new types of crime like botnets. Furthermore, it tries to improve cooperation by 'strengthening the existing structure of 24/7 contact points' (European Commission, 2010, p. 5). This directive was adopted by the Council in June 2011 (Robinson, et al., 2012, p. 29). The third important act when it comes to criminalization is the 2011 Directive 'on Combating the Sexual Abuse and Sexual Exploitation of Children, and Child Pornography' (Council of the European Union, 2011, p. 1). It harmonizes several criminal offences including provisions to fight online child pornography as it, for instance, requires member states to remove websites containing child pornography and allows them to block access to such websites in a transparent manner (Council of the European Union, 2011, p. 6). Having discussed the relevant arrangements when it comes to criminalization of cybercrime, the European institutions in the field of investigation and prosecution will in the following be presented.

Working closely in cooperation with the 27 member state law enforcement agencies and several non-EU agencies, *Europol* is the official European Union law enforcement agency with the aim to fight international terrorism, organized crime and the like (Europol, n.d.). After being created in 1995 on basis of a convention between the member states (European Commission, 2006, p. 2), Europol became fully operational in 1999 (Europol, n.d.) and was made an official EU agency in 2009. With a budget of nearly €84 million in 2011 several working units are concerned with the issue of cybercrime. Its High-Tech Crime Center (HTCC) is engaged with providing investigative support for member states, improving knowledge about cybercriminal behavior, and training. Europol mainly works with tools called 'Analysis Work Files (AWF)', which is basically an information exchange platform for member states. The AWF Cyborg particularly focuses on cybercrime. Furthermore, the 'Internet Forensic Expertise (IFOREX)' is concerned with the exchange of forensic best practices and building a technology related knowledge-base. Together with ICROS, the 'Internet Crime Reporting Online System', which aims at facilitating online reporting of internet-related crimes and thus providing an understanding of pan-European threats, IFOREX tries to tackle cybercrime on a European level (Robinson, et al., 2012, pp. 86-90).

In March 2012 the European Commission proposed the establishment of a *European Cybercrime Centre (EC3)* being stationed within Europol (European Commission, 2012a). In a press release one year later its focus has been put on 'illegal online activities carried out by organized crime groups, especially attacks targeting e-banking and other online financial activities, online child sexual exploitation and those crimes that affect the critical infrastructure and information systems in the EU' (European Commission, 2013b). Services provided by the EC3 include data fusion of law enforcement authorities, computer emergency response teams, private sector specialists, and academia in order to create benefits for member state investigators. Moreover, forensic support is provided as well as identification of potential partners and cooperation with European institutions, law enforcement agencies, international organizations and the like in order to establish contributive partnerships (Europol, n.d.). The EC3 was officially opened on 11th of January 2013 in the Europol headquarters in The Hague (European Commission, 2013b).

When it comes to judicial cooperation in cybercrime investigation *Eurojust* is the most important actor in the European Union. Established by a 2002 Council Decision for actions in investigation and prosecution of serious crime concerning at least two member states as laid out in the decision´s article 3 (Council of the European Union, 2002), it aims at fostering cooperation and having an advisory role on legal and regulatory framework issues of jurisdiction. The fact that Eurojust staff is appointed by their home countries makes them experts when it comes to supporting prosecution in the member states. In the field of cybercrime, its 'Joint Investigation Teams (JIT)' are especially

important as they speed up the process of requesting information. In general, cybercrime is dealt with in the 'Financial and Economic Crimes Team'. However, judges and prosecutors criticize the lack of training and the variance in member state legislation as well as limits in its ability to cooperate with third-states (Robinson, et al., 2012, pp. 90-92).

In 2004 the European Union established the *'European Network and Information Security Agency (ENISA)'* to guarantee 'a high and effective level of network and information security within the Community and in order to develop a culture of network and information security' (Council of the European Union, 2004). Even though ENISA has no competence relating operationally addressing cybercrime, it raises the level of security for European cyberspace in general as it has a role in providing secure networks and information. Moreover, the agency works closely together with European *'Computer Emergency Response Teams (CERT)'* as it regularly comes up with best practices for CERTs to address NIS aspects concerning cybercrime (Robinson, et al., 2012, pp. 93-94). CERTs can be seen as the fire brigade in case of cybercrime for they provide reactive services like security alerts and warnings, advisories, and security training (European Network and Information Security Agency, 2009). In September 2012, the European institutions set up a Computer Emergency Response Team for the European Union (CERT-EU), which closely cooperates with CERTs in the member states (European Network and Information Security Agency, n.d.).

4.1.1.2 Institutional and legal arrangements regarding cyberspace governance in Russia

Whit regard to criminalization of cybercrime few doctrines are relevant in the Russian Federation. The Russian security company Group-IB considers the legislative system as being rather ineffective for that reason. While the 2000 'Doctrine on Information Security of the Russian Federation' mainly focuses on the digital disparity in Russia, the 'Criminal Code of the Russian Federation' is more concrete about criminal offences in cyberspace (Levin & Ilkina, 2013). Chapter 28 concerns crimes in the sphere of computer information and encompasses three articles: Art. 272 concerns the illegal access to computer information, Art. 273 concerns the creation, use, and dissemination of harmful computer programs, and Art. 274 concerns the misuse of storage means, processing or transmission of computer information and telecommunications networks (Russian Federation, n.d.). However, the same amendment establishing these articles deleted a former clause on causing computer and computer network damage, which made the prosecution concerning denial of service attacks harder. Furthermore, Russia refused to ratify the Council of Europe Convention on Cybercrime for several reasons. Firstly, it would allow foreign law enforcement agencies to access Russian internet traffic in certain cases. Secondly, it would make the possession of malicious software illegal. Currently, Russian law only forbids the creation, use, and dissemination of such software. Moreover, a change in the legislation on online child pornography would be required as the current state of law criminalizes the

creation, use, distribution, and possession of such material, but only in combination with the intention to distribute it (Levin & Ilkina, 2013, pp. 35-36).

The investigation and prosecution of cybercrime in Russia falls within the authority of the Department 'K' of the Ministry of Internal Affairs of the Russian Federation (Levin & Ilkina, 2013, p. 30). It often cooperates with the Group-IB, as mentioned before, a Russian security company offering cyber intelligence and threat prevention, as well as cybercrime investigation and the like (Group-IB, (n.d.)). The company also established a CERT-GIB with the aim to coordinate information exchange between law enforcement agencies, corporations, and individuals, to assist cyber security in the Russian internet sphere, and to assist in cyber risk management (Group-IB, n.d.). Finally, the Russian government launched the program 'Sornyak' in 2011 to combat cybercrime concerning child pornography, which also established cooperation with several other countries on that issue (Levin & Ilkina, 2013, p. 30). In general, cybercrime investigation and prosecution in Russia is rather limited and mainly managed by private companies instead of governmental institutions.

4.1.2 Differences regarding cyberspace governance on national and sub-national level

In this section, national differences regarding cybercrime criminalization, investigation, and prosecution in the European Union as well as sub-national differences in Russia will be evaluated. An analysis of the situation in Estonia, France, and Germany will be followed by an overall conclusion on the differences within the EU. Finally, the differences in Russia will be assessed.

4.1.2.1 National differences in the European Union

Estonia: According to ENISA, 'Estonia is one of the most rapidly developing information societies in Central and Eastern Europe' (European Network and Information Security Agency, 2011a, p. 5) as it, for instance, was the first country ever to conduct online parliamentary elections in 2007. Being targeted by the 2007 allegedly Russian cyber-attack, the country released several doctrines on information security, among them the 'Cyber Security Strategy 2008' and the 'Estonian Information Society Strategy 2013', which defined the general framework, objective, and action field for Estonian information security (European Network and Information Security Agency, 2011a, p. 6). When it comes to legislation specifically designed to tackle cybercrime the Estonian 'Criminal Code' sets the basic rules including criminalization concerning computer sabotage (§206), spreading of computer viruses (§208), unlawful use of computer, computer systems or computer networks (§217), or handing over protection codes (§284) (Republic of Estonia, n.d.). Moreover, according to ENISA, Estonia uses e-identity cards for its citizens and foreigners permanently residing in the country and issued a 'Computer Protection Initiative' in 2009 aiming at making Estonia one of the most secure places when it comes to information through investments in PC protection, user awareness raising, and the widespread use of the e-identity cards. In terms of cooperation, Estonia participates in

several initiatives with the two most important being the 'Cooperative Cyber Defence Centre of Excellence' with many other countries like Germany, Italy, or Spain participating, and the 'NATO Centre of Excellence in Cyber Defence', which was established in Estonia itself (European Network and Information Security Agency, 2011a, pp. 9-14).

The Estonian Ministry of Interior is the main administrative body in cybercrime issues, whereas the IT Crimes Office of the Central Criminal Police is responsible for investigation and prosecution of cybercrime. The Police moreover cooperate with experts from Interpol and European member states in order to make their work more efficient (Valeri, Somers, Robinson, Graux, & Dumortier, 2006, p. 85). Another important body is the 'Computer Emergency Response Team of Estonia (CERT Estonia)', which has been established in 2006 in order to manage security incidents in Estonian computer networks. CERT Estonia naturally cooperates heavily with CERT-EU and CERTs from other member states and relevant third states (Estonian Information System´s Authority, 2012).

*France***:** The French Republic ratified the Council of Europe Convention on Cybercrime in 2006 as an already highly developed country in terms of anti-cybercrime actions. In 1978, it released the 'Information Technology and Liberty Act', which has been amended by the 'Godfrain Act' in 1988 including provisions on the intrusion in information systems (Valeri, Somers, Robinson, Graux, & Dumortier, 2006, p. 102). The 2004 'Reinforcing Trust in the Digital Economy Act' updated these provisions in relation to fraud, child pornography, spam and the like and established a regulatory framework together with the 'eCommerce Act 2004' and the 'eGovernment Act 2005' (Levin & Ilkina, 2012, p. 26). In 2011, France released its 'Information Systems Defence and Security Strategy' defining cybercrime as 'Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime' (Agence nationale de la sécurité des systèmes d'information, 2011). Offences regarding cybercrime are defined in the French penal code including provisions on unauthorized access to automated data processing systems (Art. 323), violations of personal rights resulting from computer files or processes (Art. 226), and online child pornography (Art. 227) (Legifrance, n.d.).

In terms of investigation and prosecution France has an extensive network of law enforcement and related agencies. The 'Central Office for the Fight against Crime related to Information Technology and Communication (OCLCTIC)' has been established in 2000 and is the main body in cybercrime investigation responsible for operational coordination on the national level and at the same time it serves as international contact-point for cross-border cybercrime activities (Valeri, Somers, Robinson, Graux, & Dumortier, 2006, pp. 105-106). It closely cooperates with the Gendarmerie´s Forensic

Department (Robinson, et al., 2012, p. 194). Furthermore, several reporting platforms have been established including 'Pharos', a platform allowing the public to report suspicious websites or messages (Levin & Ilkina, 2012, p. 27), 'Pointdecontact', a hotline against online child pornography, racist content and the like, and 'internet-mineurs.gouv.fr', a governmental website for online child pornography reporting (Valeri, Somers, Robinson, Graux, & Dumortier, 2006, pp. 107-108). Additionally, several non-governmental organizations like 'Signal Spam', 'Internet Sans Crainte', or 'Action Innocence' are active in fighting spam and providing online protection for children (Levin & Ilkina, 2012, p. 28). Contrary to other countries, France operates multiple computer emergency response teams. These include the 'Centre opérationnel pour les systèmes et sécurité de l'"information (COSSI)', 'Computer Emergency Response Team - Industrie, Services et Tertiaire (CERT-IST)', 'CERT-LEXSI', and a few smaller CERTs (European Network and Information Security Agency, 2011b, pp. 24-25). COSSI is a sub-unit of the 'French Network and Information Security Agency (ANSSI)', which has been established by the 2008 'White Paper on Defence and National Security' and is responsible for protecting sensitive government networks, developing trusted products and services, supporting government entities and critical infrastructure operators, and raising awareness among companies and the general public about information security threats (Levin & Ilkina, 2012, p. 25).

Germany: The Federal Republic of Germany ratified the Council of Europe Convention on Cybercrime only in 2009 after it was an original signatory to it. It released several acts and regulations when it comes to criminalization of cybercrime. To begin with, the German Parliament issued the 'Act to Strengthen the Security of Federal Information Technology' in 2009, making the 'Federal Office for Information Security (BSI)' the central reporting office for federal authorities cooperation in relation to cybercrime (Levin & Ilkina, 2012, p. 23). In 2011, the 'Federal Cyber Security Strategy for Germany' was then released and established a 'National Cyber Response Center (NCAZ)' as well as a 'National Cyber Security Council'. Furthermore, it aimed at effective crime control in cyberspace and effective coordinated action to guarantee European and global cyber security (European Network and Information Security Agency, 2011c, p. 6). Finally, criminal offences regarding cybercrime are defined in the German Criminal Code with provisions regarding data espionage and phishing (Art. 202), alteration of data and computer sabotage (Art. 303), computer fraud (Art. 263), forgery (Art. 269), and online child pornography (Art. 184b) (Bundesministerium der Justiz, 2012).

The German 'Federal Ministry of the Interior (BMI)' is the main cooperative government body in charge of cybercrime (Levin & Ilkina, 2012, p. 22). On the next lower level, the 'Federal Criminal Police Office (BKA)' is responsible for investigation and prosecution with its sub-unit 'SO43', which is

specialized in high-tech crimes. These bodies stand in close cooperation with private entities like credit card companies or ISPs as well as with Interpol or Europol´s AWF Cyborg (Robinson, et al., 2012, pp. 196-197). Moreover, several awareness raising mechanisms have been established. The BSI regularly provides information about illegal internet traffic, whereas initiatives like the 'Spam Summit' or the 'Internet Security for SME´s' hold meetings about spam, emerging risks for companies and individuals etc. (European Network and Information Security Agency, 2011c, pp. 23-24). Moreover, citizens can use reporting platforms like 'Jugendschutz.net' or the 'Central Unit for Child Pornography' of the BKA (Valeri, Somers, Robinson, Graux, & Dumortier, 2006, p. 115). When it comes to network and information security, the BSI is the German equivalent to ENISA and also closely cooperates with the French ANSSI. Finally, similar to the French system, many different CERTs exist in Germany, which include the CERT-Bund, which is responsible for computer and network security problems in federal institutions, CERT-Verbund, a cooperation and information sharing platform for German CERTs, and CERTCOM AG, the leading manufacturer of products and services regarding business security (European Network and Information Security Agency, 2011c, p. 18).

After evaluating the Estonian, French, and German performance in terms of cybercrime criminalization as well as investigation and prosecution, their overall differences will now be explained and a short overview on the remaining EU member states will be given.

Comparing the performance of Estonia, France, and Germany on aspects of criminalization, investigation, and prosecution regarding cybercrime, only minor differences can be defined. Overall, the three countries have the basic mechanisms necessary to combat cybercrime, but certain points can be improved. Germany, for instance, lacks criminalization regarding malicious codes, account compromise, intrusion attempts, and spam. However, it is remarkable that the country ,just like France, operates a national agency for network and information security. Estonia does not only lack such an institution, like most other EU member states, but it also lacks reporting and alert mechanisms like the German 'Jugendschutz.net' or the French 'Pointdecontact'.

There are six EU member states, which did not yet ratify the Council of Europe Convention on Cybercrime[1]. Logically, these are potential candidates to find outliers regarding the necessary mechanisms. However, all of them perform roughly on the same level as France, Germany, and Estonia do. Furthermore, all EU member states operate CERTs and when looking at the criminalization of the different aspects of cybercrime[2] only minor shortcomings can be identified:

[1] These member states are: Czech Republic, Greece, Ireland, Luxembourg, Poland, and Sweden
[2] Offences as defined in (Valeri, Somers, Robinson, Graux, & Dumortier, 2006, pp. 13-15)

Latvia and Spain do not have provision regarding intrusion attempts, whereas Spain also lacks provisions on account compromise. Moreover, Germany, Greece, and Ireland do not have provisions on spam. Finally, Ireland lacks provisions on unauthorized modification of information and, together with the UK, on unauthorized access to information systems (Valeri, Somers, Robinson, Graux, & Dumortier, 2006).

4.1.2.2 Sub-national differences in Russia

No sub-national differences regarding criminalization, investigation, and prosecution of cybercrime could be identified for the Russian federation. This does not come as a surprise when considering that regional leaders are appointed by the Kremlin according to the interests of the ruling party (Orttung, 2012).

4.1.3 Existing patterns of cooperation involving the EU and Russia

Existing patterns of cooperation regarding cybercrime will be analyzed in this section. To begin with, an assessment of European and Russian cooperation in the Council of Europe Convention on Cybercrime will be given, followed by an analysis of bilateral agreements between EU member states and Russia. Consequently, European and Russian cooperation with external partners and cooperation between the EU and Russia will be evaluated.

The most popular agreement on combating cybercrime is arguably the Council of Europe Convention on Cybercrime of 2001. Six EU member states did not yet ratify the Convention, namely the Czech Republic, Greece, Ireland, Luxembourg, Poland, and Sweden. However, with none of these countries officially mentioning any reasons not to ratify it and with three EU member states ratifying it in 2012 as well as an additional four since 2009[3], the chances for ratification of the six remaining countries seem to be promising. Also, Russia did not sign the Convention for the official reason that it would allow foreign law enforcement agencies to interpose Russian internet traffic. Despite Russia officially mentioning this as sole reason for not signing it, several other issues are said to have prevented a signature. As Levin and Ilkina (2012) put it ‚'Ratification would also obligate Russia to recognize as criminal acts such activities as the acquisition and possession of devices and computer programs designed […] for the commission of a crime (i.e. malware), as well as the acquisition and possession of computer passwords, access codes or other similar data […]' (Levin & Ilkina, 2012, p. 35). By now only the creation, use, and distribution of such software is criminalized by Russian criminal law, but not its possession, which would require a change in the Russian Criminal Code. The same would apply for the criminalization of online child pornography as for now the creation, use, distribution,

[3] Austria, Belgium, Malta (all in 2012), United Kingdom (in 2011), Portugal, Spain (both in 2010), and Germany (in 2009)

and possession of it is criminalized, but only if the intention to distribute it exists (Levin & Ilkina, 2012, pp. 34-35).

Several bilateral agreements and mutual legal assistance treaties exist between EU member states and the Russian federation (Basel Institute on Governance, 2007). The mutual legal assistance treaties in criminal matters mainly concern Russia and Eastern European states[4] and they do not explicitly address cybercrime. Yet the field of cybercrime should be covered as it is criminalized to a large degree in the relevant states. However, this did not prevent Russia from refusing cooperation when Estonia requested it after suffering the 2007 cyber attack (Tikk & Kaska, 2010, pp. 288-292). Eighteen EU member states[5] concluded bilateral agreements on cooperation with Russia in the fight against crime, which, just like the mutual legal assistance treaties, do not address cybercrime specifically. Hence, they have to be approached with skepticism when it comes to their effectivity in fighting cybercrime as e.g. Article 1 of the agreement with the United Kingdom explicitly excludes legal assistance in criminal matters or extradition (The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 1997).

The European Union on a summit with the USA in 2010 agreed to establish an 'EU-US working group on cyber-security and cybercrime' with the aim to cooperate on issues like cyber-incident exercises, best practices, awareness raising, and online child pornography removal. Furthermore, the working group tries to promote the accession of all EU member states to the Council of Europe Cybercrime Convention (European Commission, 2011).

Moreover, the European Union has an observer status in the 'UN open-ended intergovernmental expert group on cybercrime'. This group has the task to conduct a comprehensive study on the cybercrime problem and possible responses to it relating to the exchange of information on national legislation, best practices, technical issues, and international cooperation. The Russian Federation and most EU member states[6] actively participate in the expert group, including Croatia, which will enter the European Union on the 1st of July 2013 (United Nationas Office on Drugs and Crime, 2011).

In 2011, Russia drafted a UN Convention on international information security, which officially aims at reducing the risk of international cyberwar. However, as Levin and Ilkina state, the real purpose of the document seemingly is 'to protect Russia from international retaliation' (Levin & Ilkina, 2012, p. 36) as it highlights that online security problems should be solved on a national basis without foreign

[4] The following states have mutual legal assistance treaties with Russia: Cyprus, Czech Republic, Estonia, Hungary, Greece, Latvia, Lithuania, Poland, Romania, Spain, Slovakia (Basel Institute on Governance, 2007)
[5] These member states are: Austria, Belgium, Greece, Cyprus, Hungary, Italy, Ireland, Finland, France, Germany, Latvia, Malta, Portugal, Romania, Slovenia, Sweden, Spain, United Kingdom
[6] These countries do not participate: Denmark, Latvia, Lithuania, Malta, United Kingdom

intervention. Many critics stress that the offered provisions limit the freedoms of law-abiding citizens instead of affecting national security. Interestingly, other attempts by the Russian government to limit the freedom of speech on the internet have recently gained increasing attention in the media as for instance an article in the German newspaper 'Die Zeit' mentioned critics 'seeing an attempt to limit the freedom of speech' (Zeit Online, 2012). The article was referring to a newly introduced law allowing Russian authorities to ban websites without prior legal ruling. Additionally, Russia entered a pact with the United States of America concerning information exchange about cyber-offenses and between their national CERTs (Levin & Ilkina, 2012, pp. 36-37).

When it comes to cybercrime cooperation between the European Union and Russia several patterns can be observed. The Partnership and Cooperation Agreement of 1994 set the basis for the general EU-Russia relations. This agreement, however, was just a basis for further cooperation as it lacks provisions on foreign and security policy cooperation or police and judicial cooperation in criminal matters (van Elsuwege, 2012, p. 2). It was followed by a cooperation agreement between the Russian Federation and Europol in 2003, which provided the basis for cooperation in fighting organized crime, but still did not cover cybercrime (Permanent Mission of the Russian Federation to the European Union, 2013). A 'Road Map on the Common Space of Freedom, Security and Justice' was established in 2005, which includes an agenda for future cooperation, e.g. on fighting organized crime, and for the first time explicitly mentions cooperation in new crime areas like information and technology related crime, especially child pornography (European Union–Russia Moscow Summit, 2005). At the EU-Russia Summit in 2008 the two parties gave a joint statement on the launch of negotiations for a new EU-Russia agreement to replace the Partnership and Cooperation Agreement of 1994. It was especially highlighted that legally binding commitments are aimed at in all areas of the relationship (Council of the European Union, 2008). Most recently, a 'Permanent Partnership Council' meeting on Freedom, Justice, and Security was held in 2012 stressing the importance of further developing the cooperation between Europol and Russia as well as coming to an operational agreement between the two. Moreover, joint efforts on judicial cooperation in criminal matters have been highlighted in that meeting (Permanent Mission of the Russian Federation to the European Union, 2012).

4.2 Evaluating the differences regarding criminalization, investigation and prosecution, and international cooperation

Having analyzed the three independent variables, the distance between the European and Russian cyberspace governance will now be assessed with regard to criminalization, investigation and prosecution, as well as international cooperation. This will provide answers to the sub-research questions. In the following, the findings will be related to the theory and to current debates.

In terms of *criminalization* of cybercrime, EU decisions like framework decisions or directives set the guidelines for law approximation and cooperation in the EU. This led to a situation in which the member states have harmonized their laws regarding cybercrime on a basic level with minor shortcomings. However, only in six countries small outliers from the general level of law harmonization could be identified. For these reasons, the performance of EU criminalization regarding cybercrime can be classified on a medium to high level. In contrast to that, the Russian laws are seen as being rather ineffective by the Group-IB. A low degree of basic legislation exists, but several loopholes could be identified: With the establishment of the cybercrime provisions in the Russian Criminal Code, for instance, the prosecution of denial of service attacks has been made harder. Furthermore, vague formulations in the criminal code make the possession of malicious software legal and they only criminalize online child pornography if intended for distribution. The lack of sub-national differences makes harmonization of Russian laws unnecessary, yet the Russian criminalization can be classified on a low level. Comparing the two systems, big differences between them can be identified, which gives an answer to the first sub-research question. Even though the European Union has a certain degree of law harmonization, further harmonizing development is necessary. A recently agreed draft measure by the European Parliament could serve as a first step to further harmonization as it 'would require members to adopt standard terms of imprisonment for those convicted of cybercrimes' (United Press International, 2013). Russia, on the contrary, has to expand its criminalization and close the loopholes in it. This has been acknowledged in several media, e.g. a recent article in 'The Register' stated that 'Russian computer crime laws are outdated' (Leyden, 2013). However, it would be interesting to see whether political interests prevent Russia from further criminalizing cybercrime.

When it comes *to investigation and prosecution* of cybercrime, the European Union bodies like Europol or the EC3 provide a high level of cooperation and a well-developed platform for information exchange and data fusion as well as reporting and alert mechanisms. ENISA and CERT-EU improve European network security and the efficiency of national CERTs, which is supported by Germany and France operating national network security agencies, for example. Next to that, all EU member states operate national computer emergency response teams. Overall, the cybercrime investigation and prosecution system in the EU is on a high level, but more harmonization is still necessary with the EU bodies providing the necessary basis for that. In Russia, the Group-IB and the private sector in general are important for investigation and prosecution. The respective public bodies are not as extensive as in the EU whereas the Group-IB is active in intelligence, information exchange, investigation, and computer emergency response. Surprisingly, with 'Sornyak' Russia launched an internationally cooperative program against online child pornography. Nonetheless, the Russian system can again be seen as being on a low level in this area with no significant governmental

involvement or a framework of special anti-cybercrime units. In comparison, to give an answer to the second sub-research question, major differences between the two systems can be identified. Despite the high-level of cooperation between the respective bodies in the EU more harmonization among the member states is necessary. In Russia, in contrast to that, the private sector seems to be more important for investigation and prosecution than the public sector, which again raises the question whether political factors minimize the Russian interest in related governmental or public mechanisms. Interestingly, in this context, John Leyden in 'The Register' mentioned that Russian governmental bodies 'lack the technological expertise, computer forensics and legal expertise to tackle cybercrime' and that if they tried to investigate they were free to do so, 'providing the victims were non-Russians' (Leyden, 2013).

To start with in the field of *international cooperation*, many bilateral agreements and mutual legal assistance treaties exist between EU member states and the Russian Federation. However, they are rather ineffective in fighting cybercrime as the Russian refusal of the Estonian legal assistance request or the exclusion of legal assistance in criminal matters or extradition in the agreement between the UK and Russia show. For the purpose of harmonization, the EU has to promote ratification of the Council of Europe Convention by all its member states. The agreement between Europol and Russia provides a good basis for further international cooperation, but further legally binding commitments are necessary. The general need for legally binding commitments has also been acknowledged recently in a 'Frankfurter Allgemeine Zeitung' article quoting the head of the Russian 'Lewada-Centre' Lew Gudkow, who said that the EU should 'conclude agreements with Russia and insist on their compliance' (Frankfurter Allgemeine Zeitung, 2013). Overall, the EU´s degree of international cooperation can be classified on a medium level. Russian international cooperation seems to be rather perfunctory than real as the reasons for it not signing the Council of Europe Convention are highly disputable. In difference to the official reason, the true preventing factor seems to lie in the shortcomings of Russian criminalization of cybercrime. Similar to that, its UN convention draft can in fact be seen as self-protection instead of a commitment. For these reasons, the Russian degree of international cooperation can be classified on a low level leading to differences of a medium extent between the two systems regarding the third sub-research question. The EU could improve in terms of joint cooperation or acting as one entity. The Russian reasons for cooperation are commonly seen as a facade for self-protection mechanisms, which can also be seen in the lack of legally binding commitments between the EU and Russia.

Relating these finding to the theoretical framework of this paper, some interesting observations can be made. With regard to the general concept of liberalism and in line with Andrew Moravcsik´s (1992) argumentation about the behavior of states, the Russian behavior in terms of cooperation and

cyberspace governance clearly reflects its state interests, not least in the ruling party trying to preserve its own power through undermining the civil society. This has recently gained attention in the media as an article in 'The Guardian' highlighted that 'the Kremlin has decided to destroy […] civil society' (Alexeeva, 2013). The article refers to a newly introduced Russian law requiring non-governmental organizations receiving foreign funding to register as 'foreign agents', which in Russian means 'spy' or 'traitor' and thus contains a highly negative image (Alexeeva, 2013). However, the resulting lack of freedom and security on the internet minimizes norm and institution building through non-state actors, which has been highlighted by Eriksson and Giacomello (2006) as well as McEvoy Manjikian (2010), and thus contributes to making the Russian cyberspace governance ineffective. In contrast to that, the lack of harmony on the domestic level in the European Union threatens its ability to cooperate externally. This is in line with Eriksson and Giacomello (2006) emphasizing the importance of domestic political factors for international state behavior. Moreover, according to Mary McEvoy Manjikian´s (2010) description of pragmatic liberalism, focused international cooperation determines the development of cyberspace. This can be seen in the fact that the European system based on a relatively high level of cooperation is properly functioning compared to the ineffective Russian cyberspace governance with a low degree of cooperation. The EU system is furthermore being supported by the civil society promoting cyberspace development, which could not be observed in Russia.

5. Conclusion

The focus of this paper is the question to what extent the cyberspace governance systems of the European Union and Russia differ. With growing distrust in online activities like banking or purchasing among European citizens and with the 2013 'Cybersecurity Strategy of the European Union', this issue has gained even more importance over the last years. Not least the transnational nature of cybercrime and the dominance of the Russian-speaking cybercrime market in combination with the Russian refusal to sign the Council of Europe Convention on Cybercrime support its significance. This chapter will conclude the line of reasoning of the paper by providing an answer to the main research question with the help of the sub-questions and the resulting differences between the European and the Russian cyberspace governance systems in terms of criminalization, investigation and prosecution, as well as international cooperation. Moreover, relevant problems will be identified and applied to the theory. Eventually, the resulting implications for further EU policies regarding cybercrime cooperation with Russia and potential issues for future research will be presented.

Starting with the first sub-question, the governance of the EU on criminalization has been classified on a medium to high level, whereas the Russian governance has been classified on a low level. Minor shortcomings in EU law harmonization and a low degree in addition to loopholes in cybercrime criminalization in Russia have led to a big difference between the two governance systems regarding criminalization. When it comes to investigation and prosecution, the European Union has performed on a high level in contrast to the Russian low-level governance. This leaves a big difference between the two in this area, being heavily influenced by the lack of public or governmental investigation and prosecution mechanisms in Russia. Finally, with regard to international cooperation the EU governance system has been rated on a medium level due to ineffective bilateral agreements and MLAs between the member states and Russia as well as the lack of unity in signing the Council of Europe Convention. Russia, on the contrary, clearly performed on a low level as its reasons for concluding or not concluding agreements are highly debatable for they seem to be matters of self-protection rather than signs of commitment. Therefore, a medium difference between the EU and Russia regarding international cooperation could be identified. Connecting the answers to the sub-questions, the overall difference between the European and the Russian cyberspace governance systems can be classified as being medium to big with a tendency to the latter, which gives an answer to the main research question.

With regard to the theoretical framework of this paper, several interesting observations could be made. In accordance with Andrew Moravcsik´s (1992) theory of liberalism, the Russian behavior in terms of cooperation and cyberspace governance complies with the general political situation in the Russian Federation in as much as it undermines (online) civil society building and tries to preserve national interests instead of committing to international agreements. This has also been highlighted in several newspaper articles referred to in this paper. It is in so far important as it, consistent with Eriksson and Giacomello´s (2006) points about pragmatic liberalism, prevents norm and institution building in cyberspace due to the lack of online freedom and security as well as the absence of important actors like online groups. Moreover, it complies with the authors´ thesis about the importance of domestic political factors in influencing international state behavior. McEvoy Manjikian´s (2010) application of pragmatic liberalism to cyberspace is also reflected in the abovementioned points since she sees focused international cooperation as the main force behind cyberspace evolvement and security. The absence of a sufficient degree of cooperation between the EU and Russia thus prevents evolvement and security, however, when looking at the two governance systems as such, an interesting picture emerges. The EU system being based on a high level of cooperation among its different bodies is far more developed and secure than the Russian system of low cooperation. This again displays the importance of 'netizens' and online groups.

These findings have several implications for EU foreign policy regarding Russian cybercrime. If the European Union, given the current situation, aimed at concluding a cybercrime agreement with the Russian Federation in order to fight Russian cybercrime more effectively, the agreement would certainly not become extensive. Due to the problems identified in the analysis and the big difference between the two cyberspace governance systems, an agreement with Russia would at the most be realizable with significant shortcomings regarding all of the three relevant aspects, namely criminalization, investigation and prosecution, and international cooperation. The answers to the sub-questions have shown that the differences on all three aspects are too big to be easily overcome. However, three recommendations for future EU policies and actions regarding cybercrime can be given in order to improve cooperation with Russia. First of all, aiming at the facilitation of an agreement, the European Union has to foster the development of an online civil society in Russia. This means that the building of social and political organizations, online groups, non-governmental organizations and the like with relation to cyberspace is a basic condition to generate norm and institution building regarding cybercrime. Secondly, in order for this to happen the European Union has to foster democracy in Russia in general. Without basic principles of a democratic society including freedom of speech (in this case especially on the internet), a free press, civil society, and the decentralization of power, Russian behavior on the international sphere will continue to only reflect Kremlin preferences. Especially the EU Cybersecurity Strategy mentioning the protection of fundamental rights as core value makes this issue even more important. Legally binding commitments between the EU and Russia are necessary in this context. Finally, the European Union has to generate further internal harmonization regarding criminalization, investigation and prosecution, as well as international cooperation. A unified approach would enable the EU to speak with one voice in cybercrime matters and in this way, in accordance with Eriksson and Giacomello´s (2006) point about the importance of domestic political factors for international state behavior, enhance the chances for future cooperation. A first step would be the signature of all EU member states to the Council of Europe Convention on Cybercrime. Finally, several questions for future research came up in the course of this paper. It became apparent that certain political interests prevent Russia from further criminalizing and expanding its investigation and prosecution mechanisms regarding cybercrime. This was especially the case in the Russian refusal to sign the Council of Europe Convention as well as in its UN Convention draft. Future research should therefore focus on the interests at stake in this context. Next, more data on cybercrime in general, Russian cybercrime in particular, and on the incorporation of cybercrime into international relations theory is necessary to create an extensive scientific literature. This would give useful insights on what points to focus on by the EU in constructing future agreements. Finally, a more extensive study on the effectivity of the national cyberspace governance systems in Europe could presents points of

improvement for EU cyberspace governance and best practices of cybercrime prevention. However, more quantitative cybercrime data is necessary in this context.

6. Bibliography

Aaviksoo, J. (2010). Cyberattacks Against Estonia Raised Awareness of Cyberthreats. *Defence Against Terrorism Review Vol.3*, 13-22.

Agence nationale de la sécurité des systèmes d'information. (2011). *La stratégie de la France en matière de cyberdéfense et cybersécurité.*

Alexeeva, L. (2013, May 24). *Vladimir Putin´s goal is to destroy Russian civil society* . Retrieved June 8, 2013, from guardian.co.uk: http://www.guardian.co.uk/commentisfree/2013/may/24/vladimir-putin-goal-russian-civil-society?INTCMP=SRCH

Anderson, C. W. (1990). *Pragmatic Liberalism.* Chicago: The University of Chicago Press.

Babbie, E. (2011). *The Basics of Social Research 5th Edition.* Belmont,CA: Wadsworth Cengage Learning.

Barkham, J. (2001). *Cyberwar, Cybercrime, Cyberterrorism: A Bibliographic Essay.*

Basel Institute on Governance. (2007). *Russia Country Profile - Legal Frameworks*. Retrieved May 30, 2013, from Asset Recovery Knowledge Centre: http://www.assetrecovery.org/kc/node/50560f43-c065-11dd-b3f1-fd61180437d9.0

Bundesministerium der Justiz. (2012). *German Criminal Code*. Retrieved May 27, 2013, from gesetze-im-internet.de: http://www.gesetze-im-internet.de/englisch_stgb/

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of Atomic Scientists 68*, 70-77.

Council of Europe. (2001). *Convention on Cybercrime.* Budapest: Council of Europe.

Council of the European Union. (2002, February 28). Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime. *Official Journal L063*.

Council of the European Union. (2004, March 10). Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. *Official Journal L 077*.

Council of the European Union. (2005, February 24). Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal L 069*.

Council of the European Union. (2008). *Joint Statement of the EU-Russia Summit on the launch of negotiations for a new EU-Russia agreement.* Brussels.

Council of the European Union. (2011). Directive 2011/92/EU of the European Parliament and of the Council of the European Union of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. *Official Journal of the European Union*.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant theory? *International Political Science Review 2006 27*, 221-244.

Estonian Information System´s Authority. (2012). *About CERT Estonia*. Retrieved May 24, 2013, from ria.ee: https://www.ria.ee/cert-estonia/

European Commission. (2006). COM(2006) 817 final. *Proposal for a Council Decision establishing the European Police Office (Europol).* Brussels: European Commission.

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, COM (2008)448.*

European Commission. (2010). MEMO/10/463. *Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA.* Brussels.

European Commission. (2011, April 14). MEMO/11/246. *Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats*. Brussels: European Commission.

European Commission. (2012a, March 28). An EU Cybercrime Centre to fight online criminals and protect e-consumers. *European Commission - Press Release*. Brussels: European Commission.

European Commission. (2012b). *Special Eurobarometer 390 on Cybersecurity.* European Commission.

European Commission. (2013a). *Cybersecurity Strategy of the European Union.* Brussels.

European Commission. (2013b, January 9). European Cybercrime Centre (EC3) opens on 11 January. *European Commission - Press Release*. Brussels: European Commission.

European Network and Information Security Agency. (2009). *CERT factsheet.* Retrieved May 23, 2013, from enisa.europa.eu: http://www.enisa.europa.eu/activities/cert/background/cert-factsheet

European Network and Information Security Agency. (2011a). *Estonia Country Report.* European Network and Security Agency.

European Network and Information Security Agency. (2011b). *France Country Report.* European Network and Information Security Agency.

European Network and Information Security Agency. (2011c). *Germany Country Report.* European Network and Security Agency.

European Network and Information Security Agency. (n.d.). *CERT-EU.* Retrieved May 23, 2013, from enisa.europa.eu: http://www.enisa.europa.eu/activities/cert/background/inv/cert-eu

European Union–Russia Moscow Summit. (2005). *Road Map for the Common Space on Freedom, Security, and Justice*. Retrieved May 31, 2013, from President of Russia - Official Web Portal: http://archive.kremlin.ru/eng/text/docs/88030.shtml

Europol. (n.d.). *About Us*. Retrieved May 22, 2013, from europol.europa.eu: https://www.europol.europa.eu/content/page/about-us

Europol. (n.d.). *Services*. Retrieved May 22, 2012, from europol.europa.eu: https://www.europol.europa.eu/ec3/services

Europol. (n.d.). *The first years, 1999-2004*. Retrieved May 22, 2013, from europol.europa.eu: https://www.europol.europa.eu/content/page/first-years

Frankfurter Allgemeine Zeitung. (2013, June 1). *Leiter des Lewada-Zentrums - „Russland bewegt sich in Richtung Diktatur“* . Retrieved June 8, 2013, from FAZ.net: http://www.faz.net/aktuell/politik/ausland/europa/leiter-des-lewada-zentrums-russland-bewegt-sich-in-richtung-diktatur-12204341.html

Group-IB. ((n.d.)). *About the company*. Retrieved May 23, 2013, from group-ib.com: http://www.group-ib.com/index.php/o-kompanii/15-o-group-ib

Group-IB. (n.d.). *About CERT-GIB*. Retrieved May 23, 2013, from group-ib.com: http://cert-gib.com/mission.php

Kuzmin, A. (2012). State and Trends of Russian Cybercrime in 2011. *First International Workshop on Cyber Crime 2012.* Moscow: Group-IB, CERT-GIB.

Legifrance. (n.d.). *Legifrance translations.* Retrieved May 25, 2013, from Legifrance: http://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations

Levin, A., & Ilkina, D. (2012). *Securing Cyberspace: A Comparative Review of Strategies Worldwide.* Ryerson University - Ted Rogers School of Management.

Levin, A., & Ilkina, D. (2013). *International Comparison of Cyber Crime.* Ryerson University - Ted Rogers School of Management.

Leyden, J. (2013, June 6). *Russian cops lack kit to fight cybercrooks, says Brit security buff*. Retrieved June 8, 2013, from The Register: http://www.theregister.co.uk/2013/06/06/private_sector_leading_russian_cybercrime_cleanup/

Liff, A. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwardare Capabilities and Interstate War. *Journal of Strategic Studies 35:3*, 401-428.

McEvoy Manjikian, M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly 54*, 381-401.

Moravcsik, A. (1992). *Liberalism and International Relations Theory.* Cambridge: Harvard University.

Nye, J. (2003). *Understanding International Conflicts: An Introduction to Theory and History* . New York: Pearson and Addison Wesley.

Nye, J. (2004). *Power in the Global Information Age: From Realism to Globalization.* London: Routledge.

Orttung, R. (2012). *Russia*. Retrieved May 28, 2013, from Freedom House: http://www.freedomhouse.org/report/nations-transit/2012/russia

Permanent Mission of the Russian Federation to the European Union. (2012). *Russia-EU PPC on Freedom, Security and Justice held its 16th meeting*. Retrieved May 31, 2013, from russianmission.eu: http://russianmission.eu/en/news/russia-eu-ppc-freedom-security-and-justice-held-its-16th-meeting

Permanent Mission of the Russian Federation to the European Union. (2013). *Fight against transnational crime and terrorism*. Retrieved May 31, 2013, from russianmission.eu: http://russianmission.eu/en/fight-against-transnational-crime-and-terrorism

Rehn, O. (2008, May 8). EU-Russia relations: the way forward? *SPEECH/08/236*. Helsinki: EU-Russia Seminar of the Swedish People's Party in Finland.

Republic of Estonia. (n.d.). *Penal Code (Karistusseadustik), passed 6 June 2001, entered into force 1 September 2002.*

Robinson, N., Disley, E., Potoglou, D., Reding, A., May Culley, D., Penny, M., et al. (2012). *Feasibility Study for a European Cybercrime Center.* Brussels: European Commission.

Russian Federation. (n.d.). Chapter 28. Crimes in the Sphere of Computer Information. *Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on March 1, 2012)*.

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland. (1997, October 06). *Bilateral Agreements*. Retrieved May 30, 2013, from rusemb.org.uk: http://www.rusemb.org.uk/relations/6

Tikk, E., & Kaska, K. (2010). Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. In J. Demergis, *Proceedings of the 9th European Conference on Information Warfare and Security* (pp. 288-294). Academic Conferences Limited.

United Nationas Office on Drugs and Crime. (2011). *Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime*. Retrieved May 31, 2013, from unodc.org: https://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html

United Press International. (2013, June 6). *EU mulls cybercrime penalties*. Retrieved June 8, 2013, from UPI.com: http://www.upi.com/Top_News/Special/2013/06/06/EU-mulls-cybercrime-penalties/UPI-29921370526872/

Valeri, L., Somers, G., Robinson, N., Graux, H., & Dumortier, J. (2006). *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries.* Brussels: European Commission.

van Elsuwege, P. (2012, June). Towards a Modernisation of EU-Russia Legal Relations? *CEURUS*. Tartu: University of Tartu - Centre for EU-Russia Studies.

Voltolini, B. (2012). *The role of non-state actors in EU policies towards the Israeli-Palestinian conflict.* European Union Institute for Security Studies.

Zeit Online. (2012, July 12). *Russland erlaubt umstrittene Sperrung von Internetseiten*. Retrieved June 08, 2013, from Zeit Online: http://www.zeit.de/politik/ausland/2012-07/russland-internet-gesetz

7. Appendix : Dataset used in analysis

7.1 Appendix A: Institutional and legal arrangements

Authors	Title	Date	Type
Robinson et al.	Feasibility Study for a European Cybercrime Centre	2012	Report
Council of the European Union	Council Framework Decision 2005/222/JHA	2005	Legislative text
European Commission	Report COM (2008)448	2008	European Commission Report
European Commission	MEMO/10/463	2010	Directive Proposal
Council of the European Union	Directive 2011/92/EU	2011	Directive
Europol	About us	n.d., retrieved May 22, 2013	Website
Europol	Services	n.d., retrieved May 22, 2013	Website
Europol	The first years, 1999-2004	n.d., retrieved May 22, 2013	Website
European Commission	COM(2006) 817 final	2006	Council Decision Proposal
European Commission	An EU Cybercrime Centre to fight online criminals and protect e-consumers	2012	Press Release
European Commission	European Cybercrime Centre (EC3) opens on 11 January	2013	Press Release
Council of the European Union	Council Decision 2002/187/JHA	2002	Legislative Text
Council of the European Union	Regulation (EC) No 460/2004	2004	Regulation
ENISA	CERT Factsheet	2009, retrieved May 23, 2013	Website
ENISA	CERT-EU	n.d., retrieved May 23, 2013	Website
Levin, A. & Ilkina, D.	International Comparison of Cybercrime	2013	Report
Russian Federation	Chapter 28. Crimes in the Sphere of Computer Information	n.d., last amended 2012	Criminal Code
Group-IB	About CERT-GIB	n.d., retrieved May 23, 2013	Website
Group-IB	About the Company	n.d., retrieved May 23, 2013	Website

7.2 Appendix B: Differences on national and sub-national level

Authors	Title	Date	Type
ENISA	Estonia Country Report	2011	Report
Republic of Estonia	Penal Code	n.d., entered into force 2002	Penal Code
Valeri, Somers, Robinson, Graux, & Dumortier	Handbook of Legal Procedures of Computer and Network Misuse in EU Countries	2006	Report
Estonian Information system´s Authority	About CERT-Estonia	2012, retrieved May 24, 2013	Website
Levin, A. & Ilkina, D.	Securing Cyberspace	2012	Report
Agence nationale de la securité des systèmes d´information	La stratégie de la France en matière de cyberdéfense et cybersécurité	2011	National Strategy
Legifrance	Legifrance translations	n.d., retrieved May 25, 2013	Website
Robinson et al.	Feasibility Study for a European Cybercrime Centre	2012	Report
ENISA	France Country Report	2011	Report
ENISA	Germany Country Report	2011	Report
Bundesministerium der Justiz	German Criminal Code	2012, retrieved May 27, 2013	Website
Orttung	Russia	2012, retrieved May 28, 2013	Website

7.3 Appendix C: Existing patterns of cooperation

Authors	Title	Date	Type
Valeri, Somers, Robinson, Graux, & Dumortier	Handbook of Legal Procedures of Computer and Network Misuse in EU Countries	2006	Report
Levin, A. & Ilkina, D.	Securing Cyberspace	2012	Report
Basel Institute of Governance	Russia Country Profile – Legal Frameworks	2007, retrieved May 30, 2013	Website
Tikk, E. & Kaska, K.	Legal Cooperation to Investigate Cyber Incidents	2010	Conference Proceeding
The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland	Bilateral Agreements	1997, retrieved May 30, 2013	Website
European Commission	MEMO/11/246	2011	Press Release
United Nations Office on Drugs and Crime	Open-ended intergovernmental expert group to conduct a comprehensive study of the problems of cybercrime	2011, retrieved May 31, 2013	Website
Zeit Online	Russland erlaubt umstrittene Sperrung von Internetseiten	2012, retrieved June 8, 2013	Website
Van Elsuwege	Towards a modernization of EU-Russia Legal Relations?	2012	Scientific Paper
Permanent Mission of the Russian Federation to the European Union	Fight against transnational crime and terrorism	2013, retrieved May 31, 2013	Website
European Union-Russia Moscow Summit	Roadmap on the Common Space on Freedom, Security, and Justice	2005, retrieved May 31, 2013	Website
Council of the European Union	Joint Statement of the EU-Russia Summit on the launch of negotiations for a new EU-Russia agreement	2008	Press Release
Permanent Mission of the Russian Federation to the European Union	Russia-EU PPC on Freedom, Security, and Justice held its 16th meeting	2012, retrieved May 31, 2013	Website

7.4 Appendix D: Comparing the differences between the cyberspace governance systems

Authors	Title	Date	Type
United Press International	EU mulls cybercrime penalties	2013, retrieved June 8, 2013	Website
Leyden	Russian cops lack kit to fight cybercrooks, says Brit security buff	2013, retrieved June 8, 2013	Website
Frankfurter Allgemeine Zeitung	Leiter des Lewada-Zentrums – „Russland bewegt sich in Richtung Diktatur“	2013, retrieved June 8, 2013	Website
Alexeeva	Vladimir Putin´s goal is to destroy Russian civil society	2013, retrieved June 8, 2013	Website