Nuutti Laitala

HACKTIVISM AND CYBERTERRORISM: HUMAN RIGHTS ISSUES IN STATE RESPONSES

Master's thesis for the European Master's Degree in Human Rights and Democratisation

Supervised by Professor Zdzisław Kędzia

Faculty of Law and Administration

Adam Mickiewicz University, Poznan

6/19/12

Adam Mickiewicz University

Faculty of Law and Administration

Abstract

This study examines hactivism and cyberterrorism, how OSCE participating states have responded to these phenomena and have these responses respected user's human rights, especially the right to freedom of expression. *Right to Freedom of Expression* is a fundamental human right in international human rights law. This right includes the freedom to hold opinions without interference and seek, receive and impart information and ideas trough any media and regardless of frontiers. *Hacktivism* is nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. *Cyberterrorism* consists of politically motivated illegal attacks against information, computer systems, programs and data resulting in violence against noncombatant targets. *OSCE* is the world's largest regional security organisation of 56 states. The organisation has a comprehensive approach to security, including politico-military, economic, environmental and human aspects. OSCE participating states have different kinds of approaches to respond to the acts of hacktivism and cyberterrorism.

This study is based on literature review on relevant topics. It will not go deep into technical or legal details, but aims to give an overview of the situation in the OSCE participating states. Main focus for the legal instruments is on the United Nations and Council of Europe standards adopted by OSCE. A short case study on Poland is included. Software piratism, copyright issues and cyber war attacks conducted by states are outside the scope of this study. The study found out, that hacktivists and cyberterrorists share many tools and methods, but the main differences between these phenomena are intended use of violent methods and level of concern for the welfare of the other users. However, academia, governments and mass media often place hacktivism and cyberterrorism in the same category. OSCE states have responded to hacktivism and cyberterrorism with domestic legislation and institutions, international conventions, technical measures and specialized institutions. More focused and human rights respecting co-operation is needed. Current, imposed content filtering and blocking methods may violate users' right to freedom of expression.

Foreword

I would like to thank Professor Zdzisław Kędzia and Ms. Beata Zięba for their valuable help in writing this thesis and all practical arrangements in Poznan. I would also like to thank Mr. Matti Inkeroinen, Mr. Antti Airaksinen, Mrs. Jenni Tulensalo, Mr. Risto Ruotsalainen and my parents Kyllikki and Seppo Laitala for their inspiration, support and help with my studies in the European Master's Degree Programme for Human Rights and Democratisation. With the help from all above mentioned people, writing this thesis has been an interesting and rewarding learning process.

Ad Omnia Paratus, Ready for anything

Abbreviations

ARPANET	Advanced Research Projects Agency Network
CERT	Computer Emergency Response Team
CTITF	Counter Terrorism Implementation Task Force
CoE	Council of Europe
CTC	Counter Terrorism Committee
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
ICCPR	International Covenant on Civil and Political Rights
ICERD	International Convention on the Elimination of all Forms of Racial Discrimination
ISP	Internet Service Provider
NASK	Naukowa i Akademicka Sieć Komputerowa – Scientific and Academic Computer Network
NGO	Non-Governmental Organisation
ODIHR	Office for Democratic Institutions and Human Rights
OSCE	Organization for Security and Co-operation in Europe
PPBW	Polska Platforma Bezpieczeństwa Wewnętrznego
TP	Telekomunikacja Polska
UN	United Nations
UPR	Universal Periodic Review
URL	Uniform Resource Locator

Table of contents

ABSTRACT 1

1 INTRODUCTION 6

2 THEORETICAL BACKGROUND 10

2.1 THE RIGHT TO FREEDOM OF EXPRESSION 10

2.1.1 UN, UDHR, ICCPR, CoE and ECHR 10

2.1.2 Restrictions 14

2.1.3 The international protection of human rights 17

2.2 THE INTERNET 20

2.3 HACKTIVISM 22

2.3.1 Hacktivists and their motivations 23

2.3.2 The acts of hacktivism 25

2.4 CYBERTERRORISM 30

2.4.1 The challenges of defining terrorism 30

2.4.2 Cyberterrorists and their motivations 33

2.4.3 The acts of cyberterrorism 33

3 INTERNATIONAL CONVENTIONS 38

3.1 THE UN GLOBAL COUNTER-TERRORISM STRATEGY AND CTITF 38

3.2 COUNCIL OF EUROPE CONVENTION ON THE PREVENTION OF TERRORISM 40

3.3 COUNCIL OF EUROPE CONVENTION ON CYBERCRIME 41

3.4 EUROPEAN UNION COUNTER-TERRORISM STRATEGY 42

3.5 ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, OSCE 44

3.6 BUCHAREST PLAN OF ACTION FOR COMBATING TERRORISM 46

3.7 OSCE JOINT DECLARATION ON FREEDOM OF EXPRESSION AND THE INTERNET 47

3.8 THE JOINT DECLARATION OF THE UN, OSCE AND AMERICAN STATES INDEPENDENT EXPERTS 48

4 STATE RESPONSES TO CYBER-THREATS 50

4.1 BALANCING HUMAN RIGHTS AND OTHER VALUES IN THE SOCIETY 50

4.2 STATUS OF INTERNATIONAL CONVENTIONS IN THE OSCE STATES 50

4.3 NATIONAL STRATEGIES FOR INTERNET CONTENT REGULATION 52

4.4 THE ROLE OF THE INTERNET SERVICE PROVIDERS 56

4.5 THE ROLE OF COMPUTER EMERGENCY RESPONSE TEAMS 59

4.6 CASE OF POLAND 60

4.6.1 International and domestic law 60

4.6.2 Domestic institutions 65

4.6.3 Example of hacktivism in Poland 68

5 CONCLUSION 70

5.1 WHAT ARE THE MAIN DIFFERENCES BETWEEN HACKTIVISM AND CYBERTERRORISM? 70

5.2 HOW HAVE OSCE-STATES RESPONDED TO ACTS OF HACTIVISM AND CYBERTERRORISM? 71

5.3 IS THE RIGHT TO FREEDOM OF EXPRESSION TAKEN IN ACCOUNT IN THESE RESPONSES? 73

BIBLIOGRAPHY 76

LEGAL SOURCES 76

OFFICIAL DOCUMENTS 79

LITERATURE 84

FIGURE 1. The relation of hacktivism to online activism, civil disobedience, cyberterrorism and hacking. 29

TABLE 1. The status of international conventions in OSCE participating states.......... 52

TABLE 2. Categories of regulated content and laws in the OSCE states...................... 53

TABLE 3. The Polish Penal Code articles relevant to hacktivism and cyberterrorism.. 63

1 Introduction

After the Second World War the United Nations (UN), Council of Europe (CoE) and other international organisations started to develop a system for international protection of human rights as a part of the way to world peace and improving the lives of people. Today these organisations cover a wide range of activities and their initiatives have resulted to a legal framework including several human rights and fundamental freedoms. At the heart of the UN human rights law is an instrument called International Bill of Human Rights, which consists of the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). European Convention of Human Rights (ECHR) is the most important human rights convention by CoE. Parts of these instruments are customary international law, while others set binding obligations only to states, which have ratified them.

One of the fundamental human rights contained in the International Bill of Human Rights is the Right to Freedom of Expression. It was first declared in the UDHR (1948) and later made legally binding by CoE ECHR (1950) and the ICCPR (1966). ICCPR provides everyone with the freedom of expression including freedom to seek, receive and impart information and ideas regardless of frontiers in any media.[1] Correspondingly ECHR provides everyone the same right to freedom of expression with a more elaborated basis for possible restrictions, such as restrictions for protecting national security or public safety.[2] Also ICCPR allows restrictions of this right in certain special circumstances. A whole system of monitoring, reporting and complaint mechanisms has been established by the UN and CoE to ensure, that the states comply with their human rights obligations. The Internet is an important communication and media tool for the modern societies and the UN recognizes Internet access as inherent to the right to free expression. Some countries such as Finland and Estonia already consider access to Internet as a fundamental human right for their citizens.[3] The Organization for Security

[1] OHCHR, 1966.

[2] Council of Europe, 1950.

[3] Akdeniz, 2010, pp. 9-10.

and Co-operation in Europe (OSCE) is a large and important regional security organisation, which dedicates parts of it's initiatives to the right to freedom of expression on the Internet. OSCE Representative on Freedom of the Media sees unhindered access to Internet, free flow of information and Internet literacy as obligations of democratic governments. [4] Under the international law Internet media enjoys the same protection as the traditional media.

The right to freedom of expression on the Internet can be enjoyed in connection with political activities, such as production, distribution and consumption of political information, debate and discussion or organisation and mobilization.[5] Political activists and politicians have for years used the Internet more or less successfully for their campaigns. These widely accepted legal activities are not enough for some citizens. Hacktivism is performed by those who use the digital tools in a nonviolent, but illegal or legally ambiguous ways to pursuit political ends.[6] Hacktivists may for example aim for government policy change or circumvention. Their activities disrupt user's normal operations on the Internet, but do not cause permanent damage. Hacktivists may for example temporarily disable or deface government websites.[7] Hacktivism will be discussed in more detail in chapter 2.3 of this study. Terrorists have also been successful in exploiting the new technologies and are actively developing their capacities. Cyberterrorism is causing increasingly negative impact on modern societies dependent on Information Technology (IT). Acts of cyberterrorism are politically motivated attacks against information, computer systems, programs and data resulting in violence against non-combatant targets.[8] By abusing the Internet cyberterrorists may for example destroy information, spread terrorist messages and cause widespread problems to the society's vital information systems. Cyberterrorism is discussed more thoroughly in the chapter 2.4 of this study. The states respond to acts of hacktivism and cyberterrorism with international and domestic legislation, technical countermeasures and specialized institutions. The success of the terrorists in general has lead to some governments

[4] OSCE (b), 2012, pp. 1-2.
[5] Dahlberg & Siapera, 2007, p. 47.
[6] Samuel, 2004, pp. 1-3.
[7] Idem, p. 7.
[8] Denning, 2001, p. 281.

adopting strict measures on the global "war on terrorism", which have caused concern and negative impacts on human rights, including the right to freedom of expression.[9] Because of anti-terrorism atmosphere, the states may not always recognize the boundaries between conventional political activism, hacktivism and cyberterrorism.[10]

The research method for this study is a literature review on relevant hacktivism and cyberterrorism literature. The main focus is on the hacktivism and cyberterrorism related legal instruments created by the UN and CoE and adopted by OSCE. OSCE has been selected as the target organisation because of its comprehensive approach to security, which includes human rights and counter-terrorism commitments. Additionally OSCE is the world largest regional security organisation, making it possible to analyse the state responses from different parts of the world. The study aims to find out if the OSCE framework been effective and what impact it has had on hactivism and cyberterrorism from the human rights point of view, especially regarding the right to freedom of expression. Because of the high number of OSCE participating states, the study will not attempt to create a comprehensive list of all state responses. Instead, a general overview of the state responses to hacktivism and cyberterrorism in the OSCE area will be provided. A thorough analysis of the legal instruments will not either be made as this study is not primarily legal. Software piratism, copyright issues, cyberwar attacks conducted by states and "normal" cybercrime such as e-mail spamming and e-mail scams are outside the scope of this study. The goal is to answer the three following questions:

1) What are the main differences between hacktivism and cyberterrorism?

2) How have OSCE-states responded to acts of hactivism and cyberterrorism?

3) Is the right to freedom of expression taken in account in these responses?

The study starts with an introduction chapter followed by a chapter presenting the theoretical background. This theoretical background includes an overview of the most

[9] OSCE ODIHR (a), 2007, pp. 20-21.
[10] Denning, 2001, pp. 242-243.

important international organisations and conventions related to the topic, background of the Internet and concepts of hacktivism and cyberterrorism. The third chapter of the study presents several relevant international conventions and other standards in more detail. The fourth chapter discusses in a compact overview about the actual responses to OSCE participating states to hacktivism and cyberterrorism by presenting the relevant domestic laws, specialized institutions and technical measures. This chapter also includes a short case study on Poland. The last chapter contains a conclusion of the issues discussed in the study by providing answers to the research questions and some concluding remarks.

2 Theoretical background

This chapter provides an overview of the most important organisations and legal instruments in the international protection of human rights, the concept of the right to freedom of expression, the possible restrictions for this right and a snapshot of the protection mechanisms for human rights. Also the historical background for the Internet as well as the definitions, actors and acts of hacktivism and cyberterrorism will be presented.

2.1 The Right to Freedom of Expression

The right to freedom of expression is crucial to democratic societies and enables the enjoyment of many other rights. Free expression places policies of democratic governments under scrutiny and exposure of the free media. The citizens stay informed about government policies and can criticise them.[11]

2.1.1 UN, UDHR, ICCPR, CoE and ECHR

Before looking more deeply at the theoretical background of the right to freedom of expression, it’s meaningful to provide an overview of the most important international organisations and legal instruments shaping the international human rights law related to this right. These are the United Nations (UN), the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), Council of Europe (CoE) and the European Convention on Human Rights (ECHR).

The United Nations was founded in 1945 to keep peace in the world, to develop friendly relations between nations, to improve lives of poor people, fight hunger, disease and illiteracy, to promote respect for rights and freedoms and to be the centre of actions for achieving globally the above mentioned goals. The UN has 193 member states, which negotiate their views through General Assembly, Security Council, the Economic and Social council and other bodies and committees. The UN covers a wide range of activities including peacekeeping, peace building, conflict prevention, humanitarian

[11] Denning, 2001, pp 219-220.

assistance, sustainable development, counter terrorism, human rights and numerous other activities.[12]

An instrument called International Bill of Human Rights is the core of the UN human rights law. It consists of UDHR, ICCPR, its two Optional Protocols and the International Covenant on Economic, Social and Cultural Rights (ICESCR). There is also a large amount of special human rights conventions, declarations, minimum rules and other instruments supplementing and defining the International Bill of Human Rights. Some provisions of International Bill of Human Rights are customary international law, while others are only binding for the states, which have ratified the treaties.[13]

The development of the UDHR started from the experiences of the Second World War. After the creation of the UN in 1945, the international community wanted to prevent similar atrocities from happening again. As a part of this initiative, the development towards UDHR started in 1946 by drafters from various political, cultural and religious backgrounds. UN General Assembly adopted UDHR in 1948.[14] ICCPR (1966) provides a binding treaty for the values contained in the UDHR. According to ICCPR, human rights can be only fully enjoyed in conditions, where everyone can enjoy civil and political rights, but also economic, social and cultural rights. ICCPR obliges the states to promote respect for human rights and freedoms and but also recognizes the duties of an individual towards other individuals and the community where he belongs. ICCPR entered into force in 1966 and covers a broad collection of rights addressing a wide range of issues including the right to self-determination, the right to life, the right to liberty and freedom of movement, the right to equality before the law, the right to privacy, the freedom of thought, conscience and religion, the right to participate in public affairs and others.[15] ICESCR is a treaty for human rights related to economic, social and cultural issues and entered into force in 1977. This study concentrates on UDHR and ICCPR. Human dignity plays an important role in the UN human rights

[12] United Nations (d), 2012.
[13] Isa & Feyter, 2006, p. 140.
[14] United Nations (c), 2012.
[15] OHCHR, 1966.

system as an underlying value. According to the Article 1 of the UDHR "All human beings are born free and equal in dignity and rights".[16] Human dignity with equal and inalienable rights is also mentioned in the preamble of the ICCPR as the foundation of freedom, justice and peace in the world. The preamble points out, that these rights are deriving from the inherent dignity of the human person.[17]

The Council of Europe was founded in 1949 to create a European community with a close union for conflict prevention. Today CoE has 47 member states. With the exception of defence, CoE covers all other European main policy areas. The decision-making of the CoE is performed by Committee of Ministers and a consultative Parliamentary Assembly. CoE aims for a greater unity between its members, to safeguard and realize their common ideas and principles and to facilitate the economic and social progress of the member states. The members of the CoE are expected to apply democracy and human rights in practise and work in co-operation with representatives of the populations, such as non-governmental organisations.[18] The organisation also aims to solve issues of terrorism and cybercrime and facilitate co-operation between the member states in these issues.[19]

CoE is the creator of the ECHR, formally known as the “Convention for the protection of human rights and fundamental freedoms”. This convention entered into force in 1953. ECHR obliges all the member states of CoE to accept principles of the rule of law and allow the enjoyment of human rights and fundamental freedoms contained in the convention in their jurisdiction. ECHR is clearly linked with the UDHR and has fourteen protocols. ECHR also establishes the European Court of Human Rights (ECtHR) for examining the violations of the convention.[20] ICCPR and ECHR impose binding legal obligations to the states (so called hard law). Other sources of human rights law with status of hard law are the cases of international courts, such as the ECtHR. Human rights declarations are not binding for the states, but provide sources of

[16] United Nations, 1948.
[17] OHCHR, 1966.
[18] The Danish Institute for Human Rights, 2012.
[19] Council of Europe (e), 2012.
[20] Isa & Feyter, 2006, pp. 359-362.

rights and their application (so called soft law). Other human rights soft law sources are for example general comments and decisions about the covenants from the Human Rights Committee.[21]

The right to freedom of expression was first declared in Article 19 of the UDHR along with other human rights. UDHR is not a legally binding document, but it has led to the creation of several other human rights instruments.[22] According to article 19 of UDHR:

"*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*"[23]

Main elements of the right to freedom of expression are freedom of opinion, freedom of the media, including publication of views, collecting and disseminating information, freedom of communication at the national and international levels, including through electronic media. The main international guarantees of the right to freedom of expression are enshrined in the UN and CoE human rights treaties. There are also other important regional human rights conventions, such as those of Organisation of American States (OAS) and the African Union (AU), but these will not be further discussed in this study. Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) and Article 10(1) of the European Convention of Human Rights (ECHR) provide freedom of expression to everyone including legal persons. [24]

Article 19(2) of the ICCPR states:

"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

[21] OSCE ODIHR (a), 2007, pp. 34-35.
[22] Idem, pp. 43-44.
[23] United Nations, 1948.
[24] OSCE ODIHR (a), 2007, pp. 218-220.

Article 10(1) of the ECHR phrases the right to freedom of expression in a following way:

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises."

Some protected forms of expression have a direct relationship with democratic values and not all forms of speech are protected to the same degree. Political and public interest expression enjoys the highest level of protected speech, because it helps to protect democratic values and includes issues of public interest. Freedom of the press is closely tied to political expression. Other categories of protected speech are moral and religious expression, artistic and cultural expression, commercial expression and "valueless" or offensive expression. Out of these categories valueless expression has the least protection.[25] According to European Court of Human Rights (ECtHR), political expression includes not only party political issues, but also expression about matters of public interest, such as criticism of the government and politicians.[26] Some forms of speech, such as hate speech and propaganda may be entirely prohibited even in a democratic society. The possible restrictions for freedom of expression are discussed in more detail below.

2.1.2 Restrictions

The right to freedom of expression can be restricted in some instances, but only according to the rules contained in the international human rights legislation. The restrictions should not however put the right itself in danger.[27] ICCPR and ECHR both contain partially overlapping rules on when and how the restrictions should be done.

[25] OSCE ODIHR (a), 2007, pp. 218-221.
[26] European Court of Human Rights, 1992.
[27] Office of the High Commissioner for Human Rights (a), 1983.

According to the ICCPR, restrictions on the right to freedom of expression are possible under certain circumstances, such as in a state of emergency.[28] In these situations the state parties can derogate temporarily of some of their obligations.[29] There are several conditions though. The restrictions have to be consistent with the state's obligations under international law.[30] They should be provided by law and be necessary "for respect of the rights or reputation of others" or for the protection of national security, public order or public health and morals.[31] The restrictions should be removed as soon as the situation allows it. If the rights are being restricted because of a state of emergency, the state has to officially announce it to ensure the principles of legality and the rule of law.[32] Even in other circumstances, the states are obliged to notify internationally about restrictions.[33] The state of emergency and use of emergency powers have to follow constitutional law and other provisions and the derogations have to be proportionate to the requirements of situation.[34] Effective remedy and the right to a fair trial should be guaranteed in all situations. [35] Possible violations of the covenant should be investigated promptly, thoroughly and effectively in an independent and impartial way.[36]

ECHR article 10 allows restrictions, which are prescribed by law, necessary in a democratic society for protecting national security, territorial integrity, public safety, reputation or rights of others or for prevention of disorder or crime, disclosing information received in confidence or for maintaining judiciary's authority and impartiality.[37] Consequently, the European Court of Human Rights (ECtHR) has set a three-part test to help assessing the justification of content-based restrictions to the right of freedom of expression. The three parts are lawfulness, i.e. restrictions must be prescribed by law and necessary in a democratic society. Restrictions have to also

[28] OHCHR, 1966.
[29] United Nations (a), 2001, pp. 2-3.
[30] Idem, p. 4.
[31] OHCHR, 1966.
[32] United Nations (a), 2001, pp. 2-3.
[33] Idem, p.6.
[34] Idem, pp. 2-3.
[35] Idem, p.6.
[36] United Nations (b), 2004, p. 6.
[37] Council of Europe, 2010, pp. 11-12.

respond to a pressing social need and be proportionate to the legitimate aim. If these requirements are not met, the rights of users may be violated.[38]

Counter-terrorism related restrictions to the right to freedom of expression are especially relevant for the purposes of this study. Article 5 of ICCPR and Article 17 of ECHR are meant to prevent undemocratic groups, such as terrorist organisations from exploiting the human rights for example by promoting racial hatred. These articles contain the prohibition of activities aimed at the destruction of rights of others.[39] The restrictions are possible for example in cases where violence, armed resistance or insurrection is encouraged.[40] All forms of propaganda and any advocacy of national, racial or religious hatred constituting incitement to discrimination, hostility or violence are prohibited.[41] UN Convention on the Elimination of all Forms of Racial Discrimination (ICERD) (1965) has a close relationship with the Article 20 of ICCPR prohibiting the advocacy of national, racial or religious hatred constituting incitement to discrimination, hostility or violence.[42] Incitement to discrimination or violence through the Internet should be responded with strict measures.[43]

Counter-terrorism itself without specific and legitimate goals shouldn't be used as a justification for restrictions on free speech. Political expression is especially important for democratic societies and should only exceptionally, if ever be restricted in the context of counter-terrorism. Limited political expression may lead to degrading level of democracy.[44] ECHR has a set of principles for understanding better the restrictions of the right to freedom of expression in counter- terrorism issues. According to these principles, the media can only be restricted according to the principles of the right to freedom of expression. [45] The media should be allowed to impart information and ideas

[38] Akdeniz, 2010, p. 13.
[39] OSCE ODIHR (a), 2007, pp. 226-227.
[40] Idem, p. 223.
[41] Office of the High Commissioner for Human Rights (b), 1983.
[42] OSCE ODIHR (a), 2007, pp. 226-228.
[43] Office of the High Commissioner for Human Rights, 2002.
[44] Council of Europe Committee of Ministers, 2005.
[45] European Court of Human Rights, 1976.

to the public and to analyze and provide opinions even on difficult political issues.[46] The right to freedom of expression protects even ideas and information that may "offend, shock or disturb the state or any section of the population."[47]

2.1.3 The international protection of human rights

Several mechanisms have been established for ensuring that the states comply with their obligations regarding the right to freedom of expression and other human rights under the international law. These include monitoring, reporting and complaint mechanisms by the UN and the ECtHR.

The UN Office of the High Commissioner for Human Rights (OHCHR) is the main responsible for UN human rights activities and his mandate includes the promotion and protection of human rights, making recommendations to the UN bodies, promoting and protecting the right to development, providing technical assistance for human rights, coordinating human rights education and public programmes, removing obstacles of human rights and preventing human rights violations, dialogue with governments, enhancing international co-operation and rationalizing, adapting, strengthening and streamlining the UN human rights machinery.[48]

The UN Human Rights Committee is a treaty monitoring body, established by Article 28 of the ICCPR in 1977. The Committee consists of 18 independent experts, who monitor the state compliance with their obligations under the ICCPR. ICCPR sets a mandatory monitoring procedure, where the states send reports to the Human Rights Committee for examination. ICCPR obliges the states parties to send the first report within a year after the Covenant enters into force and the following reports when the committee requests them. The reporting procedure forces governments to investigate if the covenants rights and obligations are actually implemented in their domestic system and provides limited functions of assistance and control. The reports are examined in a public session with a chance for constructive dialogue with the governments. Individual

[46] OSCE ODIHR (a), 2007, p. 222.
[47] European Court of Human Rights, 1976.
[48] Isa & Feyter, 2006, p. 336.

rapporteurs, working groups of the Human Rights Committee and international and local Non-Governmental Organisations (NGOs) all contribute to the examination of the reports. The members of the committee send also personal statements of the human rights situation in the state. At the end the Committee as a whole provides concluding comments to the report including positive issues and challenges in the application of the ICCPR. These comments have detailed suggestions and recommendations. The decisions of the Human Rights Committee based on state reports are not legally binding or politically enforceable. The Committee also produces general comments for all state parties regarding the substantive and procedural provisions of the ICCPR. The Human Rights Committee has usually three open sessions per year and it works in co-operation with non-governmental organizations.[49]

The UN Human Rights Committee has also a system for individuals to complain about the human rights violations by the states. In theory this system is applicable also on complaints between the states. The complaints sent to the Committee have to fill admissibility requirements. For example groups, NGOs or other entities are not allowed to send complaints to the committee, the complaints can't be anonymous, abusive or incompatible with the Covenant. All the domestic remedies have to be also exhausted before a complaint can be sent. If the case is found admissible it is sent to the government concerned for its comments. Even though the decisions of the Committee are not legally binding and there are no sanctions, the Committee requests governments to provide victims an appropriate remedy for the found violations, such as compensation or preventing similar violations occurring in the future. A Special Rapporteur follows up, how the states are complying with the views of the committee.[50]

The UN Human Rights Council (2006) is responsible for global strengthening, promotion and protection of human rights. It also addresses violations of human rights and makes recommendations on them. The Council consists of 47 UN member states elected by the General Assembly. It has the Universal Periodic Review (UPR) mechanism to help in the assessment of member states' human rights situation and

[49] Isa & Feyter, 2006, pp. 147-150.
[50] Idem, pp. 151-153.

Advisory Committee and a complaint procedure for individuals and organisations. The Council works in co-operation with UN Special Procedures.[51] The UPR helps in reviewing the human rights records of the UN member states once in every four years and aims to improve the human rights situations in all countries. In this reporting mechanism the states declare their domestic actions in improving human rights situations and filling their human rights obligations. The UPR is one of the key elements of the Human Rights Council.[52]

The UN Special Procedures are subsidiaries of UN Human Rights Council and have the capacity of fact-finding by collecting and analyzing information regarding possible human rights violations. These subsidiary bodies may be Special Rapporteurs, envoys, experts, working groups, committees etc. and should be independent, impartial and objective. In situations with possible serious human rights violations these actors play a role of early warning system. The Special Procedures are divided into geographic and thematic instruments. Geographic instruments examine the human rights situation in a certain country and thematic issues examine human rights categories, such as torture or education on a global scale. There is also an additional mechanism of information and fact-finding by the High Commissioner for Human Rights.[53]

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has a mandate to gather information on violations of the right to freedom of opinion and expression. He also finds credible and reliable information from different actors, makes recommendations and suggestions for better protection of the right to freedom of opinion and expression, promotes and protects the right to freedom of opinion and expression by providing technical assistance or advisory services to the OHCHR. The Special Rapporteur sends urgent appeals and letters about alleged violations to member states and reports about this correspondence with the state

[51] Office of the High Commissioner for Human Rights (a), 2012.
[52] Office of the High Commissioner for Human Rights (b), 2012.
[53] Isa & Feyter, 2006, pp. 286-290.

annually to the Human Rights Council. He also makes country visits for fact-finding and reports to Human Rights Council and the General Assembly.[54]

European Court of Human Rights (ECtHR) is the most important mechanism for protecting the rights contained in the European Convention of Human Rights. It is a permanent court made of independent judges equalling the amount of CoE membership states. Claims for violations of the rights contained in the ECHR can be made by member states against other member states or by any person, NGO or group of individuals against a member state. Like in the case of the UN Human Rights Committee, the cases of alleged violations have to fill admissibility criteria, such as being compatible with the convention, filling time limits for sending the application, exhausting domestic remedies etc.[55] After a case has been found admissible, the ECtHR decides if there has been a violation of human rights contained in the convention. Contrary to the UN Human Rights Committee, the judgements of the ECtHR are binding for the states, and the Court or the state concerned may award compensation for the violations. However, the Court can't enforce its judgements. ECtHR also interprets the ECHR.[56]

2.2 The Internet

The Internet is an essential part of functional communications for every modern society. It came to the knowledge of wider audiences in 1990s, but existed already decades before this. The first recorded ideas of social interactions through computer networking were created in 1962. During the same year these ideas were transformed to be a part of a computer research program called DARPA 4 (Defense Advanced Research Projects Agency). This programme aimed to find solutions for the purposes of Cold War communication systems. The first ever computer network between two computers was built in 1965 and in 1967 the concept of ARPANET (Advanced Research Projects Agency Network) was published. By 1969 ARPANET had four host computers connected and the gradual development towards to what is known today as the Internet

[54] United Nations Human Rights Office of the High Commissioner for Human Rights, 2012.
[55] Isa & Feyter, 2006, p. 373.
[56] Idem, pp. 379-380.

had started.[57] Today the Internet is a worldwide system of interconnected academic, domestic, government and other networks providing various services available for several technical platforms. The World Wide Web (WWW) is often mistaken with the Internet, but is actually a service operating over the Internet. WWW provides the users an easy and instant access to online information.[58] The different services of the Internet have almost 2.3 billion users globally, with the biggest share of users coming from Asia, Europe and North America.[59] In the 27 EU member states alone there are nearly 360 million Internet users.[60] Even though the Internet has been allowed to develop rather freely until the recent years, there has been an element of governance during most of its existence. First initiative for governing the development of the Internet emerged in 1979 and today governments and international organisations are increasingly interested in Internet governance.[61]

Internet media enjoys the same level of protection under the international law as traditional media.[62] UN and other international organisations have recognized the value and importance of the Internet to right to free expression and in some states the access to the Internet is already a human right of the citizens.[63] Internet facilitates global exchange of ideas, free flow of information and supplements the traditional media.[64] User’s freedom to seek, receive and impart information in the Internet can have a positive contribution against racism, racial discrimination, xenophobia and related intolerance. New technologies can be used for promoting tolerance, respect for human dignity and the principles of equality and non-discrimination.[65] According to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression the Internet is a very powerful instrument for increasing transparency, access to information and citizen participation in building democratic societies. Internet

[57] Internet Society, 2012.
[58] OSCE, 2007, pp. 29-31.
[59] Internet World Stats (a), 2011.
[60] Internet World Stats (b), 2011.
[61] OSCE, 2007, p. 44.
[62] OSCE ODIHR (a), 2007, pp. 230-232.
[63] Akdeniz, 2010, pp. 9-10.
[64] OSCE (b), 2012, p. 1.
[65] United Nations (b), 2001, p. 22.

played a key role for mobilizing people to rally for human rights during the Arab Spring demonstrations in countries of Middle East and North Africa in 2011.[66] The protests in Tunisia and Egypt were started by opposition Facebook campaign and social media networks helped in organizing and disseminating information about them, including publishing the protester's demands internationally. The governments of Tunisia and Egypt tried to block these actions, but the measures taken were not completely successful.[67] However, not all the manifestations of right to freedom of expression on the Internet are positive and this right can also be exploited by different activist groups.

2.3 Hacktivism

Hacktivism has it's origins in the hacker culture so it's proper to provide a short overview on hacking. Hackers are computer enthusiastic individuals, who have existed from the very first moments of the Internet. The current Internet culture originally emerged from the hacker culture. Already in the early stage of information networks the technical characteristics of the Internet shaped the hacker culture and developed a "hacker ethic". This ethic stresses the importance of free information, mistrust to authority, decentralization, judging hackers by their skills, the creative force of computers and the power of computer to change lives for better. Gradually illegal hacking (cracking) also emerged. Today these terms are often used synonymously even though originally hacking didn't involve illegal actions.[68] In the daily language hacking is widely used as a general term covering several acts related for example to computer security, open source software development and software piracy. [69]

Hacktivism was originally presented as a term by the influential elite hacker group Cult of the Dead Cow in 1996.[70] Since then the use of this term has changed. Hacktivism is more narrowly defined term than hacking even though the academic literature still contains several definitions. For example Denning defines hacktivism as a marriage of hacking and activism covering disrupting, but not seriously damaging attacks against

[66] United Nations, 2011, p. 4.
[67] Stepanova, 2011, pp. 1-2.
[68] Samuel, 2004, pp. 41-42.
[69] Idem, pp. 1-3.
[70] Paget, 2010, pp. 10-11.

Internet sites. Jordan & Taylor describe hacktivism as a "combination of grassroots political protest with computer hacking." This study uses the definition of Samuel, which stresses the nonviolent nature of hacktivism:

"*Hacktivism is the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends.*"[71]

2.3.1 Hacktivists and their motivations

Hacker activists performing hacktivism are often called hacktivists. They are individuals or small groups of hackers, who instead of traditional hacker goals are motivated by economic, political or religious interests. Their operations often cross the national borders of states and include international co-operation between separate groups. Some hacktivist groups conducting international attacks from countries such as Russia and China seem to have links with their governments.[72] Currently there is a huge amount of online actors, who define their acts as hacktivism even though their motivations may not fall in to the above mentioned categories.[73] Hacktivists usually have more respect for wellbeing of other users than cyberterrorists and they avoid causing permanent damage. Compared to traditional hackers, hacktivists believe they can achieve more by hacktivism than just by ordinary computer hacking.[74] Some even regard hacktivism as a form of civil disobedience.[75]

Based on their background and technical skills hacktivists can be divided to more technically oriented or more artistically oriented groups. Because of their different views, these groups often disagree on the best methods and aims of hacktivism.[76] Both groups however agree about using humour to make their point.[77] The acts of hactivism can be divided into three types based on the background of hacktivists and their aims.

[71] Samuel, 2004, pp. 1-3.
[72] Paget, 2010, pp. 10-11.
[73] Almeida & Mutina, 2011.
[74] Samuel, 2004, pp. 3-4.
[75] Himma, 2005, p. 2.
[76] Samuel, 2004, p. 39.
[77] Idem, p. 7.

These types are political cracking, performative hacktivism and political coding.[78] Acts of political cracking are clearly illegal and performed by hacker-programmers. Majority of hacktivist acts fall into this category, which covers a wide range of issues and tactics. Political crackers work alone or in small groups. Because of the illegal nature of their acts, they prefer to remain anonymous or use pseudonyms.[79] Hacktivists with artist-activist backgrounds conduct legally ambiguous performative hacktivism. They see hacktivism as performance and political protest as a "speech act". Many performative hacktivists see hacktivism as a form of political art and some of them may produce other forms of Internet art. Performative hacktivism usually focuses on globalization, corporate power, human rights or similar issues and is more theory-driven than other forms of hacktivism. The acts are usually done by transnational coalition.[80] Political crackers and performative hacktivists are aiming mostly towards policy change.[81] In political coding hackers use their skills for transgressive politics. They are often operating under easily traceable pseudonyms. The ideology of political coders regards individual rights, especially those relevant to the online world as the most important political value, because they are directly related to the hacker community. Internet censorship preventing democracy activists in authoritarian regimes has been often the target of political coding and there have been software projects to help counter this censorship. The aim of political coding is often policy circumvention rather than policy change. The goal is not to change the law, but to make it unenforceable and meaningless. For example a hacktivist software project called "Hactivismo" aimed to evade Chinese government Internet censorship rather than to change the government policy.[82]

Traditional hackers believe non-violent intrusions to computer networks being morally permissible for increasing knowledge about Internet security technologies or for removing morally illegitimate barriers of information. These views are typically contested by the public, who doesn't understand or accept the hacker motives.

[78] Samuel, 2004, p. 48.
[79] Idem, 51-54.
[80] Idem, 71-73.
[81] Idem, pp. 231-232.
[82] Idem, 85-87.

Hacktivism is more acceptable justification for hacking as a form of political activism and civil disobedience to protest against laws.[83] Hactivists have many additional reasons for choosing hacktivism over the traditional activism. Mainstream media may exclude part of the political activists, but with hacktivism they have a new way of getting heard and getting their message through.[84] Unlike most political actions, that require a mass of people, hacktivism can be performed even by a single actor using efficient tools. Hacktivist acts are very cheap to perform, and since hacktivists can operate anonymously and expeditiously compared to states, the risk of getting caught is low. Hacktivists are mostly pursuing circumvention of government policies, which is easier and faster to achieve than actually changing the policies. Hacktivists can also maintain the controversial concept of online anonymity in their public political actions even though the value of this anonymity is often questioned.[85]

2.3.2 The acts of hacktivism

Hacktivist acts aim to draw media and public attention by disrupting normal network operations.[86] Samuel divides the actual manifestations of hacktivism into nine groups. These are:

1. Site defacements
2. Site redirects
3. Denial of Service (DoS) attacks
4. Information theft
5. Information theft and distribution
6. Web site parodies
7. Virtual sit-ins
8. Virtual sabotage and
9. Software development. [87]

[83] Himma, 2005, p. 1.
[84] Dahlberg & Siapera, 2007, p. 20.
[85] Samuel, 2004, p. 17.
[86] Denning, 2001, p. 264.
[87] Samuel, 2004, p. 7.

In **site defacement** hacktivists intrude the website server and make changes to the code. This can result to a message with criticism against the organization or about a current hot topic to be displayed to users accessing the website. Usually the target websites are private sites, but sometimes hacktivists manage to deface websites of embassies or other governmental authorities.[88] In **site redirect** hacktivist also intrude the server and change the settings to redirect visitors to another website, which may contain criticism about the original website. **DoS attack** is somewhat more complex and currently popular activity. The aim of DoS attacks is to significantly slow or close down the web services of companies, organisations or different Internet gateways by creating automated overload of traffic against the targeted sites. Currently hacktivists can close down even biggest websites by exploiting virus-infected “slave” computers around the world to create the traffic for the DoS attack. These networks of infected computers are often called “botnets”.[89] DoS attacks today are usually called Distributed Denial of Service (DDoS) attacks. For example “Mariposa” network for DDoS attack consisted of 12.7 million virus-infected machines.[90] Another example of DDoS attacks is the protest made by the loose group of hackers/hactivists called Anonymous. This attack targeted the international financial companies boycotting the whistleblower website Wikileaks. The DDoS attack against MasterCard, Visa, Amazon.com and others was performed with an automated and easy to use DDoS tool available both as a desktop application and as a web page. In this attack the participants could be easily traced, since the tool didn’t protect their identity.[91] Even though Samuel sees DoS attacks as a form of hacktivism, the potential destructive power of these attacks may cause many states and international organisations to classify DoS attacks as cyberterrorism. In **information theft** hacktivists hack into networks to steal information. Often they aim to demonstrate the public how poorly the information is protected.[92] Sometimes the information theft affects a great amount of people, such as the information theft of more than 70 million user’s personal information from Sony PlayStation network in 2011. Also in this case the hacker group

[88] Samuel, 2004, pp. 8-9.
[89] Idem, p. 10.
[90] European Commission, 2011, pp. 3-4.
[91] Pras, Sperotto, Giovane, Drago, Barbosa, Sadre, Schmidt & Hofstede, 2010, p. 2.
[92] Samuel, 2004, p. 11.

Anonymous was said to be behind the theft, but it never claimed the responsibility. The stolen information was not used for other purposes.[93] In **information theft and distribution** the stolen information is also published online for raising awareness of the claimed political issues, creating discussion about the poor information security or for other reasons. In **site parodies** hacktivists create a parody website, which has similar web address and outlook as the original website. The aim is to criticise the original website.[94] For example www.gatt.org contains a critical site parody of the World Trade Organization (WTO) www.wto.org website providing headlines such as "WTO Announces Formalized Slavery Market for Africa".[95] **Virtual sit-ins** consist of hundreds or thousands of hacktivists, who simultaneously access a website on their Internet browser and constantly manually reload the webpage to slow down or crash the site. Virtual sit-ins today are largely ineffective and overtaken by automated tools and will not be further discussed in this study. Acts of **virtual sabotage** are conducted to manipulate or damage the information technologies of the target. These include creating viruses or computer worms for distributing messages or sabotage. The functionality of viruses and worms varies on a wide range from simple spreading between computers to destroying data.[96] Samuel regards also **software development** as a form of hacktivism when it serves political purposes such as helping people to counter government-imposed censorship. This has happened for example with the open source tools for countering the Chinese national Internet censorship firewall.[97]

Some authorities and states have started to regard hacktivism as a moderate form of cyberterrorism because it's easy, effective and has anonymous methods. Mass media is also often stressing the links between hacktivism and cyberterrorism, a tendency that entered media coverage after 11th of September 2001 New York terrorist attacks.[98] Partly because of similar methods of action also academia tends to classify hacktivism

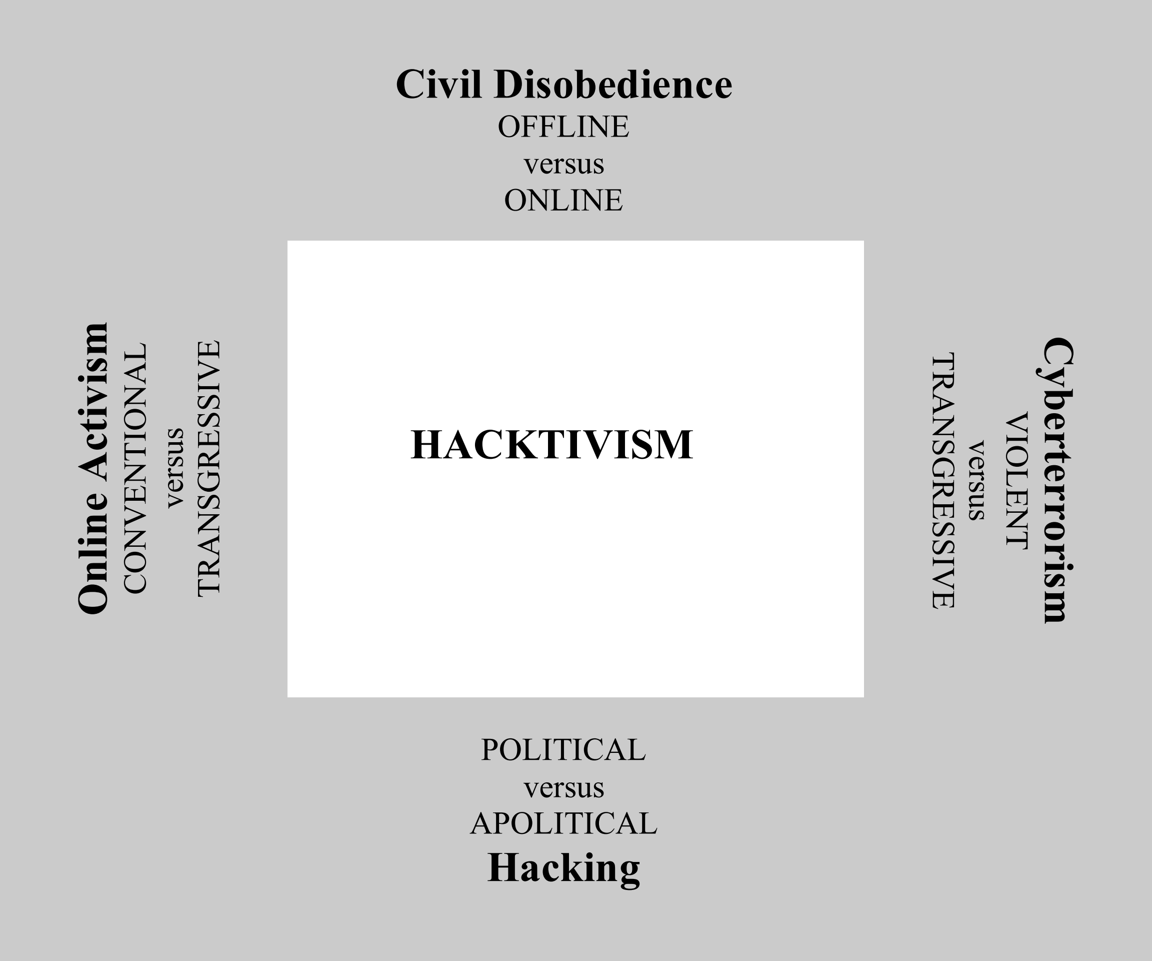
[93] Thomas, 2011.
[94] Samuel, 2004, p. 13.
[95] World Trade Organization parody website, 2012.
[96] Samuel, 2004, p. 11.
[97] Idem, pp. 13-14.
[98] Idem, p. 246-247.

as a moderate form of cyberterrorism.[99] The attitude change towards a more negative way of seeing hacktivism is caused also by hacktivists themselves. Hacktivism restrict other citizens' right to freedom of expression in many ways, such as making them unable to display their message online or access information.[100] The motives of part of the hacktivists can be questioned, as they may not be the more widely accepted economic, political or religious motives. Statistics of a service dedicated to recording website defacements shows, that in 2010 hacktivists themselves reported almost 1.5 million websites defaced. The main motivation reported for the acts was "just for fun" (829 975 cases) or "wanting to be the best defacer" (289 630 cases). Political reasons (57 083 cases) were much lower at the defacement motivation list.[101] In most of these cases the hacktivists are not performing civil disobedience by protesting or calling attention to the injustice of a law or government policy, but they are simply breaking the law.[102]

Another contested feature of hacktivists is the anonymity of the actors. In public life anonymity is on the other hand seen as a necessary and valuable part of political life and free speech encouraging the free flow of ideas by enabling people making unpopular statements. With anonymity the focus is on the speech rather than the speaker. On the other hand anonymity is considered to be threatening to democracy and public life since the accountability that encourages responsible behaviour is missing. Anonymity allows people to avoid the consequences of their actions. Hacktivists perform their acts either anonymously, with traceable nicknames and sometimes even with their real names. Political crackers perform harmful acts and may want to stay anonymous to avoid legal consequences. However, they also use anonymity to express unpopular, but not illegal opinions. Political coders use often pseudonyms, which can somehow be linked to their true identity. Performative hackers are generally known by their real names.[103] FIGURE 1 below shows the relationships between hactivism, conventional online activism, civil disobedience, cyberterrorism and hacking.

[99] Samuel, 2004, p. 26.
[100] Idem, pp. 205-206.
[101] Almeida & Mutina, 2011.
[102] Himma, 2005, p. 3.
[103] Samuel, 2004, pp. 214-217.

FIGURE 1. The relation of hacktivism to online activism, civil disobedience, cyberterrorism and hacking.



Hacktivism shares elements with civil disobedience, but contrary to civil disobedience takes places completely in the online world. Hacktivism and cyberterrorism both take place online, but in contrast to cyberterrorism, hacktivism is non-violent. While goals of conventional hacking are typically apolitical, the aims of hacktivism have a political nature. While online activism is the legal manifestation of conventional activism in the Internet, hacktivism is mostly illegal and employs unconventional methods.[104]

[104] Samuel, 2004, p. 4.

2.4 Cyberterrorism

Despite of several attempts by the United Nations and others there is still no universally accepted definition of terrorism. Cyberterrorism (sometimes also spelled cyber-terrorism or cyber terrorism) is a specific form of terrorism, so an attempt to characterize terrorism before defining cyberterrorism is provided first.

2.4.1 The challenges of defining terrorism

Terrorism has existed in different forms, such as assassinations throughout the written history. During the 20th century the waves of anti-colonial, "new-left" and religious terrorism have caused terror in the populations of the world. Much of the post-Second World War terrorism has been connected with marginalized ethnic and religious groups aiming for independence in artificial nation-states created during the colonial time. Another common motive has been a struggle against illiberal constitutions or despotic rulers. Much of the modern terrorism still derives from the same issues. Even though the Western world has it own endogenous terrorist groups, the Islamist religious terrorism has dominated the Western media through the recent years.[105] According to a report by EUROPOL (European Police Office), in 2010 the member states of the EU alone faced 249 terrorist attacks, arrested 611 individuals and tried 307 individuals for terrorist related offences. During this period there were also 46 terrorist threat statements against the EU. On the global scale the figures are much bigger.[106]

In everyday language terrorism is used to describe a wide range of activities, but a more accurate definition should be provided by domestic and international law for effective responses. Terrorism acts are criminal acts and under criminal law.[107] If the definition contained in legislation is too vague and broad, the safeguards for ordinary persons are under a threat and risk of human rights violations increases.[108] The first international attempt to define terrorism was included in the Geneva Convention for the Prevention and Punishment of Genocide (1937). This definition was criticized for lacking precision

[105] Shughart, 2006, p. 14.
[106] EUROPOL, 2011, p. 9.
[107] OSCE ODIHR (a), 2007, p. 23.
[108] Idem, p. 25.

and the convention never got enough ratification to become effective.[109] Also the member states of the UN have been unable to agree on the definition of terrorism on later attempts. The definition of terrorism was for example dropped from the draft statute of International Criminal Court. This decreases in many ways the strength of UN terrorism related actions. Usually agreeing on the definition for terrorism faces two unsolved issues. State use of armed forces is seen as something that should be included in the definition. Another issue is that the definition of terrorism should not exclude the right to resistance by peoples under foreign occupation. Several UN member states are not willing to agree on these issues for different reasons. According to a UN high-level panel report, the future definition of terrorism should include description of terrorism as:

"*Any action, in addition to actions already specified by the existing conventions on aspects of terrorism, the Geneva Conventions and Security Council resolution 1566 (2004), that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act*".[110]

The European Union Counter-Terrorism Strategy (2005) avoids giving a direct definition of terrorism. It describes terrorism as:

"... a threat to all States and to all peoples. It poses a serious threat to our security, to the values of our democratic societies and to the rights and freedoms of our citizens, especially through the indiscriminate targeting of innocent people. Terrorism is criminal and unjustifiable under any circumstances."[111]

As there is no universal consensus on terrorism and this study focuses on OSCE participating states, the terrorism definition provided by OSCE Office for Democratic

[109] OSCE ODIHR (a), 2007, p. 23.
[110] United Nations (a), 2004, pp. 51-52.
[111] Council of the European Union, 2005, p. 6.

Institutions and Human Rights (ODIHR) will be used in this study. ODIHR defines terrorism briefly as:

"*Organized and dangerous criminal activity, which attempts to undermine government and spread fear randomly*." [112]

Cyberterrorism is increasingly used, specific form of terrorism. The term "cyberterrorism" was developed during 1980s to refer to the convergence of terrorism and cyberspace, where the communication over computer networks happens.[113] Like in the case of conventional terrorism, there is no universally accepted definition for cyberterrorism. However, some papers and authors are widely cited, such as the testimony of Dorothy E. Denning before the U.S. Special Oversight Panel on Terrorism in 2000. According to this testimony, cyberterrorism covers unlawful attacks and threats against computers, networks and information stored in them with a purpose to prevent government and people from reaching political or social objectives. Cyberterrorism attacks can include serious attacks against critical infrastructures, explosions, plane crashes or serious economic loss. The result of these attacks is violence against people or property and creation of fear. According to this testimony, disrupting nonessential services does not count as cyberterrorism.[114] Denning's description of cyberterrorism covers several aspects, but is too inconclusive for this study. Instead the more concise definition of cyberterrorism provided by the United States Federal Bureau of Investigation (FBI) will be used:

"*Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents."*[115]

[112] OSCE ODIHR (a), 2007, p. 23.
[113] Denning, 2001, p. 281.
[114] Denning, 2000.
[115] Denning, 2001, p. 281.

2.4.2 Cyberterrorists and their motivations

Cyberterrorism is performed by actors who are either part of larger terrorist groups, such as the well known Al Qaeda or by solo actors.[116] They may come from several different backgrounds, but typically the motives of cyberterrorists are political, religious or ideological such as motives of militant Islamist groups.[117] There are several reasons for terrorists to choose to use the Internet for their activities, which partially overlap with the motivations of hacktivists. Cyberterrorism is anonymous, cheap, lacks physical danger and has wide media coverage.[118] Communication through the Internet is efficient and secure making it easier to avoid surveillance of the authorities with encrypted communication tools or software to divert the origins of communications.[119] Thanks to the decentralized nature of the Internet, it's also difficult to respond efficiently to cyberterrorism. While the states and large international organisations are usually centralized and slower in their actions, cyberterrorists may benefit from rapidly changing methods, tools, locations and targets.[120] In contrast with conventional acts of terrorism, modern Western societies with high level of networked infrastructures are most vulnerable to the effects of cyberattacks.[121]

2.4.3 The acts of cyberterrorism

According to OSCE ODIHR classification, cyberterrorists see the Internet in a multiple role as a target, a planning and organizing tool or a statement and propaganda medium. These general levels have sub-categories, which are listed below:

1. Digital property as target. Using cyber, physical and electronic attacks against computer networks.

2. Information Technology (IT) as a support means in terrorist operations. These include communication, planning, preparing and organizing terrorist attacks, using cryptography, intelligence collection and financial support.

[116] Theohary & Rollins, 2011, p. 2.
[117] Paget, 2010, p. 12.
[118] Denning, 2001, p. 281.
[119] OSCE, 2008, pp. 2-3.
[120] Theohary & Rollins, 2011, p. 2.
[121] OSCE, 2008, pp. 2-3.

3. Cyberspace as a channel for spreading terrorist messages. Terrorist propaganda and terrorist statements, which cause fear and publicize hate speech.

When cyberterrorists see a computer network such as the **Internet as a target**, they perform attacks to disrupt, deny, degrade or destroy information with unauthorized access, malicious code and similar activities targeting the data stream.[122] Unauthorized access can be performed for example with hacked or stolen credentials. Once the cyberterrorists infiltrate a computer network, they can perform a wide range of functions, such as deleting or stealing vital information. An example of malicious code was a sophisticated computer worm called "Stuxnet", which in 2010 managed to infect nuclear power plants in Iran. Stuxnet aimed to destroy information in industrial control systems and was able to hide from detection. The worm was also detected in other countries including Belarus, Indonesia, India, Pakistan, Germany, China and the United States. [123] Stuxnet was the first piece of malicious software targeted against industrial control system. Its code is today publicly available online as a base for knowledgeable cyberterrorists to develop new worms.[124] Possible network targets for similar cyberterrorist attacks in the future could be air control, oil industry controls or international financial transaction systems.[125] An attack against financial systems, widely reported by the media could cause unrest in the public and lead to economical damage.[126] Another option for cyberterrorists to cause slowing of operations and crashing of systems is to use DDoS attacks in a similar way as the hacktivists use them. They may even use the same publicly available tools. Cyberterrorists can also use physical attacks (such as conventional weapons) and electronic attacks (such as electromagnetic pulses) against Internet infrastructure and information, but these are outside the scope of this study and will not be further discussed.

When the **Internet is used as support means** in terrorist operations, the terrorists use it for communication (often with cryptography), intelligence collection through

[122] OSCE ODIHR (b), 2007, pp. 3-5.
[123] Kerr, Rollins & Theohary, 2010, p. 1.
[124] Theohary & Rollins, 2011, pp. 5-6.
[125] Denning, 2001, p. 282.
[126] Theohary & Rollins, 2011, pp. 5-6.

unauthorized access for planning and organizing terrorist attacks and as a financial support tool.[127] With the easy availability of free encrypted email services such as Hushmail, cyberterrorists can use the Internet as an effective and secure encrypted communication method. Even though they may be able to infiltrate computer systems to collect intelligence for organizing and planning terrorist attacks, this is often not needed thanks to the possibilities of the Internet for open source intelligence. Many useful planning services are public and free, such as Google Maps or Google Earth for mapping the possible targets for terrorist attacks with satellite images. Personal websites and profiles on social media offer information about personnel and hierarchical structure of organisations. Cyberterrorists may use the Internet as a financial support tool by campaign online and then use the same secure international financial transaction services as normal users. Another option is to gather funds with different kinds of Internet frauds.

Cyberterrorists often use the Internet for spreading **terrorist propaganda and statements**. This kind of material is widely and easily available online. It includes titles, such as Anarchist's Cookbook, Encyclopaedia of the Afghan Jihad, The Al-Qaeda Manual, The Mujahideen Poisons Handbook and The Terrorists Handbook.[128] This propaganda material can be distributed through websites, social media, blogs and discussion forums. In 2011 there were estimated 14 000 hate and terrorism related websites, social network pages, chat forums and micro blogs. The number of these sites is growing every year.[129] Cyberterrorist are also able to exploit social media combined with the official websites of terrorist organisations as a recruitment tool for potential new members. Images of successful terrorist attacks and lists of celebrated martyrs can be easily distributed online and ideology and methodology can be discussed in chat rooms.[130] Several terrorist organisations have their official websites, which ironically are falling victims to cyber attacks by hacktivists and different national intelligence

[127] OSCE ODIHR (b), 2007, pp. 3-5.
[128] Akdeniz, 2010, p. 67.
[129] Idem, pp. 49-50.
[130] Theohary & Rollins, 2011, p. 3.

services. For example Afghan Taliban's official website "El Emara" has been brought down repeatedly by hackers.[131]

The lack of universally accepted definition of terrorism is a major challenge for international co-operation in tackling cyberterrorism. However, not only terrorism, but many of the terrorism related concepts, such as "extremism", "terrorist propaganda", "harmful" or "racist content" and "hate speech" are still poorly defined.[132] Another challenge for finding efficient responses against cyberterrorism is the lack of information regarding cyberterrorist attacks, in which the Internet is a target. States and private entities may be reluctant to publicly distribute information about attacks against their vital computer networks. For example Stuxnet computer worm infected industrial control systems in several countries, but there is a lack of information on the damages it caused.[133] At the same time the technical skills of cyberterrorists seem to be growing with hiring or training hackers. The attacks can be timed simultaneously with conventional physical attacks to cause higher level of damages.[134] However, so far the cyberterrorist attacks targeting the actual infrastructure of the Internet seem to have been reasonably few.[135] An open question for the near future is the potential usage of smartphones as a tool of cyberterrorism. While the amount of smartphones is rapidly growing, the potential security leaks allowing new forms of cyberterrorism is also likely to increase.[136]

This chapter presented the theoretical background of human rights and international organisations promoting them, the right to freedom of expression, the background of the Internet and the concepts of hacktivism and cyberterrorism. There are several specific international legal instruments the OSCE participating states are applying in their responses to hacktivism and cyberterrorism. These instruments also have safeguards for

[131] The Guardian, 2012.
[132] Akdeniz, 2010, p. 19.
[133] Kerr, Rollins & Theohary, 2010, p. 1.
[134] Theohary & Rollins, 2011, pp. 5-6.
[135] Denning, 2001, p. 282.
[136] Chu, Deng & Chao, 2010, p. 1.

protecting the right to freedom of expression. Next chapter discusses these instruments in more detail.

3 International conventions

In this chapter the relevant international legal instruments by UN, CoE, EU and the approach of OSCE will be discussed. The main focus is on the right to freedom of expression and counter-terrorism in cyberspace in relation to hacktivism and cyberterrorism.

3.1 The UN Global Counter-Terrorism Strategy and CTITF

The United Nations is dedicated to countering different forms of terrorism. The UN Global Counter-Terrorism Strategy (2006) is important for the co-operation in counter-terrorism, since in the strategy UN member states agreed to a common approach against terrorism for the first time. The strategy was created to combine in one framework the UN counter-terrorism policy and legal responses from the General Assembly, the Security Council and the specialized UN agencies.[137] Along with all the other forms of terrorism, the member states aim to coordinate international and regional level efforts to counter all forms of terrorism on the Internet. Counter-terrorism measures have to respect human rights and comply with the international law.[138] The strategy is based on four pillars. These are:

1. Measures against favourable conditions to the spread of terrorism.
2. Measures for preventing and combating terrorism.
3. Measures for building state capacity for preventing and combating terrorism with strengthening the role of the UN.
4. Measures ensuring the respect of human rights and the rule of law as basis in the fight against terrorism.

This strategy is also on the focus of Counter-Terrorism Implementation Task Force (CTITF). Secretary General established CTITF in 2005 to coordinate the UN system counter-terrorism efforts. CTITF consists of 30 UN system entities and Interpol.[139] CTITF recommends multi-disciplinary counter-terrorism approach, which involves

[137] CTITF, 2011, p. ii.
[138] Idem, p. iv.
[139] Idem, p. ii.

experts in counter-terrorism, technology, law, public policy, law enforcement and human rights.[140] CTITF also aims to improve the cooperation for the strategy implementation between the UN system, international and regional organisations such as OSCE, private sector and civil society.[141]

Also other UN instruments for countering terrorism exists. The Security Council Resolution 1373 (2001) is particularly important for counter-terrorism. It obliges states for more effective national counter-terrorism measures, improved international co-operation and for creating a monitoring Counter-Terrorism Committee (CTC). According to the resolution, all states shall take actions against financing of terrorist attacks. It also requires that the states take law-enforcement steps against terrorism, foster co-operation and provide assistance in the investigations. The resolution calls on all states for participation to relevant international counter-terrorism instruments. The resolution does not try to define terrorism, but leaves this to the member states. It provides a basis for domestic legal action against terrorism. It also aims to influence national law and practice, including legislative measures. CTC is composed of members of the Security Council and reviews the counter-terrorism measures of states. After the adoption of resolution 1373 the states are required to report their compliance with the resolution to CTC.

Other key UN resolutions for countering terrorism are Security Council Resolutions 1269, 1456, 1624 and General Assembly Resolution 58/187. Security Council Resolution 1269 (1999) obliges states to co-operate for prevention and suppression of terrorist attacks and bringing perpetrators to justice. In Security Council Resolution 1456 (2003) states commit to ensure, that their counter-terrorism measures comply with and are adopted according to international law, especially human rights, refugee and humanitarian law. Security Council Resolution 1624 (2005) encourages states to prohibit incitement to terrorism, to prevent terrorist acts and to deny safe haven to perpetrators. It also encourages intercultural dialogue and broader understanding between civilizations. Finally, General Assembly Resolution 58/187 (2004) requires

[140] CTITF, 2011, p. vi.
[141] Idem, p. ii.

that anti-terrorism measures comply with state obligations under international, human rights, refugee and humanitarian law. The UN states should raise awareness about the obligations among their national authorities.[142] The 13 most important UN counter-terrorism conventions and protocols address aviation safety, internationally protected persons, hostage taking, protection of nuclear material, maritime safety, safety of fixed platforms on the continental shelf, plastic explosives, terrorist bombings, financing of terrorism and nuclear terrorism.[143]

3.2 Council of Europe Convention on the Prevention of Terrorism

CoE fights against terrorism by strengthening legal action, safeguarding fundamental values and by addressing the causes of terrorism. Ensuring respect for human rights and rule of law in the fight against terrorism are seen as the most important values.[144] Council of Europe Convention on the Prevention of Terrorism (2005) aims to ensure that:

1. Certain acts such as public provocation, recruitment and training possibly leading to terrorist offences are to be made criminal offences.

2. Co-operation on prevention of terrorism is reinforced both on internal and international level.

Both of these approaches are relevant for this study. The Convention also includes a provision of the protection and compensation to terrorism victims.[145] Punishment of terrorist acts has to be carried out respecting human rights obligations, including the right to freedom of expression. Punishment should also be proportional and exclude arbitrariness and discriminatory or racist treatment.[146]

[142] OSCE ODIHR (a), 2007, pp. 35-36.
[143] Idem, p. 34.
[144] United Nations, 2010, pp. 1-2.
[145] Council of Europe (d), 2012.
[146] OSCE ODIHR (a), 2007, pp. 229-230.

3.3 Council of Europe Convention on Cybercrime

Council of Europe Convention on Cybercrime (2001) entered into force in 2004. It is the first international treaty on crimes committed via the Internet. This convention was created to deal with infringements of copyright, computer-related fraud, child pornography and violations of network security. It aims to protect society against cybercrime by pursuing a common criminal policy, adopting appropriate legislation and strengthening international co-operation. The convention has an additional protocol, which makes publishing racist and xenophobic propaganda through computer networks a criminal offence.[147] The Convention includes computer and content related crimes and offences and principles relating to mutual assistance. The Convention also includes offences on:

1. Intentional illegal access of computer systems
2. Intentional illegal interception of non-public transmissions of computer data
3. Intentional interference with computer data including deletion or alteration
4. Intentional interference with a computer system
5. Misuse of certain devices designed or adapted primarily for the purpose of committing any of the offences
6. The possession of such devices with intent to commit such offences.[148]

CoE Convention on cybercrime has been criticized for helping the countries to adopt invasive online surveillance laws. The treaty fails to limit too broad surveillance powers of law enforcement agencies. The citizens wouldn’t for example be necessarily notified, that they have been under surveillance. The convention is also used to force service providers to store customer information. The convention is further criticized about outdated concepts of sensitive online data and storing personal data in the Internet.[149]

[147] Council of Europe (a), 2012.
[148] Akdeniz, 2008, pp. 5-7.
[149] Rodriguez, 2011.

3.4 European Union Counter-Terrorism Strategy

The development of the European Union started after the Second World War in 1951 when six European countries signed a treaty on coal and steel industries. The co-operation gradually expanded to other areas to create a common market for people, goods and services to move freely across borders.[150] Today the EU consists of 27 European member countries and covers all policy areas including a single market. The functions of the EU are based on treaties agreed by the member countries and the EU has core values of human dignity, freedom, democracy, equality and the rule of law. These values are promoted internally and globally.[151] The EU is committed to response to terrorism in human rights respecting ways. The EU approach to terrorism is based on the European Union Counter-Terrorism Strategy (2005). This holistic strategy aims to combat terrorism globally, while respecting human rights and enabling the citizens an area of freedom, security and justice. The strategy has four strands:

1. Prevent people from turning to terrorism.
2. Protect by reducing vulnerabilities of citizens and infrastructure.
3. Pursue and investigate terrorists, including planning, travel, communications, funding, materials and bringing terrorists to justice.
4. Respond in a coordinated way by minimizing and preparing the management of terrorist attacks consequences.

The European Commission assists the EU states in fulfilling these commitments, but EU states' law enforcement and intelligence authorities perform all operational work. The Commission also co-operates with non-EU partner countries and international organisations on terrorism related issues.[152]

Other relevant initiatives by the EU include the European Union e-commerce directive (2000) and the European Union directive on attacks against information systems (2010). These directives are legislative acts, which require the EU member states to achieve

[150] European Union (b), 2012.
[151] European Union (a), 2012.
[152] European Commission Home Affairs, 2012.

certain results, but don’t dictate how these results should be achieved. The e-commerce directive recognizes the importance of information society without frontiers and promotes Internet access to everyone. The directive also aims to remove legal obstacles of international co-operation in e-commerce. The right to freedom of expression is protected, taking in account the possible restrictions for protection of minors, human dignity, consumer protection and the protection of public health. The directive sets Internet Service Providers an obligation to under certain circumstances prevent or stop illegal activities. This includes the rapid and reliable procedures for removing and disabling access to illegal information. This can be achieved with technical systems of protection and identification. The service providers are not held liable for content, which of they have no knowledge or control over. This can happen for example in cases, where the information is only temporarily saved in the service provider’s systems. The governmental authorities of the EU member states are allowed to require the removal of illegal information or blocking the access to it. Removal of the illegal content has to be done rapidly, but respecting the principle of right to freedom of expression. The directive prevents member states from imposing a general monitoring obligation to the service providers.[153]

The EU directive on attacks against information systems sees vulnerability to attacks and insufficient responses from law enforcement mechanisms against transnational threats the main causes for cybercrime. Often the victims, such as economic operators and companies are reluctant to report about the crimes in fear of losing reputation. Efficient tools for anonymous and dispersed attacks and the lack of prosecution for organized crime are part of the problem. This directive takes in account new methods of cybercrimes, including the so called “botnets” for making DDoS attacks through virus infected and remotely controlled computers.[154] The definition of cybercrime contained in the directive includes illegal access to information systems, illegal systems

[153] Official Journal of the European Communities, 2000.

[154] European Commission, 2010, p. 3.

interference, illegal data interference, illegal interception and the tools used for committing offences.[155]

3.5 Organization for Security and Co-operation in Europe, OSCE

The development of OSCE started in Conference on Security and Co-Operation in Europe (CSCE). In the early 1970s it provided East and West a multilateral forum for negotiation and dialogue. As a result of this conference politico-military, economic, environmental and human rights issues were contained in an agreement called Helsinki Final Act (1975). Until the end of the Cold War in the 1990s the main function of CSCE was meetings and conferences for building and extending its members commitments. At the beginning of post-Cold War period CSCE started to manage the change in Europe and responding to new challenges and the name of the organisation was changed to OSCE.[156] Today OSCE is the world's largest security organisation with 56 participating states from Europe, Central Asia and North America. The organisation aims for peace, democracy and stability in the participating states. OSCE has a forum for high-level political negotiations on security issues and a platform for practical work. The participating states are working in co-operation on issues regarding early warning, conflict prevention, crisis management and post-conflict rehabilitation.

OSCE concentrates with its institutions, experts and field operations on a wide range of security issues. These include arms control, terrorism, good governance, energy security, human trafficking, democratization, media freedom and minority rights. OSCE sees security as a comprehensive concept including politico-military, economic, environmental and human aspects. The comprehensive approach to security is useful for responding cross-dimensional security challenges, including terrorism, organized crime, cybercrime and drugs, arms or human trafficking. Military security is advanced with promoting more openness, transparency and co-operation in issues such as arms control, and politico military security with measures such as defence reform. Economic co-

[155] European Commission, 2010, p. 13.
[156] OSCE (c), 2012.

operation and environmental issues are seen as important elements of security and human rights and fundamental freedoms vital for lasting security. OSCE helps the participating states with democratic institutions, elections, gender equality, ensuring respect for human rights, media freedom, minority rights, the rule of law, tolerance and non-discrimination. Increased co-operation between private and public sectors and civil society is seen as one goal. OSCE also operates on field operations in South-Eastern Europe, Eastern Europe, South Caucasus and Central Asia to prevent crises and help in post-conflict situations and works in co-operation with other international and regional organisations and partner countries in the Mediterranean, Asia and Australia.

The Office for Democratic Institutions and Human Rights (ODIHR) is a special institution of OSCE based in Warsaw, Poland. ODIHR works with elections, human rights and democratization. It performs election observation and election assistance to promote democratic election processes and assists OSCE participating states with expertise and practical support in their human dimension commitments implementation. This is done by strengthening the rule of law, civil society and democratic governance in long-term projects. ODIHR also assists with the human dimension activities of OSCE field missions, contributes to early warning and conflict prevention, provides human-rights training and assists participating states in the implementation of their human rights obligations and in combating discrimination and intolerance. Other activities of the ODIHR include working with Roma and Sinti issues, organising meetings on the implementation of the human dimension commitments and addressing gender issues. ODIHR has expertise in several areas including democratic elections and protecting human rights in the fight against terrorism.[157] The human rights commitments of OSCE are politically, but not legally binding to the participating states.[158]

In 1997 OSCE established a Representative on Freedom of the Media in Vienna, who observes media in OSCE region, provides early warning on violations of freedom of expression and promotes OSCE commitments regarding freedom of expression and free media. The observation of media is done to advocate full compliance with OSCE

[157] OSCE ODIHR, 2012.

[158] OSCE ODIHR (a), 2007, pp. 34-35.

principles. The early warning function is performed in co-operation with the participating states, OSCE Permanent Council, ODIHR, High Commissioner on National Minorities, other OSCE bodies and national and international media associations. If a serious non-compliance with OSCE commitments is found, the representative provides a rapid response with actions, such as direct contact with the participating state and other involved parties and assists in resolving the issue. The representative collects information about the media situation from participating states, NGOs and other sources.[159] The overall importance of Internet freedom is reflected by the words of Dunja Mijatović, the current OSCE Representative on Freedom of the Media:

"*The Internet is a fantastic resource that has fundamentally changed our societies for the better. It will continue to have a positive impact – if we allow it. The lesson is simple: The Internet must remain free.*"[160]

3.6 Bucharest Plan of Action for Combating Terrorism

The cyber threats share the global nature of the Internet. High number of attack methods is available for groups or individual activists, who can operate over the national borders with quick, automated and targeted attacks. Regional and global co-operation is needed for OSCE participating states to counter these threats. In the Bucharest Plan of Action for Combating Terrorism (2001), terrorism is recognized as an international threat to peace and security in OSCE states as well as in other areas. The terrorist attacks in New York in 2001 affected to the creation of this plan, as the international community strongly condemned the acts of terrorism. In the Bucharest Plan of Action the OSCE states have committed their political will, resources and practical means for co-operation and implementation of the international terrorism conventions in a way that respects the international law, human rights and other relevant norms of international law. In the plan UN conventions and UN Security Council resolutions are recognized as the global legal framework in the fight against terrorism. UN resolutions 1269, 1368,

[159] OSCE (d), 2012.
[160] OSCE (b), 2012, p. 6.

1373 and 1377 and 13 relevant UN conventions are listed as most important anti-terrorism conventions.[161] After adopting, signing and ratifying the international treaties, the rights in the treaties have the force of law and they are binding to the OSCE participating states. The resolutions are non-binding, but are considered to be recommendations. The obligations of the states include establishing jurisdiction over the described offences, making the offences punishable, taking offenders into custody, prosecuting or extraditing offenders, co-operation with preventive measures and exchanging information and evidence for criminal proceedings. The conventions also make the offences extraditable between the state parties.[162] The OSCE comprehensive approach and the UN legal instruments adopted by OSCE participating states in the Bucharest Plan of Action for Combating Terrorism are applied also in cyberterrorism issues.

3.7 OSCE Joint Declaration on Freedom of Expression and the Internet

OSCE Joint Declaration on Freedom of Expression and the Internet (2011) recognizes the importance of right to freedom of expression and the Internet and allows only limited restrictions to Internet access. The restrictions have to be prescribed by law and be necessary in a democratic society for the protection of rights of others. According to the declaration, restrictions should be weighted against positive outcomes of freedom of expression. In the case of the Internet these positive outcomes include for example fast and efficient forms of global communication. The Joint Declaration emphasizes Internet-specific methods of content regulation, user's self-regulation, Internet literacy, and the importance of avoiding mandatory blocking and state imposed content-filtering systems. No discrimination is allowed in the treatment of different Internet data and traffic on any grounds. Internet intermediaries should be transparent and make available the traffic and information management practices. Completely cutting off access to the Internet or parts of it and imposed Internet slow-downs are never justified.[163] Even though this declaration is not legally binding for the participants, it is important for

[161] OSCE, 2001, p. 1.
[162] OSCE ODIHR (a), 2007, pp. 34-35.
[163] OSCE, 2011, pp. 1-4.

demonstrating the commitments of the OSCE participating states to the fundamental significance of the right of freedom to expression.

3.8 The Joint Declaration of the UN, OSCE and American states independent experts

The Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the Organization of American States Special Rapporteur on Freedom of Expression (2005) clarifies how the right to freedom of expression can be limited regarding to incitement to terrorism. According to the declaration, restricting the right to freedom of expression as the only reaction to terrorism can actually serve terrorist purposes by violating human rights. However, some restrictions, such as banning incitement to terrorism may be legitimate. States should be clear on terms of restrictions and avoid vague concepts, such as "glorifying" or "promoting" terrorism. Incitement should be regarded as a direct call to terrorism, which increases the likelihood of a terrorist act. Direct link between the expression and violence needs to exist. The relationship and borderline between incitement to violence, racial hatred and the right to freedom of expression is recognized controversial in the declaration. It also stresses the importance of making the distinction between views inciting to violence and views presenting unwillingness to compromise with the authorities without incitement to violence.[164] This declaration is not legally binding for the participating organisations and individual states, but it demonstrates the willingness of the independent experts to co-operation in both preserving the right to freedom of expression and countering terrorism.

The right to freedom of expression is not the only human right, which can be negatively affected by the state's counter terrorism acts. Even though the right to respect for private life is not on the main focus of this study, it deserves to be mentioned here briefly with OSCE counter-terrorism data protection initiatives. The right to the respect for private life can be found from several international human rights instruments, such as ECHR Article 8, UDHR Article 12 and ICCPR Article 17. According to this right

[164] OSCE ODIHR (a), 2007, pp. 227.

everyone has the right to be protected against unlawful interferences to his private and family life, home and correspondence. OSCE human dimensions commitments aim to make the OSCE participating states to respect the right of protection of private and family life, home, correspondence and electronic communications. The right to private life can be limited only in accordance with law, when necessary in a democratic society for the interests of national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health and morals or for the protection of the rights and freedoms of others. Secret surveillance of communications is possible only in exceptional circumstances. The issue becomes more challenging in relation to counter-terrorism. The states may want to control the data traffic to counter cyberterrorism, which often leads to data protection issues. The states should not use their powers in an unlimited way, but the measures should follow the values of democratic society and the rule of law. Several governments are already requiring the ISPs to preserve data traffic logs for up to five years. Often these logs are not open for the citizens, which many activists find intolerable. Storing information about individual's private life in secret registers may interfere with the right to private life.[165]

This chapter presented the relevant international instruments and the approach of OSCE in countering hacktivism and cyberterrorism in a human rights respecting way. The next chapter will provide an overview on how the OSCE participating states are actually implementing these instruments and what kind of legislative strategies, national laws, specialized institutions and technical measures they have against cyber threats. The chapter also includes a short case study about Poland.

[165] OSCE, 2005, pp. 4-6.

4 State responses to cyber-threats

This chapter provides a general overview of OSCE-state responses to hacktivism and cyberterrorism. This is done by discussing the challenges of balancing different values, the status of international conventions in the OSCE participating states, national strategies and laws for Internet content regulation, the role of Internet Service Providers and Computer Emergency Response Teams. The end of the chapter contains a short case study on Poland.

4.1 Balancing human rights and other values in the society

The state responses to acts of hacktivism and cyberterrorism should respect human rights and protect their source, the human dignity. This is not an easy task. The states have legal obligations to ensure the rights of normal citizens as well as those of hacktivists and cyberterrorists. However, at the same time they also need to take in account the functionality and security of the state's critical information systems, public safety, legality of the content, the positive aspects of open and free Internet, political pluralism and the constraints of the available technology in their responses.

Hacktivists and cyberterrorists have few similar constraints and can exploit the state's human rights obligations with their actions. If the balance between rights and restrictions is not found, user's human rights may be violated either by states with too strong restrictions against all Internet users or in an opposite case by activists, who benefit from the weak state of Internet protection. In these cases the list of worst affected human rights include the right to freedom of expression, the right to privacy and the right to fair trial.

4.2 Status of international conventions in the OSCE states

The international legally binding conventions related to the topic of this study are ICCPR, ICERD, Council of Europe Convention on Cybercrime, Council of Europe Convention on the Prevention of Terrorism, ECHR and the UN Conventions and protocols of Bucharest Plan of Action for Combating Terrorism. The extent these conventions have been ratified varies between the individual OSCE participating states.

ICCPR and ICERD are ratified almost completely by all OSCE states and ECHR is also well ratified. Council of Europe Convention on Cybercrime is ratified by only half of the 45 signed countries.[166] One reason for this is that the convention has faced criticism for being outdated and being drafted mostly by European states and for European states. For example Russia hasn't signed the convention and as long as it will not sign it, the convention has less importance.[167] CoE states are not either completely agreeing on the contents of Council of Europe Convention on the prevention of Terrorism, which is ratified only by 29 states. The UN conventions in OSCE Bucharest Plan of Action for Combating Terrorism conventions and protocols are much more ratified. Currently the 56 OSCE-states have ratified 96.1%, signed 0.1% and not ratified nor signed 3.7% of the plan's universal anti-terrorism instruments. 52 states are party to all 12 conventions of Bucharest Plan of Action for Combating Terrorism.[168] Only 30% of the OSCE participating states have recognized access to the Internet as a basic human right.[169] Several OSCE participating states (Cyprus, Estonia, Georgia, Greece, Portugal, Russia and Ukraine) consider the right to access to the Internet to be protected by the state constitutions as a part of the right to access information and communication. In other states specific laws provide the right to access the Internet (Albania, Estonia, Finland, France, Germany, Hungary, Montenegro, Spain, Turkey and Turkmenistan).[170] More than 12% of the states are able to legally restrict the access to Internet for protecting national security, public health or during state emergencies.[171] These are Azerbaijan, France, Latvia, Lithuania, Portugal, Ukraine and Turkmenistan.[172] TABLE 1 presents the ratification status of above mentioned international conventions in the OSCE states.

[166] Paget, 2010, p. 25.
[167] Harley, 2010.
[168] OSCE (a), 2012, p. 3.
[169] Akdeniz, 2010, p. 9.
[170] Idem, p. 36.
[171] Idem, p. 9.
[172] Idem, p. 36.

TABLE 1. The status of international conventions in OSCE participating states.

Convention	**Status**
United Nations	
ICCPR	Ratified by all OSCE states except the Holy See.[173]
ICERD	Ratified by all OSCE states.[174]
The 13 Conventions and protocols of Bucharest Plan of Action for Combating Terrorism	52 states are party to all conventions.[175]
Council of Europe	
Convention on Cybercrime	Ratified by 33 OSCE states. Signed but not ratified by 12 states.[176]
Convention on the Prevention of Terrorism	Ratified by 29 OSCE states. Signed but not ratified by 14 states.[177]
European Convention on Human Rights	Ratified by 47 OSCE states.[178]

4.3 National strategies for Internet content regulation

In addition to international conventions, OSCE participating states have different strategic approaches for regulating domestic Internet content based on the view they have on the nature of the cyber threats. They may apply existing non-terrorist cybercrime legislation to terrorist use of the Internet. Another possibility is to apply existing, but not Internet-specific terrorism legislation. States may also develop specific legislation dealing with the terrorist use of the Internet.[179] For example the incitement to terrorism is based on specific laws in some states, while other states use hate speech or other laws.[180] There is no global agreement on the best approach of legal responses. Most countries respond to Internet terrorism by applying existing cybercrime or

[173] United Nations (a), 2012.
[174] United Nations (b), 2012.
[175] OSCE (a), 2012, p. 3.
[176] Council of Europe (b), 2012.
[177] Council of Europe (c), 2012.
[178] Council of Europe (d), 2012.
[179] CTITF, 2011, p. iii.
[180] OSCE, 2008, pp. 3-5.

counter-terrorism legislation.[181] According to UN Counter-Terrorism Implementation Task Force this is in general a better option than making new specific laws. With more general approach the prosecution is easier as there is no need to prove the intent to commit an act of terrorism.[182] Some OSCE-states have new Internet specific legal provisions, but the increased legislation has led to restrictions on the free flow of information and the right to freely impart and receive information on and through the Internet.[183] If the states create specific legislation against the terrorist use of the Internet, they should also make sure, that they are not criminalizing acts that are not criminalized outside the Internet.[184]

The amount of relevant laws regulating the Internet content varies between the 56 OSCE participating states. Presenting all these laws in the context of this study is not possible. Instead a concise snapshot of the most important categories of regulated content and laws in the OSCE states are presented below on TABLE 2. The listing of these laws is based on a study about freedom of expression on the Internet by OSCE Representative on Freedom of the Media.

TABLE 2. Categories of regulated content and laws in the OSCE states.

Category of content or laws	**OSCE state legal responses**
Incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet.	Outlawed in 40 states. [185]
Racist content, xenophobia and hate speech.	Outlawed in 45 states. [186]
Libel and insult (defamation).	Legal provisions found in 36 states. Civil law provisions applicable to the Internet exist in other states.
Extremism	Outlawed in 20 states. [187]

[181] CTITF, 2011, p. ix.
[182] Idem, pp. 3-4.
[183] Akdeniz, 2010, p. 133.
[184] CTITF, 2011, p. 9.
[185] Akdeniz, 2010, pp. 69-70.
[186] Idem, p. 13.
[187] Idem, p. 17.

Distribution of harmful content.	Outlawed in 19 states.
Prohibition of any other Internet content.	Outlawed in 15 states.[188]
Closing down or blocking access to websites or any other Internet content.	Legal provisions found in 17 states.
Blocking access to Web 2.0 applications, such as YouTube or Facebook.	Specific legal provisions found in 1 state (Italy).[189]

Despite technological and legislative instruments for Internet regulation, it's extremely difficult for the OSCE participating states to keep unwanted content completely offline. This is partially caused by the dispersed nature of the Internet and partially by lack of legal co-operation between the states.[190] States may also have difficulties to keep up with their legal responses with the fast technical developments of the Internet.[191] Generally new Internet specific legal measures are created following some technical developments of the Internet. Many of the current legal frameworks were developed before the emergence of large scale disruptive uses of the Internet such as hacktivism. With the fast pace of development a more proactive approach with an analysis of the possible near future uses of the Internet and the needs for legislation would make the new legal responses more effective.[192] Legislation alone is not enough, both adequate legislation and effective, human rights respecting technical solutions are needed to combat cyber threats.[193]

Hactivists and cyberterrorists can continue operating from countries, which didn't sign international agreements.[194] This stresses the issue of extraterritoriality of the illegal content, which is a major problem for states and the international community. When content is hosted or distributed from outside their jurisdiction, it is unclear if the providers should be liable in the country where the content is uploaded, viewed,

[188] Akdeniz, 2010, p. 18.
[189] Idem, pp. 21-22.
[190] Denning, 2001, p. 271.
[191] OSCE, 2008, pp. 3-5.
[192] CTITF, 2011, p. 9.
[193] Idem, p. ix.
[194] Denning, 2001, p. 271.

downloaded, where the server is placed or where the providers live.[195] The challenges of responding to the fast technical development of the Internet and extraterritoriality of the content are issues, which can be more efficiently responded with international co-operation. Currently the co-operation against transnational Internet crime is however not on a sufficient level. There are several reasons for this, such as lack of common understanding on what constitutes objectionable and illegal content, different approaches on the balance between right to freedom of expression and illegal content and issues connected to protecting private user data.[196]

Estonia is a practical example on how a cyber attack may change the laws and policies of an OSCE participating state. In 2007 Estonia was hit hard by a politically motivated attack, which was described by the media as cyberterrorism, but by Estonian officials just as a cyber attack. The attackers were claimed to be motivated by Estonian government decision to move the location of a Soviet war memorial. The state faced a three week series of attacks including web site defacements with political messages and DoS and DDoS attacks against various governmental and non-governmental organisations. These attacks caused a significant threat to Estonian information systems.[197] The aftermath of the attacks resulted in major changes in Estonian national cyber security policy including new laws, regulations and organisations. One of these was Cyber Security Strategy against cyber attacks, which recognizes the importance of international co-operation and global responses and suggests organisational, technical and legal changes on a national level. The strategic objectives recognized were the development and large-scale implementation of a system of security measures, increasing competence in cyber security, improvement of the legal framework for supporting cyber security, bolstering international cooperation and raising awareness on cyber security.[198] Legislative changes appeared in criminal and crisis management laws and in a lesser degree in other laws related to cyber security.[199] As an organisational change, Estonia formed Cyber Security Council for coordinating inter-agency and

[195] Akdeniz, 2010, p. 6.
[196] OSCE, 2008, pp. 3-5.
[197] Czosseck, Ottis & Talihärm, 2011, p. 1.
[198] Idem, p. 2.
[199] Idem, p. 3.

international responses to cyber threats.[200] Nationwide cyber security awareness and education was seen as a key component for improving national cyber security.[201]

4.4 The role of the Internet Service Providers

Another issue relevant to the rights of users in the OSCE participating states is the role of Internet Service Providers (ISPs). ISPs are private or sometimes state owned commercial organisations, which provide users service of accessing the Internet. ISPs sometimes regulate user generated content, which is published through their services. This is problematic, because international human rights conventions, such as Article 8 of the ECHR ensure the right to respect for private and family life, home and correspondence and forbids public authority interfering with this right, except in certain circumstances.[202]

So far there is no universal agreement regarding the role of the ISP's part in the fight against cyberterrorism. Also the liability of ISPs differs in national legislations.[203] In general ISPs are not held criminally liable if they had no intent to provide illegal content in their services. They are also not required to monitor conduct of the users to avoid criminal liability.[204] However, the public and private sectors need to cooperate since most of the technical infrastructure of the Internet is owned by private entities.[205] ISPs can be co-operating with the states for example with the identification of the users. Currently the Internet includes many technologies for effective control, but advanced users are able to bypass these control mechanisms. Users may be able to hide their identity and nationality, but usually the ISP they use can be identified. Several OSCE states require the ISPs to identify the users and provide information about them for the officials when needed.[206]

[200] Czosseck, Ottis & Talihärm, 2011, p. 4.
[201] Idem, p. 6.
[202] Council of Europe, 1950.
[203] OSCE, 2008, pp. 3-5.
[204] Akdeniz, 2008, p. 28.
[205] CTITF, 2011, p. x.
[206] Conway, 2007, pp. 8-9.

User identification is not the only task the states may delegate to ISPs. There is also a worrying tendency to shift responsibility of regulating online content to private operators. Private operators are not the appropriate instance to decide the legality of the content.[207] If this is however the case, the website blocking criteria and content removal should be transparent, compatible with international norms and standards and provide for redress mechanisms and judicial remedies. Citizens must be able to foresee the consequences of their actions on the Internet.[208] Often the users are unable to see these consequences because of lack of information from the authorities. Some studies have shown that the European ISPs tend not to challenge the request for taking down content and websites can be closed just by sending an e-mail claiming a violation.[209]

In addition to OSCE, also other organisations have guidelines on how the ISPs should regulate the Internet content. Council of Europe human rights guidelines state, that the ISPs should filter, block or remove illegal content only after verification of illegality by the law enforcement authorities to avoid interference with the rights and freedoms of the content creators.[210] The EU approach to ISP liability is slightly different. The EU Directive on Electronic Commerce makes service providers in the EU partly liable for illegal content and requires them to act without delay for removing or disabling access to that information.[211]

According to OSCE standards, the access to Internet content should not be blocked. Despite this, in several OSCE states access to illegal websites has been blocked by the ISP's, if the states can not otherwise censor the website. Often the content is hosted outside the state's jurisdiction and blocking is the fastest and easiest way to disable access to it.[212] Usually the states are not communicating about their processes regarding blocked and unblocked content and it's not necessarily clear for the users if the website is blocked or just temporarily unavailable. From a freedom of expression point of view

[207] OSCE ODIHR (a), 2007, pp. 230-232.
[208] Akdeniz, 2010, pp. 31-34.
[209] Idem, p. 182.
[210] Council of Europe, 2008, p. 6.
[211] Akdeniz, 2010, pp. 26-27.
[212] Idem, p. 6.

this is problematic. If the users can't know what is forbidden content, they may start performing self-censorship with the content they publish online.[213] For example in Finland, the Finnish police delivers a secret website block list to ISPs who perform the actual prevention of website access.[214] The aim of this block list is to prevent access to websites containing child pornography. Also other websites have ended up on the police block list. For example a website named provocatively "lapsiporno.info" (childporn.info) criticised the block list policy and ended up being blocked for an extended period, even though it didn't contain any forbidden material. Website blocking processes are lacking accuracy in several other developed states.[215] Most extreme initiatives by officials on website blocking include proposals of concrete measures to create a European cyberspace with a "virtual Schengen border". In this European cyberspace ISP would block content according to the EU block list. However there is no clarification on what would constitute forbidden content in this cyberspace.[216]

The Internet content is usually manually or automatically pre-filtered for prohibited material before being added to the block list. Most of the states use manual identification and categorization of undesirable sites based for example on the website address, also known as URL (Uniform Resource Locator). It is likely, that with the URL -level keyword filtering some completely legitimate sub domains of the website will also be blocked. The Finnish website blocking policy mentioned earlier is partially based on URL –level blocking. States may also want to develop automated tools for content filtering, but the so called Web 2.0 applications such as social media makes these tools less effective. With social media users are able to publish content without much technical knowledge or delay. Social media makes the issue also more complex, because the content and the platform for publishing it are provided by separate actors. Automated tools may function by filtering content based on a list of forbidden keywords, the state of website origin, etc.[217] It's common, that there is no notice on takedown when user generated content has been removed. ISPs themselves are reluctant

[213] Zittrain & Palfrey, 2008, p. 36.
[214] European Digital Rights EDRI, 2005.
[215] Puolamäki, 2008.
[216] Council of the European Union, 2011, p. 4.
[217] Zittrain & Palfrey, 2008, pp. 36-38.

to filter all of their traffic to prevent illegal material, because filtering is expensive and it has negative effects to the free flow of information.[218] As the content filtering procedures of the ISPs inevitably affect the right to freedom of expression and the free flow of information, from a rights-based perspective filtering and blocking of online content should be left to end users. They should be able to choose the content they want to access and install the content filtering tools by themselves if needed.[219] The wide majority of the Internet users however don't seem to be concerned about blocking and censorship measures taken by ISPs and the states. This may result from the lack of knowledge about both their online rights and freedoms and the technical measures possibly restricting these. More user education would be useful in this sense.

4.5 The role of Computer Emergency Response Teams

Governmental authorities and ISPs may regulate the Internet content, but efficient response to cyber threats and giving advice to normal users is not possible without more involvement from third party actors. Several OSCE participating states have government, university or large IT company Computer Emergency Response Teams (CERTs) for recognizing, analyzing and countering the malicious attacks against their critical computer networks.[220] The development of CERTs started in 1988, when the ARPANET had its first computer worm. This worm caused massive disruptions to the network and the authorities noticed, that without the network a coordinated response was difficult to provide. CERT Coordination Center was created for coordinating responses to network emergencies and other CERTs were quickly established in different parts of the world.[221]

The different CERTs are working in national and international co-operation also with other organisations relevant to Internet security. This includes information sharing, collaboration in solving the found issues, warning systems, research and threat assessment, technical consulting, vulnerability analysis and network monitoring. CERT

[218] Pihlajarinne, 2012.
[219] Zittrain & Palfrey, 2008, p. 36.
[220] CERT Software Engineering Institute CarnegieMellon, 2012.
[221] CERT Software Engineering Institute Carnegie Mellon, 1997.

network sensors provide statistic information and make it possible to recognize emerging threats in an early stage. CERTs also provide a channel of reporting about new cyber threats and help normal users getting better protected. The approach of CERTs is purely technical, but combined with the existing legal frameworks they can provide efficient responses to the acts of hacktivism and cyberterrorism.[222]

4.6 Case of Poland

Republic of Poland is a modern and democratic Central European state with a population of 38.4 million. It's a member state to several international organisations including UN (1945), EU (2004), OSCE (1975), NATO (1999) and others. In 2009 Poland had 22.4 million Internet users.[223] Poland was selected as the topic for this case study, because it's an active OSCE state in both human rights and counter-terrorism initiatives, has modern networked infrastructure and has been targeted by cyber attacks recently. Below the international and domestic legal and institutional responses the state of Poland has had against cyber threats will be presented. Also an example of hacktivism in Poland will be provided.

4.6.1 International and domestic law

There are different risk assessments regarding the cyber threats in Poland. According to Polish Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW) assessment the threat of cyberterrorism in Poland is relatively high, even though there have not been any serious incident lately.[224] Also the Polish Armed Forces sees cyberterrorism as a real threat to society's dependence on telecommunications and information resources, such as state defence system, administration of the energy sector, economy and state finances. Many of these possible terrorist actions have consequences also at the international level. National acts alone can't eliminate the threat, so the

[222] CERT Software Engineering Institute CarnegieMellon, 2012.
[223] Central Intelligence Agency, 2012.
[224] ENISA, 2011, p. 17.

Polish policy aims to strengthen international cooperation, international law and international organisations.[225]

Poland is a state party to several international human rights and counter-terrorism conventions relevant to hacktivism and cyberterrorism. Poland has ratified all except one of the international conventions presented earlier on Table 1. The convention, which is not ratified, is the Council of Europe Convention on Cybercrime. This convention is however signed. Poland has also signed additional protocol of this convention for the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[226] This protocol enhances the domestic and international co-operation in preventing dissemination of illegal material, such as racist or xenophobic propaganda.[227]

According to the current Polish constitution adopted in 1997, everybody has the freedom to hold opinions and to receive and impart information and ideas. [228] Article 49 of the constitution states;

"*The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute*."

Article 54(1) of the constitution states further;

"*The freedom to express opinions, to acquire and to disseminate information shall be ensured to everyone*."

Article 13 of the constitution contains a prohibition of political parties and organisations, which base their programmes on totalitarian methods, racial or national hatred, use of violence to obtain power or influence the state policy or which have secret structure or membership.[229] The concept and definition of an offence of a terrorist nature was introduced in the 2004 amended Polish Penal Code. Penal code of 6 June

[225] Council of Europe, 2008, p. 1.
[226] Idem, p. 6.
[227] Council of Europe (f), 2012.
[228] Official Promotional Website of the Republic of Poland, 2012.
[229] Sejm, 1997.

1997 penalises terrorist acts based on general criminal provisions. The definition of an offence of a terrorist nature can be found from Article 115 (20) of the penal code. According to this article, an offence of a terrorist nature is a:

"*…criminal act subject to a penalty up to 5 years or more of imprisonment, committed with the aim of seriously intimidating the population or forcing a public authority of Poland or another country or an international organisation to act or not to act, or to cause considerable interference in the economy or constitutional structure of Poland, another country or an international organisation.*"

This definition makes it possible to sanction the actors of offences of terrorist nature and apply the penal code to Polish nationals, organisational entities and aliens committing terrorist offences abroad. In Poland there are no different procedural rules for persons accused of terrorist offences, but the regular provisions of the code of penal procedure apply. There are also several special legal instruments against terrorism and laws against the financing of terrorism.[230] The Polish cybercrime legislation labels most computer misuse acts and security breaches as offences according to the Criminal Code of 6 June 1997. Criminal procedure code of 6 June 1997 regulates the procedural issues. Since then the law has been amended several times. Amendment of 18 March 2004 harmonized the Polish Criminal Code and the Criminal Procedure Code with CoE Convention on Cybercrime.[231]

Polish general legal provisions don't require closing of or blocking access to websites or other types of Internet content, but certain activities on the Internet are prohibited according to the Polish Criminal Law. Prohibited activities include acts such as promotion of fascist or another totalitarian regime. The provisions of the criminal law do not explicitly provide the possibility to mandate the service provider closing down a website, but this can be achieved based on general provisions. Criminal Procedure Code gives the possibility to impose preventive measures by mandating to refrain from certain activities, such as order to refrain from managing a website. A court in the criminal

[230] Council of Europe, 2008, p. 1.
[231] ENISA, 2011, p. 8.

proceedings or the public prosecutor in the course of preparatory proceedings may impose this preventive measure. According to Article 39(2) of the Criminal Code the order to close a website is a preventive measure, not a penalty.[232] Article 296b of the Criminal Code responds to cyberattacks and has a similar content to Article 6 of CoE convention on cybercrime. However, Article 296b has been criticized of being poorly and too widely defined, making in theory manufacturing or selling almost any operating system or personal computer illegal.[233]

Other articles of the Polish Penal Code relevant to hacktivism and cyberterrorism are Article 212, Article 216, Article 255, Article 258, Article 267, Article 268 and Article 269. These are described more in detail below in **Table 3**.

TABLE 3. The Polish Penal Code articles relevant to hacktivism and cyberterrorism.

Article	Description
Article 212	Criminalizes the offence of libel.
Article 216	Penalizes insult and defamation. Offences against honour, personal inviolability, insult and defamation are provided with fines and imprisonment. A private prosecution is required. [234]
Article 255	Criminalizes public incitement to any offence, including terrorism also in the Internet. Possession of content related to "terrorist propaganda" can be prosecuted as a preparatory act to an offence.[235]
Article 258	The provisions contain punishment between 8 months to 6 years imprisonment to persons establishing, managing or participating in organisations aiming to commit offences of a terrorist nature. The creator or leader of such organisation is subject to a minimum of 3 year imprisonment. [236]

[232] Akdeniz, 2010, p. 162.
[233] Waglowski, 2005.
[234] Akdeniz, 2010, p. 124.
[235] Idem, p. 76.
[236] Council of Europe, 2008, p. 1.

Article 267	Penalizes the act of acquiring information by opening sealed letters, breaching protected information by connecting information transmitting wire or by breaching electronic, magnetic or other special protection. These acts are penalized by a fine, penalty of restriction of liberty or deprivation of liberty for up to 2 years. The same punishment is imposed on anyone accessing, installing or using tapping, visual detection or other equipment for acquiring unauthorised information and anyone who imparts or discloses others the information obtained.
Article 268	Penalizes by a fine, penalty or deprivation of liberty for up to 2 years unauthorized destroying, damaging, deleting or altering records of essential information and preventing authorized persons from obtaining that information. If the act is performed against electronic information carrier, the penalty of deprivation of liberty can be up to 3 years. In the case of significant loss of property the deprivation of liberty the penalty can be between 3 months and 5 years.
Article 269	Penalizes with a 6 months to 8 years depravation of liberty the acts, that destroy, delete or change electronic information significant for national defence, transport safety, government, other state authority, local government, or interferes with automatic collection and transmission of such information. The same punishment is imposed for damaging a device used for the automatic processing, collection or transmission of information.[237]

In the context of right to privacy in hacktivism and cyberterrorism issues, Poland has a data protection act from 29th of August 1997 on the Protection of Personal Data. This act protects personal data, including data in computer systems. The act applies to public authorities and non-public bodies, which carry out public tasks. According to the data

[237] CyberCrime Law, 2012.

protection act, the subjects of data collection have the right to acquire information about his/her data in the systems.[238]

The EU e-commerce directive was incorporated into Polish law in 2002. The directive allows authorities ordering ISPs to block gambling websites, but the directive can be used also against copyright infringement. The implementation of the directive has been criticized for setting too many pre-publication control obligations to the ISPs, in cases such as user comments and hyperlinks. According to the directive, Polish ISPs are expected to notify users on possible content take-down procedures, but no "notice and take-down procedure" has been implemented with formal procedures. Instead some providers have their own standards for regulation.[239]

4.6.2 Domestic institutions

The Polish government has recognized possible cyber threats and is addressing the issue with Governmental Action Plan for Cyber security from 2011 to 2016.[240] **ABW** and the **Police** have in co-operation the leading role of Polish anti-terrorism action.[241] ABW is a governmental institution, which aims to protect the citizens of Poland and the internal security of the state. ABW has both operational and investigative powers and its activities are conducted according to the principle of the rule of law.[242] ABW includes a counter-terrorism department. Its main tasks are reconnaissance, countering and preventing terrorist threats to internal security and constitutional order of the Polish state caused for example by totalitarian methods, racial and ethnic hatred and violence as a tool. The counter-terrorism forces of the Police are Central Investigation Bureau (CBS) and Antiterrorism Task Force (IOA KGP).[243] So far the Polish police have no separate division for computer crime.[244] Instead the Polish Platform for Homeland Security (Polska Platforma Bezpieczeństwa Wewnętrznego, **PPBW**) was established to create computer tools for improving public security by supporting the police and

[238] Dataprotection.eu, 2012.
[239] Spindler, 2007, pp. 1-3.
[240] ENISA, 2011, p. 5.
[241] Council of Europe, 2008, p. 4.
[242] The Internal Security Agency, 2012.
[243] Council of Europe, 2008, p. 5.
[244] ENISA, 2011, p. 8.

security services. National Police Headquarters, Supreme Court National Prosecution Office, Poznan Supercomputing and Networking Center and different Polish universities all participate to PPBW.[245] The research projects of PPBW are approved and supported by the Polish government and have a measurable security impact also on the European level.[246]

Other Polish governmental authorities besides ABW, the police and PPBW taking part in network and information security are Ministry of Interior and Administration, Ministry of National Defence, Ministry of Infrastructure, Bureau of the Inspector General for the Protection of Personal Data (GIODO), National Security Centre (RCB), Bureau of National Security (BBN), Polish Committee for Standardisation, Office for Competition and Consumer Protection, Office of electronic communications and Polish chamber of commerce.[247]

Other major players in the Polish Internet security are CERTs of different Polish governmental and non-governmental organisations. The Polish Governmental CERT, which has the same name as its URL "CERT.GOV.PL", was established in 2008. It works as a part of the IT Security Department of the ABW. CERT.GOV.PL aims to protect the units of public administration against cyber threats. The focus is on protection against attacks, which may cause considerable harm to the lives and health of the people, existence of national heritage, the environment or lead to a considerable financial loss or disturb the operation of public authorities. CERT.GOV.PL provides coordination of the incident response process, publishes announcements on security threats, resolves and analyzes incidents, publishes notifications, coordinates responding to security holes, detects incidents in protected networks and administers security tests.[248]

Other relevant IT security actors in Poland are NASK/CERT Polska, Pionier CERT and TP CERT. NASK (Naukowa i Akademicka Sieć Komputerowa – Scientific and

[245] ENISA, 2011, p. 4.
[246] PPBW Polish Platform for Homeland Security, 2012.
[247] ENISA, 2011, pp. 27-31.
[248] CERT.GOV.PL (a), 2012.

Academic Computer Network) is a Polish network operator, which CERT Polska is a part of. CERT Polska has an early warning and information system ARAKIS-GOV for detecting automated threats against networks.[249] ARAKIS-GOV supports the existing standard security measures of public administration IT resources. The system provides data and statistics about the new Internet threats including computer worms and attacks coming from numerous locations.[250] CERT Polska aims to assist Polish Internet users with computer security incidents and responding to these incidents. CERT Polska also handles user-reported incidents in Polish networks.[251] The primary goals of NASK and CERT Polska include identifying groups behind computer attacks, organise takedowns and URL block listing. Currently the block listing policy is not implemented in Poland.[252]

Pionier CERT is another computer incident response team, which aims to provide members and users of Polish Scientific Broadband Network PIONIER effective incident response service. It works in co-operation with network operators.[253] Polish national telecommunications provider Telekomunikacja Polska (TP) has its own CERT team, TP CERT. It aims to assist users of its network with computer security incidents. CERT.GOV.PL, NASK/CERT Polska, Pionier CERT and TP CERT work in close co-operation with each other.[254] Besides the CERT Polska, NASK provides in co-operation with ISPs and the police a hotline called “Dyżurnet.pl” for reporting illegal content on the Internet.[255] The mission of the hotline is to remove according to the Polish law illegal content involving child abuse, threatening children's safety or promoting xenophobia and racism. According to the year 2009 statistics, majority of the reported incidents considered different forms of pornography, but also “Racism and xenophobia” and “Promoting violence against an individual” were among the categories.[256]

[249] ENISA, 2011, p. 15.
[250] CERT.GOV.PL (b), 2012.
[251] CERT Polska (b), 2012.
[252] ENISA, 2011, p. 18.
[253] Pionier CERT, 2012.
[254] TP CERT, 2012.
[255] ENISA, 2011, p. 18.
[256] Dyżurnet.pl, 2012.

4.6.3 Example of hacktivism in Poland

Adequate public information about possible cyberterrorist attacks in Poland and the state responses to them was not available during conducting this study. Instead an example of case of hacktivism connected to intellectual property rights will be discussed here.

In early 2012 the hacker/hacktivist group Anonymous launched a multiple DDoS attacks against Polish government websites. This attack was meant to be a protest after the government revealed plans to sign the Anti-Counterfeiting Trade Agreement (ACTA). Polish Parliament, Ministry of Foreign Affairs and Internal Security Agency were among the victims of these attacks. The attackers gathered more force on their attack through social media applications, such as Facebook, Twitter and IRC by listing the targets and distributing the easy-to-use software called LOIC for launching the attacks. LOIC or "Low Orbit Ion Cannon" is widely available on the Internet. However, it seems that many attackers who joined with Anonymous were more interested in causing general disruption with the provided tools than supporting or even being interested about the actual cause of the group. The availability of the DDoS software triggered other attacks without political motivation against random targets, such as Tesco supermarkets, the Polish Railways and banks. The acts of Anonymous and the solo attackers were reported within minutes after the attack by Internet news portals. This wide media coverage may have further fuelled the attacks by giving the attackers nearly instant confirmation about their success.[257]

After the attacks the Polish Ministry of Administration and Digitization published widely criticized guidelines for the protection of public administration websites. These guidelines recommend blocking users, who use technical solutions to remain anonymous. Incoming traffic to websites is filtered according to unspecified criteria. The vague definitions of the guidelines give a wide margin for the implementation of measures and are not precise on filtering and blocking measures or safeguards against abuses. Unspecified control mechanisms may violate the rights of citizens, who wish to

[257] CERT Polska (a), 2012.

obtain information about public authorities anonymously or don’t otherwise meet the unspecified criteria.[258] At the time of writing this thesis there was no other information available regarding the possible legal responses of the Polish government against these DDoS attacks. The acts of the hacktivists got a lot of international media attention and may have affected to the Polish government’s decision about ACTA. However, in the longer run their acts may be contributing in a negative way to increased government regulation of the Internet and weaken the right to freedom of expression on the Internet in Poland.

This chapter contained an overview of OSCE state responses to hacktivism and cyberterrorism by examining the status of international conventions in the OSCE participating states, the national strategies and laws for Internet content regulation, the role of ISP’s and CERT’s. Also a short case study on Poland was provided. The next chapter is the last chapter of this study and will provide a conclusion by answering to the research questions set at the introduction.

[258] Siewicz, 2012.

5 Conclusion

This chapter contains a conclusion of the study by answering the research questions set at the beginning of this study.

5.1 What are the main differences between hacktivism and cyberterrorism?

There is a plenty of academic literature available discussing either about hacktivism or cyberterrorism. However, challenges of defining these concepts in the literature are evident and updated comprehensive comparisons of the two are rare. Out of the two concepts, cyberterrorism is far more researched, but the lack of universally accepted definition for it became clear already at the early stages of this study. Even though there is less politics involved in the definition of hacktivism, as a concept and a research topic it was evasive as many authors made no difference between cyberterrorism and hacktivism. Much of the literature discussing hacktivism had also become outdated in the fast pace of technical developments. Establishing contacts to different activist groups could have provided interesting results on their definitions of hacktivism and cyberterrorism, but this was not possible due to the limited timeframe. As a result of above mentioned facts, the phenomena of hacktivism and cyberterrorism are close to each other also in this study.

Hacktivists and cyberterrorists share many methods of action and both of the groups aim for maximum media attention. The most important differences between hacktivism and cyberterrorism are intended use of violence and level of concern for the welfare of other users. While the real motivations within hacktivist groups may differ from ideological reasons to just having fun, the common feature of hacktivist acts has been avoiding causing permanent damage to infrastructure and other users. Often the aim of their actions is to ensure the free flow of information on the Internet, even though hacktivists may restrict other user’s right to freedom of expression in many ways when conducting these actions. Cyberterrorists don’t have similar constraints for their acts. They aim to cause maximum and permanent damage to the Internet and society without much concern for the welfare of others. In general the acts of hactivism and cyberterrorism don't seem to be any more effective than acts of normal activism. States and international organisations are more likely to strengthen their cyber defence and establish new institutions than change or remove policies.[259] Hacktivism and cyberterrorism may also have difficulties in winning wider support from traditional activists because of the questionable motives and illegitimate methods.

DDoS attacks as both hacktivist and cyberterrorist method has brought these phenomena closer to each other. With easily available, automated DDoS attack tools hacktivists may even unintended be able to cause just as much damage as cyberterrorists. DDoS attacks can get high media attention, but often appear being without acceptable motivation for the wider audience. These negative images combined with the increased intensity of other of cyber threats, their wide negative media attention and the global anti-terrorism atmosphere is changing the way states, media and academia see hacktivism. Hacktivism acts are today more and more easily labelled as a form of cyberterrorism even though some of the hacktivist methods could also be used in more positive ways.

5.2 How have OSCE-states responded to acts of hactivism and cyberterrorism?

Given the high number of OSCE states it was impossible to research and give a detailed state by state answer to this question within the boundaries of this study. As the study was not either meant to be a purely legal in nature, thorough analysis of legal instruments was not provided. Because of the above mentioned issues and the lack of information about state responses to cyber attacks and content related convictions, the answer to this question is given in a general level by providing an overview of the state's legal and other responses.

OSCE participating states are responding to cyber threats with international legal co-operation, domestic laws, technical counter-measures and specialized domestic institutions. International legal co-operation consists of anti-terrorism conventions,

[259] Denning, 2001, p. 243.

which are ratified by varying degrees by the OSCE participating states. Domestic laws in most states outlaw terrorist related use of the Internet, racist content, xenophobia and hate speech. Out of the 56 OSCE participating states 40 states have outlawed incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet.[260] The domestic legal responses may be based on existing non-terrorist cybercrime legislation, non-Internet-specific terrorism legislation or new specific legislation. Poland is an example on how OSCE participating state can prepare for cyber threats. This state has created a national Internet security strategy, domestic legal provisions and institutions against cyber threats and is also active with international co-operation.

Technical measures against hacktivism and cyberterrorism may consist of filtering, blocking or removing Internet content. Often private actors, such as ISPs play a significant role in this and international co-operation exists also in this field. Specialized national institutions responding to cyber threats may be for example security agencies or CERTs of public or private institutions. They have a technical role in early warning, detecting, analyzing and preventing cyber attacks with their sensor networks. These domestic institutions may also have international co-operation. All above mentioned responses are mainly cyberterrorism oriented. So far there is no hacktivism specific legislation and from the technical point of view the same tools are being used to response to all cyber threats.

The absence of statistical data about content related convictions in OSCE states and the tendency of states not to release much information about attacks against their networks make it difficult to assess the effects of the state's legal responses.[261] However, it's evident, that despite the international conventions, more co-operations is needed in countering the cyber threats. This includes approaches, which combine in an effective way both global legal and technical measures. Currently global cybercrime legislation and other specific legal responses are lacking a common approach.[262] With purely legal responses, the states are seldom able to restrict or penalize hacktivists and

[260] Akdeniz, 2010, pp. 69-70.
[261] Idem, pp. 134-135.
[262] CTITF, 2011, p. 9.

cyberterrorists. This can be caused by difficulties in recognizing the actors, extraterritoriality of illegal content or number of other reasons. Currently OSCE participating states have difficulties in keeping illegal content offline and cybercriminals can relatively easily avoid law enforcement. Similarly with the legal responses, lack of information about technical measures taken is equally a problematic for assessing the effectiveness of technical measures. States and specified institutions are often not willing to distribute technical details about the attacks their systems have faced, the impact of these attacks and how the systems are protected. Despite this, technical measures and specialized institutions seem to be relatively effective in restricting cyber threats and blocking illegal content. However, with inadequate legal framework plain technical responses are risking to restrict free flow of information and the user's right to freedom of expression.

5.3 Is the right to freedom of expression taken in account in these responses?

The answer to this question is given in a general level because of the same limitations as with the two previous questions. The states take the right to freedom of expression and other human rights in account to a degree on their responses to cyber threats, but are often inconsistent with their actions. Finding the balance between human rights and other values of the society in responding to cyber threats seems to be problematic for the states. Despite the international safeguards for human rights, several states have been unable to find this balance. State control and regulation of the Internet is on a higher level than ever before during the existence of the Internet and this tendency seems to be continuing. The proportionality of the current legal and technical measures by states in comparison to the threats of hacktivism and cyberterrorism to the society can be questioned. While it's very difficult for the states to keep unwanted content completely offline the rights of ordinary users are much more easily restricted. The current approach of the international community in issues related to hacktivism and cyberterrorism includes a variety of instruments, but lacks a common goal. It may also be too rigid and slow in responding to the rapid development and several different manifestations of the Internet content. This weakens the responses of states in cases of international co-operation.

It is important that individual OSCE states comply with international human rights law in their domestic responses. Human rights violating measures are more likely to advance the terrorist goals than actually help in countering terrorism. The international cybercrime conventions have safeguards for the right to freedom of expression, even though not all the OSCE participating states have ratified all the cybercrime conventions. These safeguards for human rights are not working properly as long as the definition of terrorism and terrorism related concepts remain as vague as they are now. The boundaries between the acts of normal political online activism, hacktivism and cyberterrorism are also blurred and the states may violate user's rights if they use the cyberterrorism approach to all of these acts. Another issue with both international and national legal responses is the vagueness of the forbidden content compared to international human rights standards. If the users don't know what is forbidden content, they may resort to self-censorship and not perform the actions they would normally do.

Strengthening the national cyber defence mainly with technical measures and specialized institutions is a technologically oriented solution, which relies a great deal on security systems and the role of the ISPs. The private actors are not the appropriate instance for deciding the legality of the content as their blocking process may lack transparency and other properties, which are required from public actors. Filtering and content-blocking systems inevitably affect Internet's free flow of information and user's right to freedom of expression. It seems that technical responses to hacktivism and cyberterrorism have the highest potential of violating the user's right to freedom of expression. Possible measures of content filtering or blocking should be left to end-users, who can install the easily available software for doing this.

Cyber threats can be most efficiently responded with a combination of human rights respecting technical and legal instruments and co-operation between different parties. The international community, states, private operators and civil society should work in co-operation to ensure, that when restrictions are necessary, the measures taken are transparent, compatible with international norms and standards and provide redress mechanisms and judicial remedies. One alternative for decreasing the state control measures would be increasing and promoting the role of civil society in protecting the rights of the citizens, but also raising awareness about cyber threats among them. Many of the current hacktivist and cyberterrorist methods rely greatly on virus-infected computers of ordinary users and would be easy to prevent if the users knew how to protect from these methods. Private operators are not part of the international human rights system, but they should be encouraged to develop ethical codes of conduct for guiding the actions in human rights related cases.

Bibliography

Legal sources

Council of Europe (f), "*Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)*", 2012, at http://conventions.coe.int/treaty/en/Summaries/Html/189.htm, (consulted on 05 June 2012).

Council of Europe (d), "*Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.: 005*", 2012, Council of Europe Treaty Office, at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=&DF=&CL=ENG, (consulted on 05 June 2012).

Council of Europe (b), "*Convention on Cybercrime CETS No.: 185*", 2012, Treaty office, at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, (consulted on 05 June 2012).

Council of Europe (a), "*Convention on Cybercrime (ETS No. 185)*", 2012, at http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm, (consulted on 05 June 2012).

Council of Europe (c), "*Council of Europe Convention on the Prevention of Terrorism CETS No.:196*", 2012, Treaty Office, at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=196&CM=8&DF=31/03/2012&CL=ENG, (consulted on 05 June 2012).

Council of Europe, "*European Convention on Human Rights*", 1950, at http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf, (consulted on 05 June 2012).

Council of Europe, "*European Convention on Human Rights as amended by Protocols Nos. 11 and 14 Council of Europe Treaty Series, No. 5"*, 2010, available at http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf, (consulted on 05 June 2012).

European Commission, "*Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*", 2010, available at http://ec.europa.eu/home-affairs/policies/crime/1_EN_ACT_part1_v101.pdf, (consulted on 05 June 2012).

European Court of Human Rights, "*Court (Chamber) Case of Thorgeir Thorgeirson v. Iceland (Application no. 13778/88) Judgement*", Strasbourg, 25 June 1992, para. 64, at http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Thorgeir&sessionid=96060858&skin=hudoc-en, (consulted on 17 May 2012).

European Court of Human Rights, "*Court (Plenary) Case of Handyside v. The United Kingdom (Application no. 5493/72) Judgement*", 7 December 1976, para. 49, Strasbourg, at http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=handyside&sessionid=96062044&skin=hudoc-en, (consulted on 17 May 2012).

Office of the High Commissioner for Human Rights (a), "*General Comment No. 10: Freedom of expression (Art. 19):. 06/29/1983.CCPR General Comment No. 10. (General Comments)*", 26 June 1983, at http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/2bb2f14bf558182ac12563ed0048df17?Opendocument, (consulted on 05 June 2012).

Office of the High Commissioner for Human Rights (b), "*General Comment No. 11: Prohibition of propaganda for war and inciting national, racial or religious hatred (Art. 20):. 07/29/1983. CCPR General Comment No. 11. (General Comments)*", 29 July 1983, at http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/60dcfa23f32d3feac12563ed00491355?Opendocument, (consulted on 05 June 2012).

Office of the High Commissioner For Human Rights, "*General Recommendation No. 29: Article 1, paragraph 1 of the Convention (Descent):. 11/01/2002. Gen. Rec. No. 29. (General Comments)*", 1 November 2002, at http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/f0902ff29d93de59c1256c6a00378d1f, (consulted on 05 June 2012).

Official Journal of the European Communities, "*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce*", 8 June 2000, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF, (consulted on 05 June 2012).

OHCHR, "*International Covenant on Civil and Political Rights*", 1966, at http://www2.ohchr.org/english/law/ccpr.htm, (consulted on 05 June 2012).

OSCE (a), "*Status in the OSCE area of the Universal Anti-terrorism Conventions and Protocols as well as other international and regional legal instruments related to terrorism or co-operation in criminal matters*", 3 January 2012, Office of the Secretary General Vienna, Action against Terrorism Unit, at http://www.osce.org/atu/17138, (consulted on 05 June 2012).

OSCE ODIHR (b), "*OSCE/ODIHR Comments on legislative treatment of "Cyberterror" in domestic law of individual states*", 27 March 2007, at http://legislationline.org/search/runSearch/1/type/2/topic/3, (consulted on 05 June 2012).

United Nations (b), "*International Convention on the Elimination of All Forms of Racial Discrimination*", 2012, United Nations Treaty Collection, at http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-2&chapter=4&lang=en, (consulted on 05 June 2012).

United Nations (a), "*International Covenant on Civil and Political Rights*", United Nations Treaty Collection, 2012, at http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en, (consulted on 05 June 2012).

United Nations (a), "*International covenant on civil and political rights General Comment no. 29 States of Emergency (Article 4)*", 31 August 2001, at http://www.unhchr.ch/tbs/doc.nsf/0/71eba4be3974b4f7c1256ae200517361/$FILE/G0144470.pdf, (consulted on 05 June 2012).

United Nations (b), "*International Covenant on Civil and Political Rights Human Rights Committee Eightieth session General Comment No. 31 [80] The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*", 29 March 2004, at http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f?Opendocument, (consulted on 05 June 2012).

United Nations, "*The Universal Declaration of Human Rights*", 1948, at http://www.un.org/en/documents/udhr/, (consulted on 05 June 2012).

Official documents

Akdeniz, Yaman, "*Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States. Report of the OSCE Representative on Freedom of the Media*", 23 September 2010, Istanbul Bilgi University, at http://www.osce.org/fom/80723, (consulted on 05 June 2012).

Council of Europe, "*Committee of Experts on Terrorism (CODEXTER) profiles on counter-terrorist capacity Poland*", April 2008, at http://www.coe.int/t/dlapil/codexter/Country%20Profiles/CODEXTER%20Profiles%20_2012_%20Poland%20E.pdf, (consulted on 05 June 2012).

Council of Europe, "*Human rights guidelines for Internet service providers Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA)*", 2008, at http://www.coe.int/t/informationsociety/documents/HRguidelines_ISP_en.pdf, (consulted on 05 June 2012).

Council of Europe (e), "*Our objectives*", 2012, at http://www.coe.int/aboutCoe/index.asp?page=nosObjectifs&l=en, (consulted on 05 June 2012).

Council of Europe Committee of Ministers, "*Declaration on freedom of expression and information in the media in the context of the fight against terrorism*", 2 March 2005, at https://wcd.coe.int/ViewDoc.jsp?id=830679&Site=CM, (consulted on 05 June 2012).

Council of the European Union, "*Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party*", 17 February 2011, Brussels, at http://register.consilium.europa.eu/pdf/en/11/st07/st07181.en11.pdf, (consulted on 05 June 2012).

Council of the European Union, "*The European Union Counter-Terrorism Strategy*", 30 November 2005, Brussels, at http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf, (consulted on 05 June 2012).

CTITF, "*Countering the use of Internet for terrorist purposes - Legal and Technical aspects*", May 2011, CTITF Working Group Compendium, at http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf, (consulted on 05 June 2012).

ENISA, European Network and Information Security Agency, "*Poland Country Report May 2011*", 2011, at http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Poland.pdf, (consulted on 05 June 2012).

European Commission, "*Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the*

Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'", 31 March 2011, Brussels, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF, (consulted on 05 June 2012).

European Commission Home Affairs, "*Fight against terrorism*", 2012, at http://ec.europa.eu/home-affairs/policies/terrorism/terrorism_intro_en.htm, (consulted on 05 June 2012).

European Union (b), "*A Peaceful Europe - the beginnings of cooperation*", 2012, at http://europa.eu/about-eu/eu-history/1945-1959/index_en.htm, (consulted on 05 June 2012).

European Union (a), "*Basic information on the European Union*", 2012, at http://europa.eu/about-eu/basic-information/index_en.htm, (consulted on 05 June 2012).

EUROPOL, "*TE-SAT 2011 EU Terrorism Situation and Trend Report*", 2011, at https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf, (consulted on 05 June 2012).

Office of the High Commissioner for Human Rights (a), "*United Nations Human Rights Council Background information on the Human Rights Council*", 2012, at http://www.ohchr.org/EN/HRBodies/HRC/Pages/AboutCouncil.aspx, (consulted on 05 June 2012).

Office of the High Commissioner for Human Rights (b), "*Universal Periodic Review*", 2012, at http://www.ohchr.org/EN/HRBodies/UPR/Pages/UPRMain.aspx, (consulted on 05 June 2012).

Official Promotional Website of the Republic of Poland, "*Freedom of Speech and the Right to Choose*", 2012, at http://en.poland.gov.pl/Freedom,of,Speech,and,the,Right,to,Choose,1612.html, (consulted on 05 June 2012).

OSCE, "*Expert Workshop on Combating the Use of the Internet for Terrorist Purposes Issues Relating to Freedom of the Media, the Right to Freedom of Expression and the Right to Respect for Private Life and Data Protection Contribution by The Office of the Representative on Freedom of the Media (RFOM) And The Office for Democratic Institutions and Human Rights (ODIHR)*", 13-14 October 2005, Vienna, at http://www.osce.org/odihr/16713, (consulted on 05 June 2012).

OSCE, "*Governing the Internet Freedom and Regulation in the OSCE Region*", 2007, The Representative on Freedom of the Media, at http://www.osce.org/fom/26169, (consulted on 05 June 2012).

OSCE (c), "*History*", 2012, at http://www.osce.org/who/87, (consulted on 05 June 2012).

OSCE, "*International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet*", 1 June 2011, at http://www.osce.org/fom/78309, (consulted on 05 June 2012).

OSCE, "*MC(9).DEC/1 4 December 2001 Annex MC09EW01 The Bucharest Plan of Action for Combating Terrorism*", 4 December 2001, at http://www.osce.org/atu/42524, (consulted on 05 June 2012).

OSCE (d), "*Representative on Freedom of the Media Mandate*", 2012, at http://www.osce.org/fom/43207, (consulted on 05 June 2012).

OSCE, "*Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation, Remarks by Raphael F. Perl − Head of the OSCE Action against Terrorism Unit*", 7-10 April 2008, Second International Forum on Information Security, Garmisch-Partenkirchen, at http://www.osce.org/atu/31428, (consulted on 05 June 2012).

OSCE (b), "*The OSCE Representative on freedom of the media. Internet freedom why it matters*", 2012, at http://www.osce.org/fom/86003, (consulted on 05 June 2012).

OSCE ODIHR, "*About ODIHR*", 2012, at http://www.osce.org/odihr/43595, (consulted on 05 June 2012).

OSCE ODIHR (a), "*Countering Terrorism, Protecting Human Rights. A Manual*", 2007, at http://www.osce.org/odihr/29103?download=true, (consulted on 05 June 2012).

Sejm, "*The Constitution of the Republic of Poland of 2nd April, 1997*", 1997, at http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm, (consulted on 05 June 2012).

The Internal Security Agency, "*About ISA*", 2012, at http://www.abw.gov.pl/portal/en/16/13/About_ISA.html, (consulted on 05 June 2012).

United Nations (a), "*A more secure world: Our shared responsibility. Report of the Secretary-General's High-level Panel on Threats, Challenges and Change*", 2004, at http://www.un.org/secureworld/report2.pdf, (consulted on 05 June 2012).

United Nations, "*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*", 16 May 2011, at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, (consulted on 05 June 2012).

United Nations (b), "*Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance Durban, 31 August - 8 September 2001*", 2001, at http://www.un.org/WCAR/aconf189_12.pdf, (consulted on 05 June 2012).

United Nations (c), "*The Foundation of International Human Rights Law*", 2012, at http://www.un.org/en/documents/udhr/history.shtml), (consulted on 05 June 2012).

United Nations (d), "*UN at a Glance*", 2012, at http://www.un.org/en/aboutun/index.shtml, (consulted on 05 June 2012).

United Nations, "*United Nations Global Counter-Terrorism Strategy: activities of the United Nations system in implementing the Strategy Report of the Secretary-General,* *Sixty-fourth session Agenda item 115*", 13 September 2010, at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/530/85/PDF/N1053085.pdf?OpenElement, (consulted on 05 June 2012).

United Nations Human Rights Office of the High Commissioner for Human Rights, "*Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*", 2012, at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx, (consulted on 05 June 2012).

Literature

Akdeniz, Yaman, "*An Advocacy Handbook for the Non Governmental Organisations The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems*", May 2008, at http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf, (consulted on 05 June 2012).

Almeida, Marcelo & Mutina, Boris, "*Defacements Statistics 2010: Almost 1.5 million Websites defaced, What's happening?*", 6 January 2011, at http://www.zone-h.org/news/id/4737, (consulted on 05 June 2012).

Central Intelligence Agency, "*The World Factbook Poland*", 3 May 2012, at https://www.cia.gov/library/publications/the-world-factbook/geos/pl.html#, (consulted on 05 June 2012).

CERT.GOV.PL (a), "*About us*", 2012, at http://www.cert.gov.pl/portal/cee/38/77/About_us.html, (consulted on 05 June 2012).

CERT.GOV.PL (b), "*ARAKIS-GOV System*", 2012, at http://cert.gov.pl/portal/cee/39/78/ARAKISGOV_system.html, (consulted on 05 June 2012).

CERT Polska (b), "*CSIRT Description for CERT Polska*", 2012, at http://www.cert.pl/txt/rfc2350.txt, (consulted on 05 June 2012).

CERT Polska (a), "*DDoS against Polish government websites*", 23 January 2012, at http://www.cert.pl/news/4856/langswitch_lang/en, (consulted on 05 June 2012).

CERT Software Engineering Institute Carnegie Mellon, "*Resource for National CSIRTs*", 2012, at http://www.cert.org/csirts/national/, (consulted on 05 June 2012).

CERT Software Engineering Institute Carnegie Mellon, "*Security of the Internet*", 1997, at http://www.cert.org/encyc_article/tocencyc.html, (consulted on 05 June 2012).

Chu, Hai-Cheng, Deng, Der-Jiunn & Chao, Han-Chieh, "*Potential cyberterrorism via a multimedia smart phone based on a web 2.0 application via ubiquitous Wi-Fi access points and the corresponding digital forensics*", 14 November 2010, Springer-Verlag, at http://www.springerlink.com/content/f34565g827508474/, (consulted on 05 June 2012).

Conway, Maura, "*Terrorism & Internet Governance: Core Issues*", 2007, Disarmament Forum, at http://www.unidir.org/pdf/articles/pdf-art2644.pdf, (consulted on 05 June 2012).

CyberCrime Law, "*Cybercrime laws Poland*", 2012, at http://www.cybercrimelaw.net/Poland.html, (consulted on 05 June 2012).

Czosseck, Christian, Ottis, Rain & Talihärm, Anna-Maria, "*Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*", 2011, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, at http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF, (consulted on 05 June 2012).

Dahlberg, Lincoln & Siapera, Eugenia (eds.), "*Radical Democracy and the Internet Interrogating Theory and Practice*", 2007, Antony Rowe Ltd.

Dataprotection.eu, “*Data Protection Act, Poland*”, 2012, at http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.PL, (consulted on 05 June 2012).

Denning, Dorothy E., "*Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy*", 2001, pp. 239-288 in Foreign Policy, vol. 23, at http://www.prgs.edu/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf, (consulted on 05 June 2012).

Denning, Dorothy, E., “*Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*”, 23 May 2000, at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, (consulted on 05 June 2012).

Dyżurnet.pl, "*About us*", 2012, at http://www.dyzurnet.pl/en/about_us/about_us.html, (consulted on 05 June 2012).

European Digital Rights EDRI, "*Finnish ISPs Must Voluntarily Block Access*", 8 September 2005, EDRI-gram - Number 3.18, at http://www.edri.org/edrigram/number3.18/censorshipFinland, (consulted on 05 June 2012).

Harley, Brian, "*A Global Convention on Cybercrime?*", 23 March 2010, The Columbia Science and Technology Law Review, at http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/, (consulted on 05 June 2012).

Himma, Kenneth, Einar, "*Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?*", 2005, Seattle Pacific University, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=799545, (consulted on 05 June 2012).

Internet Society, “*Brief History of the Internet*”, 2012, at http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet, (consulted on 05 June 2012).

Internet World Stats (b), “*European Union Internet Users 31 December 2011*”, 31 December 2011, at http://www.internetworldstats.com/stats9.htm, (consulted on 05 June 2012).

Internet World Stats (a), “*Internet Users in the World Distribution by Regions – 2011*”, 31 December 2011, at http://www.internetworldstats.com/stats.htm, (consulted on 05 June 2012).

Isa, Felipe, Gómez & Feyter, Koen de (Eds.), “*International Protection of Human Rights: Achievements and Challenges*”, 2006, HumanitarianNet, University of Deusto, Bilbao, at https://doc.es.amnesty.org/cgi-bin/ai/BRSCGI/International%20Protection%20of%20Human%20Rights:%20Achievements%20and%20Challenges?CMD=VEROBJ&MLKOB=25926890808, (consulted on 05 June 2012).

Kerr, K., Paul, Rollins, John, Theohary, A., Catherine, "*The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*", 9 December 2010, Congressional Research Service, at http://www.fas.org/sgp/crs/natsec/R41524.pdf, (consulted on 05 June 2012).

Paget, François, “*White Paper Cybercrime and Hacktivism*”, 2010, McAfee Labs™, at http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf, (consulted on 05 June 2012).

Pihlajarinne, Taina, "*Operaattorien estovelvollisuus puntarissa*", 2011, IPRinfo 5/2011, at http://www.iprinfo.com/lehti?action=articleDetails&a_id=927&id=56, (consulted on 05 June 2012).

Pionier CERT, "*About us*", 2012, at http://cert.pionier.gov.pl/tiki-index.php?page=HomePage, (consulted on 05 June 2012).

PPBW Polish Platform for Homeland Security, "*About the PPHS*", 2012, at http://www.ppbw.pl/ppbw/en-ppbw.html, (consulted on 05 June 2012).

Pras, Aiko, Sperotto, Anna, Giovane, C., M., Moura, Drago, Idilio, Barbosa, Rafael, Sadre, Ramin, Schmidt, Ricardo & Hofstede, Rick, "*Attacks by "Anonymous" WikiLeaks Proponents not Anonymous*", 10 December 2010, CTIT Technical Report 10.41, at http://www.ctit.utwente.nl/news/archive/2010/dec10/Attacks%20-anonymous.docx/, (consulted on 05 June 2012).

Puolamäki, Kai, "*Finnish Internet censorship*", 18 February 2008, Electronic Frontier Finland EFFI, available at http://www.effi.org/blog/kai-2008-02-18.html#how-the-censorship-works, (consulted on 05 June 2012).

Rodriguez, Katitza, "*Dangerous Cybercrime Treaty Pushes Surveillance and Secrecy Worldwide*", 25 August 2011, Electronic Frontier Foundation, available at https://www.eff.org/deeplinks/2011/08/cybercrime-treaty-pushes-surveillance-secrecy-worldwide, (consulted on 05 June 2012).

Samuel, Alexandra Whitney, "*Hacktivism and the Future of Political Participation*", 2004, Cambridge, Massachusetts, Harvard University, at http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf, (consulted on 05 June 2012).

Siewicz, Christopher, "*Nie zamykajcie stron rządowych dla anonimowego ruchu! To ograniczy nasze prawa*", 2 February 2012, Panoptykon Fundacja, at http://panoptykon.org/wiadomosc/nie-zamykajcie-stron-rzadowych-dla-anonimowego-ruchu-ograniczy-nasze-prawa, (consulted on 05 June 2012).

Shughart, William, F. II, "*An analytical history of terrorism, 1945–2000*", 2006, at http://www.springerlink.com/content/g561757858773k4p/fulltext.pdf, (consulted on 05 June 2012).

Spindler, Gerald, "*Study on the liability of Internet intermediaries Country Report - Poland, Executive summary*", 12 November 2007, at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/poland_12nov2007_en.pdf, (consulted on 05 June 2012).

Stepanova, Ekaterina, "*The Role of Information Communication Technologies in the "Arab Spring" Implications beyond the region PONARS Eurasia Policy Memo No. 159 May 2011*", 2011, Institute of World Economy and International Relations (IMEMO), Russian Academy of Sciences, at http://www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf, (consulted on 05 June 2012).

The Danish Institute for Human Rights, "*The History of the European Council*", 2012, at http://www.humanrights.dk/human+rights/europe,+enlightenment+and+rights/the+european+council/the+history+of+the+european+council, (consulted on 05 June 2012).

The Guardian, "*Taliban website under repeat attack by hackers Reuters in Kabul*", 27 April 2012, at http://www.guardian.co.uk/world/2012/apr/27/taliban-website-hacked, (consulted on 05 June 2012).

Theohary, Catherine A. & Rollins, John, "*Terrorist Use of the Internet: Information Operations in Cyberspace*", 8 March 2011, Congressional Research Service, at http://www.fas.org/sgp/crs/terror/R41674.pdf, (consulted on 05 June 2012).

Thomas, Keir, "*Sony Makes it Official: PlayStation Network Hacked*", 23 April 2011, PCWorld, at http://www.pcworld.com/article/226128/sony_makes_it_official_playstation_network_hacked.html, (consulted on 05 June 2012).

TP CERT, "*Activities*", 2012, at http://www.tp.pl/prt/en/tpcert/about_tpcert/activities/, (consulted on 29 March 2012).

Waglowski, Piotr, "*Wokół artykułu 269b § 1 kodeksu karnego*", 29 July 2005, at http://prawo.vagla.pl/node/5205, (consulted on 05 June 2012).

World Trade Organization parody website, "*WTO News*", 2012, at http://www.gatt.org/, (consulted on 05 June 2012).

Zittrain, Jonathan & Palfrey, John, "*Internet Filtering: The Politics and Mechanisms of Control*", 2008, In Deibert, Ronald, Palfrey, John, Rohozinski, Rafal, & Zittrain, Jonathan, (Eds.), Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge, MIT Press, at http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-2.pdf, (consulted on 05 June 2012).