Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

A legal dogmatic thesis with an empirical legal science methodology.

Louise Synnestvedt Jensen.19890525-1586. 2RV00E.

Examiner: Eva Schömer.
Tutor: Ann-Christine Hartzén
This essay is dedicated to my father Kjeld whom has always believed that his children could achieve any goals that they have set for themselves, regardless of where they come from on the social ladder. And to my daughter Alice who deserves the best that I can offer.
Abstract.

Cyber-criminal, terrorism and hacking is a topic discussed widely and many independent groups as for example Wikileaks and Anonymous are often taken into consideration when discussing cyber-crime. When researching cybercrime and it is important to first research the legal background as to the purpose of the creation of the internet, and to what extend state control is an issue in the matter of both cybercrime being carried out and the establishment of cyber activist groups. How shall the law be interpreted in the case of internet hacking and under what category do these fit, terrorists, cybercriminals or hackers.

Keywords: cybercrime, terrorism, Anonymous, Wikileaks, hacktivism, state control.
Abbreviation.

- ARPANET – Advanced Research Projects Agency.
- COE – Convention on Cybercrime.
- EUFRE - Charter of Fundamental Rights of the European Union.
- ICCPR – International covenant on Civil and Political Rights.
- IEEE – Institute of Electricals and Electronics Engineers.
- NATO – North Atlantic Treaty Organization.
- NSA – National Security Agency.
- OECD – Organization for Cooperation and Development.
- OIC – Organization of the Islamic conference convention.
- RCMP – Royal Canadian Mounted Police.
- SCIS – the Center for Strategic and International studies.
- UDHR – Universal Declaration of Human Rights.
- UNCT United Nations Conventions on terrorism.
- WHO – World Health Organization.
# Introduction

1.1 Problem formulation  
1.2 Purpose  
1.3 Method  
1.4 Perspective.

# Literary analysis

# Historical background.

3.1 The origin of internet usage.  
3.2 The growing popularity and development of the use of internet.

# Legal analysis.

4.1 Definitions  
4.2 Terrorism.  
4.3 Cyber-terrorism.  
4.4 Information warfare/Hacking.

# State control.

# Case study Analysis.

6.1 Anonymous.  
6.2 Wikileaks.  
6.3 Estonia  
6.4 Comparison.

# Conclusion

# Summary.

# Appendix

10 Bibliography.
1. Introduction.

Over the past decade terrorism has been very much in focus both on a governmental level and on a private level. Since the attack of the twin towers in New York on the 11 of September 2001 national security has been on their toes to detect any form of terrorism. What seems to have grown simultaneously with terrorist attacks the past decade is cyber terrorism, cyber terror is meant by hacking computer systems for political and or social purposes, with the aim of destroying a state’s infrastructure or leakage of classified information that could harm the state. In the case of cyber terrorism hacking it is discussed to be a vital part in the sense of hacking to access information that could be vital for a state to keep classified. Some however claim that hacking is not cyber terrorism, hacking is an innocent hobby according to some scholars and these are only exercising their freedom of expression that is laid out in article 10 of the ECHR.

Freedom of expression and accessing information is a part of the European Union law and shall be respected however there are circumstances that may put restrictions upon this. The issue is when there shall be restriction to rights and freedoms and how to compare the rights to one another for the purpose of determining which is the most important right or freedom that needs to be upheld in the given situation. This shall be examined throughout this thesis, how law shall be interpreted when put up against another law, which one shall be applicable and which shall be restricted.

1.1 Problem formulation.

As mentioned these cyber groups such as Anonymous are being defined as being both cyber-terrorists and public protectors depending on whom one talks to which is the issue at hand, in what category shall one put these? There are many categories for these groups;

- Cyber terrorists.
- Cyber activists/Hacktivists.

---

These many categorizations is the big issue, even though one says they are activists another may say that they are terrorists. However the common belief within these hactivist groups is that the assessment of information through the internet and sharing this with others is not terrorism; it is a mere case of people freely using their right to information.

The right to information is given through the ICCPR article 19(2) and in the European convention on human rights article 10(1). These articles all state the same that: “everyone has the right to seek, receive and impart information through any media and regardless of any frontiers”3. All but one has no restrictions; only in the European human rights convention can the state restrict this right if it is perceived as threatening to the national security.

The questions to be asked to examining and distinguishing hacktivists and terrorist from each other are as follows:

- How shall the different categorizations of cyber terror be interpreted in accordance with law?
- Are the reasons for the groups being formed oppression of social and or political means?
- What legal restrictions are there to the right to seek and share information?

These questions are important to answer to come to some sort of determination of whom of a terrorist and who is not in a legal sense. The problem that may occur however is the line between rightfully using ones fundamental freedoms that is set forward in the convention of European human rights and fundamental freedoms. The issue of interpreting the laws and freedoms set forward in European law in the manner that they should be interpreted; their range and rightful purpose and to determine when they are being used unlawfully. These questions shall therefore be examined through the European Union law, with few examples from international law to get a broader view upon the issues of interpreting law in the case of cybercrime.

---

1.2 Purpose.

The aim of this thesis is to form a legal discussion upon the topic of cybercrime and to discuss different cases of possible cyber terror. By examining the legal differences between cyber terrorists, hacktivists and hackers the legal definitions and European laws a clear understanding of the interpretation of the laws should met its purpose in the end.

1.3 Method.

This essay will consist of a legal dogmatic and an empirical legal science method. The legal dogmatic method is used to discuss and analyze the legal documents describing the issues of cybercrimes, as to how law is set forward in the different treaties and convention and how they shall be interpreted in this case. The empirical legal science method is a method not usually used in legal research papers due to the way that it treats the legal source material. Legal source materials are most often treated in a dogmatic manner, in an empirical legal science method however the legal source materials are mixed together with the empirical source materials. This integration of the two makes the legal documents as much part of the empiricism as the empiricism itself. Together they tell the story rather than only examining the legal source material and doctrines, to analyze their meaning and validity in a specific issue. This as opposed to how the legal source materials would most usually be treated if it had been in a more dogmatic method of writing.

There will be given a legal background of the intended use of the internet, how it has developed and the growing popularity throughout the years. An examination of state control shall also be included upon the issue of hacktivist groups being oppressed, and for the purpose of determining why groups such as Anonymous are established.

This shall to some extend show how and why these groups exist to begin with, as mentioned it shall be done within limitations. The essay will focus on one case of cyber activism/terrorism and determine whether or not they can be categorized as being cyber terrorists, the internet group Anonymous is the main topic of discussion. Anonymous is a current issue that many states take very seriously since that they are often mentioned in in connection to cybercrime.

Three cases will be examined and compared with European laws and legislations to give an example of how the laws can be applied and interpreted. The four cases are:
These three will then be briefly examined and then compared with each other and through European laws they shall be interpreted for the purpose of distinguishing the terrorists from the activists

1.4 perspectives

The perspective taken throughout the essay will be a social perspective in order to show the different sides to the subject of cybercrime, as for what purpose a hacktivist may have to justify their actions. And to see the relationship between law and social phenomenon’s that occurs in these cases.

2 Literary analysis.

- Schools of thought on cybercrime.

There seem to be many disagreements in the field of determining what should be define as cyber terrorism and if it even exists. Some argues that it does not and some argue that is the threat of the future terrorism, on this subject there are two schools of thought on this topic. The first believes that cyber terrorism is real and that it is an ominous threat to the future, and are of a more holistic point of view and therefore sees the relationship between physical security and cyber security as being adapted into international terrorism.

The other school of thought seems to think that it is over exaggerated and argue that it is a mere case of hacking or information warfare. They disagree with using the term terrorism to define hacking and information warfare since that they see these acts as harmless and not imposing fear, harm or death. This school of thought is self-proclaimed experts in the field,
neophyte media commentators or analysts as they call themselves. They are of the opinion that only the traditional terrorism is the only terrorism that is legitimate.

Dr. Irving Lachow, Professor of Systems Management at the US National Defense University in Washington, D.C. however disagrees with these theories of computer hackers not being terrorists. There is clear evidence that terrorists have used the internet to gain information that helped them launch their attacks, however their have never been any documented cyber-attack against the US.\(^7\) As it can be seen there are many disagreements on this subject, because of the many disagreements the difficult task is to pinpoint exactly what is to be perceived as cyber terrorism and mere hacking. Though evidence point towards cyber terrorism many states have not been subjected to any, at least the US claims to have never been the victim of cyber terrorism.

However other information could prove otherwise in the case of the US. Though the US may never have been subjected to cyber terrorism other states have, Estonia was in 2007 victims of a three week long cyber-attack that was so severe that it disabled the network systems and threatened the states infrastructure. This is one clear example a state being subjected to cyber-terror; however it proved hard to find any on whom to place the blame\(^8\).

There are many limitations of being able to come to a conclusion of whether or not hacking and cyber terrorism is the same, according to the information above there are so many disagreements on the matter. But the foremost important limitation to defining the problem lies in the fact that there not even is a universal definition on what a terrorist is\(^9\). If the world cannot come to an agreement on defining a so called regular terrorist how shall they then be able to reach an agreement on what cyber terrorism is?


Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

Louise Synnestvedt Jensen. 19890525-1586. 2RV00E

One could then just as easily claim that hacking is not an act of terrorism as supported by scholars, that hacking is not hurtful in the sense of causing harm, posing danger or deaths\textsuperscript{10}. So in this case one could claim that Sarah Palin is wrong Julian Assange is not a terrorist, though his acts may not have been legal it should not be defined as terrorism. One could say that Julian Assange had simply used his rights to seek, receive and impart information through any media and regardless of any frontiers, which is stated in the Universal Declaration of Human Rights article 19\textsuperscript{11}. And if so this would be the case of any hackers, they are simply seeking information as in accordance with their rights. Hacker may be violating people’s privacy but to access information which is also their right.

3 Historical Background.

3.1 The origin of internet usage.

Internet and computer science was a result of visionary thinking from the early 1960’ies, the potential of sharing information on research and development in scientific and military fields. This was the main purpose of creating the internet, for scientists and governments to have a communication network to share information on. In 1965 the first computer was connected through a dial-up telephone line; however this was not sufficient enough for a communication network due to overload. In 1969 however the problem was solved and the internet also called ARPANET became stable and sufficient. The ARPANET was created for the purpose of experts, scientists, engineers and librarians to catalogue information and to share this with the governmental institutions\textsuperscript{12}.

This brief introduction to how internet came to be created shows that the intended use was for the governmental institutions to be more organized and to be more efficient in information sharing that could be vital for the state. Stephen Cass of the IEEE describes the intentions the


internet use as being a web fountain of science. The intentions of the internet were and are to create a platform for information and data to be analyzed and structured, in order to make sense of it and to share this with other scientists and analysts. This is for the purpose of being as updated as possible of the on goings of the world and to be more aware of future issue that may arise.\(^\text{13}\)

In the 1960ies and 1970ies computer crimes were not as common as they are today; this was mostly due to the fact that not many owned a computer. At this point in history computer was mainly a tool for governmental and scientific institutions, even though these institutions were amongst the few whom used computers crimes did occur and laws were needed to help courts judge in these cases. This became most apparent in the 1970ies when one of the most known computer crimes happened. In 1971 Jerry Schneider ripped of the Pacific Telephone and Telegraph for more than 1 million.\(^\text{14}\) Schneider had through a few years obtained printouts from the company that possessed detailed information regarding the company policies and staff information. Schneider posed as a staff member of the company to retrieve even more information, with this information Schneider ordered through the company name computer equipment worth approximately 30 000 dollars. Schneider continued this scam for a brief time during which he had earned more than 1 million dollars.\(^\text{15}\) This may however not be a direct cybercrime as we know it today but it is the most known case, along with Schneider’s bank robbery live on CBS 60 minutes. In 1976 Schneider appeared on the show CBS 60 minutes on a segment of computer criminals during which he robbed a bank live on television. During the show Schneider wanted to show the audience how easy one could rob a bank with only a phone connection and credit card information. He used the credit card information of the host and within minutes the credit limit was raised from 500 dollars to 10 000 dollars, all with a simple phone connection and the knowhow. Schneider could have walked out of the studio

---

\(^{13}\) Cass, Stephen. IBM WEB FOUNTAIN. A Fountain of Knowledge 2004 will be the year of the analysis engine IEEE Spectrum Online (Jan 4, 2004). Internet news.  
http://www.websearchguide.ca/netblog/archives/001741.html

\(^{14}\) Kabay, M. E. PhD, CISSP-ISSMP Program Director, MSIA School of Graduate Studies, Norwich University. A Brief History of Computer Crime: An Introduction for Students Pp. 9  

http://www.bookrags.com/research/jerry-schneider-omc/. Jerry Schneider from Outlaws, Mobsters and Crooks. ©2005-2006 by U*X*L. U*X*L is an imprint of Thomson Gale, a division of Thomson Learning, Inc. All rights reserved.
with the 10 000 dollars however he returned the credit information as it was, since that this was only to show the easiness of computer crimes. Schneider later went on to become a computer security consultant due to his skills and knowledge\textsuperscript{16}.

3.2 The growing popularity and development of the use of internet.

The internet has since its creation in the 1960’ies developed massively and has become more and more popular. In the 1990’ies the US announced a new product for computer software called marketplace, this contained information such as names, addresses and spending habits for more than 120 million American consumers. This raised many new issues in the US concerning individual privacy, this could be bought as CD-ROM and contained further information from check out scanning’s and government files. Privacy advocates saw this as having gone too far in modern techniques and called for privacy protection and the product was later cancelled\textsuperscript{17}.

This is an early example of how the internet were to be used in the future and still it can be seen that it is used for the purpose of “spying” on individuals as well as groups. What has been learned over the years is that the technology can teach us a lot and be used for many purposes as its original intentions. However as quickly as we can use the technology for greater purposes it can turn upon us at the same speed and be used against us. It has now become more of a commonplace for people to view the new, share their different point of views and for social protests to happen\textsuperscript{18}.

The World Wide Web has become a threshold for dominating ones power, such as the case of the software called marketplace mentioned above. Many organizations and cooperate institutions show their power on the internet to gain supporters and to spread both news and

\textsuperscript{16} Gale, Thomas. Jerry Schneider. Active: Early 1970s. \url{http://www.bookrags.com/research/jerry-schneider-omc/}. Jerry Schneider from Outlaws, Mobsters and Crooks. ©2005-2006 by U•X•L. U•X•L is an imprint of Thomson Gale, a division of Thomson Learning, Inc. All rights reserved.


hidden propaganda\textsuperscript{19}. These actions of domination raise many concerns and protests, groups of individuals then protest on the internet for the purpose of others to see the corruption within the organizations and to petition that they stop. These are early cases of cyber activism and they have throughout the years only grown together with the expanding use of the internet\textsuperscript{20}.

The social movements and activist groups began to come in from the streets instead to protest on the web, for on the web they could reach more people, become more involved with other likeminded movements and faster spread the word of their believes. Though it may seem that the use of the internet became a great tool for the civil individual to gather information it became a problem for law enforcement, many conflicts appeared in discussing internet as a right in a democratized world. Many felt violated by the non-privacy on the web as well as being forced into participating, and the need of law implementations was seen needed\textsuperscript{21}.

The popularity has only continued to grow alongside the development of new technologies to make it more sufficient. The usage of the internet has rapidly advanced much due to globalization and democracy; we have all become more connected through blogs and chat rooms etc. Some of the more popular uses of the internet now is E-mailing, news surfing and shopping online. These have become everyday tasks for the civil individual to wake up and check their e-mail account and perhaps order a new pair of shoes. This virtual environment makes people more comfortable than going out to crowded stores for example and it gives shopping consumers the possibility to compare prices and qualities from the comfort of their own home.\textsuperscript{22}

There is an ability to communicate with people from other nations through e-mail and through blogging; the post office has become more inefficient in the sense of how fast you can reach another person. Communication is one of the most important aspects of life and the internet


Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

Louise Synnestvedt Jensen. 19890525-1586. 2RV00E

has opened up for a wider range of communication for more people, this aspect of internet use has become an important tool for businesses and governments.\textsuperscript{23}

The schools systems have benefited from this since computers and internet have become a help for student to better access information that could help their studies. Teens are perhaps the group of people whom use the internet the most, many sees this as an escape from reality, a place to meet new friends, game playing and a place to explore the many options of the world. It has however also become the place of crime, since that you do not have to type in your personal information many often act anonymously because of this many choose to be more straight forward with others which can result in internet harassment\textsuperscript{24}.

The use of internet can then be seen as having contributed to the advancement of society and more people turn to the internet every day to research new options and possibilities. Perhaps people rely on the internet too much in today’s society however it is a form of freedom that shall be offered, though this being seen as a right and a freedom for people to be able to use the internet freely laws and restrictions do follow the usage of internet consumption.

These are laws as can be found in the constitutions of each country and often contain laws to protect privacy, prohibit any illegal use such as harassment, propaganda, exploitation etc. These laws are not only set forward in the countries constitutions but are also included in both international and European law\textsuperscript{25}. One example is the COE convention on cybercrime article 4 (See appendix)

According to this article the states are then individually responsible for the crimes carried out on the web in their own states, except the COE other law such as patent law, copyright law and trademark law also play a part in the issue of cybercrimes. These are the law of the internet in the first hand and if these are violated severely then the courts should look to the COE convention for further guidance in determining punishment\textsuperscript{26}.


however in some cases they might need the cooperation of another, but do the state perhaps control the web too much or do the truly enforce the right of free expression that is to be promised through the human rights. How far freedom of expression/speech stretch in the sense of seeking and mediating information on the internet shall be examined further in the next chapters. Also to be examined is how articles can contradict each other in some cases and what special circumstances and restrictions there can be to these.

4 Legal analysis

4.1 Definition.

To examine if it is the act of terrorism/cyber-terrorism it is important to understand what the different terms are in order to distinguish them from each other and define the crimes.

4.2 Terrorism.

The council of the European Union provides a definition in their council framework decision of 13 June 2002 on combating terrorism. This definition has been written through a mix of different declarations and conventions; amongst them is the treaty of the European Union.27

The framework decision preamble (2) states that: “Terrorism constitutes one of the most serious violations of those principles. The La Gomera Declaration adopted at the informal Council meeting on 14 October 1995 affirmed that terrorism constitutes a threat to democracy, to the free exercise of human rights and to economic and social development.”28

This is the European definition on terrorism and it is a definition that is based upon the conventions of the treaty of the European Union. Since this framework decision of 2002 the treaty of the European Union have been updated in 2010, however the articles that used to


define terrorism are the same. (See appendix)\textsuperscript{29} There are many conventions and declarations whom discuss the action that shall be taken upon these terrorist offences, amongst them are the Council of Europe Convention on the Prevention of Terrorism\textsuperscript{30} and the European Convention on the Suppression of Terrorism\textsuperscript{31}. These together are what the European Union use in the combat against terrorism and shall be discussed further in this thesis.

\subsection*{4.3 Cyber-terrorism.}

As of now there is no European or international accepted definition upon the term of cyber terrorism. Therefore the framework decision on combatting terrorism will apply here as well, article of the framework decision refer to terrorist offences of the internet as well as terrorist offences that are done manually so to speak\textsuperscript{32}.

Article 1, 1(d).

\begin{quote}
“causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;”\textsuperscript{33} (see more in the appendix.)
\end{quote}

This definition explains the use of an information system to harm governmental and non-governmental institutions. Therefor this together with the definition on terrorism shall be used


Terrorism or hacking? A law interpretation on the concept of cyber terrorism.  

Louise Synnestvedt Jensen. 19890525-1586. 2RV00E

to define a cyber-terrorist. Also the COE convention article 4 that explain data crimes can be placed under the category of cyber terrorism

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.  

These together then created a picture of what cyber terrorism is about.

4.4 Information warfare and hacking.

Many call themselves hackers today based on the grounds that they are somewhat skilled in computer techniques, if it were only about hacking ones email account we could all be classified as hackers. The term “hacker” however was originally meant by being a very gifted programmer and now one see the term of a hacker in a more negative context, as people whom invade our computers and accesses our information.  

Information warfare itself does not have either an accepted EU or UN definition. Just like the term cyber terrorism the council framework decision and the COE articles shall apply here as well since that it describes computer crimes and data interference.  

(See appendix)

Over the years hacking has advanced and a hacking language has been developed, hackers are as stated above very gifted people whom understand the complex language of the computer science. A true hacker according to the many definitions enjoys the work of cracking systems

---

and accessing information from others, and understands the weak point in the systems. The entity of their work is data interference which is why the article above can be very much applicable when defining hacking and information warfare.\(^{39}\)

There are many examples of systems being hacked to reach information and in some cases to leak information; one example is the case of wikileaks. It is stated that Julian Assange had a contact in the military that downloaded the classified documents and handed them over to Assange and wikileaks. This was by the US as a kind of political attack that revealed their deepest darkest secrets of which could possibly damage the state in the long run.\(^{40}\) Or a more recent case of hacking is the December 2011 hacking of the UN computer system, the notorious hacking group called Team poison hacked their system and accessed password information to different UN organizations such as; The OECD, UNICEF and the WHO.

Team poison claims this to be a protest against "the bureaucratic head of NATO used to legitimize the barbarian capitalist elite"\(^{41}\) the attack on the UN organizations has forced a new revision of censorship and access of the internet in focus.\(^{42}\) This however could also be called an act of information warfare; the terms hacking and information warfare is closely linked since those both are in pursuit of accessing information and share this. Information warfare however is discussed to be somewhat more severe than normal hacking. The term information warfare is an old military term, first known as electronic warfare and is dated back to WWII; this was used during the war by the Nazi’s.\(^{43}\)

The Nazi’s use electronic surveillance, inquired secret information through that times electronics; this is one of the first known uses of information warfare. Information warfare is

---


described as warfare consisting of both offensive and defensive operations against resources and its main purpose is to exploit and control information⁴⁴.

5 State control.

With the great usage of the internet comes responsibility such as law enforcement both for the protection of internet use and to restrict this as well. Internet usage falls under the right of free speech and freedom of expression which can be found in the articles below together with the articles on restriction, protection of data and non-discrimination.

- Article 1 & 19.2 of the International covenant on civil and political rights (ICCPR)
- Article 10 & 14 of the European convention for the protection of human rights and fundamental freedoms. (ECHR)
- Article 8 & 11 of the Charter of fundamental rights of the European Union (EUFR)⁴⁵.

(See Appendix)

These articles state that we hold the right to receive and impart information without interference by public authorities and regardless frontiers. And these should then give the civil individual the right to freely seek any information they may want, however there are laws to ensure people of their personal protection. One of these can be found in the Charter of fundamental rights of the European Union article 8 that states the protection of personal data⁴⁶, this article can also be found in the individual states own laws and constitutions.

There are many controversies of the topic free speech/expression on the internet and when it may or may not be restricted, the state may not interfere with the right nor may they propagate any governmental materials into the web media that will indicate any form of state control or interference. Only in few cases according to William Fisher is fitted to make restriction onto the usage of the internet that can be approved by both the public and other institutions. These circumstances and restriction William Fisher has found through examining the first


amendment of the US constitution. These restrictions may be made during these circumstances:

“1. Speech that is likely to lead to imminent lawless action may be prohibited.

2. "Fighting words" -- i.e., words so insulting that people is likely to fight back -- may be prohibited.

3. Obscenity -- i.e., erotic expression, grossly or patently offensive to an average person, that lacks serious artistic or social value -- may be prohibited.

4. Child pornography may be banned whether or not it is legally obscene and whether or not it has serious artistic or social value, because it induces people to engage in lewd displays, and the creation of it threatens the welfare of children.

5. Defamatory statements may be prohibited. (In other words, the making of such statements may constitutionally give rise to civil liability.) However, if the target of the defamation is a "public figure," she must prove that the defendant acted with "malice." If the target is not a "public figure" but the statement involved a matter of "public concern," the plaintiff must prove that the defendant acted with negligence concerning its falsity.

6. Commercial Speech may be banned only if it is misleading, pertains to illegal products, or directly advances a substantial state interest with a degree of suppression no greater than is reasonably necessary.”

Except from these restrictions upon the usage of the internet it can be seen as a public place with no gatekeepers; however some form of control does exist on the internet. Though these are found the US constitution they are implemented in European law, Article 10 (1) of the ECHR explains the freedom of expression/speech and how they shall be no restriction upon this freedom. However the same article, sub article 2 (see Appendix) does lay out that in some cases there may be put restriction to the freedom of speech/expression. What William Fisher lays out in his argument upon when to restrict is supported by article 10 (2) of the

---

Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

An extra control system has been created through non-legal regulation and sovereign law; this is the system of the IP address. The IP address links each individual to their computer and to all that they do on the internet, if any illegal actions are carried out by an internet user they can be traced through their IP address and taken to justice. This has come with modern technology and is the main source of holding people responsible on the internet.

The British scientist Sir Tim Berners-Lee is of the opinion that people need to be protected against such software that can monitor a person’s move on the internet. People’s personal data need to be protected for the purpose upholding the privacy rights and for the consumers not to feel watched or abused on the web. Sir Tim whom is the inventor of the web warns people of this and urges them to protect any personal data that can be found or hacked into by “big brother”. Sir Tim states that even what may seem as harmless web pages such as Facebook may be part of the big brother system to monitor people’s internet habits, not everything is what it seems which is why consciousness and carefulness is a needed factor when surfing on the web.

Through this big brother system laws are easily violated, article 8 of the EUFR– protection of personal data (See appendix). Peoples feel their rights and freedoms being violated for no greater purpose other than what seem like the state wanting to check up on people’s internet usage for their own private use. The claim is that the control and surveillance are to control the crimes being carried out on the web on a daily basis, people being scammed others.

---

Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

committing fraud, the list is endless. However many intrude upon people’s privacy every day to check up for such occurrences. This violates article 8 of the EUFR because the personal data is not being handled rightfully for a specific purpose such as credit check by a bank, this would be a rightful use of personal data according to the article. Article 8 of the EUFR in itself is to protect detailed information about personal individuals, such as social security numbers, credit limits, and for an employer to make background checks before hiring. These kinds of personal data are handled by many, both over the internet and other information sources. As to how far one can go before this article is being violated is a question of interpretation. This article is however not recognized as a right in the ECHR framework which is why the interpretation can be somewhat fuzzy, and therefore video surveillance for example can be legal under some circumstances as well as background checks etc.

Sharing political views openly on the internet is part of freedom of expression/speech that is explained in article 10 of the ECHR (see appendix). Though free speech/expression is ensured under this article, sub article 2 however lays out some restrictions to how freely expression and speech can be shared. The article explain the circumstances of which there can be put restriction upon it, when it is concerning national security, threat of the democracy, morals values etc. of the state then restrictions can be made. This can also be found in similar text in the ICCPR article 19 (see Appendix).

Activist groups such as Anonymous seem to exist because of the internet surveillance; their existence is a product of oppression. These groups feel socially oppressed by the states, due to

governments trying to control the ongoing of the internet. These groups are said to expose corruption and bring down criminals on the web without any frontiers to their individual statuses. The main reason for exposure is for the people or institutions to be guilty of some kind of corrupt behavior towards the public.  

Individual people and groups on the internet are being called terrorists and extremists by the states due to them spreading their political views and expressions of the state on the web. In their own mind they are simply intervening in political and social affairs, these groups and individuals are engaging in illegal activities of internet transmission and do often walk the fine line between freedom of expression and illegal actions. However it can be argued that these groups are using their freedom of expression/speech as laid out in European law; these groups are then being targeted by the state as being cyber criminals. The definition upon cybercrime and information warfare, COE articles 1 & 4 (see appendix) is explained as data being transmitted and misused by other non-appropriate individuals/groups. This is in a law perspective valid ground for defining such groups and individuals as for example Anonymous as criminals. Since that much of the information that is being spread on the internet is political opinions and other social comments that are being presented together with exposure of states. When states then oppress these groups from spreading these kinds of information it can be argued to be in violation of article 14 of the ECHR (see appendix) that explains the concept of non-discrimination, within this article it is explained that no one shall be discriminated against due to political opinions. Groups such as Anonymous can therefore feel discriminated against on these grounds, and their right to self-determination can also be in danger for these specific groups. They raise their political opinions to the public to make them aware of certain situations and use their right of free expression/speech, to expose and fight corrupted governments and governmental institutions. They seek and impart information as in

---

62 Anonymous analytics – Acquiring information through unconventional means. About.  .  
http://anonanalytics.com/  
65 Anonymous analytics – Acquiring information through unconventional means. About.  .  
http://anonanalytics.com/  
accordance with freedom of expression/speech article 10 ECHR (see appendix), and are then being subjected to criminal charges based upon their political fight they are being discriminated against and their right of self-determination is being questioned. The ICCPR article 1 (see appendix) explains individual rights to freely determine their political status, which they then choose to spread through their freedom of expression.

Though there may be a feeling of discrimination and limited self-determination for these hacker groups, article 10 of the ECHR as stated before does have restriction to how far freedom of expression can be stretched and when there is other laws being violated when using freedom of expression to its fullest. In article 10(2) ECHR there is mentioned several circumstances for restriction, amongst them are the protection of the reputation or rights of others and preventing the disclosure of information received in confidence. These 2 are assured in the ECHR articles 8 and 14. EUFR articles 8 and 21. (See appendix) This article shall all be respected when it comes to freedom of expression/speech since that they concern the private individual, ethnical group’s etc. one thing that may happen when exercising freedom of expression is that you violated these other rights that shall be guaranteed in European law.

One example is the CASE OF MOUVEMENT RAËLIEN SUISSE v. SWITZERLAND. The issue in this case was that social/political groups had made a poster campaign of an atheist form. These groups believed in science and evolution. The text on the posters said “Science at last replaces religion”. The public saw this as offensive and as discrimination of religion; the case was brought to the European court of human rights that decided to ban the poster campaign. Not because the content was unlawful but because article 10(2) ECHR states that restrictions may be made upon the freedom of expression if it is harmful to health and morals and public interests. And therefore the European court of human rights ruled to ban the posters.

---

This case is one example of when excessing freedom of expression to its fullest can have the negative effect of being in violation of other rights. In this case the restriction was based upon public interest and the harmful effects it may have had. In other case there can be issues of discrimination against beliefs such as religious, political etc. these shall be taken into consideration since that they are ensure in the European law and shall be respected.

What can be seen as constituting people as cybercriminals are that they primarily engage in illegal transmission on the web, and in that way they are engaging in information warfare and other illegal activities, in the category of terrorists and extremists then the groups Anonymous seem to fit according to many states.

6 Case study analysis.

In order to analyze and make a distinction between terrorism and activism I have chosen three cases

- Anonymous.
- Wikileaks.
- The three weak cyber-attacks on Estonia.

These three all differs and resembles each other because they all have elements of terrorism and cybercrimes. First I will present each case separately to discuss the background information and what has happened in each case. This shall be done through examining the cases together with the appropriate articles of European Law. Then a comparison shall be drawn on these three cases to make the differences and similarities clearer.

Anonymous.

The hacker group Anonymous according to themselves and their own introduction web page anonanalytics.com also called anonymous analytics an analytics group with the main purpose of promoting access to information. They encourage free speech, access to information and


transparency. The core values of Anonymous are also part of the fundamental freedoms of European law articles:

- Article 11 of the EUFR.
- Article 10 (1) of the ECHR. (see appendix)

Anonymous was created as a decentralized network of individuals for the purpose stated above and has exposed organizations such as the church of scientology, they’ve supporting the anti-corruption movements in both Zimbabwe and India and providing the Iranian people with secure platforms to critique their governments without punishment.

Anonymous provides the public with investigations of governmental institutions and companies that may be corrupt and or oppressive to the public, and has therefore shifted their transparency from a political level onto a more corporate level. According to their introduction web page there are a team of competent analysts and investigators whom acts as a public protector.

Also freelance writer and journalist Steve Mansfield-Devine supports what is stated on Anonymous web page, in the book Network Security he has written a chapter on hactivism: assessing the damage, where he describes different hacker activist groups. Amongst them is anonymous and their origin that started with the exposure of the scientologists. The involvement of Anonymous in their “coming out into society” so to speak involved so called “Anons” gatherings in street protests, most often wearing the infamous Guy Fawkes mask as an icon of the anonymous group. This was the threshold for Anonymous and they gathered many followers after these protests and exposing the church of scientology. Through this Anonymous had established a new form of anarchic wit including important video displays on the internet containing the so called truth about a specific topic.

---

After their big break Anonymous went a little narrower and attacked both movie and music industries for their pursuit of file sharers, this is called operation payback which has never been finished due to the fact that the pursuit of file sharers continues. One can only see that Anonymous dislikes the concept of copyright and instead seeks transparency in all areas. They can be much compared to wikileaks, however with better anonymity and strategies for their actions.78

Anonymous has instead of being seen as an activist group, been perceived as a cyber - terror group whom takes down governmental and non – governmental organizations for the purpose of destruction. General Keith Alexander, director of the NSA claims that hactivist group Anonymous could bring down power grids (Electrical utility distribution system that distributes power to consumers on the internet) and through that cause a lot of damage. He therefore sees these hactivist groups as a threat to national and international security in the long run and causes a so called “digital cold war”.79

By this Anonymous is then perceived as a cyber-terrorist group, perhaps not in those exact words however that is the overall statement. The NSA and other governmental and non-governmental institutions keep their distance from them for their own protection, however though they seem to pose such a threat to these institutions one cannot deny the good they do. The recent activities of Anonymous include the exposure of a large scale pedophile ring on the internet called “operation darknet”. They hacked a closed network used by pedophiles to share child pornography on the web and released over a thousand usernames and other information about the users of the network.80 Other activities or operations has consisted of encouraging people to modify copies of the manifest written by the Norwegian mass-murderer Anders Breivik in order to both ridicule his ideology and for the purpose of the manifest to never be retrieved on the internet as he wrote it. This operation is called


“Unmanifest” which is an attempt to prevent other people from sharing his ideas and thoughts and causing the same pain and sorrow as he did\(^{81}\).

Anonymous according to their web page claim to be a protector of public interest\(^ {82}\) and are only acting in accordance with article 11 of the EUFR and article 10(1) ECHR (see appendix)\(^ {83}\) which explains the freedom of expression/speech. Though this is a freedom that all should be able to enjoy there are restrictions to this that can be applicable in this case, article 10(2) ECHR (see appendix)\(^ {84}\) clearly states that freedom of expression/speech may be restricted if necessary if this is in conflict with other rights and if it is harmful to the state.\(^ {85}\)

As Anonymous explains on the web page their main aim is to help the public and expose corruption\(^ {86}\), by exposing corruption of governmental, non-governmental institutions and private people. It is shown that they hack their way into the system to retrieve information of the institution or individual in question\(^ {87}\), this is a violation of article 8 ECHR (see appendix) protections of personal data\(^ {88}\). Though in the case of exposing the pedophile ring the intent


\(^{82}\) Anonymous analytics – Acquiring information through unconventional means. About. http://anonanalytics.com/


\(^{88}\) Eriksson, Maja K. Mårsäter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008
was to protect young children and put an end to the pornographic images\(^89\) it is still a violation of personal data and article 10(2) ECHR is applicable in this case.\(^90\)

### 6.1 Wikileaks.

The case of Wikileaks and Julian Assange was a case of information leaking; Julian Assange got a hold of classified military documents containing information of American kill squads, killing civilians. He was said to have gotten these documents from private first class Bradley Manning, an analyst in the military. Bradley had passed on these documents to Assange whom later posted them on Wikileaks for all to see\(^91\). The response of the American state was that this leak was a threat to national security and could have consequences of being seen as a vulnerable state by the rest of the world and therefore open to defeat\(^92\).

This was threatening state security and it was an act of treason and possibly terrorism. The public did not see Assange as a terrorist and felt that the information revealed was not a surprise. Timothy Garton Ash a historian commented the case of wikileaks just as the public and said: “Arab’s don’t like Iran? The Russian government is corrupt? Go on astonish us, you’ll be telling us next that the pope is Catholic”.\(^93\) This comment shows that wikileaks did not astonish many other than the governments.

Though this is not a case of a hack attack here it can be discussed that Julian Assange retrieved the information as in accordance with article 10(1) ECHR freedom of expression/speech (see appendix) it is a clear violation against article 10(2) ECHR

---


\(^90\) Eriksson, Maja K. Mårsäter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008


restrictions to freedom of expression/speech (see appendix). The documents that were leaked were of military status and were confidential and therefore it could easily be threatening to national security and the state democracy which is conditions for restricting freedoms of expression/speech.

6.2 The three weak cyber-attacks on Estonia.

In 2007 Estonia suffered a severe cyber-attack that disabled the Estonian system networks, the sites belonged to political parties, media and business communities among others. The Estonian infrastructure was threatened by this cyber-attack and the prime minister of Estonia suspected that Russian might be behind the attack.

The government closed down sites during the attack to prevent further damage on the state, the defense ministry of Estonia suspected this to be terrorist activities and for three weeks Estonia suffered under the attack. NATO was involved to investigate the attack; NATO shipped some of their cyber-terrorism experts to help Estonia get their electronic defense system up and running.

Determining guilt upon Russian involvement in the cyber-attack has proven to be difficult; the Estonian officials claim to have proof that some blame can be placed upon Russia. They claim to have found trace of evidence to Russian computing centers and the fact that many of the scripts sent as viruses were in Russian. However the Russian government denies any...
involvement in the attacks and has refused any cooperation in tracing the source. NATO has however not found any specific proof of the involvement of Russia, and states that it is depending on the actors involved in the attack how to define the attack and if it is cyber terrorism, cyber warfare etc. Article 4 of the COE (see appendix) explains data interference as damaging, deletion of data, alternation of data etc. and article 1, 1(d) of the council framework decision (see appendix) explains cybercrime as causing extensive destruction to infrastructure, data systems and public facilities. The attack on Estonia is then clearly a case of cybercrime and possible cyber terrorism.

### 6.3 Comparison.

These 3 cases in their similarities and differences all have indications of both cyber terrorism and hacktivism.

In the case of Estonia the network systems of various political parties and businesses were attacked for the purpose of disabling them, which the hackers succeeded to do. During three weeks the attack went on and was targeting the infrastructure of the Estonian state. The COE article 4 and the council framework decision article 1, 1(d) (see appendix) explains what cybercrime is and how it shall be perceived. This attacked cause serious harm to the states national security and was threatening to their infrastructure which, according to these articles is a cybercrime offence and cyber terrorism can be an applicable classification in this case.
Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

Luckily the attack was stopped before it became too severe to handle, though it had damaged enough of the state’s security settings. Wikileaks and Anonymous however are the two cases who have the most similarities when it comes to categorization. Wikileaks with help from a military Sargent with access to classified information hacked the military network to access these military files and other classified information about the war on terrorism and leaked this to the public for the purpose of awareness. The governmental response was as mentioned that this was an act of terrorism itself and that Julian Assange whom were responsible should be tried there by. This may very well be a case of terrorism, Julian Assanges actions posed a threat to the democracy and national security of America which according to the council framework decision is defined as being terrorism. In the case of Anonymous the same pattern can be found, Anonymous main aim as mentioned is to aid anti-corruption movements, expose crime and corruption and to work as a public protector. Anonymous then just as in the case of wikileaks access information that they share with the public to raise awareness and to promote free speech and transparency. Though the Sargent had access to the files that wikileaks had leaked it do fall under the category of hacking, due to the fact that the information was misused as in accordance with the COE article 6,1(see appendix). And though these 2 cases do have similarities of accessing information the difference lies in the content of the information as to what can be defined as terrorism and violation of personal data.

Wikileaks is then to be categorized more of committing information warfare and cyber terrorism than Anonymous due to the damage of the leaking. The information that was leaked by wikileaks was seen as being very damaging to national security and could possibly pose a threat to national security which according to Article 2 of the Convention on Cybercrime is defined as terrorism.

---

threat to the US if used by other nations\textsuperscript{112}, as described in the COE and the council framework decision (see Appendix)\textsuperscript{113}, \textsuperscript{114}. This is can be identified in both the definition of information warfare and terrorism; this is why wikileaks can be on the line between using free speech/information and information warfare\textsuperscript{115}.

Anonymous may also be balancing that fine line as wikileaks are, however it seems that Anonymous are firstly more organized than wikileaks and has a stronger main purpose than many other cyber groups. From the Anonymous introduction web page the sole purpose of the group can be seen very clearly, they promote freedom of speech, access to information and transparency. These are clear indicators of human rights activists on the internet, freedom of speech/expression and access to information are all laid out in article 10 ECHR and article 11 EUFR (see appendix)\textsuperscript{116}. These rights are some of few that are part of the fundamental rights and freedoms which means that they shall be ensured, however though article 10(1) ECHR shall ensure freedom of expression/speech sub article 2 can restrict this as well is freedom of expression is in contradiction to other rights and if it is threatening to the state security\textsuperscript{117}.

What Anonymous does is in contradiction to article 8 ECHR protection of personal data (see appendix)\textsuperscript{118}, when hacking a computer of either a private person or public institution personal data is in danger of being accessed and exposed. When exposing corruption of institutions and the pedophile ring the personal data that was accessed were later being exposed and shared with the public\textsuperscript{119}. Which is a clear violation against article 8 ECHR and


\textsuperscript{117}Eriksson, Maja K. Mårsäter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008.

\textsuperscript{118}Eriksson, Maja K. Mårsäter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008.

7 Conclusion.

The purpose of this thesis was to research these questions;

- How shall the different categorizations of cyber terror be interpreted in accordance with law?
- Are the reasons for the groups being formed oppression of social and or political means?
- What legal restrictions are there to the right to seek and share information?

Throughout this thesis it has been discussed how law should be interpreted in case of accessing information on the internet and what restrictions there are to this. Also a historical background has been given to show how the use of the internet has grown and become more and more popular. Within the historical background an understanding of what internet is most commonly used for has been explained and how many people may use this not only to shop for clothes but also share opinions through blogging and other social forums. But then the cybercrimes occur, people whom hack systems to disrupt it or to access information. Some only to read them privately others shares this to the public to reach a reaction towards the source of the information.

The internet was created with a purpose of helping the governmental and international institutions become more organized, and for them to catalogue important information that was to be shared with the military or other institutions. The main purpose was to have a more efficient communication system that was secure to the state. This platform for communication has over the years grown and developed into what the computer system we use today for studying, shopping, reading the new etc. the internet have become a free place for people to spread opinions and shop in private without spectators. With this increased use of the internet
spectators however do follow, when visited a web page the data is saved and through your IP address it can be proven what you have done while sitting at your computer. Why this have started to happen is much do to the crime that comes with the use of the internet.

Cybercrimes such as downloading and file sharing has become the more common offence of the internet and therefore there is an ongoing hunt for criminals on the web. While there can be argued free speech and freedom of expression on the internet some restriction do exist, William Fisher listed 6 condition of restricting this freedom (see appendix) amongst these six are child pornography, hate speech, and offensive statements of public figures among others. This is much like the ECHR article 10(2) that also states that if it is threatening to the democracy and national security freedom of expression/speech may be restricted.

Why then do people violate these? Some people/groups feel that their freedom of expression/speech is being oppressed, much due to these restrictions. Social and political groups form with the same interest of getting heard and exposing the corruption and double standards of the state. These groups question the rights set forward in national and European law and feel that their rights of self-determination ICCPR article 1 (see appendix) is being violated and that they are being discriminated ECHR article 14 (see appendix) based upon their social and political standards. This could be why they claim to follow the law through freedom of expression/speech ECHR article 10(1), ICCPR 19 (see appendix).

These groups base their actions upon this to get the attention of the public and to expose crimes. However while there is a sense of freedom of expression/speech in many of these cases such as Anonymous and Wikileaks there are other laws to take into considerations. In the case of Anonymous they claim to use their right of free speech/expression in all their actions, in their actions on exposing corruption and pedophiles on the internet ECHR article 8 protections of personal data is to be considered as well as ECHR article 10(2) restrictions on free speech/expression(see appendix). Because when using free speech/expression to its fullest they violated other rights which makes it possible to put restrictions upon free speech/expression. Wikileaks also acted in the name of free speech/expression, this case contained more delicate information that could be harmful to the democracy and national security of the US, also here article 10(2) is applicable but also the terrorist definition fits in here (see appendix). Since that the content that Wikileaks leaked was of such a threatening nature that it could endanger the democracy.
To categorize these two cases Wikileaks according to law can be seen as terrorists due to the content of the information leak. Though Anonymous expose highly important information to the public, they cannot be categorized as terrorists they have not yet exposed confidential information that could be threatening to national security or the democracy. The case of Estonia can then be discussed as being a clear case of cyber terrorism, according to the terrorist definition in the council framework decision and the cybercrime definitions of the COE (see appendix). The infrastructure and the national security of the Estonian system was being threatened during these three weeks, which in these articles is described as being terrorist offences and acts of cybercrime.

Though many opinions on this subject may be that groups such as Anonymous are acting as public protectors that has the main goal of exposing true internet crime as they did with the pedophile ring according to law they are violating the Human rights by hacking computer systems and exposing personal data. It is said that the ends justifies the means, this however is not the case when discussed through law. These are cybercrimes on different levels no matter what the intentions were.
8 Summary

Crimes of the internet are being committed on a daily basis against different institutions, governments and against civil population. These crimes are defined as hacking and cyber-terrorism with the intention of often bringing down governmental infrastructure, however not all crimes on the internet is performed by so called cyber-terrorists with the intention of interfering with the governmental structures.

Independent groups such Anonymous and Wikileaks whom takes it upon them to reveal the truth of state corruption and true criminals of the internet. Anonymous and wikileaks is product of social and political oppression by the states controlling the use of the internet. These groups feel that their rights of expression are being violated as well as they feel that the public is being left in the dark in matters that concerns them. A new witch hunt has been set in motion to bring the cyber-terrorists to justice for exposing information of corruption, child pornography and war details. The states feel it necessary to fight these criminals since that they in their opinion are a threat to the peace of the states. Some cybercrimes are in fact acts of terrorism and the responsible groups/persons should be brought to justice, in example of this are the three week cyber-attacks on Estonia. Estonia was being attacked through the internet by an unknown group whom during this period of three weeks managed to almost destroy the infrastructure of the country. This is an act of terrorism, an act of cyber-terrorism.

Laws such as the COE and the council framework decision defines cybercrime as; illegal access, illegal interception, data interference, system interference and misuse of devises. Terrorism is then being defined as being a threat to democracy and national security. This is what is to be considered when discussing what the different cases should be categorized as. Except from this law shall be discussed to determine if it is in contradiction to itself and how it then shall be interpreted in each specific case. Ex freedom of speech/expression ECHR
article 10 can contradict itself through its sub article 2. Article 10 (1) ensures freedom of expression/speech and article 10(2) can at the same time restrict it if by exercising freedom of expression/speech you violated other rights. It is here that interpretations of the law are necessary to analyze how to proceed in different cases.

9 Appendix.

THE COUNCIL FRAMEWORK OF THE EUROPEAN UNION.

Having regard to the Treaty establishing the European Union, and in particular Article 29, Article 31(e) and Article 34(2) (b) thereof, having regard to the proposal from the Commission (1), having regard to the opinion of the European Parliament (2), whereas:

(1) The European Union is founded on the universal values of human dignity, liberty, equality and solidarity, respect for human rights and fundamental freedoms. It is based on the principle of democracy and the principle of the rule of law, principles which are common to the Member States.

(2) Terrorism constitutes one of the most serious violations of those principles. The La Gomera Declaration adopted at the informal Council meeting on 14 October 1995 affirmed that terrorism constitutes a threat to democracy, to the free exercise of human rights and to economic and social development.

(3) All or some Member States are party to a number of conventions relating to terrorism. The Council of Europe Convention of 27 January 1977 on the Suppression of Terrorism does not regard terrorist offences as political offences or as offences connected with political offences or as offences inspired by political motives. The United Nations has adopted the Convention for the suppression of terrorist bombings of 15 December 1997 and the Convention for the suppression of financing terrorism of 9 December 1999. A draft global Convention against terrorism is currently being negotiated within the United Nations.
At European Union level, on 3 December 1998 the Council adopted the Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice (3). Account should also be taken of the Council Conclusions of 20 September 2001 and of the Extraordinary European Council plan of action to combat terrorism of 21 September 2001. Terrorism was referred to in the conclusions of the Tampere European Council of 15 and 16 October 1999, and of the Santa María da Feira European Council of 19 and 20 June 2000. It was also mentioned in the Commission communication to the Council and the European Parliament on the biannual update of the scoreboard to review progress on the creation of an area of ‘freedom, security and justice’ in the European Union (second half of 2000).

Furthermore, on 5 September 2001 the European Parliament adopted a recommendation on the role of the European Union in combating terrorism. It should, moreover, be recalled that on 30 July 1996 twenty-five measures to fight against terrorism were advocated by the leading industrialized countries (G7) and Russia meeting in Paris.

The European Union has adopted numerous specific measures having an impact on terrorism and organized crime, such as the Council Decision of 3 December 1998 instructing Europol to deal with crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property (4); Council Joint Action 96/610/JHA of 15 October 1996 concerning the creation and maintenance of a Directory of specialized counter-terrorist competences, skills and expertise to facilitate counter-terrorism cooperation between the Member States of the European Union (5); Council Joint Action 98/428/JHA of 29 June 1998 on the creation of a European Judicial Network (6), with responsibilities in terrorist offences, in particular Article 2; Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organization in the Member States of the European Union (7); and the Council Recommendation of 9 December 1999 on cooperation in combating the financing of terrorist groups (8). 22.6.2002 EN Official Journal of the European Communities L 164/3

The definition of terrorist offences should be approximated in all Member States, including those offences relating to terrorist groups. Furthermore, penalties and sanctions
should be provided for natural and legal persons having committed or being liable for such offences, which reflect the seriousness of such offences.

(7) Jurisdictional rules should be established to ensure that the terrorist offence may be effectively prosecuted.

(8) Victims of terrorist offences are vulnerable, and therefore specific measures are necessary with regard to them.

(9) Given that the objectives of the proposed action cannot be sufficiently achieved by the Member States unilaterally, and can therefore, because of the need for reciprocity, be better achieved at the level of the Union, the Union may adopt measures, in accordance with the principle of subsidiarity. In accordance with the principle of proportionality, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.

(10) This Framework Decision respects fundamental rights as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they emerge from the constitutional traditions common to the Member States as principles of Community law. The Union observes the principles recognized by Article 6(2) of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union, notably Chapter VI thereof. Nothing in this Framework Decision may be interpreted as being intended to reduce or restrict fundamental rights or freedoms such as the right to strike, freedom of assembly, of association or of expression, including the right of everyone to form and to join trade unions with others for the protection of his or her interests and the related right to demonstrate.

(11) Actions by armed forces during periods of armed conflict, which are governed by international humanitarian law within the meaning of these terms under that law, and, inasmuch as they are governed by other rules of international law, actions by the armed forces of a State in the exercise of their official duties are not governed by this Framework Decision,

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1

Terrorist offences and fundamental rights and principles
1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organization where committed with the aim of:

— Seriously intimidating a population, or

— Unduly compelling a Government or international organization to perform or abstain from performing any act, or

— Seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization,

Shall be deemed to be terrorist offences:

(a) Attacks upon a person’s life which may cause death;

(b) Attacks upon the physical integrity of a person;

(c) Kidnapping or hostage taking;

(d) Causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility,

Including an information system, a fixed platform located on the continental shelf, a public place or private Property likely to endanger human life or result in major economic loss;

(e) Seizure of aircraft, ships or other means of public or Goods transport;

(f) Manufacture, possession, acquisition, transport, supply

Or use of weapons, explosives or of nuclear, biological

Or chemical weapons, as well as research into, and development of, biological and chemical weapons;

(g) Release of dangerous substances, or causing fires, floods
Or explosions the effect of which is to endanger human life;

(h) Interfering with or disrupting the supply of water,

Power or any other fundamental natural resource the effect of which is to endanger human life;

(i) Threatening to commit any of the acts listed in (a) to (h).

2. This Framework Decision shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.

Article 2

Offences relating to a terrorist group

1. For the purposes of this Framework Decision, ‘terrorist group’ shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. ‘Structured group’ shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:

(a) Directing a terrorist group;

(b) Participating in the activities of a terrorist group, including

By supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that

Such participation will contribute to the criminal activities

Of the terrorist group.

Article 3
Offences linked to terrorist activities Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts:

(a) Aggravated theft with a view to committing one of the acts listed in Article 1(1);
(b) Extortion with a view to the perpetration of one of the acts listed in Article 1(1);
(c) Drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1) (a) to (h) and Article 2(2) (b).

Article 4

Inciting, aiding or abetting, and attempting

1. Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.

2. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3, with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable.

Article 5

Penalties

1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 1 to 4 are punishable by effective, proportionate and dissuasive criminal penalties, which may entail extradition.

2. Each Member State shall take the necessary measures to ensure that the terrorist offences referred to in Article 1(1) and offences referred to in Article 4, inasmuch as they relate to terrorist offences, are punishable by custodial sentences heavier than those imposable under national law for such offences in the absence of the special intent required pursuant to Article 1(1), save where the sentences imposable are already the maximum possible sentences under national law.

3. Each Member State shall take the necessary measures to ensure that offences listed in Article 2 are punishable by custodial sentences, with a maximum sentence of not less than
fifteen years for the offence referred to in Article 2(2) (a), and for the offences listed in Article 2(2) (b) a maximum sentence of not less than eight years. In so far as the offence referred to in Article 2(2) (a) refers only to the act in Article 1(1) (i), the maximum sentence shall not be less than eight years.

Article 6

Particular circumstances Each Member State may take the necessary measures to ensure that the penalties referred to in Article 5 may be reduced if the offender:

(a) Renounces terrorist activity, and

(b) Provides the administrative or judicial authorities with information which they would not otherwise have been able

To obtain, helping them to:

(i) Prevent or mitigate the effects of the offence;

(ii) Identify or bring to justice the other offenders;

(iii) Find evidence; or

(iv) Prevent further offences referred to in Articles 1 to 4.

Article 7

Liability of legal persons

1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for any of the offences referred to in Articles 1 to 4 committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on one of the following:

(a) a power of representation of the legal person;

(b) An authority to take decisions on behalf of the legal person;

(c) An authority to exercise control within the legal person.
2. Apart from the cases provided for in paragraph 1, each Member State shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of any of the offences referred to in Articles 1 to 4 for the benefit of that legal person by a person under its authority.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories in any of the offences referred to in Articles 1 to 4.

Article 8

Penalties for legal persons

Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 7 is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other penalties, such as:

(a) Exclusion from entitlement to public benefits or aid;

(b) Temporary or permanent disqualification from the practice of commercial activities;

(c) Placing under judicial supervision;

(d) A judicial winding-up order;

(e) Temporary or permanent closure of establishments which have been used for committing the offence.

Article 9

Jurisdiction and prosecution

1. Each Member State shall take the necessary measures to establish its jurisdiction over the offences referred to in Articles 1 to 4 where:

(a) The offence is committed in whole or in part in its territory. Each Member State may extend its jurisdiction if the offence is committed in the territory of a Member State;

(b) The offence is committed on board a vessel flying its flag or an aircraft registered there;
(c) The offender is one of its nationals or residents;

(d) The offence is committed for the benefit of a legal person established in its territory;

(e) the offence is committed against the institutions or people of the Member State in question or against an institution of the European Union or a body set up in accordance with the Treaty establishing the European Community or the Treaty on European Union and based in that Member State.

2. When an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralizing proceedings in a single Member State. To this end, the Member States may have recourse to anybody or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account shall be taken of the following factors:

— The Member State shall be that in the territory of which the acts were committed,

— The Member State shall be that of which the perpetrator is a national or resident,

— The Member State shall be the Member State of origin of the victims,

— The Member State shall be that in the territory of which the perpetrator was found.

3. Each Member State shall take the necessary measures also to establish its jurisdiction over the offences referred to in Articles 1 to 4 in cases where it refuses to hand over or extradite a person suspected or convicted of such an offence to another Member State or to a third country.

4. Each Member State shall ensure that its jurisdiction covers cases in which any of the offences referred to in Articles 2 and 4 has been committed in whole or in part within its territory, wherever the terrorist group is based or pursues its criminal activities.

5. This Article shall not exclude the exercise of jurisdiction in criminal matters as laid down by a Member State in accordance with its national legislation.

Article 10
Protection of, and assistance to, victims

1. Member States shall ensure that investigations into, or prosecution of, offences covered by this Framework Decision are not dependent on a report or accusation made by a person subjected to the offence, at least if the acts were committed on the territory of the Member State.

2. In addition to the measures laid down in the Council Framework Decision 2001/220/JHA of 15 March 2001 on the standing of victims in criminal proceedings (1), each Member State shall, if necessary, take all measures possible to ensure appropriate assistance for victims’ families.

Article 11

Implementation and reports

1. Member States shall take the necessary measures to comply with this Framework Decision by 31 December 2002.

2. By 31 December 2002, Member States shall forward to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. On the basis of a report drawn up from that information and a report from the Commission, the Council shall assess, by 31 December 2003, whether Member States have taken the necessary measures to comply with this Framework Decision.

3. The Commission report shall specify, in particular, transposition into the criminal law of the Member States of the obligation referred to in Article 5(2).

Article 12

Territorial application This Framework Decision shall apply to Gibraltar.

Article 13

Entry into force
This Framework Decision shall enter into force on the day of its publication in the Official Journal. Done at Luxembourg, 13 June 2002.  

**Convention on Cybercrime (COE)**

“Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.”

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.”

“Article 6 – Misuse of devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.  

European convention for the protection of human rights and fundamental freedoms (ECHR)

Article 10 – Freedom of expression

1. 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.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 14 – Prohibition of discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.\(^{122}\)

**Charter of fundamental rights of the European Union. (EUFR)**

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 11

Freedom of expression and information

\(^{122}\) Eriksson, Maja K. Mårsäter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008
1. 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.

2. The freedom and pluralism of the media shall be respected\(^{123}\).

**International covenant on civil and political rights. (ICCPR)**

**Article 1**

1. All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development.

2. All peoples may, for their own ends, freely dispose of their natural wealth and resources without prejudice to any obligations arising out of international economic co-operation, based upon the principle of mutual benefit, and international law. In no case may a people be deprived of its own means of subsistence.

3. The States Parties to the present Covenant, including those having responsibility for the administration of Non-Self-Governing and Trust Territories, shall promote the realization of the right of self-determination, and shall respect that right, in conformity with the provisions of the Charter of the United Nations.

**Article 19**

1. Everyone shall have the right to hold opinions without interference.

2. 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.

\(^{123}\) Eriksson, Maja K. Mårståter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

1. For respect of the rights or reputations of others;
2. For the protection of national security or of public order (ordre public), or of public health or morals.\textsuperscript{124}

\textbf{Treaty of the European Union.}

Article 29

(ex Article 15 TEU)

The Council shall adopt decisions which shall define the approach of the Union to a particular matter of a geographical or thematic nature. Member States shall ensure that their national policies conform to the Union positions.

Article 31

(Ex Article 23 TEU)

1. Decisions under this Chapter shall be taken by the European Council and the Council acting unanimously, except where this Chapter provides otherwise. The adoption of legislative acts shall be excluded.

When abstaining in a vote, any member of the Council may qualify its abstention by making a formal declaration under the present subparagraph. In that case, it shall not be obliged to apply the decision, but shall accept that the decision commits the Union. In a spirit of mutual solidarity, the Member State concerned shall refrain from any action likely to conflict with or impede Union action based on that decision and the other Member States shall respect its position. If the members of the Council qualifying their abstention in this way represent at least one third of the Member States comprising at least one third of the population of the Union, the decision shall not be adopted.

\textsuperscript{124} Eriksson, Maja K. Mårsäter, Olle. Åkermark, Sia S. Documents in public international law. Norstedts juridik AB. 2008
2. By derogation from the provisions of paragraph 1, the Council shall act by qualified majority:

— when adopting a decision defining a Union action or position on the basis of a decision of the European Council relating to the Union’s strategic interests and objectives, as referred to in Article 22(1),

— when adopting a decision defining a Union action or position, on a proposal which the High Representative of the Union for Foreign Affairs and Security Policy has presented following a specific request from the European Council, made on its own initiative or that of the High Representative,

— When appointing a special representative in accordance with Article 33.

If a member of the Council declares that, for vital and stated reasons of national policy, it intends to oppose the adoption of a decision to be taken by qualified majority, a vote shall not be taken. The High Representative will, in close consultation with the Member State involved, search for a solution acceptable to it. If he does not succeed, the Council may, acting by a qualified majority, request that the matter be referred to the European Council for a decision by unanimity.

3. The European Council may unanimously adopt a decision stipulating that the Council shall act by a qualified majority in cases other than those referred to in paragraph 2.

4. Paragraphs 2 and 3 shall not apply to decisions having military or defense implications.

5. For procedural questions, the Council shall act by a majority of its members

Article 34

(Ex Article 19 TEU)

1. Member States shall coordinate their action in international organizations and at international conferences. They shall uphold the Union’s positions in such forums. The High Representative of the Union for Foreign Affairs and Security Policy shall organize this
coordination. In international organizations and at international conferences where not all the Member States participate, those which do take part shall uphold the Union’s positions.

2. In accordance with Article 24(3), Member States represented in international organizations or international conferences where not all the Member States participate shall keep the other Member States and the High Representative informed of any matter of common interest.

Member States which are also members of the United Nations Security Council will concert and keep the other Member States and the High Representative fully informed. Member States which are members of the Security Council will, in the execution of their functions, defend the positions and the interests of the Union, without prejudice to their responsibilities under the provisions of the United Nations Charter. When the Union has defined a position on a subject which is on the United Nations Security Council agenda, those Member States which sit on the Security Council shall request that the High Representative be invited to present the Union’s position125.

William Fisher conditions for restriction.

1. Speech that is likely to lead to imminent lawless action may be prohibited.

2. "Fighting words" -- i.e., words so insulting that people is likely to fight back -- may be prohibited.

3. Obscenity -- i.e., erotic expression, grossly or patently offensive to an average person, that lacks serious artistic or social value -- may be prohibited.

4. Child pornography may be banned whether or not it is legally obscene and whether or not it has serious artistic or social value, because it induces people to engage in lewd displays, and the creation of it threatens the welfare of children.

5. Defamatory statements may be prohibited. (In other words, the making of such statements may constitutionally give rise to civil liability.) However, if the target of the defamation is a "public figure," she must prove that the defendant acted with "malice." If the target is not a

"public figure" but the statement involved a matter of "public concern," the plaintiff must prove that the defendant acted with negligence concerning its falsity.

6. Commercial Speech may be banned only if it is misleading, pertains to illegal products, or directly advances a substantial state interest with a degree of suppression no greater than is reasonably necessary.  

8 Bibliography.

Books.


Terrorism or hacking? A law interpretation on the concept of cyber-terrorism.


**Internet sources.**


- Cass, Stephen. IBM WEB FOUNTAIN. A Fountain of Knowledge 2004 will be the year of the analysis engine IEEE Spectrum Online (Jan 4, 2004). Internet news.
Terrorism or hacking? A law interpretation on the concept of cyber terrorism.


Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

Louise Synnestvedt Jensen. 19890525-1586. 2RV00E


Terrorism or hacking? A law interpretation on the concept of cyber terrorism.


Terrorism or hacking? A law interpretation on the concept of cyber terrorism.

Louise Synnestvedt Jensen. 19890525-1586. 2RV00E


- Zograf, Bohdan. A Brief History of the Internet. An anecdotal history of the people and communities that brought about the Internet and the Web..