Research Proposal

Working Title

Hacktivism

Virtual activism as a threat for a democratic society?

Challenges – Problems – Consequences

Submitted by

MMag. Elio Dalpra
0603304

University Degree

Doctor of Philosophy Interdisciplinary Legal Studies (PhD)

Vienna, 2016

Degree Program: A 794 242
Academic Field: Human Rights and Fundamental Freedoms
Supervisor: ao. Univ.-Prof. Dr. Hannes Tretter
# Table of contents

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Context</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>State of research</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Research goal</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Main research question</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Additional research questions</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Hypothesis</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>Methodology</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>Approach</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>Proposed outline</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>Research schedule</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>Bibliography</td>
<td>12</td>
</tr>
</tbody>
</table>
1. Context

“Austria foreign [sic!] minister [sic!]! Who do you think you are kiddly [sic]!” This phrase was part of a picture, which was posted illegally on the webpage of the Austrian Foreign Minister in June 2014 by a group of hackers called Ankincilar. This “hack” was a reaction to the statements made by Secretary of State Kurz concerning the unofficial visit of the Turkish Prime Minister to Austria.\(^1\) This has not been an isolated case: already in 2010, the group Anonymous attacked PayPal, MasterCard and VISA causing disturbances because these services refused to accept money donations for the whistle-blowing website WikiLeaks.\(^2\) In 2011, the same group released sensitive data concerning officers of the Austrian Police.\(^3\) One year later, Anonymous changed the website of the event organization which organizes the WKR-Ball.\(^4\) In contrast to these relatively unknown events, the media coverage of the disclosures by the website WikiLeaks as well as the leaked secret documents of the National Security Agency (NSA) by international newspapers has been enormous.\(^5\) Apart from that, reports about data theft, falsified bank requests, attacks through Bot-Networks and crashing websites are increasing.\(^6\) In the literature, terms like Cybercrime, Cyber warfare, Cyber terrorism and Hacktivism are suggested to pinpoint the different aspects of these manifestations. As a result, I am going to shortly describe these terms. First of all, the term Cybercrime is primarily used to describe several criminal offences in cyberspace like offences

---

against the confidentiality, integrity and availability of computer data and systems. However, Organizations like the North Atlantic Treaty Organization (NATO) bring up Cyber warfare to describe these virtual attacks in a slightly different manner:

The prospect of internet-based warfare has come to the fore after a series of high-profile international attacks. Last year, it emerged that a gang of hackers, believed to be from China, had infiltrated computer systems at the Pentagon and launched attacks on government networks in Britain, Germany, India and Australia. US officials, who have labelled the group Titan Rain, have accused them of operating under the auspices of officials in Beijing.

Similar to Cybercrime and Cyber warfare, the concept Cyber terrorism emerges. It exists momentarily only as a theoretical threat and is described by Brenner as follows:

The local Office of Emergency Services & Homeland Security receives messages via a secure government computer system informing them that a “suitcase nuclear device” is on the Bay Area Rapid Transit (BART) system. BART is a public transportation system that serves San Francisco and surrounding cities. The officials are told the device is in the hands of terrorists who will detonate it in two hours – at 3:00 p.m. The officials issue an immediate evacuation order for the San Francisco area. This produces chaos as panicked citizens desperately try to flee an impending nuclear disaster. Terrorists hacked the government computer system and sent credible, fake messages, which the local officials believed. The net result is that the terrorists achieve injury, death and destruction and dramatically erode public confidence in the government’s ability to ensure their security.

Despite all of these manifestations and definitions, there are still manifestations in cyberspace which cannot be described by Cybercrime, Cyber warfare or Cyber terrorism. These modes of activism use unorthodox methods and appear to have a political agenda. In this context, the conception of Hacktivism is enforced. Hacktivism – hacking and activism – is the combination of grassroots political protest with computer hacking. Its repertoire ranges from e-graffiti to site redirection. The first tool can be described as a photomontage. For example, a photo of the former President of the United States Georg Walker Bush holding his dog, which

---

7Convention on Cybercrime available on http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090-0001680081561 [last access 24.03.2016].
8Johnson, NATO says cyber warfare poses as great a threat as a missile attack (06.03.2008) [o.S.], in: http://www.theguardian.com/technology/2008/mar/06/hitechcrime.uksecurity [last access: 24.03.2016].
has the face of the former British Prime Minister Tony Blair. In comparison, the second tool is a virtual redirection which brings the user to an alternative webpage instead of the desired one. For instance, a user wants to access the website of Ku-Klux-Klan, but reaches the webpage of HateWatch instead. Apart from that, Denial-of-Service attacks raise public attention, as the website shutdown of the British Government illustrates. To sum up, these manifestations show a lot of similarities to Cybercrime, Cyber warfare and Cyber terrorism, but there is still quite a lot of room for interpretation. As a result, the following questions should be discussed: What is the difference between Hacktivism, Cybercrime, Cyber warfare and Cyber terrorism? How can these concepts be assessed from a legal perspective? Is Hacktivism a new form of warfare or an act of terrorism? Can Hacktivism be referred to as a criminal offence according to Austrian Criminal Law (StGB)? Can Hacktivism be seen as a political protest? Is Hacktivism a new manifestation of the Right to Freedom of Speech or the Right to Freedom of the Arts?

2. State of research

These above mentioned questions are not yet answered. A comprehensive academic interdisciplinary analysis on Hacktivism and the mentioned Human Rights and Fundamental Freedoms has not yet been conducted. There have been research results concerning the Right to Freedom of Assembly and Denial-of-Service attacks, but primarily in connection with online demonstrations and gatherings in virtual platforms. Until now, the academic discourse on virtual phenomena in cyberspace has been concentrated on a criminal and data protective

---

14 This organization dedicates its work against hate and fanaticism. For more information: Glave, Ku Klux Klan Korrekted (09.10.1999) [o.S.], in: http://archive.wired.com/culture/lifestyle/news/1999/09/21687 [last access: 24.03.2016].
angle.\textsuperscript{21} The Austrian State Authorities consider Hacktivism first and foremost as an appearance of Cybercrime.\textsuperscript{22} Moreover, some scientists see similarities between Hacktivism and Cyber terrorism.\textsuperscript{23} Apart from that, Hacktivism is described as a virtual form of protest.\textsuperscript{24} This variety of opinions illustrates that an analysis on Hacktivism as an independent phenomenon has so far been conducted only in Political Science\textsuperscript{25} and from a technological-military angle.\textsuperscript{26} Consequently, the need to analyze the ambivalent manifestations and interdisciplinary character of Hacktivism from a Human Rights perspective is the main motivation for this research proposal.

3. Research goal

Due to the above described challenges, I intend to analyze different manifestations of Hacktivism. My research focus lies on appearances which target state institutions, politicians and political parties. The reason is quite obvious: on the one hand the probability that these appearances are covered by the media is higher than appearances which target private
individuals. On the other hand, there are different legal as well as political implications concerning protest against state institutions, politicians and political parties. In my approach I categorized these different forms and as a result, address the question if these manifestations of protest are new manifestations of the Right to Freedom of Speech or the Right to Freedom of the Arts. Therefore, the scope and limitations of these Human Rights have to be analyzed. Moreover, the prohibitions of these Human Rights as well as their validity in cyberspace are part of the analysis. Consequently, the relationship between Hacktivism and legal provisions shall be examined. Hence, this analysis should be understood in the way that there are different forms of Hacktivism which are located in a legal grey zone. Particularly in this context, there is a constant development of illegal forms of protest and their evolution to legally accepted manifestations of protest.27

4. Main research question

Can different manifestations of Hacktivism be legally seen as the expression of opinions or as an art form and what are the consequences?

5. Additional research questions

• How can Hacktivism, Cybercrime, Cyber warfare and Cyber terrorism be distinguished from one another?
• What similarities exist between Human Rights cases, dealing with the Human Rights Freedom of Speech and Freedom of the Arts, and Hacktivism?
• Are there indications in the judicature of the High Courts, both on the Austrian and on the European level, which can lead to the protection of virtual forms of protest in cyberspace?
• In what way do legal countermeasures in cyberspace influence Hacktivism?
• Are legal and political arguments, including Hacktivism in the protection of the concerned Human Rights, convincing?
• How far can the exercise of Human Rights reach in this context?
• To what extend do states, politicians and political parties have to tolerate interventions through Hacktivism in their Rights?
• Does the protection of Hacktivism through the above mentioned Human Rights legalize vigilantism in cyberspace?

27 For example, the legitimate criticism of public figures: EGMR, 08.07.1986, 9815/82, Lingens/Österreich, Further examples: Berka, Verfassungsrecht (2014) 506 f., with further references; also Öhlinger/Eberhard, Verfassungsrecht (2014) 424 f., with further references.
6. **Hypothesis**

- *Hacktivism* is a manifestation of *Cybercrime* because *Hacktivism* uses illegal tools within the meaning of criminal law.
- The use of virtual force to accomplish the goals of *Hacktivists* denies any legal protection.
- Hacktivism has parallels to accepted forms of protest such as civil disobedience.
- The analyzed forms of *Hacktivism* can be seen as expressions of the mentioned Human Rights because they show similarities to caricatures and politicking through Art.
- The verdict Steel u. Morris/UK shows the acceptance of the ECHR to develop existing Human Rights mechanisms towards NGOs, due to the fact that they can initiate discussions of matters of public interest similar to the media. This verdict could likely enable a possible way to legally approve *Hacktivism*, as in a democratic society it is necessary to discuss such matters.
- The protection of *Hacktivism* through Human Rights leads to the conclusion that the discourse of different issues might be dominated by the most skilled and best equipped “hackers”.

7. **Methodology**

I worked with a combination of the methodology of two different academic fields to analyze the legal and political dimensions of *Hacktivism*. On the one hand, I used literature research combined with the analysis of the relevant legal standards and scientific doctrines as well as the judicature of the Austrian and European High Courts. On the other hand, I conducted a protest event analysis (PEA) of media articles to gain samples. Both the PEA and the legal analysis were supported by qualitative interviews with representatives of state institutions and experts.

8. **Approach**

The thesis is structured in five main bodies. The first body contains 4 main sections. The first section is the presentation of the context of the analysis and the methodology. After that, central terms are defined in the second section, including the description of *Hacktivism*\(^{28}\) plus its contextualization, which consists of methods, goals and motivation for such actions. To gain a foundation for the analysis, I discuss *Hacktivism*’s close relationship with *Cybercrime*,

---

Cyber terrorism or Cyber warfare. The third and fourth section entail different theoretical concepts of protest and the conception of Human Rights in general with special focus on the Right to Freedom of Speech and the Right to Freedom of the Arts.

The second body reviews the first part of the research question. Therefore, two different procedures of the analysis are necessary. In the first procedure, I collect qualitative and quantitative data concerning Hacktivism on the basis of a PEA. An online key term search in the databases WISO and LexisNexis University provides the scope of media articles for this analysis. As a result, these samples are structured according to the five criteria groups. In the first group I gather different action types which are used by hacktivists. The next one collects the actors of these action types. The third and fourth group capture, on the one hand, their demands and, on the other hand, their arguments. Finally, the frequency of references to Hacktivism, Cybercrime, Cyber warfare and Cyber terrorism is listed. After that I examine the samples if they show the necessary criteria to be classified as Hacktivism. For this step, the definition and the contextualization of Hacktivism from the first body are used. In the second procedure, I analyze the relevant legal standards and scientific doctrines as well as the judicature of the Austrian and European High Courts. To do this, the analysis of existing instruments – for example the Framework decision of the Council of the European Union29, the Cybercrime Convention of the Council of Europe30 and its implementation in the Austrian Criminal Law (StGB31) – to fight Cybercrime is important. Apart from that, the international Human Rights documents, the European Convention on Human Rights32, the Charter of Fundamental Rights of the European Union33 and the standards of the Austrian legal system constitute the relevant legal sources for this analysis. Further, I am analyzing the judicature of the European High Courts34 and the Austrian High Courts35. Therefore, an online search in the legal databases RIS36, CURIA37 and HUDOC38 is necessary to gather legal case materials. I

29RB 2005/222/JI, ABI L 69
31Übereinkommen über Computerkriminalität BGBl. III Nr. 140/2012 (zuletzt) BGBl. III Nr. 215/2014
34The European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU).
35The Verfassungsgerichtshof (VfGH), the Verwaltungsgerichtshof (VwGH) and the Oberste Gerichtshof (OGH).
36The Legal Information System of the Republic of Austria, in: https://www.ris.bka.gv.at/defaultEn.aspx [last access: 24.03.2015].
38The Case Law database of the European Court of Human Rights, in: http://hudoc.echr.coe.int/eng#{%22languageisocode%22:%22EN%22}%22documentcollectionid%22:%22JUDGMENTS%22} [last access: 24.03.2015].
search for cases which deal with protest, especially within the relationship between legal provision, mainly to fight Cybercrime, and the above mentioned Human Rights. Moreover, I interview representatives of state institutions and experts to gain insights in their opinions and policies concerning Hacktivism.

In the third body, the gathered PEA samples are legally analyzed to determine, if the Right to Freedom of Speech and the Right to Freedom of the Arts apply to these samples. To do that, the analysis will include a comparison between the gathered legal cases, which enjoy the protection of the above mentioned Human Rights, and the samples to assess possible similarities. This is the foundation for the Human Rights Examination which show if the PEA samples could enjoy the protection of the Human Rights Freedom of Speech and/or Freedom of the Arts. The gathered outcome of the second section should lead to a result concerning the applicability of the concerned Human Rights on Hacktivism. This analysis is completed by the results of the qualitative interviews with experts in this fields and representatives of state authorities.

I edit the second part of the research question in the fourth body. Here, I will assess if virtual activism is legitimate legal instrument of expressions in the sense of the above mentioned Human Rights. Moreover, the question if Hacktivism is a threat to a democratic society is answered. Based on these results I discuss the possible legal and political consequences of Hacktivism.

The results are assembled in the fifth body to arrive at a conclusion. In the end, perspectives for digital forms of protests as well as further working assumptions will be formulated. Again this analysis should support the development of a more detailed perspective on different shapes of Hacktivism which are located in a legal grey zone. My thesis should help develop a more differentiated awareness of these forms by presenting alternatives to the range of arguments which identify all forms of protest in cyberspace as criminal offences, warfare or acts of terror.

9. Proposed outline

Introduction

1. Section – Theoretical foundation

I. Initial point of the thesis
   1) Presentation of the question and the main objective
   2) Methodology and methodical approach
II. Protest
   1) Concepts of protest
   2) Direct relation of protest and anonymity in cyberspace
   3) Direct relation of protest and violence

III. Human Rights
   1) Human Rights in cyberspace
   2) Relevant Human Rights
      (a) Right to Freedom of Speech
      (b) Right to Freedom of the Arts

IV. Hacktivism
   1) Explanation/contextualization
   2) Manifestations
   3) Similarities to Cybercrime, Cyber terrorism and Cyber warfare

2) 2. Section – Data collection

I. Protest Event Analysis (PEA)
   1) Results
      (a) Structuring results in specified criteria groups
   2) Preparing foundation for analysis
      (a) Assess which samples show the necessary criteria to be classified as Hacktivism

II. Analysis of the judicature of the European High Courts and the Austrian High Courts
   1) Collecting Human Rights cases in which protesting is essential
      (a) Caricatures, Blogs, Postings etc.
      (b) Politicking through art etc.

III. Conducting qualitative Interviews
   1) Experts
      (a) Human Rights Experts
      (b) Protest(-movement) Experts
   2) State authorities
      (a) Ministry of Interior
      (b) Justice spokesman of Austrian political Parties
3. Section – Analysis

I. Examination of legal standards and scientific doctrines

1) Analysis of relevant legal provisions for this research proposal
   (a) Austrian Constitutional Law, Austrian Criminal Law
   (b) European Convention on Human Rights, European Charter of Fundamental Rights

2) Analysis of legal scientific doctrines
   (a) Prevailing doctrines – minority opinions etc.
   (b) Concurring opinions – dissenting opinions etc.

II. Human Rights Examination of the PEA samples

1) Analysis of comparability, parallels and similarities of the PEA samples and judicature of the Austrian and the European High Courts

2) Assessment of the protection of Hacktivism through the Human Rights Freedom of Speech and Freedom of the Arts
   (a) Scope of protection of these Human Rights
      • Boundaries and range of these Human Rights
   (b) Legal reservations of these Human Rights
      • Prevention of disorder or crime
      • Protection of morals
      • Protection of the reputation or rights of others
      • Preventing the disclosure of information received in confidence
      • Maintaining the authority and impartiality of the judiciary
   (c) Proportionality

4. Section – Legal and political consequences

I. Discussion of the gathered outcome

1) Human Rights interventions in cyberspace
   (a) Limitations of the relevant Human Rights
      • Censorship – prohibition and repression of opinions
      • Hate Speech and incitement – instigation of violence
   (b) Role of anonymity and effective Human Rights Protection
      • Anonymity as obstacle – Prosecution of activists
   (c) Regulations of expressions?
2) Attack on the legal and political foundation?
   (a) Protest in cyberspace as a threat to state authorities?
   (b) Countermeasures of the state
       - Prevention of criminal offences and its impacts
3) Activism, a threat to a democratic society?
   (a) Virtual violence as an obstacle for legitimate protest
       - Intrusions in computer systems = violence?
       - Publication of data = criminal offence?
       - Virtual activism = vigilante justice?
   (b) Hacktivism necessary in a democratic society?
       - Selective flow of information as a need for activism
       - Shocking, offending and unpleasant expressions as thought provoking impulses
       - Shifting public matters, interest and information
   (c) Necessity to address matters of public interest and concern
       - Technical weaknesses as a source for information
       - Parallels to investigative journalism
       - New source of information

5. Section – Conclusion

I. Outcome

II. Future perspectives of Hacktivism

III. Formulation of further working assumptions

10. Research schedule

Autumn 2014 till spring 2016: Presentation of the thesis; Submission of the proposal.
Autumn 2014 till summer 2017: Completion of the elective subjects; Collection, examination, reading and evaluation of the relevant scientific literature and judicature; Scheduling and conducting interviews. Issue a first draft.
Summer 2017 till January 2018: Revising of the first draft; Inclusion of criticism; Completion of the thesis.
Spring/summer 2018: Defensio
11. Bibliography

Monographs


Collective volumes


---

The literature of the bibliography is only a short extract of the relevant scientific literature.


**Journals**


- **Die Presse** (02.04.2012) Anonymous April, April!, Wien: Die Presse Digital GmbH & Co KG.

- **Der Standard** (26.10.2011) 25.000 Polizisten finden sich plötzlich im Netz, Wien: Standard Verlagsgesellschaft m.b.H.

- **Der Standard** (27.01.2012) Keine Angst vor „blöden Buben“, Wien: Standard Verlagsgesellschaft m.b.H.

