TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Social Sciences

Tallinn Law School

Ann Väljataga

E-Democracy´s Missing Component: Possibilities for Decriminalising Online Collective Action Protests

Master´s Thesis

Supervisor: Agnes Kasper, PhD.

Tallinn 2016

I hereby declare that I am the sole author of this Master's Thesis and it has not been presented to any other university of examination.

Ann Väljataga

" ..... " 2016

The Master Thesis meets the established requirements

Supervisor Dr. Agnes Kasper

" ..... " 2016

Accepted for examination " ..... " 2016

Board of Examiners of Law Master's Theses

.....

Table of Contents

List of Abbreviations 4
Introduction 5
Methodological remarks 10
1. Comparison of offline and online protests 11
1.1. Why there should be room for civil disobedience both offline and online? 11
1.2. Cyber protests 16
1.2.1. What is hacktivism? 16
1.2.2. Which hacktivist tools would constitute the most suitable equivalent for a physical space protest? 20
1.3. Conclusions 29
2. Current legal framework 32
2.1. Criminal and humanitarian law 32
2.1.1. Regional instruments 32
2.1.1. International instruments 34
2.1.3. National legislation 36
2.2. Fundamental Rights 42
2.3. Conclusions 46
3. Case law analysis 48
3.1. Anonymity and accountability of the protester 48
3.2. The speech-conduct dichotomy 53
3.3. Is there a right to protest on private property? 55
3.4. Inconvenience and economic loss caused to the target and third parties 59
3.5. Coercion, force and violence within a protest 62
3.6. Duty to notify 65
3.7. Conclusions 66
4. Model Regulation 68
4.1. EDT digital sit-in in support of the Mexican Zapatistas 71
4.2. "Deportation class" action against Lufthansa 71
4.3. Operation AvengeAssange 72
4.3. D.G vs Estonia 74
4.4. Conclusions 76
Conclusions 77
Kokkuvõte 83
List of Sources 85

List of Abbreviations

Anons	members of the hacktivist group Anonymous
AnonOps	operations conducted by the hacktivist group Anonymous
AU	African Union
CERT	Cyber Emergency Response Team
CII	critical information infrastructure
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DDoS	distributed denial of service
DoS	denial of service
DRM	digital rights management
ECFR	European Charter of Fundamental Rights
ECHR	European Convention on Human Rights
ECmHR	European Commission on Human Rights
ECtHR	European Court of Human Rights
EDT	Electronic Disturbance Theatre
ENISA	European Union Agency for Network and Information Security
FBI	Federal Bureau of Investigation
ICCPR	International Covenant on Civil and Political Rights
ISP	internet service providers
JS	java script
LOIC	Low Orbit Ion Cannon
NATO	North Atlantic Treaty Organisation
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
TOR	The Onion Router
UDHR	Universal Declaration of Human Rights
UN	United Nations
URL	uniform resource locator
VPN	virtual private network

Introduction

> *"The invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. This invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly efficient regulation possible. The struggle in that world will not be government's. It will be to assure that essential liberties are preserved in this environment of perfect control."*[1]
>
> *Lawrence Lessig*

With fluctuating frequency and intensity protests have been taking place since the plebeian secessions in ancient Rome and medieval peasant riots. The historical culmination of western protest movements is thought to be the Great French Revolution, ever since there have been more and less turbulent periods with the most notable waves of protests occurring in the 1850-s and 1960-s. The recent years have witnessed a growth in the global protest movements. In 2011 after the infamous Occupy movement and Arab Spring the Time magazine chose the faceless and nameless protester, one of the crowd, as the person of the year. However, the real efficiency and purpose of modern global protests has been often questioned. Bulgarian scholar Ivan Krastev, who has published extensively on contemporary protest movements, for instance sees in the majority of them an attempt to disrupt democracy just for the sake of disruption, without any endeavour to evolve into a political movement or offer an alternative "positive program"[2]. Therefore the classical historical vision of a protest as an organised movement, carrying the seal of one or another political ideology, led by a charismatic leader and seeking to access to representative democratic institutions is waning in the physical space[3], whereas in the cyberspace it has never really been born.

As most of the social phenomena and power structures, today protest movements too are highly digitalized, and perhaps even more efficient in the virtual than in the tangible reality. Cyberspace[4] makes possible near-instantaneous encounters and interactions between spatially distant actors,

[1] Lessig, L. Code and Other Laws of Cyberspace, v2. Basic Books 2006, p 23.
[2] Krastev, I. Democracy Disrupted - the Global Politics or Protest. University of Pennsylvania Publishing 2014, p 13 ff.
[3] Ibid.
[4] Cyberspace is defined as a time-dependent set of interconnected information systems and the human users that interact with these systems (Lorents and Ottis, Cyberspace: Definition and Implications, NATO CCDCOE, 2010)

creating possibilities for ever-new forms of association and exchange[5], including these of an outlawed character. Online activism has been on the rise, with many of its forms resembling legally unambiguous extensions of the traditional activist´s tools such as petitions, campaigns, leaflets, manifestos etc. These tools only use the internet as an immensely popular forum, but would nevertheless be still possible in a non-networked world.

Another category of methods that are used to express opposition are more environment-dependent and can only be applied in the cyber-sphere. These tools are usually legally more controversial and border on cybercrime, however often their real life analogies have in time obtained the status of a legitimate act of protest. Therefore, studying civil disobedience means aiming at a moving target. Cohen and Arato have summarized the changing nature of civil disobedience: "Few would be shocked today by a workers´ strike, a sit-in, a boycott, or a mass demonstration. These forms of collective action have come to be considered normal, yet all of them were once illegal or extralegal or could again become illegal under some circumstances"[6] Could this ever happen to cyber protests? If yes, then which conditions should be in place in order to maximize the public good and minimize the harm that comes with this relatively new form of protest?

Cyber protests are most often associated with the infamous hacktivist group Anonymous that has stood up against a range of political issues by launching distributed denial of service (DDoS)[7] attacks against the websites of government bodies and prominent organisations, including the Australian Parliament, PayPal, MasterCard, Visa, the US Federal Bureau of Investigation and the US Department of Justice. These cyber-attacks have not, so far, led to anything resembling the physical and emotional impact of terrorist attacks in New York and Washington, Bali, Madrid, London or Mumbai. The tradition of hacktivist political resistance however goes back to mid-nineties, when activists organised cyber operations in support of the Zapatista movement in Mexico and the protests against the World Trade Organisation that took place in Seattle in 1999. Regardless of whether the underlying motivation is political or criminal, the last decade has witnessed a remarkable increase in the number of DDoS attacks, for instance in the third quarter of 2015, Kaspersky observed on the average 800 - 1000 individual DDoS attacks per day.[8] While

5 Yar, M. The novelty of "cybercrime" an assessment in light of routine activity theory. European Journal of Criminology 2, no. 4, p 409.
6 Cohen, J.L., Arato, A. (Eds.). Civil society and political theory. MIT Press 1994, p 516.
7 "Denial of service" refers to a cyber-attack 'which prevents a computer user or owner access to the services available on his system' Such an attack can be performed without direct Access to a system, by 'flooding' Internet-accessible computers with communications, so that they become 'overloaded' and are rendered unable to perform functions for legitimate users. Yar, M. Cybercrime and Society. Sage 2013, p 51). See also: *Infra*, chapter 1.2.1.
8 Kaspersky Security, DDoS Security Report 2015Q3, available at: https://securelist.com/analysis/quarterly-malware-reports/72560/kaspersky-ddos-intelligence-report-q3-2015/ (last accessed 1 May 2016).

in 2006 University of Cambridge researcher Richard Clayton assessed around 4000-5000 attacks per month as a relatively high number and already then predicted the massive increase.

Today, civil society, including the more resistant groups, on the Internet has to find its place in an environment that is characterized by four interconnected, partially competing and partially overlapping processes: militarisation[9], criminalisation[10], securitisation[11] and privatisation[12].

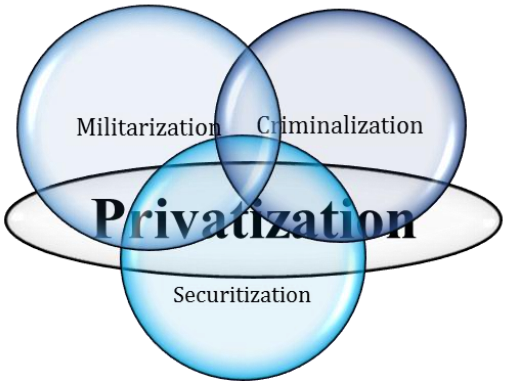

Figure 1: Current processes in cyberspace. Is there still room for civil liberties?

Although the vast majority of the tools and techniques used by cyber protesters today qualify as cybercrime, due to the alleged relative ease of conduct and efficiency a regulatory disconnection has emerged – despite the criminalization, disruptive acts of online civil disobedience are not disappearing anywhere. In 2011 Joshua McLaurin wrote while discussing the legal status of DoS and DDoS attacks "The rationale behind the use of criminal law for this purpose (regulating DoS and DDoS attacks A.V.) is pragmatic and straightforward: Given the evolving opportunities for individuals to use technology to threaten others' privacy, safety, and material assets, it is appropriate to update criminal laws that already exist to protect against such threats in the physical

[9] Militarisation is the process through which a society prepares for armed conflict and shifts the focus to the strategic-military dimensions of a problem and the adoption of something for use by or in the military. *See*, *e.g.* Dunn-Cavelty, M. The Militarisation of Cyberspace: Why Less May Be Better. NATO CCDCOE, 2012 p 3.
[10] Criminalisation is the process through which behaviours and individuals are labelled as crimes and outlawed. The Sage Dictionary of Criminology. Eds. McLaughlin, E., Muncie, J. Sage 1990, p 103.
[11] Securitisation is the process of moving a political agenda into the forefront of security, presenting issues as a significant or existential threat that warrants taking extraordinary measures, including the use of force. Kasper, A. The Fragmented Securitization of Cyber Threats. Eds. Kerikmäe, T. *et al*. Regulating eTechnologies in the European Union. Springer International Publishing 2016, pp 157-158.
[12] Privatisation is the transfer of control ownership from the public to the private sector, such a transfer being necessarily being necessarily associated with marker liberalisation and deregulation, changing the macroeconomic context , the competitive environment and the labour market of the country. Maheswari, S. R. A Dictionary of Public Administration. Orient Longman 2002, p 429.

world."[13] Besides criminal law, principles of international humanitarian law are at least in theory capable of being applied in cyberspace, since the protection of networks and critical infrastructures is considered one of the foremost military objectives. Another branch of law that calls for updates is fundamental rights, the latter however is known to be particularly slow to adapt to new shapes.

Therefore the question arises, whether universal criminalization is the most feasible normative reaction to the realities of cyber protests? By drawing an analogy with the legal regulation of protests and civil disobedience offline, the thesis seeks answers to these questions and aims to provide a draft set of requirements and conditions that a legally conducted online protest should meet. The first chapter builds on the presumption that a certain degree of civil disobedience is natural and inevitable in a democratic society and gives a brief overview of the law and legal theory regarding civil disobedience in physical space. For this the relevant elements of the freedom of expression and right to assembly are being looked into. Also the concept of direct action and the conduct/speech distinction are being explained. In the second part the taxonomy of the different methods of online activism and civil disobedience is introduced and some illustrative examples of operations are provided. The chapter explains why this thesis focuses primarily on acts of online civil disobedience that allow for collective action and manifestations of online activism or lone-wolf tools are not discussed.

In the second chapter, the most important legal instruments that currently regulate cyber protests are presented. The first part of the chapter is dedicated to the analysis of the legal instruments that criminalize online civil disobedience, Council of Europe Convention of Cybercrime (Budapest Convention), International code of conduct for information security, African Union Convention on Cyber Security and Personal Data Protection**,** Tallinn Manual, Computer Fraud and Abuse Act (CFAA), Directive 2013/40/EU on attacks against information systems (often referred as the Botnet Directive) are compared. In the second part instruments that may potentially grant some forms of online civil disobedience the status of a legitimate protest are analysed, for this ICCPR, ECFR, ECHR, UDHR are looked into. The objective of the second part is therefore to map the current legal status of online civil disobedience and establish whether at the moment there exists any alternative legal approaches besides criminalization.

The third chapter analyses some of the most eminent examples of currently existing national and international case law on protests that have taken place in the physical world and in the cyber

[13] McLaurin, J. Making Cyberspace Safe for Democracy: the Challenge Posed by Denial-of-service Attacks. Yale Law & Policy Review 2011, 30 (1), pp 211-254, p 213.

sphere. Although case law on the latter is very limited, the chapter aims to see if and how are principles expressed by the courts in physical protest cases applied to cyber protests, or have the courts so far created precedents that leave no avenues for a cyber protest to qualify as a manifestation of the freedom of assembly. This chapter explores the issues of accountability, anonymity, symbolic speech, expressive conduct, violence, coercion and disruption in cyber sphere and how the problematics of distinguishing between public and private space is solved in online and offline protest cases.

Based on conclusions made in the previous three chapters, the fourth chapter aims to come up with a model set of rules that online protests should meet in order to be regarded as legal. In order to put the model into context, some of the most controversial and notable hacktivist operations are analysed in the light of the draft rules. Need for a new regulation has been increasingly brought to fora by academics, on top of that Council of Europe (CoE) is currently drafting a report on freedom of assembly and association on the internet. Among other issues CoE´s report aims to tackle the question of whether and to what extent should there be a right to digital assembly and admits that universal criminalisation might have a negative effect e-democracy as a whole. In the draft report CoE admits the potential need for an analytical framework, which would be able to address specific elements such as intent (to protest or express political or social dissent, to get the attention of the general public and contribute to the political debate) and overall impact (causing of temporary harm as opposed to permanent negative consequences for the general public), and to put in balance all these considerations.[14] One of the essential benefits of this kind of framework according to CoE is that it would enable national authorities in particular law enforcement authorities and judges to consider the different elements on a case by case basis.[15]

[14] Council of Europe, Report on the Freedom of Assembly on the Internet, 30. Sept 2015.
[15] Ibid.

Methodological remarks

Numerous high profile studies have been published on the problematics of applying humanitarian and criminal law designed for physical space in the cyberspace, significantly less has been written on the implications on the freedom of peaceful assembly and the civil society as a whole. The thesis applies qualitative research method to explore in which regards is "cyber" different and in what way is it just the same as the physical world, by applying analogy where possible and suggesting alternative approaches where not. This is achieved by conducting extensive desk research, which is followed by a systematic review of scholarly literature and primary legal sources.

While doing that the author dwells on acknowledging that "when such analogies are appropriately chosen and systematically applied, they can clarify the present situation and offer decision-makers strategic insight; vice versa, poor analogies obscure objectives, unnecessarily complicate choices, and create blind spots. In every case, analogies are bound to fail unless they incorporate objective analysis and their hand is not overplayed."[16] Although comparative legal analysis is not the primary methodology of the thesis, since only a supranational legislation would be capable of regulating cyberprotests or any other cyber phenomena, examples of case law and legislation are brought from different jurisdictions.

The first three chapters of the thesis are of reflective character and aim to give an overview of the current legal framework and the problems that it entails, the last chapter takes a prescriptive turn and attempts to propose solutions to the main research question: "How should a legally acknowledged cyber protest be regulated?"

[16] Czosseck, C. and Geers, K. (Eds.). The Virtual Battlefield: Perspectives on Cyber Warfare. Vol. 3. Ios Press, 2009, p vii.

1. Comparison of offline and online protests

1.1. Why there should be room for civil disobedience both offline and online?

From a purely positivist perspective, when the main riddle is phrased as: "When are illegal acts legal?", legal analysis of civil disobedience has been deemed tautological, since the definition itself implies acting contrary to the law. Therefore the scholars representing strict legal positivism have often argued that the quests for the justification for civil disobedience within the law are futile to begin with[17]. However counterintuitive or tautological, a large body of work exists on the matter. The peak period of writing and publishing on civil disobedience through the lens of modern jurisprudence were the 1960-s and 1970-s, due to the influential opposition movements like the civil rights movement and the widespread anti-war protests. As new forms of civil disobedience are moving the boundaries and the purely positivist approach is sometimes thought of as incapable of effectively tackling the jurisdictional and regulatory conflicts in cyberspace, the natural law theory of civil obedience is highly suitable in discussing the legal status of cyber protests.

Dan Svantesson writes about applying natural law theory in cyberspace:
"In embracing natural law theory as our savior, we need not seek refuge in some mysterious metaphysical reasoning to justify this approach. All we need to do is to ask what alternatives there are. I have found none and would, thus, in the interest of advancing this area of law, like to challenge my fellow scholars to put forward a superior alternative."[18]

The most commonly presented classical natural law justification of civil disobedience is based on the premise that complying with unjust laws equals opposing to the establishment of just and efficient laws and institutions. Often examples of undemocratic legal systems are brought in order to illustrate this principle and it is claimed that although in general laws have to be followed, but not for example in Nazi Germany or Communist Soviet Union. These arguments tend to fall short because their credibility relies excessively on historical perspective and distance. A future-looking or present-focused and applicable concept of civil disobedience is therefore still largely up to discretion[19].

[17] See, *e.g.* Powell Jr. L. F. Lawyer Looks at Civil Disobedience. Washington and Lee Law Review 1966, vol. 23, pp 205-207.
[18] Svantesson, D. The Holy Trinity of Legal Fictions Undermining the Application of Law to the Global Internet. International Journal of Law and Information Technology 2015, 23 (3), pp 219-234.
[19] Habermas, J. Civil Disobedience: Litmus Test for the Democratic Constitutional State. Berkeley Journal of Sociology, 1985, pp 95 -116, p 98.

John Rawls' has defined a civil disobedience act as a public (*a*), non-violent (*b*) and conscientious (*c*) act contrary to law (d) with the intent to bring about a change in the policies or law of the government (*e*). [20] Rawls´ definition thus consists of five elements, which cumulatively have to be met by acts of civil disobedience.

Rawls argues in favour of civil disobedience that constitutional drafting in a nearly just society is always a case of imperfect procedural drafting, which means that there can be no guarantee that the enacted legislation is just, even though a standard of just legislation has been established. By agreeing to form a democratic constitution, an individual agrees to comply with the majority rule and the laws enacted under it. While a citizen submits in his conduct to the judgement of the democratic authority, he does not submit his judgement to it. The disobedient express, that from their viewpoint the conditions of social cooperation are not being followed.[21] Civil disobedience should however not be seen as a normal means of dialogue, but is addressed to the sense of justice of the majority in cases of clear and severe violations of justice that are followed by a deliberate refusal of review and correction. Another condition that needs to be met is that the disobedient act would be reasonably expected to bring about the pursued consequences. Later analysis gives proof that online protests too have led to the sought result.

While reflecting on the different techniques adopted during the antiwar student protests that took place in the US during the 1960-s and 1970-s, Harrop A. Freeman lists the terms most frequently used terms connected to the activities: (1) non-resistance, (2) passive resistance, (3) non-violent resistance, (4) super-resistance, (5) non-violent non-cooperation, (6) non-violent direct action, (7) civil disobedience, (8) non-violent coercion, (9) war or revolution without violence, (10) Satyagraha or soul force, (11) pacifism. All of the terms (with perhaps the exception of 10), have remained relevant in the general protest discourse.[22] As the four underlying active concepts Freeman lists coercion, force, violence and resistance. He proceeds to define each concept respectively. Force is the physical power to effect change in the material or immaterial world. Coercion is the use of either physical or intangible force to compel action contrary to the will of the individual or group subjected to the force. Violence is the wilful application of force in such a way that it is physically injurious to the person or group against which it is applied. Resistance is any opposition either physical or psychological to the will or action of another; it is the defensive counterpart of coercion. Direct action traditionally encompasses forms of protest that seek an

[20] Rawls, J. A Theory of Justice. Cambridge MA, Harvard University Press 1971, p 364.
[21] Ibid.
[22] Freeman, H. A. The Right of Protest and Civil Disobedience. Indiana Law Journal, 1966, 41(2), pp 229 – 231.

immediate result such as strikes, boycotts, however often techniques the more proactive methods of awareness raising such as demonstrations and blockades also are included in the concept.[23] From the aspect of cyber civil disobedience, the most relevant concepts in Harrop´s systematisation would be (6) non-violent direct action, (7) civil disobedience and (8) non-violent coercion.

Freeman defines force and violence narrowly, meaning that the first encompasses only physical acts and the second applies only to offenses against persons, leaving violent acts against property out of the scope. In case of cyberattacks that have not evolved into full-blown episodes of terrorism, we can mostly talk about violence against property. Freeman sees civil disobedience as the median term among the listed concepts, however his definition of civil disobedience is another aspect where his approach might prove to be too narrow and fall anachronistic. Namely, "[I]t (civil disobedience, A.V) has one distinguishing characteristic: it is against a specific law or act of the State having the effect of law, which is disobeyed; and the law is that of the state having jurisdiction of the protestor. In a very real sense, therefore, civil disobedience is civil non-violent resistance or coercion just as we speak of "civil" war.*"* This limits the definition to cover only to acts that are committed within one jurisdiction, which makes the application of the concept to cyber protests particularly complicated.[24] A good example that exceeds the definition of civil disobedience is the aforementioned DDoS in support of the Zapatista movement which while organised by a movement based in the US against the Mexican government, succeeded in attracting participants from 46 countries across the world[25].

Another argument that has been brought in defence of civil disobedience is that on certain occasions the common law doctrine of necessity defence applies. For necessity defence to apply the applicants ought to prove lack of reasonable alternative courses of action and the direct causal relationship between the civil disobedience and the harm it seeks to avoid. In their influential article from 1984 Bauer and Eckerstrom[26] argue that a plain and simple interpretation of reasonable alternatives being equal to available alternatives falls slightly short-sighted since in reality a reasonable alternative would have to be an effective one.

[23] Ibid.
[24] Ibid.
[25] Jordan, T., Taylor, P. Hacktivism and Cyberwars: Rebels with a Cause? Routledge 2004, p 87.
[26] Bauer, S. M., Eckerström, P. J. The State Made Me Do It: The Applicability of the Necessity Defence to Civil Disobedience. Stanford Law Review 1987, vol. 39, no. 5, pp 1173-1200, p 1180.

While elaborating on the causal relationship, they bring an example from *United States v. Seward*, where police arrested antinuclear protestors for blocking a roadway. The district court required the defendants to establish that a reasonable man would think that blocking the entry to Rocky Flats (a nuclear weapons facility) for one day would terminate the official policy of the United States government as to nuclear weapons or nuclear power. They proceed to admit that according to such strict interpretation few acts could ever meet this standard, and those that do would most likely to be chastised even more by courts.[27] On the other hand a connection between the pursued aim and chosen form of protest should nevertheless exist. Therefore to assess whether an act of civil disobedience is justified, we should take into consideration whether it can be reasonably expected to contribute to the collective aim in question.

The latter is particularly relevant is a situation where all the power structures and traditional forms of governance are moving from real space to cyberspace. In the light of the general appraisal of e-participation and online citizen empowerment[28], it would seem only logical, legally and morally consistent, that somewhere in the discourse there would be a place for online civil disobedience as a natural manifestation of democratic collective action. However, mostly it is not the case, scholars and experts tend to stop the discussion at the point where it moves further from e-voting or petitioning into the transgressive forms of citizen participation. In other cases, instances of online civil disobedience are discussed without acknowledging the complexity of the legal status of such acts.[29]

To identify the research subject, key terms like protest, direct action and civil disobedience should also be briefly explained. These concepts cannot be used interchangeably, although the lines are vague. Protest is any form of organized public display of discontent, direct action has a stronger coercive element and it targets the object in a more immediate way, civil disobedience covers the whole array of legally ambiguous or illegal forms of protest and direct action, direct action again is perhaps the most widely misused among the three. Direct action is traditionally meant to cover forms of activism that attempt to immediately halt injustice, examples of direct action would be

[27] Ibid.
[28] See, *e.g.* Coleman, S. New Mediation and Direct Representation: Reconceptualizing Representation in the Digital Age. New Media & Society 2005, 7, pp 177-198.
[29] See, *e.g.* the discussion on the online protests against Lufthansa in Knaut, A. Informed Strategies of Political Action in IP-Based Social Media. International Federation for Information Processing. Eds. Hercheui, M.D *et al*. IFIP Advances in Information and Communication Technology. Springer 2012, pp 376-386; Rucht, D. Die Bedeutung von Online-Mobilisierung für Offline-Proteste. Ed Voss, K. Internet und Partizipation. Bürgergesellschaft und Demokratie. Springer 2014, 42, pp 115-128.

tree spikes or three sits. Since the author agrees with academics[30] who have claimed that most of the time online mass action does not constitute direct action, in that it does not seek immediate influence. Term online civil disobedience indicates legally unrecognised forms of cyber activism, protest refers to any means of online or offline collective action of expressive nature that aims to bring about political change, whereas the legality or illegality is not emphasised.

Helen Fenwick suggests a taxonomy of different forms of public protests, ranging from the peaceful expression of views to rioting that includes peaceful persuasion, offensive or insulting persuasion, intimidation, symbolic or persuasive physical obstruction or interference, actual physical obstruction or interference, forceful physical obstruction and violence.[31]

From Fenwick´s taxonomy symbolic or persuasive physical obstruction or interference and actual physical obstruction are the most relevant to online mass action protests, although the physical dimension is missing. Another distinction should be made between speech and protest, especially since the US techniques of protest that constitute forms of expression fall under the protection of the First Amendment, in Europe the European Convention of Human Rights and the EU Charter of Fundamental Rights foresee a freedom to assembly and association (Article 11). The level of protection granted to public protests does not vary remarkably across these legal systems, however the distinction has brought about captivating academic discussion and interesting case law on the question of expressivity of public collective action in the US[32], whereas in Europe the extent to which a public protest resembles actual speech is not held as important, although usually an assembly I thought to involve a certain degree expression.

This subchapter has mostly analysed the more traditional forms of civil disobedience and the arguments that justify them. Majority of them cannot be applied directly in cyberspace, since the concepts of public and private sphere, peace and violence are altered, not mention the requirement of physical presence, which has been rendered meaningless.

[30] Sauter, M. The Coming Swarm: DDOS Actions, Hacktivism and Civil Disobedience on the Internet. Bloomsbury Publishing 2014, p 111ff. ; Morozov, E. Pro-Wikileaks Denial-of-service Attacks: Just another Form of Civil Disobedience. Slate 2010 , Dec. 13 available online at : http://www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html (last accessed 1 May 2016)
[31] Fenwick, H. The Right to Protest, the Human Rights Act and the Margin of Appreciation. Modern Law Review 1999, 62(4), p 175.
[32] See *infra* chapter 3.2.

Drawing from the legal theories and positive law from both sides of the Atlantic, the key components of a justifiable civil disobedience are:

- peacefulness/non-violence
- public nature
- physical presence
- deliberate will to express opposition to a law or policy
- connected to the object of protest and could be reasonably expected to have an influence
- collective aim

1.2. Cyber protests

1.2.1. What is hacktivism?

1990-s witnessed an increasing politicization of the hacker community, when previously it had been mainly focusing to issues closest to the underlying technologies of it, during this period techniques of hacking started to be used for various political purposes. In her PhD thesis Alexandra Samuel introduced a model which enables to distinct hacktivism from other related forms of bottom-up political activity: civil disobedience, online activism and cyber-terrorism. On the conventional vs violent scale, hacktivism is located in the middle ("transgressive area" – something that exceeds the boundaries of social acceptability but is not necessary harmful or violent), with online activism being defined as conventional as opposed to the violent nature of cyber-terrorism. In contrast to hacktivism, civil disobedience is a wider term and usually refers to something that is taking place in the real-space. In online civil political action just as in case of cybercrime computer assisted activism (those forms of activism that pre-date Internet but which take a new life in cybersphere) and computer-focused activism (those forms of activism that have emerged in tandem with the establishment of the Internet, and could not apart from it)[33] can be distinguished.[34]

[33] Compare Furnell on cybercrime:"On this classification, the main way in which cybercrime can be subdivided is according to the role played by the technology i.e. whether the Internet plays a merely 'contingent' role in the crime (it could be done without it, using other means), or if is it absolutely 'necessary' (without the Internet, no such crime could exist). This kind of classification is adopted by policing bodies such as the UK's National Hi-Tech Crime Unit, which distinguishes between 'old crimes, new tools' and 'new crimes, new tools". Furnell, S. M., Warren, M. J. Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium? Computers & Security 1999, 18(1), pp. 28-34, 28.

[34] Samuel, A. Hacktivism and the Future of Political Participation. Unpublished PhD Thesis. Harvard University 2004, pp 4-6, available at: http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf (last accessed 1 May 2016)

Samuel´s dissertation defines hacktivism as following: A transgressive but non-violent type of political activism, which is exercised in the cybersphere. The leader of one of the first hacktivist groups Cult of the Dead Cow, Oxblood Ruffin defines hacktivism as "using technology to improve human rights across electronic media." According to Samuel's scale this definition seems more suitable to describe online activism. Alternative definitions include: illegal political or ideological action in cyberspace (linking activism with hacking), such as movements related to anti-globalization, animal rights, workers´ rights, movements against wars, environmental changes, piracy organizations, etc. (e.g. the Anonymous group).[35]

In 1998 a hacktivist group called Electronic Disturbance Theatre's (EDT) attempted to support the Zapatistas through online action. They launched a software tool called Floodnet that constantly reloaded a targeted website (often that of the Mexican President in an attempt to slow it down by bombarding it with requests. Floodnet also automated the production of satirical messages from the targeted site.[36] For example, someone targeting a computer would see messages reporting a failure to find a page on a site, with the automated message reading something like 'no human rights found on this server' or 'no democracy found on this server.[37]

During the World Trade Organization (WTO) meeting in Seattle in 1999, there were simultaneous online and offline protests. As demonstrators occupied the streets, hacktivists occupied websites. These protests were set up by a group called the Electrohippie Collective. The electrohippies created a small software program that was embedded in a webpage. Anyone who chose to go to that web-page to participate in the protest would automatically download a copy of the program and begin using it from their computer. The program repeatedly loaded pages from the WTO network. If enough people went to their site, if enough computers were thus running the ehippies program, the WTO network would be overwhelmed with requests and brought down.

A healthy amount of citizen activism (including disobedience) is nothing to be afraid of and is protected by the freedom of expression and assembly, which both constitute cornerstones of the principle of democracy. Therefore, while malevolent "black hat" hacking is quite clearly a crime or sometimes even terrorism, hacktivism falls to a certain extent under the scope of fundamental freedoms. Michael N. Schmitt has created a criteria, according to which to assess of whether or not a form of hacktivism falls under the definition of terrorism. Only when an attack is a) designed

[35] Bernik, I. Cybercrime and Cyber Warfare. John Wiley & Sons 2014, pp 73.
[36] Jordan, Taylor, (2004), *supra nota* 25.
[37] Ibid, p 90.

to be b) sufficiently destructive as to b) severely harm and d) terrorize civilians, it becomes cyber-terrorism.[38] To assess the lawfulness of web sit-ins and other forms of political hacktivism, Schmitt's criteria[39] is used for establishing if a cyber activity can be qualified as use of force or a softer measure. Digital activism (publications, petitions and lobbying) is considered to be legitimate means of expression and does not score high on Schmitt's criteria.[40] But these measures are not exclusive to the internet and are older than the cyberspace, other strictly internet specific measures are more problematic. The preconditions described above leave a wide margin of interpretation and several questions arise. It includes an element of *mens rea* – a direct intent - and many undetermined legal conceptions (sufficiently destructive, severe harm and terrorize civilians*)*, for what reason every case of hacktivism has to be assessed on individual basis.

ENISA reports that throughout the observed years 2012-2015 the threat agent group has remained stable as regards motivation and capability levels. The report states:
"Some campaigns have been assessed during this year that fully comply with the activism attitude of this threat agent group. Some discussion/protests have taken place regarding the legal practice of sentencing hacktivists with the same rules as terrorists." [41]

As operations fully complying with the activist agenda the operations against Saudi-Arabian government[42] and Ku-Klux-Klan name leak[43] were referred to. Both would fall under the category of transgressive actions pursuant to Samuel´s division. The case in reference to the prosecution of hacktivists under terrorism laws was this of an Anonymous hacktivist Jeremy Hammond who had been on FBI´s terrorist watchlist for more than a year before he was arrested in 2013. ENISA also mention the perspective of state and hacktivist cooperation as a potentially extremely efficient tactic, while admitting that it would not always please the nations involved in such conflicts. In such cases when the hacktivist communities join forces and states the concept of *levée en masse*[44] might apply to the engaged hacktivist communities.

[38] Denning, D. The Ethics of Cyber Conflict. Wiley Publishers 2008, p 407.
[39] Schmitt, M. N. Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law 1999, 37, p 885.
[40] Denning (2008), *supra nota* 38, p 417.
[41] European Union Agency for Network and Information Security (ENISA). Threat Landscape 2015, p 38.
[42] Deutsche Welle, Anonymous targets Saudi-Arabian Government, 2 October 2015, available online at: http://www.dw.com/en/anonymous-hacktivist-explains-why-group-is-targeting-saudi-arabian-government/a-18758195 (last accessed 1 May 2016)
[43] The Guardian, Anonymous leaks a list of Ku Klux Klan Members, 6 November 2015 http://www.theguardian.com/technology/2015/nov/06/anonymous-ku-klux-klan-name-leak (last accessed 1 May 2016).
[44] Waters, C. New Hacktivists and the Old Concept of *levée en masse*. Dalhousie Law Journal 2014, 771 (37), pp 775-779.

In her book "Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger" U.S. information security analyst and former government and army official Julie E. Mehan presents a chart based on her research that paints quite a different picture of the dangers posed by hacktivists. The chart below shows the percentage of known, successful attacks attributed to hacktivism in 2013.[45] This might be explained by the fact that the majority of hacktivists´ targets have been US corporations or state agencies, and also by the grave impact of large-scale information leaks partially connected to hacktivist operations.

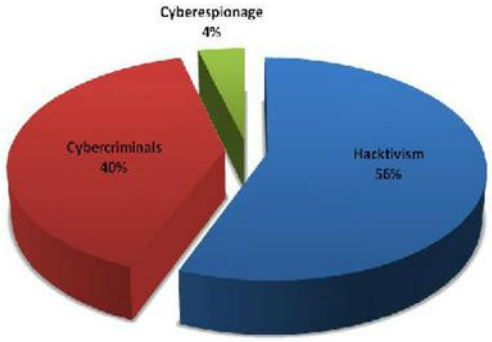

Figure 2. Percentage of known, successful attacks attributed to hacktivism in 2013.[46]

The line between a cyber terrorist and hacktivist is not always clear, ENISA for example considers the first to be ideologically and second socially motivated. Third category, the cyber fighter, on the other hand is nationally motivated, while cyber criminals tend to be driven by financial gain. This is another moment where cyber activism differs from its offline predecessor, the main factor separating activism from crime and terrorism is motivation, whereas the borders between ideology, social causes and nationalism are blurry to say the least.[47]

[45] Mehan, J. E. Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger. IT Governance Ltd 2013, 2nd ed., p 122.
[46] Mehan (2013), *supra nota* 45.
[47] An interesting case illustrating the discussion on the differences between hacktivists and cyber terrorist is of the Turkish hacktivist collective RedHack. RedHack is responsible for numerous high-profile and politically influential information leaks and DDoS attacks. From 2012 there have been ongoing investigations, some of suspected RedHack activists were investigated and sentenced under terrorism charges, in 2015 however the terrorism charges were overturned and replaced by computer offenses under the Turkish Penal Code, because RedHack activities did not constitute significant harm to the civilians and no evidence of terrorist motivation and no links to leftist and separatist terrorist groups could be established. See: Redhack members acquitted in terror case, Hurriyet news, available at: http://www.hurriyetdailynews.com/redhack-members-acquitted-in-terror-case.aspx?pageID=238&nid=79748 (last accessed 18 April 2016); Tatar, Ü., Çelik, M.. Hacktivism as an emerging cyberthreat. *Terrorism Online: Politics, Law and Technology* (2015), p 54 ff.

In the physical world the precept of "different goals-same methods" holds true perhaps for certain instances of most radical ecosabotage[48]. In the cybersphere on the other hand, a common device can be proliferated in a way that it enables to commit acts of espionage, crime or terror with an intensity and effect comparable to highly organised and abundantly financed state or separatist actors.[49] Christian Czosseck suggests in NATO CCDCOE´s "Peacetime regime for state activities in cyberspace" that the cyber attacks against Estonia in 2007 that are often referred to as the first cyber war in human history and partially responsible for the general cyber war hype of the following years, were in fact technically hacktivist operations, which gave proof that a massive uprising of mere citizens can indeed have an impact that a State might recognise as a national security incident."[50]

1.2.2. Which hacktivist tools would constitute the most suitable equivalent for a physical space protest?

Table 1: Different activist repertoires: some examples

	Offline	Online
Conventional	**Activism:** Voting Electioneering Non-violent protest marches Boycotts	**Online activism:** Online voting Online campaign donations Online petitions
Transgressive	**Civil disobedience:** Sit-ins Barricades Political graffiti Wildcat strikes Underground presses Political theater Sabotage	**Hacktivism:** Web site defacements Web site redirects Denial-of-service attacks Information theft Site parodies Virtual sit-ins Virtual sabotage Software development

Figure 3.[51]

[48] Welchman, J. Is Ecosabotage Civil Disobedience? Philosophy & Geography 2001, 4 (1), pp 97-107.
[49] Wittes, B., Blum, G. The Future of Violence: Robots and Germs, Hackers and Drones: Confronting A New Age of Threat. Basic Books 2015, p 27.
[50] Czosseck, C. State Actors and their Proxies in Cyberspace. Ed. Ziolkowski, K. Peacetime Regime for State Activities in Cyberspace. NATO CCDCOE 2013, pp 7-9. See also Rid, T. Cyber War Will Not Take Place. Journal of Strategic Studies 2012, 35(1), pp 5-32, p 8.
[51] Samuel (2004*), supra nota* 34, p 6.

Samuel brings examples of the most common hacktivist techniques, it becomes evident that while there are conventional online equivalents for forms of activism that are based speech and voting, activities that require physical presence and are more symbolic have only transgressive equivalents. Therefore, it can be argued that the legally permitted repertoire for an online activist is narrower than this of offline activists, since the activities that make up online transgressive activism are criminalised. Web-site defacement (E-graffiti) means modifying a site's content, but while graffiti is painted on the external walls of a building, website defacement is done from the inside, by breaking into the website and inserting the messages that an activist seeks to disseminate. Site redirect directing the target site's traffic to another website generally containing criticism at the address of the very institution that runs the target site. Document disclosure covers unauthorized access of the target's information flow and leaking the information received. The physical space equivalent of document disclosure would be common burglary. Virtual sit-ins and DDoS attacks both aim to slow down the target server by overburdening it with traffic. The main difference is that DDoS attacks are carried out by a network of inflicted computers, botnet (with voluntary or involuntary involvement), virtual sit-ins on the other hand require individual participation and are sometimes carried out by making subsequent requests manually or by implementing a code which automatically keeps reloading the target site. Technically however what Samuelson refers to as a virtual sit-in is also known as client-side DoS. The technological threshold separating online activism from hacktivism is whether or not there has been unauthorised intrusion into other parties´ network. The odd item on the list in this respect are again (D)DoS attacks that find their place in the transgressive division without necessarily involving unauthorised access.

According to ENISA Cyber threat landscape 2015, hacktivists are considered to be the primary source of threats such as web based attacks, web application attacks, botnets, DDoS, phishing, data breaches, identity theft and information leakage. Besides that, ENISA perceived hacktivists as a secondary threat group for spam, exploit kits and malware. Hacktivists are estimated to be the fourth influential threat group with approximately 2% of the attacks coming from socially motivated hackers[52]. ENISA cyber threat reports from 2012 from 2015 have detected DDoS as a threat of increasing occurrence and importance.[53]

Samuel´s and ENISA´s taxonomies can be easily consolidated, but we should keep in mind that a gap of 10 years that lies between the publication of Samuel´s dissertation and ENISA´s most recent

[52] For comparison see Mehan (2013), *supra nota* 45.
[53] European Union Agency for Network and Information Security (ENISA). Threat Landscape 2015, p 41.

threat landscape report. Another difference is that while Samuel focuses more on the external aspects of the forms of activism, on how they do come across to the general public, then ENISA bases its taxonomy on the precise technical steps that have to be taken in order to conduct any of these operations. ENISA does not distinguish between a virtual sit-in and DoS attacks, Samuel does not separate botnet enabled attacks from non-automated or volunteer conducted attacks. Website defacements and redirects classify as web application attacks, information theft might fall under both data breaches and information leakage. What Samuel refers to as virtual sabotage might be considered a web based attack, malware injection or web application attack in ENISA´s glossary.

As noted above, the majority of the attacks require illegal access, which in itself makes decriminalising them more complicated. The strictly computer-based elements of information theft and leakage are legally unambiguous, as they require breaking and entering into a system. The act itself has no socially symbolical meaning, the following steps of publishing and distribution on the contrary are significant to the freedom of expression and free society has a whole.[54] Since the legal questions surrounding information leaks and whistleblowing are not in fact technology-specific[55], these issues, though undoubtedly influential and live, are left outside of the scope of the present thesis.

Therefore as potential candidates for forms of digital civil disobedience, that are suitable equivalents for physical space collective action, we are left with website defacements and DDoS attacks. Pop-up[56] website defacements have been suggested to constitute a legitimate form of online protest, since they seem to overcome the private property problem. Most often (D)DoS attacks have been deemed as the heir of the legal and socio-political status of the physical world protests. The legal conundrums that surround the legitimisation of DDoS attacks include all the main problems associated with the freedom of assembly in the physical space and in addition pose new The questions about anonymity, accountability and proportionality. Because of their relevance and complexity these two hacktivist tools are analysed in more detail in the following subchapters.[57]

[54] See also Gillespie, A.A. Cybercrime: Key Issues and Debates. Cambridge University Press 2015, p 104.
[55] For a pre-Internet analogy of the Snowden revelations see, e.g. Medsger, B. The Burglary: The Discovery of J. Edgar Hoover's Secret FBI. Vintage Press 2013.
[56] Zatz, N. Note, Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment. Harvard Journal of Law & Technology 1998, 12, p 149.
[57] Hampson, N.H. Hacktivism – a New Breed of Protest in a Networked World. Boston College International and Comparative Law Review 2012, vol. 35, pp. 511-542, p 540.

1.2.2.1 Denial of Service and Distributed Denial of Service attacks

From the legal viewpoint, the most controversial of the hacktivist measures are (distributed) denial of service, (D)DoS, attacks, for they have the power to cause significant damages, yet when supported by strong political agenda and carried out in moderation, they offer a tool whereby the object of protest cannot avoid being targeted by virtue of its power or its location, or a people's poverty or oppression.[58] In essence DoS refers to a cyber-attack "which prevents a computer user or owner access to the services available on his system"[59]. Such an attack can be performed without direct access to a system, by flooding Internet-accessible computers with communications, so that they become 'overloaded' and are rendered unable to perform functions for legitimate users.

DDoS attacks may involve hijacking the servers belonging to third parties who have in no way expressed their consent to participate in such activities, also the critical mass of requests can be achieved by voluntary participation. At its most basic level, a denial-of-service attack seeks to render a server unusable to anyone looking to communicate with it for legitimate purposes. When this attack comes from one source, it is called a denial-of-service, or DOS, attack. When it comes from multiple sources, it is called a distributed denial-of-service, or DDOS, attack.[60] EDT used a tool called FloodNet for creating traffic to target websites, Anonymous operates a similar tool called LOIC. The FloodNet tool was created in 1998 by the EDT and operated by[61] exploiting the Java reload function. Participants ran FloodNet from a browser window by navigating to a specific page and allowing the tool to run in the background. FloodNet stayed true to one-person/one-computer operation model, refusing to amplify the resulting flow of traffic with tools such as botnets (volunteer or otherwise) or other exploits.[62]

LOIC was first developed by an open source software engineer Praetox as a stress testing tool, various later versions and alterations are available on GitHub. A major breakthrough in the development of LOIC occurred when a developer called NewEraCracker added a functionality called HiveMind, which enabled the users to become a part in a voluntary botnet that was remotely controlled by AnonOps administrators. This broke the principle of one person/one computer and thus constitutes a major step away from being equivalent to the physical space assemblies.

[58] Ibid.
[59] Esen, R. Cyber Crime: A Growing Problem. The Journal of Criminal Law 2002, 66 (3), 269-283, p 270.
[60] Sauter, M. "LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. American Behavioral Scientist 2013, 57(7), p 1002.
[61] Jordan, T. Activism! Direct Action, Hacktivism and the Future of Society. Reaktion Books 2002, p 124.
[62] Sauter (2013), *supra nota* 60.

FloodNet and a later JavaScript version of LOIC functioned from a website, while the two abovementioned versions of LOIC required download and installation.[63] The JavaScript enabled LOIC was used for the first time for operation MegaUpload, in 2014 a new feature was introduced that broke the principle of voluntarism by making bona fide bystanders click on a link *#opmegauploadretaliation* and thus participating in a DDoS attack. This development was later chastised by many members of the group.

The amplification factor therefore is crucial also in deciding whether similar fundamental rights should be granted to cyber protesters, or even in deciding to what extent should a particular act of DoS/DDoS be criminalized. In 2006 Richard Clayton wrote in his paper on the technical aspects of criminalizing DoS/DDoS attacks:

"It would be unwise to make a distinction between cyberprotest and DoS/DDoS by concentrating on the tools that are used (even standard browsers can be scripted in standard ways, so there's no need for a special program to be built) but the emphasis should be placed upon intent and amplification... one might still prosecute for excessive noise if a single protester brought a lorry with 100 bullhorns to a demo, whereas 10,000 protesters, just 100 of whom had a bullhorn, might well escape action by the authorities."[64]

Anonymous is notorious for its DDoS attacks and even labelled as a terrorist group by some authorities. In 2012 Keith Alexander, the general in charge of the U.S. Cyber Command and the director of the National Security Agency, warned that "the hacking group Anonymous could have the ability within the next year or two to bring about a limited power outage through a cyberattack."[65]

If this sinister prediction would ever turn into reality, then Anonymous would definitely be worthy of the title. However until today its actions do not meet the criteria set above, even massive DDoS attacks do not count as something designed to severely harm the civilian population. Every protest brings about inconveniences, strikes suspend the traffic, or shut down schools hence infringing with the right to education, interrupt the work of the factories and therefore quite obviously are

[63] Ibid.
[64] Clayton, R. Complexity of Criminalising Denial of Service Attacks, 2006, available online at: http://www.cl.cam.ac.uk/~rnc1/complexity.pdf (last accessed on 1 May 2016)
[65] Benkler, Y. Hacks of Valor: Why Anonymous is Not a Threat to National Security. Foreign Affairs 2012, vol. 2, available online at: http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor# (last accessed on 1 May 2016)

not in perfect line with the freedom of entrepreneurship. A protest designed to please everyone directly or indirectly involved would not be a protest at all. Professor of Information Law at Harvard Law School Yochai Benkler sums the inevitability of annoyances up as following: "When addressed, these actions should be treated as a disruption to the quality of life, similar to graffiti."[66]

To step out of the legal grey area, in 2013, Anonymous submitted a "We the People" petition asking the White House to recognize DDoS attacks as a valid form of protest protected by the First Amendment. Anonymous analogized DDoS attacks to physical "Occupy" encampments, arguing that protestors are similarly "occupying" a particular webpage through the use of repeated refreshes to delay or deny access to that virtual location for a finite period of time. The petition states that:

"With the advance in internet technology, comes new grounds for protesting. Distributed denial-of-service (DDoS), is not any form of hacking in any way. It is the equivalent of repeatedly hitting the refresh button on a webpage. It is, in that way, no different than any "occupy" protest. Instead of a group of people standing outside a building to occupy the area, they are having their computer occupy a website to slow (or deny) service of that particular website for a short time."

As part of this petition, those who have been jailed for DDoS should be immediately released and have anything regarding a DDoS, that is on their "records" cleared.

During the cyber-attacks against Estonia against 2007 only one person was prosecuted under §206 of the Penal Code, a second year student of Tallinn University of Technology who participated in a DoS attack targeted at the website of the Reform Party, he was charged with a fee of 17 500 kroons.[67] The cyber-attacks against Estonia included various activities, including those, which by character are pure manifestations of hacktivism and some, which obviously crossed the line between progressive social activism and political crime.

Some authors argue that DDoS attacks with voluntary participation can be perceived as a form of assembly and legitimate civil activism. Among social activists there have always been the ones who have yearned for destruction or made the shift from disobedience to violence out of ignorance. Setting cars on fire and robbing shops are plain and simple offences against property, expressions

[66] Ibid.
[67] HMKo 13.12.2008, 1-07-15185.

of fury, which are not immediately connected to the political rationale of the movement.[68] These acts are aimed at destruction not interruption, voluntary DDoS attacks on the other hand do not aspire to demolish a site but only cause more or less grave setbacks in its functioning. This of course does not indicate that indiscriminate, maleficent large-scale DDoS-ing should be legally or ethically justified.

In 2010 after Anonymous had organised a wide-scale DDoS attack against MasterCard and Amazon for cutting off the donations to WikiLeaks, heated disputes on the criminality of this act followed. American open software pioneer Richard Stallman acclaimed in The Guardian that in his opinion the attacks represented a new form of protest and should not constitute cyber crime. He wrote:

"The Anonymous web protests over WikiLeaks are the internet equivalent of a mass demonstration. It's a mistake to call them hacking (playful cleverness) or cracking (security breaking). The LOIC program that is being used by the group is prepackaged so no cleverness is needed to run it, and it does not break any computer's security. The protesters have not tried to take control of Amazon's website, or extract any data from MasterCard. They enter through the site's front door, and it just can't cope with the volume... No – the proper comparison is with the crowds that descended last week on Topshop stores".[69]

Benkler seconds to Stallman´s argumentation, writing that:

"A DDoS attack causes disruption, not destruction, and the main technique that Anonymous has used requires participants to join self-consciously and publicly, leaving the internet addresses traceable. By design these are sit-ins: Participants illegally occupy the space of their target."[70]

After operation PayBack, the grapevine of the US hacker community 2600 took a contrary stand and published an editorial note where it chastised the operation, saying that:

"While there is great sympathy in the hacker world for what Wikileaks is doing, this type of activity is no better than the strong-arm tactics we are fighting against. These attacks, in addition to being a misguided effort that doesn't accomplish very much at all, are incredibly simple to

[68] Benkler (2012), *supra nota* 65.
[69] Richard Stallman, "The Anonymous WikiLeaks Protests Are a Mass Demo Against Control", The Guardian 17.12.2010, available online at: http://www.theguardian.com/commentisfree/2010/dec/17/anonymous-wikileaks-protest-amazon-mastercard (last accessed 1 May 2016)
[70] Benkler (2012), *supra nota* 65.

launch and require no technical or hacker skills. While writing such programs requires a good degree of ingenuity and knowledge of security weaknesses, this doesn't mean that everyone who runs them possesses the same degree of proficiency, nor should we necessarily believe people who claim to be doing this on behalf of the hacker community. There are a number of positive steps people - both inside and outside of the hacker community - can take to support Wikileaks and help spread information. This is never accomplished when all one tries to do is silence one's opponent. That has not been, and never should be, the hacker way of dealing with a problem."[71]

As it also draws from 2600´s note, another argument frequently brought against the legitimation of certain instances of DDoS attacks is that they are censorial by nature and exercising freedom of speech or assembly by silencing opponents is like fighting fire with fire, meaning that the chosen method is detrimental to the cause. In addition to that, it is frequently claimed that since in its basic character a DDoS attack is an anti-communicative weapon, it fails to get across any social message and the general public perceives it most often simply as a nuisance without acknowledging its real causes.[72] Furthermore, low participation threshold is sometimes thought to render DDoS attacks into mere manifestations of "slacktivism", which implies that the participants are not always deeply invested in the political causes in question. However, the same low participatory threshold grants (D)DoS attacks a truly democratic and indiscriminate character, which when combined with strong political agenda has the potential to become a powerful form of protest.

1.2.2.2 Website defacements

As opposed to (D)DoS attacks, website defacements and redirects do require illegal access and altering of the computer data. A website defacement occurs when an attacker breaks into a web server and defaces the hosted website. Once defaced, the website, or at least some of its pages, may no longer appear or function as it did before. Besides that many associate,d damaging effects may occur such as, damages relating to the reputation of the business, legal entanglements—when transactions, reports filling and the like fail to be available.

[71] Doctorow, C. 2600 Magazine condemns DDoS Attacks against Wikileaks Censors. available online at: http://boingboing.net/2010/12/10/2600-magazine-condem.html (last accessed 1 May 2016)
[72] Li, X. Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime. Harvard Journal of Law and Technology 2013, 27, p 301; McLaurin, J. Making Cyberspace Safe for Democracy: the Challenge Posed by Denial-of-service Attacks. Yale Law & Policy Review 2011, 30(1), pp 211-254, p 245.

A very illustrative and clear-cut case of website defacement occurred during the 2007 cyber attacks against Estonia, when an apology was published on the homepage of the leading coalition party. In the apology written in Russian the then Estonian Prime Minister Andrus Ansip apologized for deporting a Soviet World War II war memorial and declared that from then he considers the relocation of the latter to be his personal responsibility.

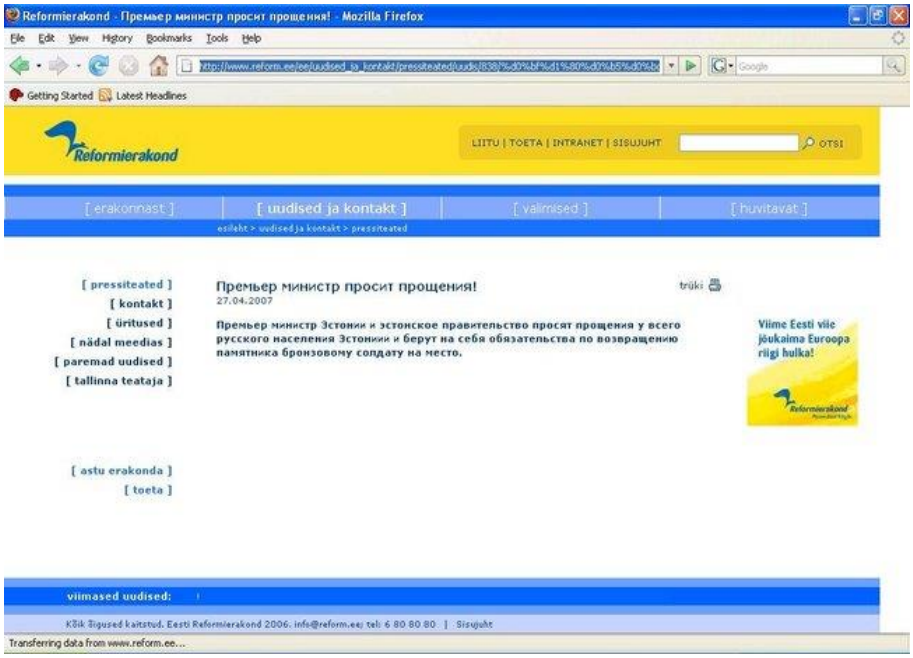

Figure 4. Defaced website of the Reform Party.

In addition to directly modifying the contents, websites can be defaced by changing their scripts so that running the URL would open pop-up windows, which the hacktivists can use for conveying their messages. Li considers the foremost reason why First Amendment cannot protect (D)DoS attacks to be that they take place on someone else´s property. He argues that a pop-up website defacement is the closest that it can get to a legitimate online protest.[73]

Although a pop-up that displays obscene materials is unlikely to qualify for First Amendment protection a pop-up window that displays a message with substantive criticism of the target likely meets the test for symbolic speech. In the latter case, the intent to convey a symbolic message is readily discernible from the content, and the audience viewing the pop-up window is likely to understand that message, regardless of whether or not the audience sympathizes with it.[74]

[73] Ibid, p 327.
[74] Li (2013), *supra nota* 72.

This however mostly applies to the result of the pop-up website defacement, the act leading to it however is possibly more intrusive than running a voluntary (D)DoS attack. Although, a pop-up website defacement may look like an online version of a flashmob or graffiti, pop-ups are created usually by exploiting the site´s vulnerabilities and altering the site´s code. This is not what Stallman would call entering through the main door.[75] Though, more convenient to the public and arguably less of a nuisance to the site owner, pop-ups created using cross site scripting or SQL injections are equally infringing upon the right to property. The western approach to cybersecurity, which sees code as the predominant threat and also the main object of protection in the cybersphere[76], would probably perceive both on-site and pop-up website defacements that alter code as fundamentally more intrusive. However, as Li argues, pop-up website defacements by not rendering the site inaccessible would indeed be less invasive towards the content of the original webpage than a (D)DoS attack[77], the same cannot be said about the code. Therefore since from the viewpoint of the code, a pop-up website defacement does not in fact overcome the private property problem, and furthermore is more of a tool of a lone activist/criminal and not so suitable for collective action, the following parts of the thesis focus on the legal status of (D)Dos attacks as the closest analogy for physical space protests.

1.3. Conclusions

What then are the main differences and similarities of online and offline protests that are germane to the legal regulation? The main difference from which all the following ones derive is obviously the requirement of physical presence. When the expression of discontent is separated from the physical person, the mass of participants and impact that a protest might have is not anymore proportionate to the number of people willing to fight for the cause, but often bound to the employed technical means and skills. The second consequence of such separation is the presumed anonymity of cyberprotesters, which again leads to the issues of accountability and impunity[78]. One of the justifying arguments for civil disobedience is the participants´ willingness to be identified and held accountable for the misconduct. This is equivalent to a kind of martyrdom, readiness to sacrifice personal freedom or assets in order to communicate the gross injustice of

[75] Stallman (2010), *supra nota* 69.
[76] Kerr, O. Are We Overprotecting Code - Thoughts on First-Generation Internet Law. Washington and Lee Law Review 2000, 57, p 1287.
[77] Li (2013), *supra nota* 72, p 325.
[78] Sorell, T. Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. Journal of Human Rights Practice 2015, p 17.

positive law[79]. It is often argued that this aspect of martyrdom is missing from the ethos of cyberprotesters.[80]

Another problem that comes with the absence of physical presence is the question of (non-) voluntarism, meaning that while in the physical world the participants´ consent can be assumed, in the cyberspace many among the computers that are involved in an attack do not represent an owner who cares for or is even aware of the cause that is being fought for. And lastly, another feature that distinguishes online protest from their physical space predecessors is that its most common techniques and methods are confusingly similar to these employed by terrorists, criminals and in the course of active defence, hackback operations or sometimes espionage also by state actors. This kind of distribution of offensive capabilities among an interdependent network of almost equally potent and borderless threats and agents is highly characteristic to the warfare, crime, terror and also indeed civil disobedience of the new digital era[81].

In the physical space protest methods are quite specific to civil movements, we do not see criminals, terrorists or spies demonstrating their viewpoints on the streets, since usually secrecy is an underlying condition for their success. Cyberprotesters on the other hand can be (, albeit sometimes with great difficulties) identified by the authorities, but usually they remain unknown to the wider society, the opposite is true in physical space where the mass of protesters on the contrary seem to remain anonymous to the authorities, unless asked to identify themselves, but seek the attention and recognition of the general public.

Moving on to the similarities that speak in favour of applying the physical space analogy in cyberspace, we see that the main shared characteristic is motivation. Both online and offline civil disobedience is triggered by the wish to raise public awareness and ultimately to bring about change in society. This again leads to complications in establishing what can be considered to be an effective means of protest, since a reasonable protest has to be effective, while not achieve its efficiency through terror or coercion. Therefore the direct action element should be strong enough to deliver the message across the interested groups and also send a sufficiently clear signal to the targets, saying that in order to maintain or gain public approval and basic ethical standards they should change their practices. At the same time the inconvenience and damage caused to the target

[79] Rawls (1971), *supra nota* 20, p 366.
[80] See, *e.g.* Sorell (2015), *supra nota* 78; O'Malley, G. Hacktivism: Cyber Activism or Cyber Crime. Trinity College Law Review 2013, 16, pp 156-158.
[81] Wittes, Blum (2015), *supra nota* 49.

and public should not evolve into a general sense of fear and terror. Inconvenience is another common feature and in order to be able to regulate (cyber)protests, one should determine how to estimate the proportionality. Another common and crucial intricacy is this of the private and public space. Courts have oscillated between prioritizing property rights over the freedom of assembly and vice versa, considering the increasing privatization of the public sphere, completely ruling out the freedom of assembly on private property entangles numerous social risks that a regulation of protests should aim to mitigate. The next chapter explains how these aspects are usually ignored in the current cybercrime regulation, international fundamental rights norms on the other hand include principles that in theory may be applied to cyber protests but this allegation has to date yet to be substantiated by a court.

2. Current legal framework

2.1. Criminal and humanitarian law

2.1.1. Regional instruments

Despite, the countless hardships in establishing geographical jurisdictional borders in cyberspace, states, international and regional organisations have made endeavours on the regulatory level to address the questions of internet jurisdiction. The consensus seems to be while efficient law enforcement is obscured in the borderless online world, the starting points to solve the riddle would be harmonisation and mutual assistance. In November 2001 the Council of Europe published the Convention of Cybercrime for signatures. Article 5 of the Convention states that "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 serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."[82] Therefore, Article 5 calls for inter alie the criminalisation of DDoS attacks. Qualifications include that the hindrance must be unauthorized (without right) and intentional. Explanatory note of the Convention elaborates that "Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."[83]

Botnet-operated DDoS attacks also constitute illegal access according to Article 2 since the victims´ computers are accessed, and data interference under Article 4, since malware in the victims' systems alters the data so that it will enable the criminals to take remote control of the computer. In cases where DDoS attacks are used as extortion tools or as a method to distract attention from other crimes, they are penalized under Article 11 on aiding and abetting.

Article 83(1) of TFEU gives European Union the competence to harmonise national criminal law in limited areas, computer crime being on area where the EU has to act and identify common standard between Member States. A Commission note on Network and Information Security

[82] CoE, Convention on Cybercrime, CETS 185, 23 November 2001.
[83] CoE, Explanatory Report to the Convention on Cybercrime. Budapest, 2001. available online at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.

highlighted the potential effects of not addressing in computer crime on the EU area of freedom, justice and security. In 2001 the Council of European Union adopted the Framework Decision on Attacks against information Systems, which contained the principal definitions of technical terms and offences and recommended sanctions. In 2013 the need to widen and update the scope of offences led to the introduction of EU directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.[84] The directive prescribes that Members State ought to criminalize illegal access to information systems (Article 3), illegal systems interferences (Article 4) and data interferences (Article 5). The Directive foresees that these acts have be unauthorized to be punishable as a criminal offence, again Member States have been left with some room for deliberation: criminalizing these offences is only mandatory for cases which are not minor. The penalties for the aforementioned offences ought to be effective, proportionate and dissuasive, with imprisonment terms ranging from 2 or 3 (system and data interferences affecting multiple systems) years.[85]

Recital 11 of the Directive explains that the Directive provides for criminal penalties at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. A case may be considered minor, for example, where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary. Recital 29 of the Directive emphasises that the Directive respects human rights and fundamental freedoms, including freedom of information and expression. Freedom of assembly is however not mentioned.

The most recent regional instrument, the African Union Convention on Cyber Security and Personal Data Protection[86] calls for the Member States to adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. Article 29 forbids the hindering,

[84] Summers, S. et al. The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society. Bloomsbury Publishing 2014, p 234 ff.
[85] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
[86] African Union Convention on Cyber Security and Personal Data Protection, available https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (last accessed 1 May 2016).

distortion or an attempt to hinder or distort the functioning of a computer system. This wording most evidently also covers DDoS, similarly to the European instruments, the AU Convention also acknowledges that while implementing the rules international human rights standards should be followed. Furthermore, it acknowledges the tertiary position of civil society in the cyberspace, stating in Article 26(1) that fostering the involvement of civil society is one of the essential facets of the promotion of cyber-security culture.

2.1.1. International instruments

The draft international code of conduct for information security proposed by the member states of the Shanghai Cooperation Organisation calls the parties to recognize that the rights of an individual in the offline environment must also be protected in the online environment and rapidly goes on to mention the grounds on which these rights may be restricted.[87] Since the code is essentially more concerned with information security, this mainly encompasses content-related rights to information and expression, which are subject to certain restrictions as provided by law and necessary for respect of the rights or reputations or others of for the protection of public interests. The code does not foresee any specific norms for combating DDoS attacks, however its main emphasis on state sovereignty, regime stability, military issues. Furthermore, as follows from above it allows for the curtailing of the international human rights so that they would comply with relevant national laws and regulation. The code therefore states that human rights, including the right to peaceful assembly, might stand inferior to national laws.

Difficulties in identifying and classifying the status of civilian hacktivists conducting operations similar to these of cyber combatants in the context of armed conflict make international humanitarian law another branch of law that might occasionally determine the position of hacktivists. NATO's Tallinn Manual on the International Law Applicable to Cyber Warfare applies to cyber operations that take place in the context of international armed conflict explicitly permits the elimination of civilian hackers in "war scenarios." The Tallinn Manual's Rule 30 offers defines cyber-attack as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. Although causing disruption, confusion and defacement, it is unlikely that physical harm to persons or physical

[87] Shanghai Cooperation Organisation, International Code of Conduct for Information Security, available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf (last accessed 1 May 2016).

objects could be attributed to a DDoS attack[88]. These activities, therefore, likely fall below the threshold of "consequential harm" and are therefore unlikely to fall under the category cyber attacks within the meaning of the manual. As the manual´s editor in chief Michael N. Schmitt states, "state practice provides no support for the notion that causation of inconvenience is intended to be prohibited in international humanitarian law."[89]

Rule 27 does, albeit tacitly and with serious qualifications, provide for *levée en masse.* It states: "In an international armed conflict, inhabitants of unoccupied territory who engage in cyber operations as part of a *levée en masse* enjoy combatant immunity and prisoner of war status." The notion of direct participation of civilians in cyber operations is addressed in Rules 29 and 35. The Manual states that attacks by non-state actors can trigger the right of self-defence. The latter is probably the most contested rule in the manual, since it had been often interpreted as creating the grounds for disproportionate counter-attacks targeted towards civilians.[90]

Schmitt has commented on these issues in an interview given to New Scientist in 2013[91]. When asked whether a serious cyberattack conducted by a non-state hacktivist group could warrant an armed response, he explained the viewpoints presented among the group of experts. A minority of the group believed that the law of self-defence only applies to cyber operations that qualify as armed attacks if they are conducted by states, in case of other actors regular law enforcement should be applied. The majority on the contrary concluded that the law of self-defence applies to cyberattacks by non-state actors if they are organised groups. If a terrorist group launches cyber operations at an armed-attack level, the NATO panel felt that a state could respond in the same way as you could if a terrorist group were bombing you. However, when a lone activist is behind the attack, according to the panel the law of self-defence would not apply, since we would be simply dealing with an individual conducting a severe crime. The main criteria foreseen in the Tallinn Manual that a hacktivist operation should meet to be considered an attack are therefore the level of organisation within the hacktivist group and severity of the danger posed to national security. In reality, this would limit the application of the rule to attacks against critical information infrastructures.

[88] Schmitt, M. N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press 2013, pp 102, 106.
[89] Schmitt, M.N. Cyber Operations and the Jus in Bello: Key Issues, 41 Israel Yearbook of Human Rights 2011, p 105.
[90] See for example: Marks, P. The Right to Bear Cyber Arms. New Scientist 2013, 4/13, vol. 218, issue 2912, pp 26-27.
[91] Ibid.

2.1.3. National legislation

This subchapter aims to give an overview of the national cybercrime legislation that concerns online civil mass action. Since most of the offline protesters are apprehended under trespass laws, for comparison also the sanctions prescribed for trespass in the each respective judicial system are brought out. While acknowledging that penal codes contain multiple other norms that may be relevant for both an act of physical space sit-in and an activist DDoS attack, such as coercion and vandalism, the ways in which these are applied to cyber offenses is case-specific and would be subject to further research . This chapter addresses the stark contrast between the prosecution of online and offline activists that derives from the generally deterrence-prone patterns of regulating cybercrime. The countries which are being looked into were chosen according to the following criteria:

1. Is it a country that generally embraces internet freedom and free speech?
2. Has there been documented academic or political discussion over the problematics of criminalising DDoS attacks?
3. Has there been relevant illustrative case law?

Both UK and Germany have faced some problems drafting a regulation that would unconditionally cover DDoS attacks, the Higher Regional Court of Frankfurt in Germany also is responsible for the often cited *Lufthansa* judgment, which to date constitutes the only judicial acquittal of political DDoS attacks. Estonia serves as a good example of a country that has fallen the victim to a large-scale attack of hacktivist character, which resulted in a single criminal judgment that did not discuss intent and motivation. Majority of the targets of recent large-scale hacktivism are US state agencies or companies, which is why US is an unavoidable subject as regarding theory, legislation and case law.

2.1.3.1. United Kingdom

Section 1 of the The Computer Misuse Act of 1990 criminalises unauthorised access in cases where the perpetrator is aware of being not authorised. The intent however does not have to be directed at accessing any particular target. Section 2 foresees an aggravating circumstance to unauthorized access – intent to commit or to facilitate commission of further criminal offences. Section 3 penalises unauthorised acts with intent to impair, or with recklessness as to repairing, operation of a computer. Subsection 2 stipulates that this provision applies if the person intends by doing the act to impair the operation of any computer; to prevent or hinder access to any program or data

held in any computer; to impair the operation of any such program or the reliability of any such data; to enable any of the aforementioned things to be done. Subsection 5 sets forth that the core terms of this provision should be interpreted in a wide manner, so that among others a reference to impairing, preventing or hindering something includes a reference to doing so temporarily

Section 3 was phrased in its current form in 2006, since the regulation in force until then enabled ambiguous interpretation as regards of whether (D)DoS attacks that do not encompass unauthorised access are covered. Here it would be suitable to give a brief overview of the arguments brought in favour of amending the act, for they serve as a good example of the problematics of criminalising (D)DoS attacks, namely having to choose between two evils- excessive generalisation and making the illegality of the attack depend on the exact mechanisms used.

Previously the offence in Section 3 criminalised unauthorised modification of computer material. Section 3 of the CMA did not require unauthorised access to a computer system, merely unauthorised "modification of the contents of any computer". The requisite intent that accompanied this offence was to render unreliable the data stored on a computer, or impair its operation.[92] Richard Clayton commented on the complexity of criminalising (D)DoS under CMA:

"In general, where a DDoS attack takes place then an offence will have been committed because many machines will have been taken over by the attacker and special software installed to implement the attack. Even when a system is attacked by a single machine, an offence will sometime be committed because the contents of the system will be altered. However, when the sole effect of an attack is to fill a nearby link with useless traffic, then it may be hard to show the elements of a CMA offence are present, although a DoS attack has certainly occurred."[93]

ENISA´s "Good Practice Collection for CERTs on the Directive on attacks against information systems" explains the impact of the introduced amendments[94]:

"Up until 2006, builders of botnets were clearly committing an offense, but users of botnets (the botnet herders) weren't necessarily. Existing provisions focused on unlawful access, and builders

[92] Internet Crime Forum Legal Subgroup: Reform of the Computer Misuse Act 1990, www.internetcrimeforum.org.uk/cma-icf.pdf
[93] Clayton, *supra nota* 64.
[94] ENISA. Good Practice Collection for CERTs on the Directive on Attacks against Information Systems. ENISA 2013, P/28/12/TCD, Version: 1.5, 24 October, p 16.

(who infected third party machines) were guilty of that crime. However, botnet herders who launched e.g. DDoS attacks didn't fall under this rule. Therefore, changes in the legislation were needed, and separate rules for (D)DoS attacks were introduced. Under the amended Section 3 of the Computer Misuse Act, it is an offence to deliberately or recklessly impair the operation of any computer or program, or reliability of data, or to prevent or hinder access to data. That includes both the previous offence of unlawful modification of data, and any additional DoS activities."

2.1.3.2. Germany

Sections 303a and 303b of the Penal Code (*Strafgesetzbuch*) of the Republic of Germany respectively criminalize the acts of data tampering (data interference in the CoE Convention) and computer sabotage. Data tampering stands for unlawful deletion, suppression, rendering unusable or alteration of data, the perpetrator shall be liable to imprisonment not exceeding two years or a fine. All the activities that qualify as data tampering require unlawful access as the "root" crime. 303a does not require the presence of *mens rea,* and acts triggered by either criminal intent or recklessness are punishable.[95]

Intent and motivation however are decisive elements of computer sabotage (Section 303b). Computer sabotage means interference with data processing operations which are of substantial importance to another by *1)* committing an offence under penalized under 303a *2*) entering or transmitting data with the intention of causing damage to another *3*) destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier. Aggravating circumstances are targeting data processing operations of substantial importance for another's business, enterprise or a public authority and causing major financial damages to the target. Also more severe punishments are foreseen for financial motivation and acting as a member of a group whose purpose is the continued commission of computer sabotage are considered and in case a critical information infrastructure of Germany is targeted. In the most serious aggravated cases the offender may be sentenced to 10 years of incarceration.

Similarly to the United Kingdom, Germany amended its computer crime regulation in 2007 in order to unambiguously cover (D)DoS attacks. This reform was explicitly prompted by the

[95] Criminal Code (*Schutzgesetzbuch*), in the version promulgated on 13 November 1998, Federal Law Gazette I p. 3322, last amended by Article 1 of the Law of 24 September 2013, Federal Law Gazette I p. 3671 and with the text of Article 6(18) of the Law of 10 October 2013, Federal Law Gazette I p 3799.

judgement of the Higher Regional Court of Frankfurt in *Vogel vs Lufthansa*[96], where the court stated that temporary suppression of access of data was not punishable under Section 303a.[97] In order to tackle DDoS attacks subsection 303b(2) was introduced.[98] Germany differs from the other countries in the sample in particular because *Vogel* was the very first DDoS case to be brought to the court and it resulted in acquittal, thus creating a different precedent. In 2011, i.e. five years after the introduction of Section 303b(2), the Lower Regional Court of Düsseldorf sentenced a hacker to 34 months of prison for a DDoS-based extortion scam against gambling websites during the World Cup of 2010.

2.1.3.3. Estonia

The Estonian Criminal Code includes all the offenses the penalizing of which is foreseen in the CoE Convention of Cyber Crime and EU Directive 2013/40. An act of cyber civil disobedience might fall under Article 206 or 207 of the Criminal Code, the first stands for the interference of computer data, second for hindering of the functioning of computer systems. Interference covers the illegal alteration, deletion, damaging or blocking of data in computer systems and is punishable by pecuniary punishment or up to three years of imprisonment, on aggravating circumstances the imprisonment term may extend to five years. These aggravating circumstances include commitment against data in numerous computer systems, use of spyware or malware, being committed by a group, targeting a computer system of a vital sector and significant damage.

The second norm, Article 207 covers the hindering of the functioning of a computer system, the same aggravating circumstances and sanctions apply, however in addition the hindrance of the functions of a computer system used in providing public services is included among these. Up until 2015 the Criminal Code did not include a separate norm for illegal access, since then the key offense of cybercrime has been incorporated in Article 217. Illegal obtaining of access to computer systems is punishable by pecuniary fees or up to three years of imprisonment, when committed on aggravated circumstances, i.e. causing significant damage, targeting computer systems belonging to a vital sector or containing a state secret, classified foreign information or information prescribed for official use only, up to five years of imprisonment can be prescribed.

[96] Ss 319/05, Vogel, 22 June 2006.
[97] Dudek, D. *et al*. Zitterbart, Netzsicherheit und Hackerabwehr. Universität Karlsruhe 2008, p. 58, available online at: https://doc.tm.uka.de/tr/TM-2008-3.pdf#page=52 (last accessed 19 April 2016)
[98] Ibid.

Article 266 on illegal entry and failure to comply with demand to leave – trespass- foresees a pecuniary punishment. When committed with the intention of occupying an area, building or premises or of interfering with the regular operation thereof the act might also result in up to three years' imprisonment. Although perceived by specialists as the physical world equivalent[99], the penalties prescribed in Article 266 are much more lenient, usually consisting of pecuniary fees in qualified cases sometimes also detention can be prescribed

2.1.3.4. United States

Article 1030(a)(5) of the Computer Fraud and Abuse Act (CFAA) prohibits a person from knowingly causing the transmission of a program, information code, or command, where as a result of such conduct he intentionally causes damages without authorization to a protected computer. This subsection therefore do not require unauthorized access but instead sets forth "unauthorized intentionally caused damage" as the key element.[100] A DDoS attack falls under the notion of "transmission of program, information code, or command", but so does a regular visit paid to any webpage. 1030(e)(8) defines damage as any impairment to the integrity or availability of data, a program, a system, or information – server overload caused by a DDoS attack fits the definition. Section 1030(a)(5)B criminalises unauthorized access of a protected computer that leads to damage. Therefore the *actus reus* in the present norm is "unauthorized access", the damage that follows might be accidental. A (D)DoS attack would definitely be punishable under 1030(a)(5)A, a botnet-operated zombie attack would be punishable on multiple accounts, including 1030(a)(5)B. Aggravating circumstances in the occurrence of which imprisonment of 10-20 years or fines up to 250 000 mat be prescribed include repeated offenses, resulting in a loss that over the course of the year exceeds 5000 dollars, targeting medical services, threatening public health or safety, affecting a justice, national defence, or national security entity computer or more than 10 computers in the course of the year.

As concludes from the current CFAA regulation government websites and financial institutions face the harshest penalties, in particular where national security is concerned. For comparison, criminal trespass[101] is usually considered a misdemeanour punishable by imprisonment for not more than six months, a fine of not more than 750 dollars or both. A particularly heavy-handed judgement is this of the Kansas District Court in the case of Eric Rosol, a man who ran LOIC from

[99] Hirsnik, E. Arvutikuritegevuse regulatsioon Eestis. Juridica 2014, 8, p 612.
[100] Computer Fraud and Abuse Act, 18 U.S.C. 1030.
[101] 25 Code of Federal Regulations, Section 11.411

his computer for 1 minute and thus participated in a DDoS attack against the webpage of US Oil Company Koch Industries. The operation against Koch lead to 15 minutes of downtime, Rosol was sentenced to two years of probation and ordered to pay 183 000 dollars in restitution to Koch Industries.[102]

2.1.3.5. Comparative summary

The table gives a comparative overview of the regulation criminalising hacktivist DDoS attacks, where no additional crimes (e.g. use of botnets) have been committed. Although no legal system was studied that would allow for a DDoS to go unpunished, the analysis proved that there are minor yet potentially important differences in the degree of *mens rea* required, the foreseen aggravated circumstances and the elements of the offence.

	Regulation(s) that criminalise DDoS	Mens rea	Aggravating circumstances	Elements of the crime
Estonia	Article 207 CC	Intent	-committed by a group -use of malware -against CII-s -significant damage	Illegal interference or hindering the functioning of a computer system
Germany	Article 303b(2) CC	Intent	-for financial gain -against CII-s	Entering or transmitting data with the intent to cause damage
United Kingdom	Section 3 CMA	Intent/recklessness	-against CII	Unauthorised acts with intent to impair, or with recklessness as

[102] Yang, G. The Commercialization and Digitization of Social Movement Society. Contemporary Sociology: A Journal of Reviews 2016, 45(2), p 124.

				to repairing, operation of a computer
United States	Article 1030a(5)A CFAA	Intent	-against CII -significant damage	Unauthorized intentionally caused damage

Figure 5. Current regulation on DDoS attacks that do not involve unauthorised access

2.2. Fundamental Rights

2.2.1. International and regional instruments

Fundamental rights are purposefully phrased and interpreted as broadly as possible, for only so can they aim to be the living instrument that provides protection for the basic human values in all the time and context dependent scenarios, at the same time it takes time for the international courts to admit that one or another distinctly modern phenomenon is considered to be a human right, since once a statement is made it is expected to determine the case law and sense of justice for many generations. Therefore redesigning fundamental rights is an exceptionally great leap, which is in general approached with the highest degrees on deliberation and caution. The fundamental clash between the discourses of criminal law and fundamental rights comes from the fact, that while the first is predominantly positivist the second leans more towards natural law. Since humanitarian law seeks answers to questions such as what is left of fundamental rights in situations where they cannot be fully exercised, also humanitarian law follows the basic principles of fundamental rights theory. It has was argued the first chapter that for regulating cyberspace, legal systems and branches that base themselves on natural law theory are better positioned.[103] Mostly because the purely positive law tends to fall short when jurisdictions and rules are in conflict, which is certainly true in the case of regulating cybercrime and cyber-rights.

However, to date no international fundamental rights instrument explicitly recognizes the right to cyber protests. Although there are first signs that in future these rights might become covered: in the introduction of the present paper it was mentioned that Council of Europe is currently drafting a report on the freedom of assembly on the internet[104], also the advocacy organisation for the freedom of expression Article 19 explicitly mentions the inclusion of electronic forms in its online

[103] Svantesson (2015), *supra nota* 18.
[104] CoE, Report on the Freedom of Assembly on the Internet, 30 Sept 2015.

guidelines on the right to protest.[105] Principle 8 section 1d stipulates that: "States should, therefore refrain from imposing restrictions on online protests. In this respect, the internet should be considered a quasi-public place which is routinely used for public purposes."

The freedom of assembly is foreseen in Article 21 of the International Covenant on Civil and Political Rights, Article 20 of the Universal Declaration of Human Rights, Article 11 of the European Convention on Human Rights, Article 12 of the EU Charter of Fundamental Rights and in the First Amendment. All of these instruments foresee varying degrees of positive obligations for the states to ensure the respect for the freedom of peaceful protest. Other fundamental rights that are related to online and offline protests are the freedom of opinion, religion and expression and its traditional twin-right – the right to association. Grounds for restricting the right to peaceful assembly are listed exhaustively and include: national security or public safety, prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

Rights that most often conflict with the freedom of peaceful assembly are right to property, also on some instances freedom of opinion and expression. The *travaux preparatoires* of the European Convention on Human Rights states that a board wording was deliberately preferred, although some drafters had preferred explicitly spelling out that the right should include freedom to hold assemblies, meetings, street processions and demonstrations. The opponents on the other hand argued that the freedom does not necessarily include the right to hold pageants or processions on streets or public places. Therefore the place-aspect of the right was perceived as the most problematic of the time-place-manner conditions. However, the emergence of new forms of protest was not predicted at the time of the drafting. Also, the general consensus was that protests should be protected not only against governmental interferences but against all kinds of interferences.[106]

A proposal was made so that restrictions should be allowed provided that they are in accordance with the law, so that forms of administrative action would be covered. Since this would be in conflict with the *travaux preparatoires* of the ICCPR and the regulations on all the other rights, the idea was dropped.[107] In the end, the ICCPR was worded so that administrative action against assemblies could be covered, ECHR however remained true to the initial "prescribed by law",

[105] Article 19, Principles of the Right to Protest, Principle 8(1.d), available online at: https://right-to-protest.org/wp-content/uploads/2015/06/right-to-protest-for-web.pdf (last accessed 1 May 2016).
[106] CoE, *Travaux préparatoires* of the European Convention on Human Rights, DH(56)16, CDH(74)39, available online at: http://www.echr.coe.int/Documents/Library_TravPrep_Table_ENG.pdf
[107] Ibid.

adding that "this Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State."[108] The oldest of the international human rights codes Universal Declaration of Human Rights simply states that "Everyone has the right to freedom of peaceful assembly and association", as for restrictions Article 30 stipulates that: "Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein". The *travaux preparatoires* of ECHR and ICCPR reveal nothing that would speak against extending the scope of protection also to cyber protests. However, even if certain forms of DDoS attacks would gain protection under ECHR/ICCPR/ECFR, the same problems as in the case of physical protests would arise. Therefore, in the following chapter cases which cast some light to the problematics of anonymity, public/private space, positive obligations and accountability are looked into.

Taken together, ECHR, ECFR, ICCPR and UDHR foresee the freedom of peaceful assembly, without elaborating on the time, manner and place of exercising the freedom. This freedom can be restricted for the protection of any of these legitimate aims occur: national security, public safety, public order (prevention of disorder or crime), public health or morals, the rights and freedoms of others. However, any such restrictions must be clearly explained on the basis of legitimate prescribed by law and deemed necessary in a democratic society. The Joint Guidelines on Freedom of Peaceful Assembly of the Venice Commission and the OSCE explain that an assembly should be deemed peaceful if its organizers have professed peaceful intentions and the conduct of the assembly is non-violent. The term "peaceful" should be interpreted to include conduct that may annoy or give offence, and even conduct that temporarily hinders, impedes or obstructs the activities of third parties.[109]

European and international legal instruments distinguish between the freedom of expression and the freedom of assembly and association. Another distinction should be therefore made between assembly and association, Orsolya Salát suggests that in an assembly the physical element is of foremost importance, since the defining characteristic of an assembly is its *taking place and taking a stance* in the literal sense.[110] The temporal aspect setting assemblies apart from association is

[108] Ibid.
[109] Joint Guidelines on Freedom of Peaceful Assembly of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 2010, p. 1718.
[110] Salát, O. The Right to Freedom of Assembly. Oxford, Hart Publishing 2015, p 65.

that main object of protection of freedom of assembly is limited to the point in time where the assembly actually happens, for this moment to happen also the preparation period needs to be included under the scope of protection. The French Constitutional Council distinguishes between meetings and demonstrations, on the basis of the first being rather a forum of exchange of opinion, while the second´s main objective is communicating the already formed opinion to the general public. Different proportions of speech and conduct exist within these forms of assembly.[111]

According to OSCE the freedom of peaceful assembly covers a broad variety of gatherings, including:[112]

- static assemblies, such as meetings, mass actions, rallies, sit-ins, pickets and flash mobs;
- moving assemblies, such as parades, marches and processions; and
- combinations of static and moving assemblies.
- some funerals, as they might have, or might take on, political overtones and be used as public demonstrations;
- open-air religious assemblies; and
- movements of people in vehicles, such as convoys or mass cycle rides, as these might also be used as a means of demonstration or protest.

The US constitutional law perceives certain acts of civil disobedience as extensions of the freedom of speech and dwells on the balance of conduct and speech as the litmus test for eligibility for First Amendment protection. The conduct element has to be proportional to the significance of the speech – the ideas and agenda behind the actions. The distinction however is vague, since speech does not always mean verbally expressed ideas and convictions, and conduct active physical or mental behaviour. Traditional means of protest that fall on the "speech" end of the spectrum include petitions, pamphleteering, publishing and distributing campaign materials. Meetings, parades, marches and processions contain elements of both. Sit-ins, pickets and blockades and forms of direct action however have the strongest conduct element. Besides targets, whether public or private, protests cause inconvenience to the general public as well, to which degree there exists an obligation to tolerate it, is another question frequently posed in case law and scholarship.

[111] Ibid.
[112] OSCE, CoE Venice Commission, Guidelines on Freedom of Peaceful Assembly, OSCE/ODIHR, Warsaw/Strasbourg 2010, available online at: http://www.echr.coe.int/Documents/Library_TravPrep_Table_ENG.pdf

To paraphrase an anonymous Zuccotti Park protester holding a poster with the sentence "Sorry for the inconvenience but we are trying to change the world" or Martin Luther King who insisted rightly but with a hint of arrogance that "no social revolution can be neat and tidy at every point", the unanimous position seems to be that a certain extent of inconvenience and obstruction is imminent to public demonstrations. The scale of allowed obstruction and inconvenience is again open to deliberation. The more an act leans towards direct action, the more distress it is likely to bring about. The freedom to peaceful assembly covers both organized and spontaneous protests, whereas the number of participants is not relevant. Therefore a lone-wolf activist can be a protester in the physical space, provided that he communicates the collective agenda he presents in an understandable manner.

Traditionally the right to peaceful assembly requires that the protest is targeted against a public authority and comes from the citizens subordinated to that authority, this is quite evidently an outdated concept. Firstly, due to the globalization of world policy and economics and secondly due to the increasing privatization of public goods and services. The latter has been recognized by judges both in Europe[113] and the US[114]. This is vital in the context of cyber protests, for although the Internet serves as the public forum of choice for many, it is in the major part in fact privately owned.

2.3. Conclusions

This chapter gave a short overview how hacktivist (D)DoS attacks have been incorporated in the criminal law instruments. Council of Europe Convention on Cybercrime foresees the criminalisation of unauthorized interference, leaving at the same time it up to the states to stipulate the exact conditions. Albeit all the observed national systems are relatively compatible and share the basic principles of regulating cyber security, meaningful differences in sanctions, required degree of *mens rea* and aggravating circumstances exist. Two of the states have explicitly amended their legislation as a result of facing difficulties in criminalising (D)DoS attacks, by today however all forms of DoS are criminalised, regardless of the targeted site, the tools deployed, prior notification or lack thereof, involvement of botnets and whether the participation in one has been voluntary or not. The two main stumbling blocks on the road of criminalisation have been firstly that DDoS attacks do not necessarily require unauthorized access and that the impairment that they

[113] ECtHR, *Appleby and Others v. The United Kingdom.* 44306/98, 06 May 2003. Judge Maruste´s dissenting opinion.
[114] *Marsh vs Alabama*, 326 U.S. 501, 66 S. Ct. 276, 90 L. Ed. 265, 1946 U.S.

cause is of temporary nature. Motivation has been taken into account in Germany, where one of the aggravating circumstances is financial motivation, which is also thought to be the main factor distinguishing hacktivism from cybercrime. However political intent has not been listed among the mitigating circumstances.

Humanitarian law might in some instances view hacktivism as a terrorist activity, up until today however this option is only hypothetical. According to the Tallinn Manual a sufficiently organised hacktivist group that conducts operations which score high on the Schmitt criteria might invoke military responses. This however does not apply to lone wolf actors, who should according to the manual be prosecuted under criminal law. The level of organisation is another aspect that is particularly complicated to determine in case of cyberoperations, since shared intent, deliberate cooperation, voluntarism, responsibility and accountability are extremely difficult to prove. The cumbersome prosecution of the participants in the cyberattacks against Estonia and Georgia serves as good evidence of the fact.

The freedom of peaceful assembly is incorporated into all of the principal international human rights instruments, however to date there is no case law that would separately state that under certain circumstances a DDoS attack could be included in its scope of protection. Understandably, not much can be found on the issue in the *travaux preparatoires* of binding international human rights documents, however neither was anything found that would give rise to the assumption that electronic assemblies would be outright excluded from the scope of protection. Therefore, whether or not an analogy between online and offline assemblies would hold ground, should be determined by analysing the courts´ interpretation on the various aspects of the freedom of assembly such as: the essence of public forum, the proportionate extent of inconvenience, the anonymity/identifiability of the protester and the limits between coercion and protest.

3. Case law analysis

3.1. Anonymity and accountability of the protester

One argument frequently brought against the legitimization of online protests is that the protesters usually remain anonymous or are however able to do so when they wish and have the necessary technological skillset to use privacy enhancement technologies while participating in protests. In the latter case we would be talking about true anonymity, while simply not revealing your biographical data and participating through an online "avatar" would in fact constitute pseudo anonymity, in the sense that although the names and identities are hidden, they can be easily traced down[115]. Offline protester is thought to be more easily identifiable and held accountable, thus seen as risking more personal values for the cause and therefore being a more serious protester. Due to loose personal ties online protester on the other hand is sometimes perceived as a mere "slacktivist"[116] or "clicktivist", someone activating LOIC for the fun and countercultural appeal of it, without much to lose and at best equipped with a wavering and poorly motivated personal dedication to the issues at stake.

Gabriella Coleman writes that "civil disobedience they say lacks legitimacy if it does not carry the stamp or seal of one´s legal identity – if it is not legitimated by the risk of punishment. But as Molly Sauter has convincingly argued, this conception of civil disobedience is as narrow and limited as it is historically specific, she insists, "deeply rooted in concepts of Christian martyrdom and the moral superiority of nonviolent civil disobedient over their opponents in insisting that online civil disobedience expose themselves to often extreme punitive state action because of their activism ensures that only hose with the most extreme views and the least to lose (i.e., those with the least investment in society) will participate in these actions."[117]

Pseudo-anonymity is not only characteristic to cyberspace, but has been debated in courts and literature also in the context of physical space protests. Indeed, how identifiable is a protester among the mass at for example the global anti G8 protest? In case of unmasked protesters, to the

[115] On the distinction of true and pseudo anonymity see Chawki, M. *et al*. Cybercrime, Digital Forensics and Jurisdiction. Springer 2015, vol. 593, pp 99-101.

[116] Here the author begs to differ, the term „slacktivism" was introduced by Payam Akhavan in his article „Making human rights sexy: authenticity in glamorous times", where he defined it as substituting "feel good" activism for meaningful engagement, the feel-good element of committing a cybercrime and potentially facing harsh penalties is low to say the least, or as Molly Sauter put it when commenting on operation PayBack:"Internet civilians did not simply wake up one day and decide to join up with the one Internet subculture blessed with the worst reputation in town." Clicktivism on the contrary is a more neutral concept referring to the low participatory threshold of online protests (see Czosseck, *supra nota* 50.)

[117] Coleman, G. Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. Verso Books 2014, p 423.

ones who already know him or her, probably effortlessly, to the general society and the authorities on the other hand identifying a single protester is not such an easy task. Does the anonymity or lack thereof influence the compliance of a protest with the law? Does the right to peaceful assembly encompass the presumption that the protesters should be identifiable? Identifiability and attributability place certain restrictions to who and on which conditions is able to participate in protests. The Executive Director of the Information Society Project at Yale Law School Margot E. Kaminski wrote that:

Ultimately, the core of the expressive right to anonymity is about power. Individuals have more power when they organize as an anonymous group against a government than when they act as easily identifiable individual targets. And historically, large assemblies in real physical space have functionally enabled most of their participants to remain anonymous. Anonymous speech has also permitted assemblies to start, by protecting channels of information distribution that are accessible by and to all people.[118]

In fact, a situation where the government requires for the identification of the protesters when they have acted in accordance with the law, might be considered a violation of the right to privacy and freedom of assembly. In 1995 Mr Friedl an Austrian national who had organised and participated in a protest in Vienna, lodged an appeal against Austria in ECmHR, where he claimed that during an entirely peaceful protest he and other participants had been photographed and asked to present identification documents by policemen. The case resulted in a friendly settlement, which means that the Commission did not publish its viewpoints in detail. The Commission nevertheless expressed that no violation of Article 8 had occurred, since the photographs were taken without directly connecting them to the identities of the participants. The recorded personal data and photographs were not entered into data processing systems and no action had been taken to identify the persons photographed on that occasion by means of data processing.[119] Though, no final judgment on the matter was issued, these principles would still look interesting when analysed through the lens of cyber protests. Provided that the participants´ IP addresses can be traced and are subject to automatic processing as it is allowed under many national data retention regimes, an online protester would in fact have a lesser degree of anonymity in front of the authorities.

[118] Kaminski, M. E. Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech. Fordham Intellectual Property, Media & Entertainment Law Journal 2013, 23(815), p 894.
[119] ECmHR, *Friedl vs Austria*, 28/1994/475/556, 30 November 1994, para 24 ff.

It follows from the Commission´s rationale that in cases of peaceful assemblies the requirement of absolute identifiability of the protesters would constitute a disproportionate infringement of the right to privacy and accordingly also prevent citizens from exercising their freedom to peaceful assembly. The taking of photographs in *Friedl* was not deemed disproportionate exactly due to the lack of such direct identification. Concluding from *Friedl* a protester does not have to be instantly identifiable, which seems to grant cyber protesters hiding behind pseudo anonymity a legitimate argument. In the physical space we cannot talk about true anonymity in the absolute meaning that it has (been attributed) in cyberspace, pseudo anonymity however exists and is at least equally if not more available than in the online world.

Protesters have been taking steps to avoid identification throughout the history of public protest, this has involved applying face-paints, wearing masks and/or uniforms. Regardless of the measures taken in real life, they can only offer pseudo or traceable anonymity. Although empowering from the aspect of individual freedom of expression, whether and to what degree anonymity actually promotes the free marketplace of ideas, is whole another question. Masks can be prohibited primarily due to security and law enforcement reasons. In some cases (e.g. pantomime, masquerades etc.) wearing a mask can be seen as an essential part of the expression, while in others it serves as a necessary prerequisite for the freedom of expression. Although anonymity, decentralisation and ambivalent organisation are key features of cyber activism[120] in case of a DDoS attack anonymity is not part of the distributed message, which reads „I dissent to these policies or laws“, but merely allows for a person to send out this message.

Therefore, we are dealing with instrumental anonymity akin to this that was analysed by the Federal Court of Texas second in *Aryan*[121] , where the university had prevented students from wearing masks, while protesting against the Shah of Iran.[122] The court stated that masks cannot be banned for security reasons, unless there is proven causal relationship between anonymity and violence. Secondly, the appellants were not acquired to prove that identification would lead to reprisals. The courts held that the fact that there is that the appellants had fear that retaliatory measures would be taken up against them should they be identified, was sufficient to justify the wearing of masks. Here again, it should be reminded that the physical space context in *Aryan* did not in fact allow for true, untraceable anonymity, wearing a mask complicates identification but unlike some techniques applied in cyberspace does not rule it out completely. In Germany although

[120] See Coleman, G (2014), *supra nota* 117.
[121] *Aryan v. Mackey*, 462 F. Supp. 90, 94 (N.D. Tex.1978)
[122] Kaminski (2013), *supra nota* 118, p 854 ff.

the Assembly Law prohibits the use of "protective weapons" including masks, the ban is not absolute and the in 2005 the Federal Constitutional Court ruled that protesters wearing animal masks at a protest against life patents cannot be subjected to obligation to identify themselves at the requests of the police as there was no showing of direct danger to public order or safety.[123] Therefore, metaphorically speaking no protester is required to wear a name-tag, in the age of CCTV and remote facial recognition an unconditional ban on masks could easily end up being tantamount to such requirement.

No court so far has delivered a judgment on identifiability and public protests in a situation, where absolute untraceability would be possible. Since untraceability rules out law enforcement even on instances were actual violence has occurred, it should not be allowed in public protests. When applying the real space analogy however traceable anonymity would be on many occasions a necessary condition for a peaceful assembly. A certain continuum of anonymity precludes profiling, political persecution, direct and indirect discrimination and promotes freedom of expression and opinion. However since a real life protester cannot claim for absolute anonymity, in order to be proclaimed as the heir of the social of legal legacy of sit-ins and street processions, an online protest also should not be conducted by a mass of untraceable individuals. Therefore the blanket use of rerouting or TOR would be prohibited, but does that necessarily imply that registration of the participants with their real names would be reasonable and proportionate requirement?

Kaminski writes about online political speech:
"It is one of the few avenues of distribution of expression that is open to "little people," rather than controlled by big media conglomerates. In recognizing the significance of protecting a particular distributive method because of its accessibility to non-elites, the Court in *Watchtower*[124] laid the groundwork for a heightened-or at least equal-protection for online forums."[125]

While analysing the anti-mask case law from the perspective of online speech, it should be kept in mind that firstly in the US public assemblies are protected by First Amendment freedom of speech, secondly due to that the degree of protection is determined by the speech/conduct balance. Kaminski´s analysis focuses primarily on forms of online speech like forum posts and

[123] BVerfGE, 1 BvR 943/02, 25 October 2007.
[124] *Watchtower Bible v. Vill. of Stratton*, 536 U.S. 150 (2002).
[125] Kaminski (2013), *supra nota* 118, p 895.

commentaries which in their essence lean more towards pure speech than conduct and are therefore more expressive and subject to stronger First Amendment protection. A DDoS is a mute tool and in order to establish to what extent the freedom of speech protects a phenomenon like that, case law on the distinction between speech and conduct will be looked into in more detail.

The existing case law affirms that there is no requirement for absolute identifiability and since it has always been an unrealistic possibility so far, neither is there an unequivocal ban of absolute anonymity. Although, absolute anonymity escapes law enforcement and therefore hiding behind it while protesting for a public cause equals denying the rule of law altogether.

In 2010 outstanding Belarussian academic and information society theoretic Evgeny Morozov published an article in defence of political DDoS attacks, where he referred to a Dutch study, according to which the participants in Operation Payback were in fact surprisingly traceable.[126] The study argues that neither desktop-based nor the JavaScript version LOIC did not attempt to protect the identity of the user, as the IP address of the attacker can be seen in all packets sent during the attacks. Internet Service Providers can resolve the IP addresses to their client names, and therefore easily identify the attackers. Moreover, Web servers normally keep logs of all served requests, so that target hosts also have information about the attackers.[127] In addition to that the authors refer to the EU data retention directive which was in force at the time of the publication of the paper. The directive obliged the European ISPs to retain logs of communications from 6 to 24 months and make it available for intelligence or law enforcement purposes.[128] One may argue that the abolition of the directive thus leads to the anonymization of the protesters, while in reality the majority of EU Member States still continue to retain data under national legislation and many of the ones that either revoked or never introduced data retention are in fact reconsidering the introduction of it.[129] Therefore, in case of operation Payback and the likes we are talking about pseudo- or identifiable anonymity, which is not completely forbidden in the context of protest, however this does not apply to all documented hacktivist operations.

Another more recent study published by the Israeli network security company Radware looks into the possibilities of remaining anonymous while participating in a DDoS through the use of anonymization techniques, such as VPN, proxy chaining and TOR. The main conclusions are that

[126] Morozov (2010), *supra nota* 30.

[127] Pras, A. et al. Attacks by "Anonymous WikiLeaks Proponents not Anonymous. DACS, University of Twente 2010, available online at: http://doc.utwente.nl/75331/1/2010-12-CTIT-TR.pdf (last accessed 1 May 2016)

[128] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[129] Council of the European Union, Eurojust, Eurojust's analysis of EU Member States' legal framework and current challenges on data retention, 26 October 2015, available at: http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf

despite that the application of the technologies is on the rise, they do not guarantee full anonymity. Even if almost impenetrable veil is cast in front of the identity of the attacker, it comes at a certain cost – according to the report TOR networks suffer from both latency and limited bandwidth, which can sometimes seriously weaken high-bandwidth DDoS attacks, making them a total failure[130]. Also, using TOR for DDoS attacks can impact the TOR network itself. For example, LOIC cannot be used via proxies (including anonymising systems such as TOR) because that would just end up DDoS-ing the proxy. Furthermore, the report goes on to note that public proxy lists and VPN services are constantly monitored and published, making it quite easy to blacklist IPs and defend against DDoS attacks arriving from a blacklisted source. Although true anonymity cannot be ruled out, it becomes apparent that unlike the participation itself, successful anonymization requires advanced technological skills that an average participant is likely to lack, and therefore to date the narratives of universal untraceability remain myths.

3.2. The speech-conduct dichotomy

A DDoS attack is often described as the counteragent of expression and is almost entirely an act of anti-speech, placing it on the conduct-end of the spectrum. McLaurin argues that a DDoS attack could not qualify as protected speech pursuant the test established in *United States vs O´Brien*[131], which aims to answer whether a government interference in the right to expressive conduct is justified though exploring these four aspects:

- if it is within the constitutional power of the government
- if it furthers an important or substantial governmental interest
- if the governmental interest is unrelated to the suppression of free expression
- if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

In O´Brien the defendant had burned his draft card as symbolic action against the recruitment to Vietnam War. The Supreme Court argued that by complying criminal liability and introducing bans of deliberate destruction of draft card, it had fostered an important government interest. McLaurin is positive that a *DDoS* attack akin to Operation Payback would fail the *O´Brien* because

[130] Radware Network Security, Shooting Behind the Fence; How Attackers Remain Anonymous While Performing DDoS Attacks, 2013, available at: https://security.radware.com/uploadedfiles/resources_and_content/attack_tools/shooting_behind_the_fence_ert_research_paper.pdf (last accessed 1 May 2016)

[131] *United States v. O'Brien*, 391 U.S. 367, 369-70 (1968).

of its essentially censorial character and very low resemblance to pure speech.[132] Interestingly, he does not proceed to mention the risks that a DDoS creates by abusing the vulnerabilities of the basic architecture of the web.

O´Brien has been viewed critically in scholarly literature. Orsolya Salat comments on O´Brien: "Clearly, the majority and the concurring do not find it important that to burn the draft card is certainly among the most effective and powerful ways of protesting against the war. Neither does it bother the Court that in effect it imposes its own view on how to communicate a specific message." [133]

James M. McGoldrick states that its flaws are myriad, including the fact *O´Brien* overstated the weight of questionable governmental purposes and undervalued the effectiveness of the symbolic aspects of O'Brien's expressive conduct.[134] Therefore applying the *O´Brien* test to any modern form of symbolic speech might be a dubious choice to begin with.

While symbolic speech is assessed according to *O´Brien* and subject to intermediate scrutiny, questions relating to restricting "pure speech" (emphasis added A.V.) are approached by applying the time-manner-place and content-neutrality criteria and subject to strict scrutiny. In *Universal Studios v Corley,* the Second District Court of New York held that computer code is considered to be symbolic speech and not pure speech. A DDoS attack basically consists of running a code of varying complexity – from automated requests to simply hitting the refresh button a hundred times per minute. In *Corley* the object of dispute was whether the publication of a code for software that enables to crack the DRM settings of DVDs belongs to the scope of First Amendment. In case of DDoS it wouldn´t be the writing and publication but the running of the code that the court would have to elaborate on.[135]

A DDoS therefore contains two acts: person A writes a programme that enables to commit a DDoS attack, persons B, C, D (the list might as well include person A) implement the code to overload server S. The first act is the creation of a tool that produces amplified traffic, such code can be and was originally written for the purposes of stress testing, therefore there should be no prevailing governmental interest in banning writing or publishing such code, regardless of whether it

[132] McLaurin (2011), *supra nota* 13.
[133] Salát (2015), *supra nota* 110, p 201.
[134] McGoldrick Jr JM. United States v. O'Brien Revisited: Of Burning Things, Waving Things, and G-Strings. University of Memphis Law Review, 2005(36). p 906.
[135] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

constitutes expressive conduct, symbolic speech or pure speech. In *Spence* the Supreme Court set forth that in order for an act of expressive conduct to qualify as symbolic speech the audience should be able to comprehend the message behind it.[136]

The activation of a code that creates amplified traffic to a website by itself contains very little if any meaningful speech, though the choice of target expresses a certain idea, therefore a DDoS attack without any attempt to communicate the agenda to the intended audience is hardly expressive enough to be deemed worthy of First Amendment protection. However, in case the attack takes place within the frames of wider political turbulence, which is covered by media, also when announcements and expressions of motivation have been published before the attack or at the time of it, the message behind the page failing to load should be comprehensible or at least sufficiently easy to find out. In case of real life protests too, it wouldn´t be reasonable to make the validity of the expression depend on a passer-by's willingness or capability to understand, why exactly are the people marching, sitting or chanting.

To this date no court has taken a stance on the expressive element of a DDoS attack. Academic literature and expert opinion on the expressiveness of a DDoS attack is largely divided, with authors such as Samuel[137], Hampson[138], Benkler[139], Sauter[140], Knapp[141], Morozov[142] and O´Malley[143] attributing some expressive value to it and Li, McLaurin and Zuckerman[144] denying it on most occasions. Most prominent information society activists and visionaries to admit that there is a quantum of meaningful expression in a political DDoS attack include Richard Stallman and Ricardo Dominquez, Oxblood Ruffin[145] of the hacktivist group Cult of the Dead Cow on the other hand opposes to that.

3.3. Is there a right to protest on private property?

[136] Zuckerman, E. *et al*. 2010 Report on Distributed Denial of Service (DDOS) Attacks. Berkman Center Research Publication 2010, 16,
[137] Samuel (2004), *supra nota* 34, p 80ff.
[138] Hampson (2012), *supra nota* 57, p 540.
[139] Benkler (2012), *supra nota* 65.
[140] Sauter (2014), *supra nota* 30.
[141] Knapp, T. M. Hacktivism-Political Dissent in the Final Frontier. New England Law Review 2007, 49, p 263.
[142] Morozov (2010), *supra nota* 30.
[143] O´Malley (2013), *supra nota* 80.
[144] Zuckerman, E. et al. 2010 Report on Distributed Denial of Service (DDOS) Attacks. Berkman Center Research Publication 2010, 16, p 4.
[145] Mills, E. (2011), Old-time Hacktivists: Anonymous, You Have Crossed the Line, CNET, 30 March 2011, available at: http://www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/ (last accessed 1 May 2016)

The US Supreme Court created a precedent that allowed for quite liberal interpretation of the conditions on which is there a right to protest on private property in *Marsh vs Alabama*, where it established the "company town" doctrine, in which it treated a private corporation that performed certain traditional government functions as the equivalent of a state actor for the purposes of First Amendment. Justice Black wrote in his concurrent opinion that:

"The title of the land belongs to government or to a private person is not decisive, as the more the owner opens up his property for use by the public in general, the more his rights become circumscribed."

The Supreme Court continued to hold up the principles expressed in *Marsh*[146] up also in *Logan Valley*[147], but turned away from in *Lloyd Centre vs Tanner*[148], from then on as a general tendency the Court has moved away from *Marsh* and given priority to the right to property. Nunziato draws attention to the fact that the Court had rendered a different judgement in *Lloyd Centre* since in *Logan Valley* the protesters had protested directly against the activities of the shopping centre, whereas in *Lloyd* the object of protest was not related to the activities of the private company owning the mall. What distinguishes a DDoS attack from other forms of protest is that although they take place on private property, they are normally always targeted towards the entity that owns the website, which however might not overlap with the owners of the server. Majority of the known cases involving DDoS attacks have been brought to court by owners of the sites, i.e. the target companies or public authorities and do not concern the harm or inconvenience caused by the owners or other users of the server.

ECtHR has referred to *Marsh* in its judgement of 2003 in *Appleby vs UK*, which ultimately concluded that the state´s positive obligation to protect the freedom to peaceful assembly, did not extend to meetings that were held on private property, judge Maruste stated in his dissenting opinion:

"In my view, the property rights of the owners of the shopping mall were unnecessarily given priority over the applicants' freedom of expression and assembly /…/ The case raises the important issue of the State's positive obligations in a modern liberal society where many

[146] *Marsh*, *supra nota* 114.
[147] *Amalgamated Food Employees Union Local 590 v. Logan Valley Plaza Inc.,* 391 U.S. 308(1968).
[148] *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972).

traditionally State-owned services like post, transport, energy, health and community services and others have been or could be privatised. In this situation, should private owners' property rights prevail over other rights or does the State still have some responsibility to secure the proper balance between private and public interests?

In these circumstances, it is hard to agree with the Chamber's finding that the authorities bear no direct responsibility for the restrictions applied to the applicants. In a strict and formal sense that is true. But it does not mean that there were no indirect responsibilities. It cannot be the case that through privatisation the public authorities can divest themselves of all responsibility to protect rights and freedoms other than property rights. They still bear responsibility for deciding how the forum created by them is to be used and for ensuring that public interests and individuals' rights are respected. It is in the public interest to permit reasonable exercise of individual rights and freedoms, including the freedoms of speech and assembly on the property of a privately owned shopping centre, and not to make some public services and institutions inaccessible to the public and participants in demonstrations."[149]

Leading British scholar on the law of public protests David Mead shared judge Maruste´s criticism and wrote in his commentary of the decision that "It had failed to put in place a legal framework which would have provided effective protection for rights of freedom of expression and peaceful assembly while at the same time balancing those rights against the rights of property owners."[150] Time and again, protests have been held in private property such as cemeteries, malls, and in front of abortion clinics. The private/public dichotomy is highly appropriate also in cases of cyber protests, since although the Internet functions as a public forum of unprecedented amplitude, as a matter of fact it is owned and run by private companies.[151]

Another legal scholar who views Appleby as a failure to understand the importance and role of political speech as a prerequisite to a "functioning democracy" and the constitutional challenge posed by privatization is Oliver Gerstenberg. Gerstenberg compares Appleby to German Constitutional Court´s judgment in *Lüth*[152]. In *Lüth* a private person publicly called for the boycott

[149] ECtHR, *Appleby and Others v. The United Kingdom* (44306/98), 06 May 2003. Judge Maruste´s dissenting opinion
[150] Mead, D. Strasbourg Succumbs to the Temptation to Make a God of the Right of Property: Peaceful Protest on Private Land & (and) the Ramifications of Appleby v. UK. Journal of Civil Liberties 2003, 8 (2), pp 98-112, p 98.
[151] Nunziato, D. C. The Death of the Public Forum in Cyberspace. Berkeley Technology Law Journal 2005, pp 1115-1171.
[152] Gerstenberg, O. What Constitutions Can Do (But Courts Sometimes Don't): Property, Speech, and the Influence of Constitutional Norms on Private Law. The Canadian Journal of Law and Jurisprudence 2004, 17 (1), p 6.

of the products of another private person and thus committed an act which was criminalised according to the German law[153]. In civil court the company whose products were boycotted prevailed and the defendant was ordered to stop campaigning for the boycott. The Constitutional Court however explained explain that the constitutional rights weren't only "subjective rights" of the individual but also, and at the same time, "objective principles for the whole legal and social order."[154]

In *Appleby* the applicants emphasised that through the privatization of the shopping centre the state had escaped its constitutional responsibilities, although previously it had invested in the building and development of the centre. The latter implies that the centre was intended to carry a public function and indeed, once the construction was finalized it became the main actual meeting point and business area of the town. In addition to that, the applicants argued that the state had failed to protect the democratic value of freedom of expression and assembly by preventing third parties from infringing them, thereby not recognizing the horizontal effect of fundamental rights. According to the court and the UK Government however there were alternative reasonable fora where citizens could engage in political expression and assembly. The same argument was brought in the context of free expression on the Internet by US Supreme Court in Cyber Promotions vs AOL, where it concurred with AOL that the latter did not perform a public function by providing e-mail service and that the AOL users could be also reached through alternative channels. Nunziato highlights however that all of the mentioned reasonable alternatives were means of offline communication, which in principle indicates that in search for a legally acknowledged public forum, one should go two or three decades back in time, just like the applicants in Appleby were advised to pamphleteer in a relatively abandoned old city centre.

State action seems to have precedence over private interests when regulating online defamation and copyright infringements, however when it comes to protecting the freedom of expression and assembly it seems to relinquish. The law enforcement/criminalisation paradigm therefore has priority over the general trend towards privatisation, civil rights more often than not are put second. An interesting parallel situation would arise when private companies would use their property rights to interfere with other online political processes such as e-voting.[155] Disruption of democratic

[153] BVerfGE 7, 198, *Lüth,* 15 January 1958.
[154] Ibid.
[155] A situation where such claims might have emerged, occurred for example in the Netherlands during the last decade, when the whole process of e-voting was in fact outsourced to private developers. For a critical view on the Dutch e-voting framework see: Oostveen, A.M. Outsourcing Democracy: Losing Control of e-Voting in the Netherlands. Policy & Internet 2010, 2(4), pp 201-220.

elections is criminalised in most jurisdiction, but so is violent and/or arbitrary interference in peaceful assemblies. Most likely and rightly so the right to vote would be given absolute prevalence over any claims that an ISP or cable and broadcasting company might have. In case of an online protest the property rights on the contrary are given uncompromised precedence. This creates a logical dissonance in the whole theory of e-democracy, which seems to recognise the almost complete privatisation and the death of public forum on the Internet, at the same time treating this environment as an important carrier of public functions and medium for participation in one context, while completely denying the public role in another.

Therefore, the simple distinction between private and public space in cyberspace would lead to complete denial of the right to peaceful assembly and indeed also expression, which again is not the sought result. Moreover, making the right to property the absolute in cyberspace entangles a myriad of risks from the perspective of national security, democracy and the availability and integrity of CII-s. Therefore when considered alone the argument that a site or server is privately owned should not make it immune to the effects of fundamental rights and freedoms. Other factors, such as the *de facto* public functions that the web-environment fulfils, the public risks that an attack towards it creates and the character of the site (whether it is functional or representative[156]) should also be taken into account.

3.4. Inconvenience and economic loss caused to the target and third parties

As it concludes from the previous chapter, the horizontal effect of the freedom of assembly is rarely recognized in physical space and almost never in cyberspace. In the physical world however indirect third party effect of fundamental freedoms has been acknowledged by the ECJ on *Schmidberger vs Austria*[157] and *Commission vs France*[158]. In *Schmidberger* a group of environmental activists organised a protest on a public highway which was widely used for the purposes of intra-community trade, during the protest the transportation route was closed for 30 hours and the applicant Eugen Schmidberger who operated a transportation company argued that the failure on behalf of the Austrian government to prevent such a protest from taking place violated the right to free movement of goods within the EU. Austrian government had acted in accordance Article 2 of the

[156] On this distiction see: Sauter (2014), *supra nota* 30, p 14 ff. Representative sites are sites that mark the presence of an entity on the web, meanwhile a site when the company only operates on the internet.
[157] C-112/00, *Schmidberger vs Austria*, 12 June 2003.
[158] C-265/95, *Commission v. France*, 9 December 1997.

Regulation(EC) 2679/98 on the functioning the internal market in relation to the free movement of goods among the Member States, which prohibits applying the norms of the regulation in a way that would affect in any way the exercise of fundamental rights

Eva Julia Lohse highlights that when fundamental rights are weighed against the EU fundamental freedoms, it appears that in their essence these two categories are in fact very similar. Albeit, originally designed as a remedy against trans-border discrimination, the EU fundamental freedoms soon acquired the function as right to access to the market.[159] Furthermore, in *Procureur de la Republique v ABDHU* ECJ spoke of freedom of trade as a fundamental right, later the Charter of Fundamental Rights explicitly contained freedom to conduct business[160]. As opposed to the right to property, freedom of trade has been subordinated to citizens´ right to assemble. Besides, the subjective individual rights rising from EU law, Member States are obliged not to create, foster or ignore conditions that halter free movement of goods. In *Schmidberger* the state failed to act out of respect for the fundamental rights of the protesters, which according to ECJ presents a legitimate justification. Would the free movement of goods and services also have to capitulate to the fundamental rights in the cyberspace, for example in the context of the European digital single market? Could there ever be a cyber *Schmidberger* or would the private property argument again triumph?

Article 30, read in conjunction with Article 5 of the Treaty, are also applied where a member State abstained from adopting the measures required in order to deal with obstacles to the free movement of goods which were not caused by the State. As opposed to *Schmidberger*, the protests in *Commission vs France* were sporadic, unpredictable and had lasted for approximately 10 years, although many of the perpetrators were identified or identifiable, prosecutions were rare. Taken together, these factors contributed to the final judgment in which ECJ ruled that the French government´s efforts to tackle the situation had been manifestly inadequate and France had thus contravened Article 30.

ECtHR has on multiple occasions ruled that some disruption to public order and private interests is allowed. Nevertheless, in the first grand chamber judgment on the right to protest *Kudrevičius and Others v. Lithuania*[161] ECtHR held in force the judgment of the Lithuanian Supreme Court which had ruled that disruption of public order constituted a valid justification for the implementation of

[159] Lohse, E. J. Fundamental Freedoms and Private Actors–towards an 'Indirect Horizontal Effect'. European Public Law 2007, 13, no. 1, p 170.
[160] 240/83, *Procureur de la Republique v ABDHU*, 7 February 1985.
[161] ECtHR, *Kudrevicius vs Lithuania*, 37553/05, 15 October 2015.

criminal liability. The applicants were farmers who had organised and participated in roadblocks on public roads in order to protest against the decrease of the prices of locally produced dairy products. Among other arguments, the Grand Chamber concluded that an appropriate balance of rights had been achieved in the case at hand, since the activities of the farmers had no direct connection with the object of their protest and infringed on the right of free movement of others, this logic speaks in favour of cyberprotests, where the place of protest usually overlaps with the target. It has been argued that this makes the actual social costs of a DDoS attack relatively low, since often there will be alternative avenues that consumers/clients could still use.[162]

Economic loss suffered by the target on the other hand might be noticeably greater. In case of attacks against critical infrastructures this generalisation however does not hold true neither offline nor online. The choice of target as a criterion for legitimation of an online protest will be elaborated on in the next subchapter. When faced with a choice between two forums – one in which public attention is guaranteed and possibly higher social costs might occur, albeit the target is easily able to overlook the protests and another, where social costs and attention tend be lower, but the target could not ignore the actions that are taking place - which one would a reasonable protester choose? Would choosing the second one automatically succumb into coercion? Protesters both online and offline seem to be in a predicament, because on one hand the courts favour activities that are more oriented towards public attention and awareness raising, on the other hand, a reasonable protest should be expected to have some real influence on the cause, meaning that it should be able to impact the targets.

Some commentators have argued that *Kudrevičius* marks an unexpected turn towards weakening the protection of the right to assembly[163]. Previously, the court has ruled in *Stankov vs Bulgaria*,[164] *Kuznetsov v. Russia* and *Lucas vs France*[165] that Article 11 is not applicable to gatherings where the organisers and participants have violent intentions, incite to violence or otherwise reject the foundation of a democratic society. In *Primov*[166] and *Ziliberberg*[167], the Court had stated that an individual does not cease to enjoy the right to freedom of assembly as a result sporadic or punishable acts committed by others in the course a demonstration when the individual in question remains

[162] Eds. Grady, M.F., Parisi, F. The Law and Economics of Cybersecurity. Cambridge University Press 2005, p 23.
[163] See, e.g. Strasbourg observers, Can You Hear the People Sing?, 2 December 2015, available online at: https://strasbourgobservers.com/2015/12/02/do-you-hear-the-people-sing-kudrevicius-v-lithuania-and-the-problematic-expansion-of-principles-that-mute-assemblies/ (last accessed 1 May 2016)
[164] ECtHR, *Stankov vs Bulgaria*, 29221/95 29225/95, 2 October 2001.
[165] ECtHR, *Lucas vs France*, 37257/97, 28 November 2000.
[166] ECtHR, *Primov vs Russia*, 17391/06, 12 June 2014.
[167] ECtHR, *Zilberberg vs Moldova*, 61821/00, 1 February 2005.

peaceful in his or her own intentions and behaviour. In *Primov* it concluded that the possibility that persons with violent intentions might join a demonstration does not take away the right to peacefully assemble from other participants. The latter is relevant to political DDoS attacks, where some members may choose to use botnets and thereby are uncontestably committing a crime.

In *Lucas* and *Barraco*[168] the Court explains further that the core of Article 11 values does not encompass physical conduct purposefully obstructing traffic and the ordinary course of life. In *Schwabe*[169] the Court stipulates that a real risk of a protest descending into violence due to other actors than the organisers, does not exclude the protest from the scope of protection of Article 11. As mentioned before, there is virtually no case law on DDoS attacks that would reflect upon the fundamental rights aspects, which does not imply that these arguments have not been raised. Evgeny Morozov writes: Would we advise anyone participating in lunch-counter sit-ins during the civil rights era not to do it because it may popularize sit-ins as a tactic that might be abused by all sorts of crazy people and criminals?[170] Thereby Morozov is hinting at the fundamental idea that the mere potential of violence whether in nearer or farther future does not automatically render an act of protest illegitimate. This leads us to the question what is virtual violence?

3.5. Coercion, force and violence within a protest

The Lufthansa case which is often perceived as a triumph for the online civil society was prosecuted under German Penal Code Article 240, which stands for coercion. This means that the Higher Regional Court of Frankfurt had in fact approached the online sit-in just as it would have its physical world equivalent, admitting that there are no applicable computer crime norms. This is probably because a regulation directly criminalising client-side "front-door entry" DDoS attacks[171] was at the time missing from German criminal law. Numerous cases of sit-ins have been charged with a violation of Art 240 of the German Criminal Code[172], in substance, the offense punishes a person who uses force (or certain other means) to coerce someone to an act or omission. The accused had called in June 2001 participants to access Lufthansa´s webpage with the intent to overwhelm the Lufthansa server, the motivation behind the DDoS attack was the fact that the German airline had

[168] ECtHR, *Barraco vs France*, 31684/05, 5 March 2003.
[169] ECtHR, *Schwabe vs Germany*, 8080/08 8577/08, 1 December 2012.
[170] Morozov, E. Should we oppose sitins just because crazy people can abuse them?, Foreign Policy, 16 December 2010, available online at: http://foreignpolicy.com/2010/12/16/should-we-oppose-sit-ins-just-because-crazy-people-can-abuse-them/ (last accessed 1 May 2016)
[171] See Stallman (2010), *supra nota* 69.
[172] Quint, P. E. Civil Disobedience and the German Courts: the Pershing Missile Protests in Comparative Perspective. Routledge 2007, pp 166-168.

been deporting refugees for financial benefit. The online demonstration wasn´t an isolated stand-alone event but took place simultaneously with street demonstrations, petitions and an active media campaign. The participants downloaded a special software that enabled to multiply the number of requests sent out per second. The online demonstration lasted for two hours, during which Lufthansa´s servers got around 1,262,000 pings from 13,614 different IP addresses. The target and public were informed beforehand, so that Lufthansa was able to prepare for the action by renting extra server space. Altogether Lufthansa´s costs amounted to approximately 70 000 euros.[173]

The court of first instance of Frankfurt ruled against one of the main organisers of the online demonstration that the DDoS attack had equalled the use of force against both Lufthansa and the legitimate customers. The Higher Regional Court however overturned these convictions stating that in the given case a DDoS did not amount to either violence or threat of a substantial evil. The use of force under coercion law has been substantiated by German criminal courts many times in circumstances where actual physical violence, threatening and physical harm were hard indicate. Peter Quint writes on the application of the coercion rule on physical world sit-ins:

"Protesting an increase in streetcar fare, a group of students staged a mass "sit-down strike," blocking streetcar traffic at two important points in the city of Cologne. Some protestors were dispersed by mounted police and high-pressure hoses. In the prosecution of demonstration leaders, the BGH declared that the students who sat on the tracks "coerced the streetcar drivers with force to stop their vehicles." The Court reached this conclusion even though the students "did not stop the streetcars through the direct application of physical strength, but rather—expending only minimal physical energy—[they] set in motion a psychologically determined process."[174]

Above Quint is referring to the *Laepple* judgment, where the court confirmed that a certain kind of coercive effect may constitute "force" under §240, even though the weakening of the will is not accomplished by physical action directly applied to the body of the victim, however the effects occur directly in the physical worl.[175] The Higher Regional Court of Frankfurt dwelled on the jurisprudence of the Federal Constitutional Court while arguing that purely spiritual or psychological means of influencing do not qualify as force. The District Court of Frankfurt had compared a mouse click with pulling the trigger of a gun, the Higher Regional Court however

[173] Franfurt District Court, 991 Ds 6100 Js 226314/01, *Vogel*, 11 July 2005, para 8 ff.
[174] Quint (2007), *supra nota* 172.
[175] Quint (2007), *supra nota* 172.

claims that unlike pulling a trigger the movement is not directed towards bodily harm and hence cannot be perceived as force.[176] The effect of the mouse click activating the software is limited to the Internet, which also the District Court had admitted to be a technical construct, and not towards the bodies of the users. Secondly, no threatening with substantial evil had occurred, since the activities did not involve a threat, no future-oriented fear of violence was induced, the acts were restricted in time to the duration of the online demonstration.[177] Thirdly, the court did not recognise that DDoS would have constituted coercion through use of force against property, since this would mean that every theft could also be perceived as coercion. As a result of the operation, the users had to change their behaviour only in the sense that they couldn´t access Lufthansa´s webpage for ticket reservation or other purposes. The court drew an analogy with theft, since stealing an item prevents a legitimate user from using it, but does not coerce her into stopping using it. The court therefore concluded that no coercion had taken place, since there was no coercive motivation involved.[178]

Use of force or violence could however undoubtedly be established in cases where critical infrastructures are attacked. Certain digital networks are vital to the functioning, security and health of the society, interfering in some military ammunition networks is equal to actually using the weapons or making them unusable for the protection of national security. Utilities and finance are integral to the health of the economy and people. While in the Lufthansa case, the effect of the attack was indeed limited to the technical construct within which it took place, then attacks against flight coordination systems would have a grave and catastrophic effect in the physical world. Authors who otherwise have approved the idea of legitimising political DDoS attacks, have always drawn a line at critical infrastructures. An attack against a critical infrastructure would most likely also cross the border between crime and terrorism and should be assessed accordingly, without contemplating whether or not there was a coercive motive or was it an expression of political dissent. The majority of scenarios invoked in the discussion about the possibility of cyber war concern attacks against CII-s and the only currently thinkable acts that according to experts would grant a state the right of self-defence against a group of civilians would also probably be committed against CII-s. Therefore, as these attacks are clearly non-peaceful and often belong to the realm of international humanitarian law, they are outside the scope of the present research. This being said, the first step in clarifying whether or not a DDoS could be considered a legitimate act or protest

[176] Frankfurt OLG, 1 Ss 319/05, 22 May 2006, para 43.
[177] Ibid, para 64.
[178] Ibid, para 68.

should be eliminating critical information infrastructures from the possible targets. Secondly, coercive intent should be removed from the equation.

3.6. Duty to notify

In the case law of ECtHR little can be found that would speak against the requirement of prior notification or even permit. In *K vs Netherlands*[179], the applicant´s plea was declared manifestly ill-founded, where she was asked to leave the train station where she had been protesting alone without having notified the authorities or applied for permission beforehand. An example of a case where the application of riot control measures at a protest that had breached the duty to notify was considered a violation of Article 11 is *Oya Ataman vs Turkey*.[180] In *Oya Ataman* the unnotified yet peaceful demonstration was dispersed by tear gas and many of the participants were arrested, the Court found that in the present circumstances, where no threat of violence or disturbance of public peace had occurred, yet the protest had obstructed the flow of traffic, the interference had been disproportionate.

The duty to notify is foreseen by all the states that were observed in the previous chapter. In the UK the duty applies only to processions and not to stationary assemblies. The German Constitution however guarantees the right to assemble without prior notice or permit, however outdoor assemblies are subject to administrative restrictions. The Constitutional Court asserted in *Brokdorf*[181] that this is necessary due to the fact that outdoor assemblies have impact on the public order and third parties, which often calls for precautionary and assisting measures. A cyberprotests is not an outdoor or an indoor protest, but nevertheless has a strong external impact, therefore applying *Brokdorf* to a political DDoS appears sound from the legal perspective. Also in Brokdorf the Court reiterated that the fact that the organisers had disregarded the duty to notify is not a sufficient reason for the dispersal of the assembly[182]. In the United States the regulation of protests is subject to state law and prior restrictions are allowed as long as they are content-neutral.

Therefore, duty to notify is a generally acknowledged restriction, which should also apply to cyber protests, especially since because they are characterized by lack of accountability and expressivity. Therefore by introducing the duty to notify, in addition to enabling the authorities and target to

[179] ECtHR, *K vs the Netherlands*, 21563/08, 25 September 2012.
[180] ECtHR, *Oya Ataman vs Turkey*, 74552/01, 5 December 2006.
[181] BVerfGE 69, 315, *Brokdorf*, 14 May 1985
[182] Ibid.

prepare for the event, also the often feared complete impunity would be ruled out and at least some minimal level of expression would be included, which also helps to clarify the intent.

3.7. Conclusions

Most common arguments against granting the status of legitimate act of protest to DDoS attacks are the lack of accountability, low resemblance to pure speech, violation of property rights, inconvenience and disrupt caused to third parties and their fundamentally coercive nature. The most cyber-specific of these is the private property problem, since the borderless arena of free speech in fact lacks the concept of public forum altogether, meanwhile public fora are waning also in the physical space. In these circumstances, the blanket preference of property rights over freedom of expression and assembly has been criticised by judges and scholars alike. Moreover, admitting the absolute prevalence of private property in the cyberspace might be in conflict with other public interests. For an approach that would be in line with the wider concept of e-democracy, other aspects besides property ownership should be taken into consideration when deciding over the legality of a cyberprotest.

The anonymity of a cyberprotester is often overestimated, since absolute identifiability cannot be demanded from an offline protesters, neither should this be the case for an online protesters. Protests where no involuntary botnets were used and IP addresses of the participants are traceable should be made tantamount to offline protests, where many participants choose to cover their faces. Massive use of tools that obstruct identification and allow true anonymity however undermines the credibility and legitimacy of an operation, therefore the organisers of the protest should make all efforts to ensure accountability. However following from the ECtHR case law on acts of violence taking place during a public protest, the offenses committed by one participant should not have an impact on the legitimacy of the actions of others or the protest as a whole. Therefore the fact that some participants are using effective technological means to hide their identities should not deprive the whole protest of the protection of the fundamental right to assembly. However, within a regulatory framework that to a large extent serves the purposes of deterrence and sets forth sanctions remarkably more severe than for physical space civil disobedience, it would often prove unfeasible to expect absolute voluntary identifiability on behalf of the protesters. Another aspect worth emphasising about anonymity and accountability is that it should in fact come in last in the formula, since it only plays an essential role in cases where actual violations have taken place, and hence should not be the first criterion according to which to assess

a protest. Nevertheless, similarly to physical space protests, to ensure certain degree of proportionality and accountability a duty of prior notification should be introduced.

When conducted simultaneously with offline activities and communicated openly to the public, a DDoS may be expressive enough to mediate a political idea. Making the legitimacy dependent on the extent to which the public actually engages in the issue in question and is able to understand that, might ultimately restrict the freedom of assembly regardless of the forum that it is being exercised in and be in conflict with the principle content-neutrality. A mute attack without a previously published agenda or manifesto however would fail to express an idea or fight for a collective aim, therefore making it ineligible for fundamental rights protection.

Peacefulness is the foremost condition envisaged in all international human rights instruments and constantly reiterated by courts. What distinguishes cyber peace from cyber violence? Acts of protest are in practice frequently prosecuted under coercion charges. This aspect stands out since unlike the others it has been discussed by a court in the context of a large scale hacktivist operation. However, in the case in question, the court did not find that a DDoS attack constituted coercion, since its effects were limited to the Internet and there were neither coercive motives nor physical consequences that would cross the line between inconvenience and violence emerged. Indeed, usually this would be the case for political voluntary DDoS attacks, however attacks that may culminate with real space violence or physical damages should be eliminated from the discussion about peaceful assemblies and find their place within the sphere of criminal or humanitarian law, this means that attacks against CII-s are out of the scope of the present analysis.

4. Model Regulation

The previous chapters have given an overview of the main problematics of regulating collective action cyberprotests and enable to draw conclusions on how should regulating assemblies in the cyberspace differ from the regulation that applies in the physical space. In a nutshell, a political collective action DDoS should be non-violent, public, allow for accountability, represent a collective aim and the impact of it should be proportional to the number of participants. The first step while reflecting upon the legitimacy of a cyber protest would therefore to make sure that no critical information infrastructures are impacted. Secondly, since a DDoS itself is not a communicative tool, an online assembly should be accompanied by a public announcement and a debate taking place simultaneously with it, so that the political motives would become understandable to the audiences. Thirdly, the use of anonymization techniques should be banned and penalized, however the penalties should become enforceable only when breaches of law have taken place. One obvious example of the illegitimate means would be the use of botnets, which should be prosecuted under national computer crime laws. Time and duration of the protest should be pre-regulated and coercive intent ought to be ruled out, this includes direct demands on the object of protest.

Authors have come out with alternative regulations, perhaps the most relevant one is the model suggested computer scientists of University of Eindhoven, which consists of three clusters[183]. They define a digital assembly as "a group of people that publicly expresses their opinion", the first cluster of requirements derives directly from the definition and foresees three conditions: visibility, expression of opinion and collective nature. The latter has two sub-requirements, firstly that the one person-one vote rule should be followed and secondly that the impact of the protest should be proportional to the number of participants and size of the target. They proceed to explain that:

"It should not be possible for one person to take down another party single handed – e.g. by exploiting a vulnerability. Comparably, a small group of protesters should not be able to take down a corporation that is much larger. Thus, the used techniques should comply with this requirement of group proportionality."[184]

[183] Slobbe, J., Verberkt, S. L. C. Hacktivists: Cyberterrorists or Online Activists? 2012, unpublised preprint article *arXiv preprint arXiv:1208.4568,* available at: http://arxiv.org/abs/1208.4568 (last accessed 1 May 2016), p 24 ff.
[184] Ibid.

The author of the present thesis is of the opinion that the principal aspects of group proportionality are already covered by the one person-one computer principle. The author of the present thesis is however of the opinion that the number of participants and the impact should be proportionate to the relevance of the cause and not depend on the size of the target.

The second cluster focuses on the requirements for the legitimacy of a digital assembly. [185] These requirements overlap to a large extents with the conditions described in Chapter I and the Rawlsian theory of the justification of civil disobedience. The first requirement is that the protest is organised in the general interest the motivation being willingness to express dissent. Secondly, the damages should be proportional. Thirdly alternatives should have been pursued, which however in reality would prove to be difficult to define since the sought alternatives should be reasonably expected to be efficient. Therefore, while for instance protesting against a corporation that mainly operates on the Internet, a protest on the sidewalks in front of their registered location, would hardly be a meaningful or efficient alternative.

The third cluster foresees methods that would enable to preserve order within a digital assembly. The first condition would be supervision by the police, the second is the existence of a central organisation responsible for the announcement of the protest. The central organisation however is primarily responsible for delivering the announcement to the target, so that when the circumstances require it could enforce an injunction if it thinks the protest disproportionally harms his interest. Notifying the target constitutes the third condition. The duty to notify the authorities depends on domestic regulation, but should however be in line with constitutional rights and international fundamental rights instruments containing the right to peaceful assembly.[186] In the majority of aspects, the regulation proposed by Slobbe and Verberkt coincides with the one that the author would subscribe to and that indeed would follow logically from the preceding analysis.[187] However, in some minor aspects it also differs.

The author would propose a following system of assessment. As a first step the political intent should be established, thereafter critical infrastructures or other systems the attacking of which would result in physical harm, should be excluded from possible targets. Following that, the target should be notified prior to the attack, so should be the law enforcement units focusing on cybercrime in the jurisdiction where the servers of the target are situated. Similarly to real life,

[185] Ibid, p 33 ff.
[186] Ibid.
[187] Ibid.

notification and presence of law enforcement cannot be considered disproportionate restrictions. Notification would therefore be obligatory, prior permit however would not constitute a necessary requirement and the only potential ground for prohibition would be a possible interference with critical infrastructures. A framework for enforcing an injunction against the planned protest should be in place, enabling the object of protest to present counterarguments or apply for delay. The requirement of prior notification of the authorities and the target require that a certain degree of accountability exists, although this might be contradictory to the fundamentally decentralised nature of the Internet. In addition to fulfilling the notification requirement, the protest should be announced publicly via popular digital or traditional media channels, this also contributes to the fulfilment of the condition of sufficient expressivity.

If these prior requirements are met, the organiser should make every effort to ensure that the principle of group proportionality is followed, however neither the organisers nor law obedient participants should be held accountable for the individual violations of the aforementioned principle taking place during the protest. Secondly, the organisers should make every endeavour in order that ensure that the participants refrain from using techniques that allow for untraceable anonymity, since it undermines the principle of accountability and robs the protest of social significance. However, again in circumstances where skilful mass application of tools enabling true anonymity is highly unlikely, no law obedient participant or organiser should have the liability for the breaches of law committed by unidentifiable participants. Finally, it should be noted that the mere compliance with the abovementioned criteria does not automatically imply that any interference with such a digital assembly would violate a fundamental right, it only indicates that as such assemblies would fall under the scope of protection of the right to assembly, any interference should be assessed according to the classical three tier-test of legitimate aim, necessity and proportionality.

To see whether the suggested criteria would help to establish whether a hacktivist DDoS operations could be considered an assembly, subsequently they are applied to some of the cases mentioned in previous chapters: the virtual sit-ins arranged by EDT in support of the Zapatista movement, operation PayBack, *Lufthansa vs Vogel* and Harju County Court´s judgment in *D.G.*

4.1. EDT digital sit-in in support of the Mexican Zapatistas

In 1999 the hacktivist movement Electronic Disturbance Theatre organized a massive virtual sit-in at Mexican government´s website in support of the Zapatista movement. Prior to launching the ping flood, the government was notified in a series of emails. The DDoS took place within the context of a large and well documented political campaign, furthermore the used FloodNet version called upon the users to "send your own message to the error log of the institution or symbol of Mexican Neo-Liberalism of your choice,"[188] which in practice meant that when users tried to access the webpage during the protests, the error 404 "Page unavailable" announcement came back with messages such as "No human rights found on this site" or "No democracy found on this site". Therefore, it is safe to say that the expressive element was certainly present and also the political intent was sufficiently clear, whereas no coercive demands were involved in the campaign. [189]Although automated traffic amplification tool FloodNet was used, it didn´t break the group proportionality requirement, since all the participants were able to send equal number of requests per second and albeit exceeding a person´s capacity to physically repeatedly hit the refresh button, the number of requests were proportional to the capacity and default configuration of the computers. Electronic Disturbance Theatre had public spokespeople communicating with other activists and both sides of the conflict, therefore the accountability element wasn´t missing although the majority of participants remained anonymous. Therefore, taking into consideration that there was no defined system of notification in place at the time, EDT can be said to have done reasonable efforts for prior notification and as all other criteria is fulfilled, the EDT operation would constitute a legitimate act of protest according to the proposed regulation.

4.2. "Deportation class" action against Lufthansa

The Lufthansa case has already been judicially approved, so the main purpose of testing it against the suggested criteria, is to see whether it could also be approved, when the temporary disruption of the functioning of an information system is penalised. The organisers who belonged to the Libertad! and "Kein Mensch ist illegal" movements, notified the target and also followed the standard procedure of prior notification foreseen in the the Federal Act concerning Assemblies and Procession, which meant that they informed City of Cologne's Department of Public Safety of the upcoming demonstration taking place on *www.lufthansa.com*. Taking into consideration that there were no mechanisms or bodies in place that would deal with incidents of cyber collective action,

[188] Sauter (2013), *supra nota* 60, p 112.
[189] Taylor (2004), *supra not*a 25.

following the standard course of notification was the most optimal avenue. After the notification Lufthansa had enough time to rent extra server space and therefore managed to cope with the protest in a way that leaves the question whether or not any actual downtime occurred still unclear. The fulfilment of the duty to notify covers both the accountability and intent requirements and enables to mitigate the potential damages or inconvenience. The fact that the protest took place within a wider context grants it sufficient expressivity. Although, again an automation tool similar to FloodNet was used, it did not break the group proportionality or one computer-one participant principle, nor were the use of botnets established. Therefore, even in the current German computer crime legislation, which criminalises temporary interruption, there should be room for peaceful assemblies, among which the Deportation class protests belong.

4.3. Operation AvengeAssange

Operation PayBack consisted of multiple attacks against organisations, politicians and financial institutions worldwide that had according to the organisers expressed reactionary views on information freedom, WikiLeaks and copyright issues. A series of DDoS that went under the name AvengeAssange were launched in support of WikiLeaks in late 2010. According to an overview given by Steve Mansfield-Devine in Network security, the tools most commonly applied were desktop LOIC, JavaScript LOIC and HiveMind mode, main targets of the Anonymous attacks over the first couple of weeks of December 2010 were:[190]

- financial organisations – such as MasterCard, Visa and PayPal – which blocked payments to Wikileaks.
- the website of the US senator who wants Assange to be tried under espionage laws.
- US politician Sarah Palin, who called for Assange to be treated like a terrorist, also found her website under attack from some Anons, but only a minority.
- the Swedish law firm representing the two women who have made allegations of sexual misconduct against Assange.
- the Swedish prosecutor's office responsible for the case.
- Swiss bank PostFinance which suspended Assange's defence fund account.

As it is characteristic to the amorphous nature of Anonymous, the channels used for notification were sporadic, the attacks were nevertheless conceivably connected to the political aims. As there was no legitimate notification procedure in place, establishing whether or not the notification

[190] Mansfield-Devine, S. Anonymous: Serious Threat or Mere Annoyance? ."Network Security 2011, no. 1, pp 4-10.

requirement was in fact fulfilled is complex. Although information about the planned attacks was circulating online, for example on Anonymous Twitter account and the IRC site of Operation PayBack was regularly updated, furthermore the Anons IRC group contains a list of potential target addresses and the statuses of planned, ongoing and past operations. However, a site owner or ISP cannot be expected to regularly visit the pages in order to determine if they might be on the list of targets. Therefore, in the case of operation AvengeAssange it is feasible to assume that that the efforts to communicate the planned attack to not measure up to the fulfilment of the notification requirement. When applying the arguments of ECtHR and German Constitutional Court however, although deemed an administrative offence the failure to notify does not always justify the dispersal of the assembly or enforcing criminal charges upon the participants. However, in the present case it results in lower levels of accountability. Therefore, the applied anonymization techniques should be looked into.

Mansfield-Devine enounces that: "Given that the DDoS attacks mounted by Anonymous are unambiguously illegal in most countries (and all of the countries in which Anons are likely to have been operating), it's interesting to note that one thing the LOIC tool makes no attempt to do is conceal the identity of the attacker." He proceeds to describe the majority of participants as cannon fodder for Anonymous, the traceability however counts for higher accountability. Therefore even if the accountability does not constitute an issue, it is ultimately not due to the participants´ willingness to be publicly associated with the operation and the political views that it represents. The lack of the latter is proved by the somewhat inefficient tips shared in the IRC group on how to avoid liability, which included claiming that the computer was infected with a virus or making your wifi router to be open, so that it would be possible to claim that somebody else had used it for the attacks.[191] Operation Payback consequently is unlikely to meet the accountability criterion even in the sense that the general mentality promoted by the protesters would stand for not avoiding liability.

Another problematic aspect is the group proportionality, Mansfield-Devine writes that „cybercrime gangs using DDoS as a blackmail tool, or state-sponsored hackers using it as a weapon of war, will deploy botnets comprising tens of thousands of machines focused on a single target. Even at the peak of the Anonymous attacks, the number of participants was in the low thousands, and most of the time there were only hundreds of LOIC clients firing at the same time at the same target."[192] He adds that only the users of HiveMind LOIC benefitted from some degree

[191] Ibid.
[192] Ibid.

of automation.[193] Therefore, what in his interpretation counts for inefficiency, counts as group proportionality pursuant to the suggested legitimation criteria. The amorphous nature and multiplicity of targets impair the levels of unity and mobilization, which also holds true to real life demonstration. Therefore, albeit the use of small botnets was identified, in general the group proportionality principle seems to have been followed. Concluding from the facts analysis presented above the author is of the opinion, that operation AvangeAssange is not as a whole compatible with the suggested criteria since: a) the organisers failed to notify the objects of protest, the authorities and the public in a comprehensible way b) the organisers made active (although unsuccessful) efforts to circumvent accountability. The other criteria, i.e. choice of a suitable target, expressivity and group proportionality however were sufficiently present.

4.3. D.G vs Estonia

Lastly, the sole case that was prosecuted as a result of the cyber-attacks against Estonia of 2007, is taken under observation. This case differs from the latter three, since it concerns the actions of a single participant, whereas in *Vogel* the defendant was identified as one of the organisers and the legitimacy of the whole operation was evaluated. The D.G judgement does not contain any analysis of the legitimacy of the large scale DDoS attack against the Reform Party website or other targeted sites. Similarly to the operation analysed in 4.2, the organisers had failed to notify the target, responsible authorities and the public. Harju County Court does not reflect upon the aspects relevant to the right of assembly. However, as the cyber-attacks started simultaneously with the physical space riots in Tallinn, the onset of them was spontaneous and no prior notification was given.[194]

Furthermore Article 64 of the Law Enforcement Act of the Republic of Estonia prohibits meetings that are directed against the independence and sovereignty of the Republic of Estonia or at changing the constitutional order of the Republic of Estonia by force, incites a breach of the territorial integrity of the Republic of Estonia by force, incites hatred, violence or discrimination on the basis of nationality, race, colour, sex, language, origin, religion, sexual orientation, political views, or property or social status, or aims to commit criminal offences or to incite them.[195]

[193] Ibid.
[194] HMKo, 1-07-15185, 13 December 2008
[195] Law Enforcement Act, RT I, 23.03.2015, 207.

As according to the model regulation, organising or participating in a cyberprotest would not constitute a criminal offence when other conditions are met, the cyber-attacks would not be automatically viewed illegitimate due to aiming to hinder the functioning of a system. However, in order for it to gain expressivity the individual case should be looked at within the general symbolic context of the attacks, which included incitement to hatred on national grounds, a breach of the territorial integrity and was at least partially directed against the independence and sovereignty of the Republic of Estonia. The defendant was not however proven guilty of any of the aforementioned offences, nor was his intent to protest against the removal the Soviet War memorial questioned by the court. Mere opposing to the removal of the memorial would not amount to an act directed against the independence and sovereignty of Estonia.

No other elements of criminal conduct or intent were present in the defendant´s actions, also the chosen target did not constitute a system of vital importance. The changing of the default number of pings sent per second, should be assessed according to the overall impact of the attack. In the present case, since no computers were hijacked, the defendant can be said to have acted within the frames of the group proportionality principle. However, since the cyber protest had failed to meet the requirements of notification, accountability and also were likely to qualify for prohibition under Article 64 of the Law Enforcement Act, the right to peaceful assembly foreseen in Article 11 of the ECHR and Article 47 of the Constitution of Estonia do not outweigh the states right to impose sanctions on individual participants[196]. Therefore, applying the analogy of ECtHR case law allows to conclude that invoking criminal liability does not disproportionately infringe upon the individuals´ right to assemble in cases where the assembly turns into a riot and the sanctions are necessary in a democratic society.[197] Here, it should be noted that the prescribed pecuniary punishment of 17 500 kroons, i.e. 350 fine units, does not notably exceed the charges prescribed for trespass which amount to 300 fine units, or on aggravated circumstances, which *inter alia* encompass the intention of occupying an area, building or premises or of interfering with the regular operation thereof, to up to three years' imprisonment. Therefore, the judgment of Harju County Court cannot be considered disproportionate to the national regulation of physical space protests. As the protests failed to meet any of the suggested criteria to be qualified as a form of legitimate assembly, the protection granted by fundamental rights is accordingly weaker and a state´s power of discretion when imposing restraints or sanctions again stronger.

[196] *Kudrevicius, supra nota* 161.
[197] Ibid.

4.4. Conclusions

Drawing on the analyses of the previous three chapters, the final chapter aimed to come up with a criteria which enables to distinguish whether or not a digital assembly qualifies for the protection under the scope of fundamental rights and freedoms. The results of the first three parts of the present thesis, allow to conclude that the key elements of the test would be:

- choice of target
- duty to notify
- expressivity
- accountability
- group proportionality

Five real-life incidents were thereafter studied, which exposed that the most problematic aspects are notification and the willingness to be held accountable. However, the accountability condition was not in fact greatly impaired by the anonymity that the participants are often perceived to have in the cybersphere. Furthermore, none of the observed incidents included grave violations of the group proportionality, which are often associated with the occurrence of cybercrime, e.g. the use of botnets, within the collective action protest. While analysing the fulfilment of the duty to notify it should also be kept in mind that since cyberprotests are to date not covered by any human rights instrument, the procedure of organising one is completely unregulated, therefore no jurisdiction has so far in fact prescribed the duty to notify. The analysis gave evidence that although no single form of physical space protest serves as the perfect analogy, in its motivation and fundamental principles a protest online is not that different from one taking place on the streets. Also, similar risks are associated, the latter however should not mean that online protests ought to be universally criminalised. Some additional guarantees to prevent crime and ensure network security would however be beneficial, this mainly implies that due to lower levels of accountability and visibility, in order to follow the classical theory justifying civil disobedience, also lower levels of spontaneity should be allowed.

Conclusions

The aim of the present thesis was to determine the main factors that have so far prevented online collective action protests from gaining the status of a legitimate form of protest. Internet serves as the global public forum of unprecedented scope and the general theories and appreciation of e-democracy and online citizen empowerment tools would not be complete without one of the cornerstones of democratic societies – the freedom of assembly. However, when analysing the perspective of decriminalising online protests, it becomes clear that within the modern cybersphere there is little space for civil society. The Internet is almost entirely owned and operated by the private sector, in addition to that it is largely controlled by military and law enforcement interests. As a result of the emerging threats of cyberspace, legislators have made efforts to phrase the cybercrime regulations as broadly as possible, so that to ensure technology and indeed also intent- and purpose-neutrality.

In order to see whether a legally conducted cyber protest would be a feasible future prospect, the main criteria that is deemed necessary for a traditional physical space protest to qualify as legitimate, was studied. The analysis enabled to conclude that according to the natural law theory of civil disobedience and also to the commentaries of the fundamental rights instruments that include freedom of assembly a protest needs to meet the following conditions:

- non-violence
- public nature/visibility
- collective political aim
- expressivity
- willingness to take responsibility

Therefore, in cases where a cyber protest meets the aforementioned requirements, it should be assumed that it could be viewed as a legal form of assembly? Political distributed denial of service attacks are well suited to become the digital heir of the legacy of collective action protests such as sit-ins or processions, since they enable group of people to target the object of protest collectively. Secondly, the participation does not require advanced knowledge in technology. However, unlikely in the physical space, the online tools used by civil activists are identical to these that are applied by criminals or terrorists, which makes the political intent to bring about social change and malicious activity more difficult to distinguish.

Therefore, in the current context the prevalent response to the rise of phenomenon of cyber protests has been universal criminalisation. The road to it has not always been smooth, since most commonly cyberprotests do not involve the root of cybercrime (not computer assisted crime) – illegal access and then to cause moderate damages that fall within the definition of inconvenience. A certain degree of the latter again is again perceived as an inevitable feature of public protests in the physical space and therefore not as sufficient grounds for criminal liability. Also, similarly to processions or sit-ins in the majority of the cases the harm caused is only of temporary. These factors have lead for example Germany and UK to amend their cybercrime legislation in 2007 and 2006 respectively in order to be in line with the Council of Europe Convention on Cybercrime, which criminalises system interferences, under which DDoS attacks generally fall. The complexity of criminalising DDoS attacks has also contributed to the outcome of the only known case where a hacktivist DDoS attack was in fact acquitted by a court.

However, as of today, no studied national law would enable decriminalising a DDoS, regardless of the motivation, intent or tools used. The numbers of hacktivist DDoS are nonetheless on the rise, also there seems to be considerable support to decriminalising certain forms of digital assemblies among scholars. Whereas, there is definitely also a considerable opposition. The main arguments brought by the opponents are that due to the anonymity that is characteristic to the cyberspace, there can be no real accountability as it is defined by the tradition of civil disobedience. The second argument often presented is that a DDoS by itself is a censorial tool, which only aims to silent the opponent, and therefore cannot be considered to be a form of expression. Both arguments are contestable since anonymity in cyberspace is rarely truly untraceable and also in physical space it would be disproportionate and probably also profoundly unnecessary in a democratic society to count on the absolute identifiability and traceability of the participants in a public demonstrations. As for the inexpressive nature of cyberprotests, they rarely take place as isolated operations and are usually comprehensibly related to physical space protests and political events. Thirdly, the circumstances described in the first paragraph have made it nearly impossible for the citizens to exercise their freedom of expression or assembly in an online environment that would be analogous to traditional public forum in the physical space. The latter is not distinctive to cyberspace, since also the physical space is subject to ever-increasing privatization of the public services and the rising role of corporations in designing public policies.

The aforementioned circumstances make it complicated to find a suitable forum for protesting, since a demonstration is originally perceived as the citizens´ action against the public authority that takes place in the public space. Therefore, the author is of the opinion that the question of private property should not be the sole factor determining whether or not an online protest should fall under the scope of protection of the freedom of assembly. Other condition such as the actual public importance of the online target or whether the website is functional or purely representative should be considered. Ruling out the option to peacefully assemble in cyberspace purely due to the non-existence of the public forum would possibly be a myopic approach, since it would give the right to property absolute prevalence over an important fundamental freedom. The latter path may pose many threats in the long run, when considering the gradual process of digitalising public services, such as for example e-voting. Therefore, creating an avenue for freedom of assembly on the Internet would add the missing piece to the landscape of e-democracy. The main outcomes of this research are that the problematics of regulating cyberprotests does not differ from regulating offline protests to such a degree that would enable the complete criminalisation of the first while the latter is perceived as one the foundations of democracy. At the same time, applying direct analogy would ignore the borderless nature of the internet and the distribution of offensive capabilities within.

As a result of the analysis of the case law of ECtHR and national courts, it became evident that none of the arguments most often brought against the legitimation, have been given an unambiguous interpretation in the context of offline protests. For example, as a general trend (e.g. ECtHR judgment in *Appleby* and US Supreme Court in *Lloyd Centre vs Tanner*) the courts have argued in favour of protecting the right to private property, strong arguments have also been presented against this tendency. Similarly, the question of anonymity is unsolved in real space and therefore cannot be expected to offer infallible guidance when deciding over cyber protests, the analysed case law does not enable to conclude that identifiability is thought to be one of the prerequisites of a legal protests. There are judgments both in favour and against anti-mask laws and the practices of identifying protesters at peaceful protests. Generally, anonymity is allowed as long as it promotes the freedom of assembly and is not connected to violent aims. This is highly relevant to cyberprotests, since the intrinsic anonymity is often thought of as one of the major stumbling-blocks in legitimatising political collective DDoS attacks.

Another problematic is the speech-conduct dichotomy, this is a discussion mostly held by the scholars and judges of the United States, since the First Amendment views the freedom of

assembly as an extension of freedom of speech. However, it does not mean that a level of expressivity is of no account elsewhere, as a protest has to sufficiently expressive to communicate the underlying political agenda either by the use of symbolic actions or words. Some of the observed hacktivist DDoS attacks have been more verbally expressive, other less. For example the operations conducted against the Mexican Government by the Electronic Disturbance Theatre enabled participants to send custom-made political messages to the targets and public, this most certainly counts as a form of expression. Also, since a political DDoS is seldom an essentially secretive act (unlike a coercive criminal DDoS) and is usually connected to some live and topical ongoing political turmoil, the reasons why a site is made temporarily available is generally easy to find and comprehensibly mediated to the general public and the targets. Therefore the author suggests that the expressivity of any act of protest, whether on- or offline, should be assessed within the wider context that potentially grants it with meaning. Alternatively, making the legitimacy of protest strictly dependent on the audience´s willingness and capability of understanding the social causes in question would probably harm the principle of content-neutrality.

Possibly the least controversial was the case law on inconvenience caused to the target and third parties, where the general judicial position seems to be that there is an obligation to tolerate the inconvenience and potential economic loss that occur due to others exercising their freedom of peaceful assembly. However, a state has a positive obligation to protect the third parties and targets from assemblies that are not peaceful and have escalated into sporadic riots. An example of the latter would be the judgment of CJEU in *French Blockades*. In addition to that, ECtHR has on multiple occasions reiterated that the mere potential of breaches of law or violence unless sufficiently grounded with facts, does not deprive the participants of their freedom of assembly. Also, participants´ freedom of assembly is not dependent on offences committed by other participants. This would imply that the fact that participant A has decided to use a botnet to amplify the number of requests sent to the target, would not mean that peaceful participant B who is acting in accordance with the group proportionality principle would cease to protected by the her fundamental freedom of assembly.

Where inconvenience ends, violence begins, violent assemblies are outside of the scope of the freedom of assembly and also generally excluded from the forms of morally justified civil disobedience. The aspects of violence and coercion within a cyberprotests are well illustrated by the Lufthansa case, where it was found that no coercion or violence had occurred since no physical

consequences were invoked and only temporary damages had been caused. Therefore, for a serious incident of cyberviolence a system which directly interacts with the physical space and is able to cause harm therein should be attacked, this mainly encompasses critical information infrastructures. The latter category of targets should therefore be strictly excluded from the sphere of impact of any digital collective action that claims to be peaceful.

The problematics of accountability, visibility and also foreseeability that come with the anonymity and spontaneity allowed by the Internet, could be balanced by the simple introduction of the duty to notify both the targets and the national authorities responsible for the network security in the jurisdiction where the targeted server is located. Just as in the case of real life protests, a system of notification would help to mitigate the risks caused to the target and general public and also would benefit the organisers since it would lessen the possibility of the protest being exploited by people with non-peaceful intent. The history of hacktivist operations demonstrates that as a rule the organisers have sought ways to notify the targets and the public, this also serves the purposes of communication, expressivity and accountability. In the lack of a regulation, it is however difficult to assess the efficiency and legitimacy of the notification. This tendency nevertheless proves that the hacktivist community is not so much driven by the countercultural appeal of operating in the legal grey area and would probably use the prescribed channels of notification if that would be one of the requirements of legitimising online protests.

The first steps towards creating an option to protest legally in the cyberspace have been recently taken by the Council of Europe and international NGO Article 19, these steps however do not go much further from acknowledging the process. This thesis aims to contribute to the process by offering an evidence-based criteria according to which cyberprotests could be estimated. Based on the foregoing analysis in the fourth chapter the author of the thesis proposes a model set of rules, which would enable to assess whether or not an individual instance of digital protest qualifies to be protected under the scope of the fundamental freedom of assembly. In a nutshell, the criteria foresees that the target has to be suitable, meaning that information systems the disruption of which might cause physical harm, would be ruled out. Secondly, that the duty to notify is fulfilled. Also, that the principle of group proportionality is followed, which does mean individual violations would impact the legitimacy of the protest as a whole or the freedom of assembly of the peaceful participants. On a similar line, the organisers should supervise the participants not to explicitly avoid accountability, however individual deviations should not deprive the whole protest of the protection under fundamental rights instruments. Finally, the protest should be expressive enough,

which means that the essentially mute DDoS attacks should only take place when there is sufficient information available about the political causes that it supports. The organisers should unambiguously publish their intent to connect the conducted DDoS with a specific social goal.

Each of the proposed criteria opens doors for further and more detailed legal and technical research. For instance, the duty to notify requires a well-defined regime of notification. This includes establishing authorities would be most suitable to be held responsible for overseeing online protests. Also, before concrete legislative drafting, the allowed durations and notification periods, would be subject to further analysis. The detailed regulation of the duty to notify should be able to cope with the jurisdictional problems of cyberlaw. Secondly, although the present research allows to conclude that currently the anonymization does not pose a real threat to peaceful cyber protests, since it generally still allows for sufficient accountability at an equal level to offline protests, the future perspective of protests held by untraceable masses should be studied from both legal and technical point of view. Also, the historical context in which the requirement of accountability has evolved is an interesting field of study, since it implies that protests are more open to people who could bear the consequences of civil disobedience, which might include costly litigation and also affect social, professional and family relations. Therefore the extent to which the accountability requirement is in fact necessary in a democratic society could possibly be debated, the latter has been reiterated also for example by MIT researcher Molly Sauter who has published extensively on hacktivist DDoS attacks.

Furthermore, the real risks and benefits of decriminalising hacktivist DDoS attacks could only emerge after this has been implemented in practice for a period of time, so that the ways in which it impacts the behaviour of the participants and the general culture of protests and how it correlates to cybercrime could obtain clear outlines. However, the author is of the opinion that the leap would be worth taking, since it would add the missing piece to the puzzle of e-democracy and be in synchronicity with the general transition of public expression, participation and politics to the digital realms, which were initially designed as forums where little people might have a powerful voice.

Kokkuvõte

Magistritöö eesmärgiks oli uurida võimalusi digitaalsete massimeeleavalduste seadustamiseks. Koosolekuvabadus on üks demokraatia alustalasid ning teoreetiliselt peaks kuuluma õigus meelt avaldada ka e-demokraatia juurde. Traditsiooniliselt iseloomustavad õiguspäraselt korraldatud ning läbi viidud massimeeleavaldust järgmised jooned:

- rahumeelsus
- nähtavus
- kollektiivne eesmärk
- väljenduslikkus
- valmisolek võtta vastutus aset leidnud õigusrikkumiste eest

Tehniliselt pakuvad teenustõkestusrünnakud (DDoS) võimalust ühineda mõne riigiasutuse või korporatsiooni vastu ning muuta selle asutuse esindus internetis ehk koduleheküIg seeläbi kättesaamatuks. Sellistel rünnakutel on palju ühist blokaadide või istumisstreikidega, kus inimhulgad hõivavad organiseeritult mõne ruumi eesmärgiga väljendada oma meelsust ning muudavad nii selle ruumi harjumuspärase kasutuse raskemaks. Samuti ei ole need rünnakud oma põhiolemuselt vägivaldsed ja sarnaselt protestimarsside või istumisstreikidega põhjustavad üldjuhul vaid mööduvat ebamugavust ning võrdlemisi väikeste summadega piirduvat materiaalset kahju. Viimane ei kehti rünnakute kohta, mis mõjutavad kriitilise infrastruktuure, sellised sihtmärgid peaksid seega olema välistatud.

Ometi, ei ole sellised teenustõkestusrünnakud seni leidnud tunnustust kui protestimisviisid ja on nii regionaalsete kui ka vaadeldud siseriiklike õigusallikate järgi pea igal võimaliku juhul kriminaliseeritud. Paljud akadeemikud ja hiljuti ka Euroopa Nõukogu on juhtinud tähelepanu vajadusele detailsema regulatsiooni järele, mis võtaks arvesse korraldajate ja osalejate motivatsiooni ning rünnaku tegelikku mõju ühiskonnale ning sihtmärgile. Ühiskondlikes huvides läbi viidud DDoS operatsioonide seadustamise teevad keeruliseks mitmed asjaolud, esiteks ei kuulu DDoS rünnakud ainult protestijate ampluaasse vaid seda kasutavad ka küberkurjategijad, -terroristid ning mõningatel juhtudel ka riigiasutused oponentide vaigistamiseks. Seega pelgalt valitud meeleavaldustaktika järgi ei ole võimalik tuvastada protestidele omast poliitilist ajendit. Ühtlasi, ei võimalda DDoS rünnakud protesti ajendiks olevat poliitilist agendat ei sihtmärgile ega avalikkusele piisavalt selgelt edastada, seega, et meenutada seadustatud protesti, peaksid poliitilised DDoS rünnakud aset leidma mõne laiema poliitilise sündmuse kontekstis ja korraldajad peaksid tegema kõik pingutused garanteerimaks, et nende sõnum on hõlpsasti arusaadav.

Teiseks, peaksid protestijad kinni pidama grupiproportsionaalsuse põhimõttest, mis tähendab et küberprotesti mõju kunstlikuks suurendamiseks ei tohiks kasutada kaaperdatus robotvõrke. Robotvõrkude kasutamine kvalifitseeruks kuriteona ka protesti kontekstis. Kolmandaks, ei tohiks küberruumis võimalik anonüümsus takistada võimalikku vastutust. Siinkohal aga tuleks uurida, kuidas on seadusandjad ja kohtud suhtunud anonüümsusesse füüsilises ruumis aset leidnud protestide puhul, näiteks maske ning näokatteid puudutav kohtupraktika võimaldab järeldada, et teatud anonüümsus on kogunemisvabaduse garantiiks. Tehniline kirjandus jällegi toob välja, et absoluutset tuvastamatut anonüümsust võimaldavad lahenduste kasutamine ei ole poliitiliste DDoS rünnakute korraldamisel või neis osalemisel levinud ega tõhus. Seega võib eeldada, et praeguste tehniliste võimaluste puhul ei ole absoluutne tuvastamatu anonüümsus ja sellega kaasnev karistamatus tegelikkuses nii suur probleem kui seda sageli portreteeritakse. Nii ekspressiivsuse kui anonüümsuse probleemi lahendamisel oleks kasu teatamiskohustuse sisse viimiseks, mis võimaldaks sihtmärgil ning kolmandatel isikutel riske ning kaasnevat ebamugavust leevendada ning oleks kasulik ka korraldajatele ning protestijatele endile, kuna suurem järelevalve aitaks vältida aktsiooni ärakasutamist kuritegelikel eesmärkidel.

Antud töö autor pakub välja, et küberprotestid võiksid kuuluda kogunemisvabaduse kaitsealasse juhul, kui need vastavad järgmistele tingimustele:

- valitud sihtmärk on sobiv, s.t. operatsioon ei too kaasa füüsilisi kannatusi
- teatamiskohustus on täidetus
- operatsiooni eesmärk on arusaadavalt edastatud avalikkusele ja sihtmärgile
- korraldajad teevad mõistlikke pingutusi absoluutse anonüümsust võimaldavate tehnoloogiate massilise kasutamise vältimiseks
- operatsiooni mõju sõltub osalejate arvust

Kaitsealasse kuulumine ei tähenda aga, et riikidel puuduks võimalus vajadusel protestidesse sekkuda ning kohaldada kriminaalvastutust toimunud õigusrikkumiste eest.

List of Sources

Books and articles

1. Bauer, S. M., Eckerström, P. J. The State Made Me Do It: The Applicability of the Necessity Defence to Civil Disobedience. Stanford Law Review 1987, vol. 39, no. 5.

2. Benkler, Y. (2012), Hacks of Valor: Why Anonymous is Not a Threat to National Security, Foreign Affairs, vol. 2.

3. Bernik, I. Cybercrime and Cyber Warfare. John Wiley & Sons 2014

4. Chawki, M. *et al*. Cybercrime, Digital Forensics and Jurisdiction. Springer 2015, vol. 593 Coleman, G. Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. Verso Books 2014.

5. Coleman, S. New Mediation and Direct Representation: Reconceptualizing Representation in the Digital Age. New Media & Society 2005, 7.

6. Cohen, J.L., and Arato, A (eds.). Civil society and political theory. MIT Press, 1994

7. Czosseck, C. and Geers, K. (eds.). The Virtual Battlefield: Perspectives on Cyber Warfare. Vol. 3. Ios Press, 2009.

8. Czosseck, C. State Actors and their Proxies in Cyberspace. Ed. Ziolkowski, K. Peacetime Regime for State Activities in Cyberspace. NATO CCDCOE 2013.

9. Denning, D. The Ethics of Cyber Conflict. Wiley Publishers 2008.

10. Esen, R. Cyber Crime: A Growing Problem. The Journal of Criminal Law 2002, 66(3).

11. Fenwick, H. The Right to Protest, the Human Rights Act and the Margin of Appreciation. Modern Law Review 1999, 62(4).

12. Freeman, H. A. The Right of Protest and Civil Disobedience. Indiana Law Journal, 1966, 41(2).

13. Furnell, S. M., Warren, M. J. Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium? *Computers & Security* 1999, 18(1).

14. Gerstenberg, O. What Constitutions Can Do (But Courts Sometimes Don't): Property, Speech, and the Influence of Constitutional Norms on Private Law. The Canadian Journal of Law and Jurisprudence 2004, 17 (1).

15. Gillespie, A.A. Cybercrime: Key Issues and Debates. Cambridge University Press 2015 Grady, M.F., Parisi, F. (Eds.) The Law and Economics of Cybersecurity. Cambridge University Press 2005.

16. Habermas, J. Civil Disobedience: Litmus Test for the Democratic Constitutional State. Berkeley Journal of Sociology, 1985.

17. Hampson, N.H. Hacktivism – a New Breed of Protest in a Networked World. Boston College International and Comparative Law Review 2012, vol. 35.
18. Hirsnik, E. Arvutikuritegevuse regulatsioon Eestis. Juridica 2014, 8.
19. Jordan, T. Activism! Direct Action, Hacktivism and the Future of Society. Reaktion Books 2002.
20. Jordan, T., Taylor, P. Hacktivism and Cyberwars: Rebels with a Cause? Routledge 2004.
21. Kaminski, M. E. Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech. Fordham Intellectual Property, Media & Entertainment Law Journal 2013, 23.
22. Kasper, A. The Fragmented Securitization of Cyber Threats. Eds. Kerikmäe, T. *et al*. Regulating eTechnologies in the European Union. Springer International Publishing 2016.
23. Kerr, O. Are We Overprotecting Code - Thoughts on First-Generation Internet Law. Washington and Lee Law Review 2000, 57.
24. Krastev, I. Democracy Disrupted - the Global Politics or Protest. University of Pennsylvania Publishing 2014.
25. Knaut, A. Informed Strategies of Political Action in IP-Based Social Media. International Federation for Information Processing. Eds. Hercheui, M.D *et al*. IFIP Advances in Information and Communication Technology. Springer 2012.
26. Knapp, T. M. Hacktivism-Political Dissent in the Final Frontier. New England Law Review 2007, 49, 259.
27. Lohse, E. J. Fundamental Freedoms and Private Actors–towards an 'Indirect Horizontal Effect'. European Public Law 2007, 13, no. 1, 159-190.
28. Lorents, P., Ottis, R., Cyberspace: Definition and Implications, NATO CCDCOE, 2010
29. Li, X. Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime. Harvard Journal of Law and Technology 2013, 27.
30. Mansfield-Devine, S. Anonymous: Serious Threat or Mere Annoyance? ."Network Security 2011, no. 1, pp 4-10.
31. Mead, D. Strasbourg Succumbs to the Temptation to Make a God of the Right of Property: Peaceful Protest on Private Land & (and) the Ramifications of Appleby v. UK. Journal of Civil Liberties 2003, 8 (2).
32. Medsger, B. The Burglary: The Discovery of J. Edgar Hoover's Secret FBI. Vintage Press 2013.
33. Mehan, J. E. Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger. IT Governance Ltd 2013, 2nd ed.

34. McLaughlin, E., Muncie, J. (Eds.). The Sage Dictionary of Criminology. Sage 1990.
35. McLaurin, J. Making Cyberspace Safe for Democracy: the Challenge Posed by Denial-of-service Attacks. Yale Law & Policy Review 2011, 30 (1).
36. Nunziato, D. C. The Death of the Public Forum in Cyberspace. Berkeley Technology Law Journal 2005.
37. O'Malley, G. Hacktivism: Cyber Activism or Cyber Crime. Trinity College Law Review 2013, 16.
38. Oostveen, A.M. Outsourcing Democracy: Losing Control of e-Voting in the Netherlands. Policy & Internet 2010, 2(4).
39. Powell Jr. L. F. Lawyer Looks at Civil Disobedience. Washington and Lee Law Review 1966, vol. 23.
40. Quint, P. E. Civil DMsobedience and the German Courts: the Pershing Missile Protests in Comparative Perspective. Routledge 2007.
41. Rawls, J. A Theory of Justice. Harvard University Press 1971.
42. Rid, T. Cyber War Will Not Take Place. Journal of Strategic Studies 2012, 35(1).
43. Rucht, D. Die Bedeutung von Online-Mobilisierung für Offline-Proteste. Ed Voss, K. Internet und Partizipation. Bürgergesellschaft und Demokratie. Springer 2014, 42.
44. Salát, O. The Right to Freedom of Assembly. Oxford, Hart Publishing 2015.
45. Sauter, M. “LOIC Will Tear Us Apart”: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. American Behavioral Scientist 2013, 57(7).
46. Sauter, M. The Coming Swarm: DDOS Actions, Hacktivism and Civil Disobedience on the Internet. Bloomsbury Publishing 2014.
47. Schmitt, M. N. Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law 1999, 37.
48. Schmitt, M.N. Cyber Operations and the Jus in Bello: Key Issues, 41 Israel Yearbook of Human Rights 2011.
49. Schmitt, M. N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press 2013.
50. Sorell, T. Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. Journal of Human Rights Practice 2015..
51. Svantesson, D. The Holy Trinity of Legal Fictions Undermining the Application of Law to the Global Internet. International Journal of Law and Information Technology 2015, 23 (3), pp 219-234.

52. Summers, S. *et al*. The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society. Bloomsbury Publishing 2014.

53. Waters, C. New Hacktivists and the Old Concept of *levée en masse*. Dalhousie Law Journal 2014, 771 (37).

54. Welchman, J. Is Ecosabotage Civil Disobedience? Philosophy & Geography 2001, 4 (1).

55. Wittes, B., Blum, G. The Future of Violence: Robots and Germs, Hackers and Drones: Confronting A New Age of Threat. Basic Books 2015.

56. Yang, G. The Commercialization and Digitization of Social Movement Society. Contemporary Sociology: A Journal of Reviews 2016, 45(2).

57. Yar, M. Cybercrime and Society. Sage 2013.

58. Zatz, N. Note, Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment. Harvard Journal of Law & Technology 1998, 12.

59. Ziccardi, G. Resistance, Liberation Technology and Human Rights in the Digital Age. Springer 2013.

News articles and commentaries

1. Morozov, E. Pro-Wikileaks Denial-of-service Attacks: Just another Form of Civil Disobedience. Slate 2010, available online at: http://www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html

2. Morozov, E. Should we oppose sitins just because crazy people can abuse them?, Foreign Policy, 16 December 2010, available online at: http://foreignpolicy.com/2010/12/16/should-we-oppose-sit-ins-just-because-crazy-people-can-abuse-them/

3. Morozov, E. More on DDoS as Civil Disobedience, Foreign Policy, 14 December 2016, available online at: http://foreignpolicy.com/2010/12/14/more-on-ddos-as-civil-disobedience/

4. Schmitt, M., Marks, P. The Right to Bear Cyber Arms. New Scientist 2013, 4/13, vol. 218, issue 2912.

5. Slobbe, J., Verberkt, S. L. C. Hacktivists: Cyberterrorists or Online Activists? (2012) *arXiv preprint arXiv:1208.4568*

6. Stallman, R., "The Anonymous WikiLeaks Protests Are a Mass Demo Against Control", The Guardian 17 December 2010.

7. The Guardian, Anonymous leaks a list of Ku Klux Klan Members, 6 November 2015 http://www.theguardian.com/technology/2015/nov/06/anonymous-ku-klux-klan-name-leak

8. Deutsche Welle, Anonymous targets Saudi-Arabian Government, 2 October 2015, available online at: http://www.dw.com/en/anonymous-hacktivist-explains-why-group-is-targeting-saudi-arabian-government/a-18758195

Research papers

1. Clayton, R. Complexity of Criminalising Denial of Service Attacks, 2006, available online at: http://www.cl.cam.ac.uk/~rnc1/complexity.pdf

2. Dudek, D. *et al*. Zitterbart, Netzsicherheit und Hackerabwehr. Universität Karlsruhe 2008, p. 58, available online at: https://doc.tm.uka.de/tr/TM-2008-3.pdf#page=52

3. Pras, A. et al. Attacks by "Anonymous WikiLeaks Proponents not Anonymous. DACS, University of Twente 2010, available online at: http://doc.utwente.nl/75331/1/2010-12-CTIT-TR.pdf

4. Samuel, A. Hacktivism and the Future of Political Participation. Unpublished PhD Thesis. Harvard University 2004.

5. Zuckerman, E. *et al*. 2010 Report on Distributed Denial of Service (DDOS) Attacks. Berkman Center Research Publication 2010, 16.

Case law

European Court of Human Rights

1. *Appleby and Others v United Kingdom*, 44306/98, 6 May 2003.

2. *Barraco vs France*, 31684/05, 5 March 2003.

3. *Kudrevicius vs Lithuania*, 37553/05, 15 October 2015.

4. *Lucas vs France*, 37257/97, 28 November 2000.

5. *Primov vs Russia*, 17391/06, 12 June 2014.

6. *Oya Ataman vs Turkey*, 74552/01, 5 December 2006.

7. *Schwabe vs Germany*, 8080/08 8577/08, 1 December 2012.

8. *Stankov vs Bulgaria*, 29221/95 29225/95, 2 October 2001.

9. *Zilberberg vs Moldova*, 61821/00, 1 February 2005.

European Commission of Human Rights

Friedl vs Austria, 28/1994/475/556, 30 November 1994.

European Court of Justice

1. C-265/95, *Commission v. France*, 9 December 1997.

2. C-112/00, *Schmidberger vs Austria*, 12 June 2003.

3. 240/83, *Procureur de la Republique v ABDHU,* 7 February 1985.

National Courts

Estonia

HMKo, 1-07-15185, 13 December 2008.

Germany

Federal Court of Justice

BGHSt 23, 46, *Laepple* , 8 August 1969.

Federal Constitutional Court of The Republic of Germany

1. BVerfGE 69, 315, *Brokdorf,* 14 May 1985

2. BVerfGE 7, 198, *Lüth,* 15 January 1958.

3. BVerfGE, 1 BvR 943/02, 25 October 2007.

Frankfurt District Court

991 Ds 6100 Js 226314/01, *Vogel*, 11 July 2005.

Frankfurt Higher Regional Court

Ss 319/05, *Vogel*, 22 June 2006.

United States

United States Supreme Court

1. *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972).

2. *Amalgamated Food Employees Union Local 590 v. Logan Valley Plaza Inc.,* 391 U.S. 308(1968).

3. *Marsh v. Alabama*, 326 U.S. 501 (1946)

4. *United States v. O'Brien*, 391 U.S. 367, 369-70 (1968).

5. *Watchtower Bible v. Vill. of Stratton*, 536 U.S. 150 (2002)

District Court for the Eastern District of Pennsylvania

Cyber Promotions, Inc. V. *America Online, Inc.*, 948 F. Supp. 436 (E.D. Pa. 1996).

District Court for the Northern District of Texas

Aryan v. Mackey, 462 F. Supp. 90, 94 (N.D. Tex.1978)

District Court for the Southern District of New York

Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001)

Legislative Acts

Council of Europe

1. Convention on Cybercrime, CETS 185, 23 November 2001.
2. European Convention on Human Rights

European Union

1. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
2. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Estonia

1. Penal Code, RT I, 17.12.2015, 9.
2. Law Enforcement Act, RT I, 23.03.2015, 207.

Germany

1. Criminal Code, in the version promulgated on 13 November 1998, Federal Law Gazette I p. 3322, last amended by Article 1 of the Law of 24 September 2013, Federal Law Gazette I p. 3671 and with the text of Article 6(18) of the Law of 10 October 2013, Federal Law Gazette I p 3799.
2. Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 11 July 2012, Federal Law Gazette I p. 1478.

United Kingdom

Computer Misuse Act 1990, as last amended 28 April 2016.

United States

1. The First Amendment to the United States Constitution,
2. Computer Fraud and Abuse Act, 18 U.S.C. 1030.

Other international instruments

1. African Union Convention on Cyber Security and Personal Data Protection
2. International Code of Conduct for Information Security
3. NATO CCD COE Tallinn Manual on the International Law Applicable to Cyber Warfare.

International organisations reports and policy documents

1. OSCE, CoE Venice Commission, Guidelines on Freedom of Peaceful Assembly, OSCE/ODIHR, Warsaw/Strasbourg 2010, available online at: http://www.echr.coe.int/Documents/Library_TravPrep_Table_ENG.pdf

2. CoE, Explanatory Report to the Convention on Cybercrime. Budapest, 2001. available online at:https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

3. CoE, *Travaux préparatoires* of the European Convention on Human Rights, DH(56)16, CDH(74)39, available at http://www.echr.coe.int/Documents/Library_TravPrep_Table_ENG.pdf

4. CoE Cybercrime Convention Committee, Guidance Note no. 5 on DDoS Attacks, 2013, available online at: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)10REV_GN5_DDOS%20attacks_V7adopted.pdf

5. CoE, Report on the Freedom of Assembly on the Internet, 30 Sept 2015.

6. Council of the European Union, Eurojust, Eurojust's analysis of EU Member States' legal framework and current challenges on data retention, 26 October 2015, available at: http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf

7. ENISA, Cyber Threat Landscape 2015.

8. ENISA, Good Practice Collection for CERTs on the Directive on attacks against information systems, ENISA P/28/12/TCD, Version: 1.5, 24 October 2013.

Electronic materials published by NGOs and think-tanks

1. Article 19, Principles of the Right to Protest, available online at: https://right-to-protest.org/

2. UK, Internet Crime Forum Legal Subgroup: Reform of the Computer Misuse Act 1990, www.internetcrimeforum.org.uk/cma-icf.pdf