

Framing Hacktivism: The Criminalization of Redhack in Turkey

By

Nazlı Bülây Doğan

A Dissertation Submitted to the
Graduate School of Social Sciences & Humanities
in Partial Fulfillment of the Requirements for
the Degree of
Doctor of Philosophy
in
Design, Technology and Society



August 2019

Framing Hacktivism: The Criminalization of Redhack in Turkey

Koç University

Graduate School of Social Sciences & Humanities

This is to certify that I have examined this copy of a doctoral dissertation by

Nazlı Bülay Doğan

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

Assoc. Prof. Erdem Yörük (Advisor)

Asst. Prof. Ergin Bulut

Asst. Prof. Başak Can

Assoc. Prof. Begüm Özden Fırat

Asst. Prof. Murat Yüksel

Date:

ABSTRACT

This dissertation examines the criminalization of Redhack, a popular hacktivist group in Turkey in the 2010s. The multi-dimensional study is based on an analysis of the construction and the perception of crime frames about hacktivism, by focusing on the case of Redhack. With a qualitative approach, the dissertation analyzes political actors, news media agents, actors involved in the judicial processes related to the hacktivist group, the audience interacting with the group in the social media platform Twitter, and the hacktivist group itself. In dialogue with the hacktivism literature, this dissertation contributes to critical criminology and to critical terrorism studies, beginning with the question of whether Redhack is considered as a source of “moral panics” in Turkey. The examination exhibits that Redhack is criminalized through the activation of the older frame of terrorism instead of newer frames of cybercrime and cyberterrorism. The dissertation finds that this emergence of the terrorism frame for a hacktivist group is the joint product of the contemporary political context in Turkey, the residues of sociopolitical anxieties from the Turkish history crystallized in the “folk devils” of terrorism, the characteristics of the group itself, and the worldwide rise of the terrorism discourse. The dissertation also shows that the abstention from constructing cyber related crime frames for Redhack implies a positive framing – even an imagery – of cybercrime and cyberterrorism in Turkey that is not preferred to be activated for an existing group. This positive framing is closely related to the fascination with information and communication technologies (ICTs) for actors involved in the crime framing of Redhack. Moreover, the criminalization of Redhack indicates the effort of the state and the power elite to make more legible this challenging new development – hacktivism – through the terror frame. In that sense, the dissertation provides insight into the duality of techno-fetishism and anxieties felt for ICTs in the national scale. Without being limited to the domain of ICTs and to the national scale, the study sheds light on the wider processes of criminalization constructed upon the discourse of terrorism worldwide.

ÖZETÇE

Bu tez, 2010’lar Türkiye’inde popüler bir hacktivist grup olan Redhack’in nasıl suçlaştırıldığını incelemektedir. Çok boyutlu olan bu çalışma, Redhack örneğine odaklanarak hacktivism hakkında inşa edilen ve algılanan suç çerçevelerinin çözümlemesi üzerinedir. Tez, niceliksel bir yaklaşımla, siyasi aktörleri, haber medyasını, bahsi geçen hacktivist grupla ilgili yargı süreçlerine dâhil olmuş aktörleri, sosyal medya platformu Twitter üzerinden grupla etkileşimde olan kitleyi ve hacktivist grubun kendisini inceler. Hacktivism literatürü ile diyalog içinde olan bu tez, eleştirel kriminoloji ve eleştirel terör çalışmalarına da katkıda bulunur. Tezin başlangıç sorusu, Redhack’in Türkiye’de bir “ahlaki panik” olarak değerlendirilip değerlendirilmediğidir. İnceleme, Redhack’in yeni oluşturulan siber suç ve siber-terör çerçevelerinden ziyade daha eski olan terör çerçevesinin etkinleştirilmesiyle suçlaştırıldığını ortaya çıkarmaktadır. Tez, terör çerçevesinin hacktivist bir grup için yeniden ortaya çıkmasının dört farklı sebebi olduğunu öne sürer: Türkiye’deki siyasi bağlam, terörist “halk şeytanları” kavramında billurlaşan Türkiye tarihinden artakalan sosyo-politik kaygılar, Redhack grubunun kendi özgüllükleri ve dünya çapındaki terör söyleminin yükseliş. Tez aynı zamanda, Redhack için siber ile ilgili suç çerçevelerinin kullanılmasından geri durulduğunu gösterirken; siber suç ve siber-terörle ilgili Türkiye’de olumlu bir çerçeveselendirme – neredeyse bir imge – olduğunu da ortaya çıkarmıştır. Çalışma bu bağlamda, Redhack’in suç olarak çerçeveselendirilmesiyle ilişkili görüşülen veya yazılı/sesli kaynaklar sayesinde incelenen aktörlerde, bilişim ve iletişim teknolojilerine (BİT) dair bir büyülenme olduğunu ortaya koyar. Bunun yanı sıra devlette ve iktidar elitinde, meydan okuyan hacktivism örneklerini terör çerçevesiyle daha okunabilir kılma çabası da gözükmemektedir. Bu anlamda çalışma, tekno-fetişizm ile BİT’e dair hissedilen kaygıların ikililiğini gün yüzüne çıkarır. Daha geniş açıdan tez, BİT alanına ve Türkiye ölçeğine sınırlı kalmaksızın, dünya çapında farklı örneklerde inşa edilen terör söylemine dayalı suçlaştırma söylemlerine ışık tutar ve bu alandaki yeni eleştirel çalışmaların önünü açar.

ACKNOWLEDGMENTS

During the period that gave birth to this dissertation, many people became part of this process. I want to thank my advisor Erdem Yörük and thesis committee members Ergin Bulut and Başak Can for their contributions to the dissertation. My previous advisor Murat Yüksel was always supportive of my work with his strong and constructive criticism. I am deeply thankful to Begüm Özden Fırat not just for her contribution as a committee member but also for being a great academic supporter and a considerate friend. Another person to whom I owe a debt of gratitude is Hakan Yücel. This dissertation would not have been possible without his encouragement and his guidance. From the very first beginning to the end, I always felt his support whenever I needed it.

Research for this dissertation has become possible with the scholarship from TÜBİTAK BİDEB. Thanks to the Fulbright Visiting Scholar Program, I was able to study in the Annenberg School for Communication at UPenn. I am immensely grateful to Marwan Kraidy to give me this opportunity of being part of the CARGC team. His guidance and his support were priceless. I am deeply thankful to Marina Krikorian, Samira Rajabi, Rayya El Zein, and all friends in CARGC for their support and friendship, too. I also want to thank the faculty at Annenberg, especially Guobin Yang, Jessa Lingel, and Klaus Krippendorff, whose doors were always open to those seeking advice. During my PhD, I met many academicians who were generous enough to support me. Burcu Baykurt and Gülay Kılıçaslan were such brilliant figures whose support made me believe in the academic solidarity once more. Aslı Telli Aydemir, Bilge Yeşil, Burak Doğu, Erkan Saka, Gabriella Coleman, Köksal Bayraktar, Marco Deseriis, Mutlu Binark, Tim Jordan, and Ufuk Eriş did not refrain from giving me advice and encouragement when I consulted them. I also want to thank my former professor from Galatasaray University, Füsün Üstel, for being an inspiration with her academic competence and her courageous political stance.

Interviews constitute a central place of this dissertation. I am grateful to the interviewees for giving their time, their trust, and their support. I am equally grateful to the

specialists who ensured access to primary sources. During the exhaustive studies necessary for this dissertation, I sought shelter in many libraries. Boğaziçi University Library, Alexandra Elbakyan's archive and other digital *libraries* were my heroes.

I am thankful to all friends who were by my side when I was trying to complete this dissertation. Pinar has been an inseparable part of my life for 20 years. It did not change for the PhD period either. Alongside her priceless emotional support, her technical support to the thesis as a computer engineer contributed enormously. Like Pinar, Belin endured with me all the hardships of a depressed PhD student life, including all the academic staggers and emotional rise and falls. Ali Seyhan was never too far away, even if he was physically. Whenever I needed his friendship, he was always there. Michael was a great housemate to share academic exasperations and to laugh about life. Şevket shared with me my interest in cyber issues. Deniz saved me about technical issues. İlknur was my study partner during the unending evenings in the library. Some days, I talked face to face just with her and with my cat Adolfin. Tuğba, Ferit, Elif, and Aynur were the sudden gifts of friendship in the US.

Then come my thanks to my comrades. I am deeply indebted to İbrahim for his generous and careful feedback on this dissertation. He was the first person to read the drafts of the dissertation. Many times, he helped me out from the tangled mental state that I often buried myself. Knowing his support always makes me act and write more courageously. Caner kindly helped me as a social scientist and Selçuk managed to support me despite the physical distance between us for the most part. All friends in İstanbul and in İzmir, İsmail, Süleyman, Ceyda, Meryem and many others, are strong-willed to *change the world rather than being stuck with interpreting it*. Last but not least, I cannot forget Göksu. I am still surprised at his incredible talent of making me such a cheerful, peaceful and strong person. Knowing him made me understand what *the optimism of the will* really means. I am deeply grateful to him and to all other comrades, for the real meaning that they give to this life.

Finally, I am deeply thankful to my parents, Ferhan and Nevzat, for their support and love. They always had more faith in academia than I ever had. Fortunately, we share other dreams: our precious Özgen Berkol Doğan Science Fiction Library became an indispensable part of my life since its foundation in 2012. Hereby, I like to take this opportunity to thank my brother after who our library was named. Missing him so much, I feel enormously fortunate to keep his memory in my heart.

TABLE OF CONTENTS

List of tables.....	x
List of figures.....	xi
Nomenclature.....	xiii
Chapter 1: Introduction: A study of hacktivism, a study of cybercrime.....	1
1.1. Research design and methods	4
1.2. Difficulties, limitations and backdoors	5
1.3. Outline.....	11
Chapter 2: Contextualizing hacktivism: Theoretical roots to problematize criminalization	14
2.1. A critical review of hacktivism literature.....	15
2.1.1. First generation: Dichotomy between cyberterrorism and civil disobedience	16
2.1.2. Second generation: Specter of cyberterrorism.....	17
2.1.3. Third generation: Focusing on the crime discourse.....	19
2.2. Contextualizing hacktivism.....	21
2.2.1. Reference works for contextualization: At the boundaries of hacktivism.....	21
2.2.2. Sources of contextualization.....	23
2.3. Conclusion.....	30
Chapter 3: Hacktivism in mirror: Meanings, perceptions, experiences.....	31
3.1. Footsteps of hacktivism: Political engagement with computer and network technologies (1950-1980).....	32
3.2. Hacking against the neoliberal drive (the 1980s).....	35
3.3. Globalism is the enemy! Hacktivism and anti-globalization (the 1990s)	39
3.4. Globalism is still the enemy! The rise of patriotic hacking (the 2000s)	43
3.4.1. Patriotic hacking experiences in different contexts.....	44
3.4.2. Patriotic hacking experiences in Turkey	46
3.5. Time of crises, time of uprisings (the 2010s).....	49
3.5.1. Leak hacktivism: WikiLeaks and Tunisian uprising	50
3.5.2. Leak hacktivism in Turkey	52

3.6. Conclusion.....	56
Chapter 4: Hactivist experience in turkey: The case study of redhack.....	57
4.1. The acts of Redhack	58
4.1.1. Techniques of hacktivism: Shall we hack together?	77
4.1.2. Motivations of hacktivism: Reactive fusion of humor and leftist legacy	80
4.2. Judicial processes of Redhack.....	88
4.2.1. Oscillations: Cybercrime or terror?	94
4.2.2. A Game of targets: Punishing the periphery	98
4.3. Conclusion.....	99
Chapter 5: Usual suspects of the crime framing: Sponsoring and employment of the official frames.....	101
5.1. The quasi-silence of political actors.....	102
5.2. Passive framing of news media	109
5.2.1. Frame diversity: Many ways to define Redhack	110
5.2.2. Emergence of self-frames	113
5.2.3. Increasing silence about framing Redhack.....	116
5.2.4. Positive and negative frames	117
5.2.5. Political economy of news framing	119
5.2.6. Reflection of judicial processes in the terror framing	121
5.3. Conclusion.....	125
Chapter 6: Unofficial crime frames for redhack: Analyzing the construction of the criminalization	128
6.1. Digging a hidden source: Methodological notes on the analysis of unofficial frames	128
6.2. Cybercrime and hacking frames: Imagining the threat	130
6.2.1. Unavoidable technological threats and deep concerns of incompetency	131
6.2.2. Motivations matter, or not: How to designate cybercriminals?	135
6.2.3. Other lines of divergence: Permission, reporting, state service, public good ...	138
6.2.4. A Change in the perspective: State (cyber)crimes and ghosts of counter-guerilla	141
6.2.5. Relativity of good hackers: Positionality, motivation, skills.....	144
6.2.6. Insiders and outsiders: Against the criminalization of hackers	147
6.2.7. Implications of framing Redhack as cybercriminal.....	152
6.3. Cyber-terror and terror frames: Containment of the dissidence.....	153

6.3.1. Narrow frames of political hacking vs. Unchained paranoias of cyber-terror ..	154
6.3.2. Shaping harm to find out cyber-terrorists: From bad intentions to data theft ...	158
6.3.3. Chronic anxieties of defining cyber-terror	160
6.3.4. Anxieties alleviated: Moral panics of terror, agreed-upon terrorists as folk devils	162
6.3.5. Limits of being critical: Relative opposition to terror labels.....	167
6.3.6. Implications of framing Redhack as terrorist	168
6.4. Conclusion.....	170
Chapter 7: Perceptions of the criminalization: Counterframing and reframing strategies .	175
7.1. The Rise of the discussion: Temporality of the terror framing	178
7.2. Counterframing strategies: Using political satire to criticize the terror label	187
7.3. Supportive reframes: Agreed-upon terrorists, performativity, nationalism	193
7.4. Reframing strategies: Targeting the state with its own frame.....	197
7.5. Conclusion.....	201
Chapter 8: Conclusion	203
References.....	216
Appendix: Applicable articles in judicial processes related to redhack	251

LIST OF TABLES

Table 4.1: Data leaks by Redhack.....	62
Table 4.2: Data Interference by Redhack.....	66
Table 4.3: Judicial Processes related to Redhack.....	88
Table 5.1: Examples of the frame elements about Redhack in news outlets.....	112
Table 5.2: Hürriyet newspaper online news archive.....	123
Table 5.3: Changing crime frames for Redhack in Sabah newspaper.....	125

LIST OF FIGURES

Figure 4.1: Number of (latest) tweets by the account @TheRedHack by month.....	60
Figure 4.2: Number of retweets per number of tweets by the account @TheRedHack by month	60
Figure 4.3: [We felt about ;) -> “I liked the possibility to drink tea with you one day at http://icisleri.gov.tr #WeAreRedhack” RT @YalchinAkdeniz]	83
Figure 4.4: [Aww Central Bank, did you get an owie at http://www.tcmb.gov.tr/ ;()]	84
Figure 7.5: Number of tweets containing the keywords “terör [terror]” and “Redhack” and their retweet numbers by month (March 2012-October 2017).....	179
Figure 7.6: [Today, after 14 p.m., everywhere, in every square.. #ResistanceNews]	182
Figure 7.7: [While we focus to work, please write the protests, the announces, the declarations, the urgent needs under the hashtag #ResistanceNews..]	183
Figure 7.8: [The resistance keeps growing. Please write the protests, the announces, the declarations, the urgent needs under the hashtag #ResistanceNews and follow it!]	183
Figure 7.9: [For an equal, just, classless world, for fraternity, for liberty and independence, we march with all of our hearts. They can stop us, if they can!]	183
Figure 7.10: [Those who hand out buses, raincoats, lunch.. say TOMA, [pepper] gas, truncheon when it comes to us. Will you be quiet?]	183
Figure 7.11: [Gazi, Sarigazi, Okmeydani, Nurtepe, Caglayan, 1 Mayis, Kadikoy, Gulsuyu... Your home, your sister, your mother, they are waiting for you! #1MilliontoTaksimToday]	184
Figure 7.12: [Even we cannot decipher the encoded Necati Sasmaz speech, the global technology is not that much developed, we are sorry.. #RedHack ;)]	188
Figure 7.13: [You did everything, you would do this, too. Bring us whatever this prosecutor drinks]	189
Figure 7.14: [General Staff declared to hit successfully many storehouses and concentrations belonging to the terrorist organization redhack in the air operation / Zaytung]	189
Figure 7.15: [After that moment, I do not know if we will do terror but we will make them give error a lot for sure ;) ->>]	189
Figure 7.16: [We figured out why they declared us as terrorist.. The prosecutor who studied for 25 years thought this photo real ;) ->>>]	190
Figure 7.17: [A brand new miracle to call our own: Redhack is our new terrorist organization!]	190
Figure 7.18: [The ones who declared Redhack a terrorist organization by the pretext of hammer and sickle would just as soon shut down hardware stores for being weapon providers].....	190

Figure 7.19: [<i>@RedHackers Redhack Did you submit a petition to become an official terrorist organization with a residency certificate from local authorities?</i>]	191
Figure 7.20: [<i>hammer and sickle + manifest = terrorist organization we will progress a lot with this equation. that's nice. it works. it is a mighty prosecutor, after all, right? #Redhack</i>]	191
Figure 7.21: [<i>@allahcc, explain that to us. Did you create those who declared #Redhack a terrorist organization, too? Why did you create? Is it another exam for us? #whatever</i>]	192
Figure 7.22: [<i>The judicial power who declares Redhack a terrorist organization do not consider those who killed Hrant Dink a terrorist organization</i>]	192
Figure 7.23: [<i>They said Redhack was an armed terrorist organization. That was indeed true. They had a bomb and today, they dropped it with the truths about reyhanlı</i>]	192
Figure 7.24: [<i>Redhack is a pro-DHKP-C, leftist terrorist organization. Those who do not believe can google Redhack DHKPC. This groups wants nothing but anarchy in Turkey</i>]	194
Figure 7.25: [<i>Redhack is terrorist. They did not deny their relation to DHKP/C, to PKK. Those who defend them should investigate first truthaboutredhack.blogspot.com #RedCakeisBestEverTerrorist</i>]	194
Figure 7.26: [<i>Redhack is terrorist! If they say they are not, then they should tweet that dhkpc and pkk are terrorist organizations</i>]	195
Figure 7.27: [<i>Just one question to shameless Redhack. Why they block those who ask whether Pkk is a terrorist organization or not ;)</i>]	195
Figure 7.28: [<i>#ExplainRedhackWhetherPkkIsTerrorist is nonsense? Redhack is a terrorist organization by itself</i>]	195
Figure 7.29: [<i>Redhack's inability to not declare Pkk as a terrorist organization is so meaningful! They talk around it :)) #ExplainRedhackWhetherPkkIsTerrorist</i>]	196
Figure 7.30: [<i>The group called Redhack is not an addressee of #TC group. A mentality who cannot say Pkk is a terrorist organization and who defends Kck people cannot be an addressee to us. #TC Group</i>]	196
Figure 7.31: [<i>It is true that what we are doing is illegal but no one can say that we are doing a bad thing.</i>]	197
Figure 7.32: [<i>"Terror is the distrust between neighbors. It is to put notice box for informants!" #RedHackInHalkTV @TheRedHack</i>]	199
Figure 7.33: [<i>"Terror is the police invading your house at the morning." [from the speech of Redhack in Halktv]</i>]	200
Figure 7.34: [<i>The Ministry of Foreign Affairs calls "our friends" international terrorist groups #Redhack</i>]	200
Figure 7.35: [<i>Terror is the detention of Türkan Saylan who educated 40,000 children in her seriously ill condition! @TheRedHack #RedHackInHalkTV</i>]	200
Figure 7.36: [<i>"Terror is the assault of the police against its citizens crying Allah Allah" @RedHack</i>]	200
Figure 7.37: [<i>Terror is beating someone to death in darkened streets #RedHack #TodayIsRedHack</i>]	201

NOMENCLATURE

AKP	Justice and Development Party
ARPA	Advanced Research Projects Agency
BİK	Information and Communication Technologies Authority
cDc	Cult of the Dead Cow
CGN	Carrier Grade NAT
CHP	Republican People's Party
CTS	Critical terrorism studies
ÇYDD	Association for the Support of Contemporary Living
DHKP-C	Revolutionary People's Liberation Party/Front
DDOS	Distributed denial-of-service
EDT	Electronic Disturbance Theater
EZLN	Zapatista National Liberation Army
FETÖ/PDY	Fethullahçı Terror Organization/Parallel State Structure
FSF	Free Software Foundation
ICT	Information and communication technologies
ISIS	Islamic State of Iraq and the Levant
LEA	Law enforcement agent
MHP	Nationalist Movement Party
MLKP	Marxist–Leninist Communist Party
ODTÜ	Middle East Technical University
PKK/KCK	Kurdistan Workers' Party/Kurdistan Communities Union
RIP Act	Regulation of Investigatory Powers Act
TAK	Kurdistan Freedom Hawks
TCP/IP	Transmission Control Protocol/Internet Protocol
THKP-C	People's Liberation Party-Front of Turkey
THKO	People's Liberation Army of Turkey
TKP/ML	Communist Party of Turkey/Marxist–Leninist
TMK	Anti-Terror Law of Turkey
TOMA	Armored water cannon used for riot control
TPC	Turkish Penal Code
TWAT	The War against Terrorism
WFD	World's Fantabulous Defacers
WTO	World Trade Organization
YÖK	Council of Higher Education

CHAPTER 1

INTRODUCTION:

A STUDY OF HACKTIVISM, A STUDY OF CYBERCRIME

You will never succeed in making us believe that there is a crime where there is no crime, you will only succeed in converting crime itself into a legal act. You have wiped out the boundary between them, but you err if you believe that you have done so only to your advantage. The people sees the punishment, but it does not see the crime, and because it sees punishment where there is no crime, it will see no crime where there is punishment.

(Marx, (1842) 1996, p. 51)

[W]e must not say that an action shocks the common conscience because it is criminal, but rather that it is criminal because it shocks the common conscience. We do not reprove it because it is a crime, but it is a crime because we reprove it.

(Durkheim, (1893) 1960, p. 81)

Problematization of the concept of *crime* is one of the fundamental topics of social sciences since the 19th century. The main reason of that interest is undoubtedly its exhibition capacity of what is considered as *deviance* and *anomaly* in societies. In that line, studying crime was always considered fundamental to understand the complexity of societies through its focus on legal lines that exhibit what remained within legality and therefore, what were the norms in the first place.

Two introductory quotations about the constructed nature of crime, one from Marx and the other from Durkheim, cannot be thought apart from the historical context in which they were developed. These sociological approaches to crime and punishment takes its source from the tumultuous decades of the 19th century during which immense social

changes through economic, political, and social revolutions were experienced. It was during the period of the development of German capitalism that Marx became interested in *Debates on the Law on Theft of Woods* ((1842) 1996). Even though Marx did not return to the issue of crime in his later writings, “class struggle first presented itself to Marx’s serious attention as a form of crime” (Linebaugh, 1993, p. 102). It can be argued that the later conception of crime as a “useful” concept for the bourgeoisie to the disadvantage of the worker (Marx, 1993, p. 52) derives from this initial attention given to the crime question. On the opposite direction, for Durkheim, crime and the punishment given to that crime were considered as positive constructions because of their ability to act as solidarity-producing mechanisms for the whole society (Garland, 1991, pp. 122-127). Later Marxist studies will challenge this implicit agreement thesis suggested by Durkheim and incline more to focus on the ideological domination and repression ensured by crime and punishment. These two approaches¹ constituted the main veins of the sociological approaches to crime and punishment within the development of the sociology discipline.

Despite above mentioned canonical discussions about the sociological aspects of crime, the penological tradition² that considers crime and punishment as notions standing outside of society (Garland, 1991, p. 117) has a non-negligible shadow over the knowledge production of social sciences even in the contemporary era. What matters for the sake of this dissertation is the influential manifestation of this penological approach when I began my research about the criminalization of hacktivists – political hackers – in Turkey in the 2010s.

The rise in the penological approach cannot be thought separately from the larger sociopolitical context. This approach fulfills the necessities of the global change towards the preoccupation with lawlessness and the insertion of the penal policies as a core constituent of the state under neoliberalism. This is what Wacquant called “the punitive turn” (Wacquant, 2016). In this construction of the criminality such as an urgent motif, the

¹ Works of Foucault in the 1970s followed the critical tradition in the sociology of crime with a divergence towards the “microphysics of power” (Garland, 1991, p. 134). Foucauldian approach cannot be ignored, as it is the third main vein of the sociological approaches to crime and punishment. However here, the emphasis is put on the early examples of the sociological approach meditating on the constructed nature of crime in the 19th century to crystallize their opposition to the extant penological approach in the 21st century.

² Garland defines the penological approach as to view punishment as a technique of crime control rather than a philosophical problem (Garland, 1991, pp. 115-116).

states affirm their rights to enforce order by violent means through their law enforcement agencies and the penological approach provides the ideological ground for this intervention.

When I began my study about Redhack in 2013, a specific hacktivist group in Turkey, the crime perspective of the issue was not at all a part of the research project. The study was purely within the limits of activism, social movements, and collective action. Yet, it was fascinating to find out how in discrete instances, the ghost of crime came to dominate what I defined as activism. In that sense, this dissertation project began to evolve towards the perspective of critical criminology, as it was what was needed the most as being “the counter-voice to neoliberalism and conservatism” (Young, 2002, p. 259). Exposing the hegemonic nature of the crime discourse through a specific hacktivism experience that emerged through new technologies and within the social movement waves of the 2010s became the new focus of the dissertation. Following that, the discourse of crime became the study object, so the actors constructing and perceiving that crime discourse, so the state, the news media, the audience and even the group itself, all of them as active agents of the crime discourse. The shift from studying hacktivism as a fact to the study of the crime discourse about hacktivism is from one side the acceptance of the importance of the penological approach and of the inevitability to ignore it. On the other side, it became the tactic to resist the hegemony of the crime discourse through the adoption of the critical approach.

The 2017 meeting of the American Society of Criminology was the peak of the encounters of my project with the penological approach, especially on the popular issues of cybercrime and cyber-terror. Actually, the criminology field was already reformed with the critical approach since the 1970s with the rise of critical criminology and this reform had already taken another acceleration with the current interest in cultural criminology. However, the popular area of *cyber* was hardly blessed with this critical approach except for few examples. Most discussions focused on how to detect cybercriminals, how to prevent cybercrime, and how to be helpful to the states to enhance the fight against cybercrime and cyber-terror. At that time, the dissertation project was evolving slowly to how the hacktivist group in question, Redhack, was criminalized within the Turkish context. Such description of the issue already reveals the key points of the position adopted

in this study: Seeing crime as a constructed process, by using “criminalization” and considering the actors as activists rather than criminals, by using the attribution of “hactivist.” Such position acknowledged the assumption that “the criminalization process then is that cultural process whereby those in power come to define and shape dominant forms of social life and give them specific meanings” (Presdee, 2000, p. 17). This position meant facing directly the hegemonic discourse of crime, the one constructed from the perspective of the powerful social actors, powerful enough to label what is crime and what is not.

At the beginning of this study in 2013, *activism* was a hot topic with all its prefixes. From 2013 to 2019, the global context was transformed from the agenda of uprisings to the bitterness of the rise of the right. This dissertation is also the product of its time. In that sense, it is not surprising that the effort to understand the perspective of the ones who frame activism as crime, the labelling and the criminalization processes became the objects of study. Yet, it is always an ideological preference to call events as activism or crime. This is binding for the case of Redhack, too. Whether this is a study of hacktivism or a study of cybercrime or a study of cyber-terror changes little, except being the manifestation of the side taken by the researcher: the side of those who label or those who are labelled. In this way, I want to be evocative about the connection between social movements studies and criminology, especially when the study object is a group aspiring to social change.

1.1. Research design and methods

This dissertation explores one specific case study in Turkey, the criminalization of the hacktivist group called Redhack who became nation-wide famous during the 2010s, especially between 2012 and 2014. Following that, the research question of this dissertation is how Redhack is criminalized and whether hacktivism is considered as a source of moral panics in contemporary Turkey.

Even though the dissertation is constructed upon one hacktivist group, the study of its criminalization involves multiple sites. The idea of multiple sites comes from the methodological suggestion of the anthropology discipline to follow the study objects among complex intermingling of cultural spaces (Burrell, 2009, pp. 183-184). In this case it

is by *following the crime discourse* that I configured the study as a multi-sited research. Therefore, the project became a multidimensional research including the construction of the crime discourse by state actors and its circulation by news media, alongside the counterframing and reframing strategies developed both by the group and by the audience.

Data is collected from legal and judicial materials about the judicial processes related to Redhack, news scanning, in-depth interviews with actors worked in judicial processes related to cybercrime and (cyber-)terror, audio and written interviews of the group and from the social media platform Twitter. They are used to systematically classify the deeds of the group, to analyze how they are framed as crime, and to examine reframing and counterframing strategies of the audience and the group itself in relation with the crime frames constructed by the state and by the news media. To analyze the collected data, content analysis, framing analysis, and the analysis of temporal trends are used concomitantly.

The objective of the study was to fulfil a qualitative analysis. This choice was justified in the analysis of the in-depth interviews conducted with the judicial actors, as well as in the study of the perception of the criminalization from the social media platform Twitter. For example, in many examples, the thin line that diverged positive framings from the negative ones was drawn with humor and satire. Such contextualized expressions are quite resistant to be quantified and less susceptible to the usage of computational methods. Instead, they need to be understood with their latent, underlying, or nonobvious meanings. For that reason, qualitative data that permits to locate meanings people place on the events, processes, and structures of their lives and to connect these meanings to the social world around them (Miles, Huberman, & Sald, 2014, p. 11) is considered as the best method to be used in the analysis of the construction and the perception of crime frames.

1.2. Difficulties, limitations and backdoors

Conducting a multi-sited research became an issue with unpredictable difficulties in all shapes and sizes. First difficulty of the research was the ambiguous boundaries of where the case study was beginning and where it was ending. As what I was chasing was the crime discourse, the literature of hacktivism and the history of hacktivism were intermingling. In

other words, what the academicians focusing on hacktivism could not be considered distinguished from the more general crime discourse in which they were producing their works. In that sense, they were part of the criminalization process, too. However, contextualizing every academic work written about hacktivism from the perspective of its position in the general criminalization process would be a complicated work that would surpass the limits of a dissertation project. For that reason, I had to ignore the academic “contribution” to the crime discourse about hacktivism.

Subsequent difficulties were directly related to the case study. Foreseeable difficulties of studying an illegal group imposed its own necessities. The question of how to collect data lead me to decide whether I would use interviews as a data collection technique in the issue of the examination of Redhack. This questioning had two concerns: technically, how I could reach the group and ethically, whether my intervention would cause harm to my interviewees.

Actually within the hacktivism literature studies, a tendency to examine the discourses and practices of groups in question through interviews is visible. Eriş’s work (2009) on the hacker culture in Turkey, Milan’s book (2013) on hackers and hacker groups in different countries, Coleman’s study (2014) on the group Anonymous, Tanczer’s articles on how hacktivists address gender issues (2016) and how hacktivists distinguish hacktivism from cyberterrorism (2017) and the collective work on the motivations of ideologically motivated hackers in Turkey (Holt, Freilich, & Chermak, 2017) are all based on data collected from interviews conducted with self-identified hackers and/or hacktivists.

Hackers are actors willing to talk about their performances, as it can be seen from the large amount of written and audiovisual interviews given by Redhack. This willingness is partly the result of the hacker culture: the quest for recognition with their hacking achievements and their self-confidence in their abilities to remain anonymous.

From a broader angle, there is another reason for these actors to wish to tell their stories. As Malthaner (Malthaner, 2014) claims in his work about choices and dilemmas in the fieldwork, in hostile political contexts, actors “become eager to tell their story and present their point of view to outsiders” and reward researchers for “taking the effort and the risk to study events on site” with “even more open, trustful, and rich in information” encounters (p. 191).

The choice of the researchers cited above to conduct interviews with hackers and hacktivists is meaningful when such richness of the data is provided by potential interviewees. These researchers focusing on hackers and hacktivists developed tactics to provide the security and anonymity necessary for their interviewees. For example, Coleman mentions in her book that when she conducted digital ethnography, she preferred to quit IRC (internet relay chat) channels in times of discussions about illegal activities. By this way, she remained ignorant about any potential intelligence data and she protected not just the participants of the research, but also herself (Coleman, 2014, p. 10).

However, the case of Redhack was much more delicate than abovementioned studied cases had ever been before. When I was in the middle of my project, new judicial processes were still adding to existing processes in result of the new hacking activities of Redhack. Not just the group but any person interacting with Redhack through social media was susceptible to terrorism charges. Under these conditions, any contact request – especially the ones that could be established in a more informal manner, following the suggestion of Malthaner for authoritarian regimes (2014, p. 179), could endanger key persons. At the end, this intense atmosphere and ethical concerns born from this atmosphere led the research to depend on secondary sources about the examination of the self-perception of the group. In-depth interviews through which criminalization could be unveiled were reserved to the actors outside of the group. However, that time, new difficulties were encountered.

First main challenge was the question of who could be and should be included in the sampling for interviews when I was trying to find out the construction of the crime framing among the judicial actors related to cybercrime in Turkey. Sampling strategies for collecting data through in-depth interviews had many dead-ends. The best-known method of snowball sampling failed many times. One reason was that actors were distrustful to talk about judicial processes. The other and the unexpected reason was that many actors had an explicit disdain for their colleagues or for other professionals related to the judicial processes. When I asked interviewees if they know other people who would be interested to talk about these issues, “they do not know it, you do not need to talk with them” was a sentence that I heard several times. It was later, near the end of the interviews that this

unwilling attitude to include other actors found its meaning within the larger and complicated issue of *being an expert*.

A positively unexpected change in the sampling was the inclusion of experts as interviewees. When preliminary interviews were conducted in 2017, law enforcement agents, lawyers, prosecutors, and judges were the candidates of judicial actors that would be interviewed. While judges were excluded from the sample due to the lack of connection, experts [*bilirkişi*] were included after the suggestion of many interviewees because of their competence on information and computer technologies (ICTs).

As the knowledge and competence were so important for the interviewees, inevitably, a knowledge hierarchy was formed several times between me and the interviewees, in proportion with their expertise. Before the interviews, I had the bias that I would experience the difficulties of “studying up” (Nader, 1972) through the interviews with state agents, especially with law enforcement agents. My bias was constructed upon the unequal power relation between me and my informants endowed with the state’s punitive power. The methodological question of “how to get information from people who are suspicious of your motives” asked by researchers conducting ethnography with police (Loftus, 2009, pp. 201-202) was binding for my case, too. However, the case study exhibited that the power inequality between the researcher and the researched is not always one-dimensional. In the case of law enforcement agents, I considered my informants as powerful actors based upon my vulnerability in front of them. However, it was mostly the interviews with experts that constructed a research atmosphere in which their knowledge on ICTs and their social position put me in an unequal position with them – here, expertise is taken both as the profession and the expert knowledge. These were the people who had voices and generally had no difficulty being heard, quite similar to how Forsythe remarks her informants in her fieldwork on technoscience (Forsythe, 1999, p. 8).

If the training that they acquired on ICTs was one reason of the patronizing attitude of interviewees, the other reason was undoubtedly my gender role in the male-dominant milieu of ICTs. Quantitatively, among the 25 people with whom I conducted interviews, only two of them were women. Qualitatively, in many interviews conducted with men

interviewees, dynamics of “hegemonic masculinity”³ (Connell, 1995) were embedded. This was the result of the professional field from which the interviewees were coming from: ICT sector, law enforcement, and the judiciary. All of them are male-dominant work atmospheres where gendered division of labor is quite visible. From one side, it was an advantage to gain access – to be considered easily as a subordinate eager to learn as a young woman researcher. However, once the access was gained, it turned into a disadvantage because of the considered lack of credibility and following that, an immense effort was required for the researcher to assert herself. As interviews are processes in which the interviewer controls the interaction, they were easily considered as threats to hegemonic masculinity based on the questioning and the putting of the elements of manly self-portrayal into doubt (Pacholok, 2012, p. 204). That complicated the acceptance process as I had to balance between not threatening openly their bias and asserting myself.

In one of the preliminary interviews, one interviewee explained how a dissertation should be written alongside how the interview questions should be. This failed interview gave important lessons about conducting further interviews: to not have more than one interviewee in one interview and to not meet with the interviewees in their workplace if it is a hostile environment for the researcher, unless there are no other options.

However, the difficulties of studying up did not obscure the fact that even in this unequal relation constructed to researcher’s disadvantage, the personal and professional vulnerability of the interviewees was not neglected. Following the suggestion of Pacholok (2012), I was careful to keep in mind that power differences between researcher and researched cannot be restricted to up/down formulations. In that line, their “possession of power” was not a pretext to neglect elite informants’ vulnerability (Forsythe, 1999).

Another cluster of difficulties is about the access to judicial documents. As many judicial processes about Redhack are conducted under confidentiality order, the access to these documents are quite difficult and restricted with the few information that the lawyers possess about the case. In some cases, even though there is an investigation for many years,

³ Connell defines this concept as “the configuration of gender practice which embodies the currently accepted answer to the problem of the legitimacy of patriarchy, which guarantees (or is taken to guarantee) the dominant position of men and the subordination of women.” (Connell, 1995, p. 77).

there is no indictment prepared about the investigation. That makes the perspective of the judiciary much more implicit and obstruct any research about the cases.

And last, difficulties about the analysis of the social media platform also effected the study. Social media platforms are important potential sources for research conducted in social sciences. Twitter is such a worldwide popular platform that many researchers focus for data collection. However, data collection from Twitter is a complicated issue. Methodological affordances provided by the company and its limitations are highly discussed by researchers working in this area (Gaffney & Puschmann, 2014). After the development of Twitter Advanced Search Engine, now Twitter allows collecting retrospective data. However, as this engine is a quasi-manual tool, it does not permit the collection of big data.

The other option for a retrospective study is to seek the help of companies specialized in collecting data from Twitter. That second option is restricted to researchers with access to high economic resources, as the costs of these services are quite high. This makes researching social media a privilege inaccessible for low-income researchers. The solution found in the scope of this study was the extensive manual use of Twitter Advanced Search Engine and the cooperation with a computer engineer for the data pre-processing of the manually collected tweets and later, for the visualization of this data.

Mentioned above, the illegality of the study object – the hacktivist group – brought along its own difficulties. One that was directly related to the analysis of Twitter was the withheld position of the group's official Twitter account within the Turkish borders. I had to analyze such data sources when I was abroad. While this was a legal constraint that I had to find a backdoor, there were also extra-legal constraints. One example would concretize this issue.

During the preliminary analyses on the Twitter data, I constituted a sample with few thousands tweets to catch an impression about the perception of the crime framing of Redhack. As the number of tweets was not too high, I was able to read all the tweets in the sample. Some tweets were posted by people that I knew: Some of them were posted by public figures and some others were posted by people that I knew personally. In one case, I talked to such a person that I knew personally and informed her that I included her tweet in my sample. Later, this Twitter user said to me that she deleted her tweet after my

involvement. This incident was crucial for two reasons. First, it concretized how people were unconscious of the possible consequences of their acts in the social media. It was after my access to that tweet that this user became aware of the public accessibility of her tweet. And second, it made apparent the fear atmosphere that the citizens using the social media platforms to express their political views experience. Undoubtedly, there were others like this specific Twitter user who did not want to “have a problem” because of their tweets. I confronted similar issues in the later stages of the study. In several cases, a tweet collected before could not be accessed few years later. Either it would be deleted by the user or its access would be denied by Twitter as a result of a legal demand. That forced – at least one part of – the study to be dependent on ephemeral data sources.

1.3. Outline

The dissertation begins with theoretical and historical chapters before embarking upon the case study. Chapter 2 positions the dissertation within the hacktivism literature and presents the theoretical research question by problematizing the definition of hacktivism within the duality of civil disobedience and terrorism. This questioning allows the criticism of the hacktivism literature and invites the search for theoretical tools from other literatures. Following that, I benefit from the sub-disciplines of critical criminology and critical terrorism studies, alongside the framing analysis to develop a distinctive theoretical platform in which the implicit question of whether the criminalization of Redhack corresponds to a moral panic would be crucial.

Chapter 3 explores the historical context of the theoretical question formed around the definition of hacktivism. In that line, it exhibits how the meaning of hacktivism is changing historically through a close relation with its perception and with the experiences of hacktivism. The historical inquiry will begin from the development of computer and network technologies and the first actors engaging politically with these technologies. After the examination of several historical periods, it will reach the hacktivist experiences of the 2010s characterized with the global economic crises and global uprisings. In this way, the global context of the hacktivist experience that would be studied in the case study would be exhibited in this chapter.

Chapter 4 is the first step to uncover the criminalization of the hacktivist group Redhack to understand the contextual meaning of hacktivism in Turkey in the 2010s. This is a referential chapter for later chapters as it exhibits the acts of Redhack and presents the judicial processes about Redhack. This chapter also develops some initial discussions about their acts and the judicial processes about the group.

Chapter 5 examines the construction of the crime frames for Redhack with a specific focus on the discourse of political actors and of news media. These are considered as potential constructors of the crime frames, as the literature of framing analysis suggests. However, the chapter will exhibit their quasi-absence as active agents of framing. For that reason, I will turn to judicial processes and to judicial actors to uncover the hidden agents of the criminalization process.

With a reference to the official frames constructed by political actors, Chapter 6 examines the personal “unofficial” frames developed by the judicial actors interested/worked in cybercrime related judicial processes in Turkey. In this examination, the criminalization of Redhack is discussed under two main categories: frames of cybercrime and hacking on one side, and frames of cyber-terror and terror on the other side.

In Chapter 7, I focus on the issue of framing contest based on one specific crime framing of Redhack – the terror framing – and ask if the terror framing constructed for Redhack resonates with the general perception. In an intermingled structure, the chapter examines the counterframing and reframing strategies of both the group itself – Redhack – and the strategies performed by the audience of the crime frames in Twitter.

The dissertation adopts an approach in which the crime framing of hacktivism and the question of whether it is constructed as a source of moral panics are considered as deeply embedded and interactive process between different actors including the state agents, the news media, the audience, and the group itself.

In the conclusion, evoking the conceptualization of moral panics and folk devils and based upon the findings of the case study, the question of whether the criminalization of Redhack with the labels of cybercrime and cyber-terror gives rise to a moral panic in Turkey will be answered. I claim that the reactivation of older moral panics of terrorism within the criminalization of Redhack is dependent on the current absence of the perception of hackers and hacktivists as folk devils in Turkey based upon the fascination with

cybercrime. Alongside the discussion on the fascination with crime, the discussion of legibility would appear to understand the reactivation of the terror frame for a hacktivist group. Following that, the sociopolitical implications of this peculiar criminalization compared to the global trends will be discussed in national and global contexts. Ultimately, alongside being part of the hacktivism literature and of framing analysis, this dissertation contributes to critical criminology and to critical terrorism studies by making claims about the contextualized nature of cybercrime and (cyber-)terror discourses at the end of the 2010s, as a concrete case study from recent history.



CHAPTER 2

CONTEXTUALIZING HACKTIVISM:

THEORETICAL ROOTS TO PROBLEMATIZE CRIMINALIZATION

In this chapter, I try to contribute to hacktivism literature by identifying there a problem of disembeddedness, a tendency to define hacktivism without considering the contexts that give birth to hacktivist experiences. The mainstream tendency within the literature to define hacktivism as civil disobedience and as opposite to cyber-terrorism reduces the explanatory power of the concept of hacktivism. Both civil disobedience and terrorism are concepts defined by legal norms closely dependent on economic, political, and social contexts. Disregarding these contexts results in an abstract conceptualization of civil disobedience and terrorism. Following that, this negligence reduces hacktivism to an ungrounded category that does not compromise with hacktivist experiences from different contexts. For that reason, an investigation of legal aspects is fundamental to embed hacktivist experiences into their corresponding contexts. This legal perspective would give the opportunity to problematize the aforementioned duality of civil disobedience and cyber-terrorism to define hacktivism and contextualize hacktivist experiences. In line with this perspective, this chapter will exhibit which theoretical tools can be used to contextualize hacktivism through an investigation concerning its criminalization.

The chapter begins with the critical review of hacktivism literature in terms of the definition of hacktivism dependent on the concepts of cyberterrorism and civil disobedience. This part is divided to three subparts. First generation of studies defines hacktivism through an opposition to cyberterrorism. In the second group, this opposition to cyberterrorism is much more implicit. Last generation is still concerned with the relation between hacktivism and cyberterrorism. Different from earlier studies, this time, these studies problematize the labelling of hacktivism by cyberterrorism through the examination

of the discourse of cyberterrorism for hacktivism. I will follow and deepen this last generation, as the beginning point of my examination.

Following that, in the second part, I propose an investigation on the criminalization of hacktivism as a way to overcome this dichotomy between cyberterrorism and hacktivism. This part exhibits my theoretical orientation to contextualize hacktivist examples. For that purpose, first, I will look beyond the boundaries of hacktivism to embrace eye-opening studies from near study areas. These are works examining crime frames for hackers and critical studies about cyberterrorism discourses. They diverge from mainstream crime and terrorism studies with their explicit constructionist perspective. Such perspective would be helpful to investigate the criminalization of hacktivism. Then, as the second subpart, I will go back to the theoretical roots of this constructionist approach for crime. After an introduction about the theoretical background of considering crime as a social construction, I will pass to critical criminology, as the source of the core concepts used in the recent works about cybercrime and cyberterrorism. This subpart will continue with the examination of these rediscovered concepts. Last, I will turn to the concept of *framing*, as the other root of critical cybercrime and cyberterrorism studies. Following that, I will investigate how to use framing analysis with a focus on power relations through the concepts of ideology, hegemony and discourse.

2.1. *A critical review of hacktivism literature*

Hacktivism studies constitute an emergent interdisciplinary academic field. Scholars from many different fields including anthropology, communications, criminology, political science, security, and sociology are interested in this phenomenon. However, the existence of different academic lenses does not always correspond to the polyphony of perspectives. Within the development of hacktivism field, the perspective of security studies heavily dominated the field, especially at its beginning.

2.1.1. First generation: Dichotomy between cyberterrorism and civil disobedience

The early literature on hacktivism has a tendency to define hacktivism with a serious effort to compare hacktivism with civil disobedience and differentiate it from cyberterrorism (Wray, 1998; Denning, 2001; Huschle, 2002; Samuel, 2004; Auty, 2004; Krapp, 2005). For that reason, defining hacktivism remains limited with the concepts of civil disobedience and terrorism within this first generation.

Civil disobedience is a specific activism type. It is defined as “a public, nonviolent, conscientious yet political act contrary to law usually done with the aim of bringing about a change in the law or policies of the government” (Rawls, (1971) 1999, p. 320). From the perspective of the first generation of hacktivism studies, the distinctive feature of hacktivism is its ability to combine civil disobedience with computer technologies (Samuel, 2004, p. 2). Hacktivism is “electronic civil disobedience” (Wray, 1998), “cyber disobedience” (Huschle, 2002), or simply, “a form of civil disobedience” (Krapp, 2005) in the first generation of hacktivism studies. This tendency to define hacktivism by civil disobedience would be influential in more recent works, too. Yet this time, the ambiguous position of civil disobedient toward the law would be accentuated by the problematization of legality (Shantz & Tomblin, 2013).

The problem of defining hacktivism dependent upon civil disobedience does not arise from the ambiguity of the concept of civil disobedience. On the contrary, civil disobedience is a well-defined concept. The problem results from the decontextualized use of the concept. When civil disobedience is used as a definitional tool for hacktivism, it reduces the scope of hacktivism to specific hacktivist experiences adopting particular ideological orientations while excluding other experiences. In other words, it limits hacktivism to a specific activism type and deprives the concept of hacktivism of a larger inclusivity.

If civil disobedience is used to define what hacktivism is, cyberterrorism determines what hacktivism is not. According to this perspective, when political hacking possesses the intent for “severe economic damage” or “loss of life,” then it surpasses the boundaries of hacktivism and becomes cyberterrorism (Denning, 2001, p. 241). This divergence between cyberterrorism and hacktivism are carefully drawn in many works following that

perspective (Samuel, 2004; Krapp, 2005). This time, defining hacktivism as opposite to cyberterrorism is problematic in two levels. First, it generates ambiguous definitions for hacktivism as acts “not causing serious damage” (Denning, 2001, p. 241) or “not malicious acts” (Auty, 2004). Second, terrorism is not an agreed on concept, as civil disobedience is. There is an ambiguity within the concept itself. As the definition of terrorism is heavily dependent upon individual framings and sociopolitical contexts, terrorism-related definitions make hacktivism a much more disembedded concept. Actually in a paradoxical way, many scholars defending this perspective are aware of the ambiguities of limits dividing hacktivism and cyberterrorism (Denning, 2001, p. 241; Auty, 2004, p. 219). However, this recognition does not result in the formation of a definition of hacktivism independent from cyberterrorism.

In sum, the tendency of defining hacktivism through the concepts of civil disobedience and cyberterrorism was the main concern of the first generation of hacktivism studies. Examples from the literature show how this perspective gives rise to semantic ambiguities about the meaning of hacktivism. Moreover, such perspective results in an abstract notion of hacktivism that ignores contextual differences and thus, cannot be compatible with diverse hacktivist experiences from different contexts.

2.1.2. Second generation: Specter of cyberterrorism

The earlier generation of hacktivism studies was occupied with defining hacktivism through the dichotomy between civil disobedience and cyberterrorism. Different from them, second generation of hacktivism studies worked on elaborated studies that focus on different social and political issues related to hacktivism in the 2000s (Jordan, 2002; Jordan & Taylor, 2004; Taylor, 2004; Thomas, *Hacking the body: code, performance and corporeality*, 2005) and in the 2010s (Lindgren & Lundström, 2011; Coleman, 2013; Zajácz, 2013; Coleman, *Hacker, Hoaxer, Whistleblower, Spy: the Many Faces of Anonymous*, 2014; Sauter, 2014; Goode L., 2015; Kubitschko, 2015; Tanczer, *Hacktivism and the male-only stereotype*, 2016; Schrock, 2016; Deseriis, 2017). However, the specter of cyberterrorism was still sensible within some influential works from this generation. To

concretize this tendency, I will take two important examples that influenced posterior works on hacktivism.

The influential work of Jordan and Taylor (2004) does not refer to the concept of cyberterrorism to define hacktivism. However, they accentuate “electronic civil disobedience” (2004, p. 3) as the distinctive feature of *mass action hacktivism*, one of the two main types of online politics that forms hacktivism, together with *digitally correct hacktivism*. In this schema, mass action hacktivism uses technologies for political goals in line with the anti-globalization movement. And the other type of hacktivism – digitally correct hacktivists – struggles against any restriction of free speech by defending “politics in technologies” (2004, p. 110). Jordan and Taylor’s work is a reference source for many other studies with its eye-opening discussions on these two hacktivism types. However, in this work, there is an exclusion of other hacktivist experiences than the ones that can be categorized under these two activism types. In that sense, the determination of political goals as a definitional component of hacktivism is limiting the inclusivity of hacktivism as a term. When hacktivism is defined with the defense of free speech in internet or with the struggle against anti-globalization, the question of what will happen to other hacktivist experiences with different political goals remains without answer. Here comes the specter of cyberterrorism. When a hacktivist experience could not be included in the hacktivism definition drawn by the categorization of Jordan and Taylor, it would implicitly fall to the category of cyberterrorism.

Another important example from this line is the work of Coleman (2014). Working on a specific hacktivist group from the 2010s, Coleman conducts a detailed anthropological work. However, reminding the first generation of hacktivism studies, she cannot abstain from using terrorism as the opposite of what she considers as hacktivism. This time, the distinctive feature of the hacktivist groups is their use of humor, *lulz*, considered in a total opposition to the position of *jihadist terrorists* who cannot understand this humor (2014, p. 15). This time, terrorism considered in opposition to hacktivism is disembedded from its context with an implicit labelling process. In contrast to the contextualization effort made for the hacktivist experience through the anthropological perspective, the decontextualized consideration of the *terrorist* experience influences negatively this effort.

The second generation of hacktivism studies is rich with its multidimensional corpus. Different from the first generation, these studies are not explicitly occupied with dissociating hacktivism from terrorism. However, the specter of terrorism is still there to trigger an abstract conception of hacktivism that include specific hacktivist experiences at the expense of others. So in this part, I tried to exhibit the implicit presence of civil disobedience and (cyber)terrorism as defining concepts of hacktivism. This ongoing tendency would be ended by the third generation of hacktivism studies focused on the crime discourse about hacktivism.

2.1.3. Third generation: Focusing on the crime discourse

A more recent trend in hacktivism studies tries to problematize the disembeddedness of boundaries between cyberterrorism and hacktivism. These studies critically examine the crime discourse about hacktivism (Vegh, 2002; Vegh, 2005; Heineman, 2007; Vlavo, 2015; Klein, 2015; Tanczer, 2017). This corpus develops two important perspectives. The first perspective emphasizes the discourse of criminalization used in news media and in official documents against hacktivists. The other one aims to deconstruct the criminalization discourse by making visible the self-perception of hacktivists.

Vegh's early studies (2002; 2005) are examples where the crime discourse about hacktivism was exhibited. In these works, how news media and governmental entities share the same position against hackers and hacktivists to discredit them and to label internet as a terrorist territory is emphasized. Mainstream US media's portrayal of hacktivism before and after 9/11 is a significant example in which the shift from criminals to cyberterrorists is highly visible in the discourse of criminalization used against hacktivists. Based upon five daily U.S. newspapers of the period, Vegh shows how the discourse on the vulnerability of the American cyberspace resulted in the creation of the crime frame "potential terrorist hacker" (2005, p. 9). More the media echoes the governmental approach to consider the repression of hacktivism as the "elite's crusade," more the perception of hacking as "an activity that may potentially threaten the dominant order" solidifies (2002, p. 1). This framing enables the promulgation of repressive laws and regulations against digital political protest (2005, p. 11).

One decade later, two studies focusing on the crime discourse about hacktivists stood in this corpus. Vlavo (2015) examined legal and judicial changes related to the framing of hacktivism as cyberterrorism. This study revealed the interactivity between the discourses of cyberterrorism and cyber-protest within the discourse about hacktivism. In this line, Vlavo defended how cyberterrorism was formulated as a response to the earlier concept of cyberprotest, as a governmental and corporate control tool (2015, s. 8-9). As another example, Klein (2015) studied the framing of hacktivism in news media, too. In this study, the focus was on the increasing negative framing of one specific hacktivist group.

Within the second approach consisting of the self-perception of hacktivists, most important point is the vocalization of hacktivists' objections to seeing hacking and hacktivism portrayed as violent acts (Heineman, 2007; Tanczer, 2017). In these studies, self-perceptions are frequently accompanied with external perceptions about them to emphasize the divergence between the two sides. This confrontation of rhetorical constructions of hacktivism deconstructs labels of cyberterrorism advocated mostly by governmental and corporate entities.

I find these approaches belonging to the third generation of hacktivism studies very important, as a contextualization effort for hacktivist experiences. They problematize ungrounded boundaries between hacktivism and cyberterrorism by focusing on the crime discourse about hacktivists. However, they lack another important step. They do not problematize the categories themselves, cyberterrorism and terrorism. They take them for granted and continue to use them as negative benchmarks by terms like "true terrorist organizations" (Klein, 2015, p. 398).

To advocate for a more inclusive problematization, I need to deepen the way paved by this third generation and go further to the direction indicated by these works. The link to this further road lies at the boundaries of hacktivism. These would be the studies on cybercrime and cyberterrorism frames, alongside critical works on the discourse about cyberterrorism.

Briefly, crime discourse in news media and official documents and the self-perception of hacktivists about this discourse are the two main objects of study in the third generation of hacktivism studies. Even though these studies do not problematize the

original categories used in this criminalization, they pave the way to the deeper examination of crime discourse about hacktivists. In that sense, these studies enable the problematization of the concepts of terrorism and cyberterrorism, alongside the contextualization of hacktivism.

However, such an examination requires reference to other study areas than hacktivism studies. Therefore, now, I lean beyond the boundaries of hacktivism and investigate the studies about cybercrime and cyberterrorism frames, alongside critical works on the discourse about cyberterrorism. These works will reveal the theoretical roots that I will rely on to overcome the problem of disembodiedness within the hacktivism literature.

2.2. Contextualizing hacktivism

How cybercrime and cyberterrorism are framed through cultural products, in news media, and in official documents is a topic highly discussed within and beyond the boundaries of hacktivism. In this field that we can call critical cybercrime studies, crime frames for hackers and the discourse about cyberterrorism occupy an important place. In this part, first, I will review these studies that influence heavily the criminalization of hacktivists, even though they are not focusing directly on hacktivist experiences. Following that, I will continue to go deeper by focusing on three fundamental approaches that these studies ground on: the social construction of crime approach, the concepts adopted from the critical criminology, and the perspective of studying framing with a focus on power struggles.

2.2.1. Reference works for contextualization: At the boundaries of hacktivism

Beyond the boundaries of the criminalization of hacktivism, two specific study areas share the same fundamental perspective: the examination of crime perceptions about hackers (Nissenbaum, 2004; Yar, 2006; Wall, 2008; Wall, 2012; Steinmetz, 2016) and the analysis of the discourse about cyberterrorism (Thatcher, 2006; Wykes & Harcus, 2009; Jarvis, Macdonald, & Whiting, 2015; Bowman-Grieve, 2015; Jarvis, Macdonald, & Whiting,

2016). The perspective that they share is their approach to emphasize the constructed nature of crime frames.

Defining hacktivism as political hacking already reveals the commonality between hackers and hacktivists. Thus, crime perceptions about hackers concern deeply the criminalization of hacktivist experiences. The main argument of the criminalization approach is that governments, law enforcement, the computer security industry, businesses, and the media actively construct hacking as cybercrime (Yar, 2006, p. 23). Scholars advocating this perspective defend that criminalization processes should be analyzed not just related to their immediate context but also through their implications for the global political economy. In this line, Nissenbaum (2004) argues that there are two reasons for “demonizing hackers:” the struggle over how normalcy is defined to designate the good citizen in the age of computer and to justify increases in security, surveillance, and punishment (pp. 199-200). For that reason, there is a deep connection between the demonization of hackers and the perception of internet as a criminal place. This crime perception of the internet gives rise to cultural anxieties, *moral panics*, about internet-related issues. And the construction of hackers as an urgent threat to the society reflects in the *labelling* of them as cybercriminals, to the point to consider them as *folk devils* (Yar, 2006, p. 23). In this context, distorted imagery about hackers feeds the panic over technology, crime, terrorism, and economic losses and results in the legitimization of security institutions (Steinmetz, 2016, p. 214).

Security discourse about hackers benefits also from popular culture products. The “unquestioning assuredness” in public opinion about “the seriousness of what hackers have done” is cemented by social science fiction – cyberpunk literature (Wall, 2012, pp. 4-7). Moreover, the popularity of movies about criminal hackers is part of this construction since the end of the 1980s (Steinmetz, 2016, pp. 180-182).

A similar constructionist approach can be followed in studies on the discourse about cyberterrorism. The construction of the concept of cyberterrorism can be linked to wider issues of national security, civil liberties, and state control of information and communication technologies when it is analyzed through the concept of *moral panics*, once again (Thatcher, 2006). In her dissertation, Thatcher analyzes images, orientations, stereotypes, and symbolization of cyberterrorism alongside representational trends about it

through the UK news media. In another example, Wykes and Marcus (2009) express how old myths of race and crime intermingle with new technologies of internet through the broadening discursive criminalization (p. 220). Moreover, this discourse effects changes in policy and legislation, even though it is disconnected from 'real' data (2009, p. 215).

Following the same perspective, Bowman-Grieve (2015) turns once again to the concept of *moral panics* to emphasize the instrumentalization of mobilizing fear through cyber-terror to promote social control (p. 103). In recent examples, Jarvis, Macdonald and Whiting (2015; 2016) study the news media coverage of cyberterrorism. They uncover the constitutive role of the news coverage to the production of cyberterrorism by framing and interpretation through language, images, and other discursive practices (2015, p. 73).

Crime frames about hackers and the discourse of cyberterrorism are reference study areas from where problematizing the criminalization of hacktivists can take its sources. For that reason, in this part, I summarized works that engaged critically with these issues. The review exposed the common components of these two corpuses: the constructionist approach, the presence of the concepts of *moral panics* and *folk devils*, and the emphasis on the framing as the constitutive process of criminalization processes. In following parts, I will concentrate on these components.

2.2.2. Sources of contextualization

Going down the foundations of a perspective in question provides the instruments to deepen this perspective. That is why in this part, I will excavate the fundamental mechanisms underlying examinations about crime perceptions about hackers and the analysis of the discourse about cyberterrorism. First mechanism is the constructionist approach for crime. Second is the adaptation of concepts from critical criminology. And third is the use of framing analysis that emphasizes the examination of power in the meaning-making processes.

The social construction of crime and the constructivist turn in terrorism studies

Social constructionist approach grounds on the assumption that the reality is socially constructed. Relatedly, social processes are the core moments where such constructions are exposed. In 1966, Berger and Luckman (2013) coined the term “the social construction of reality,” as an important milestone for the social constructionist tradition. The process of constructing the reality is the dialectical relation between the social reality and the individual existence. Different and sometimes opposite intellectual traditions use this same perspective (Hacking, 1999, p. 6) because social constructionism is a useful critical tool to challenge the status quo. That is the reason why many scholars studying cybercrime from a critical perspective shares the constructionist approach to overcome postulates about crime.

The conception of crime as a social construction is actually an old approach shared by many influential figures from sociological thought. In classical texts (Durkheim, (1893) 1960; Marx, (1842) 1996; Weber, (1919) 1946) and in many other important works on the relation of state formation and violence (Tilly, 1985; Benjamin, 1986), the constructionist approach for crime is emphasized especially through its relation with violence and law. Contemporary works from legal anthropology (Conley & O'Barr, 1997; Latour, 2002) and criminal anthropology (Comaroff & Comaroff, 2016) also address this issue by asking questions about the meaning of crime-and-policing in the late modern world.

As an unorthodox sub-field within the criminology field, critical criminology literature (Young, 1971; Cohen, (1972) 2011; Turk, 1972; Quinney, 1977; Ferrell, Urban Graffiti: Crime, Control, and Resistance, 1995; Schwartz & Milovanovic, 1996; Pratt, (2002) 2013; Sim, 2004) is another important corpus that emphasizes the socially constructed nature of crime by combining labelling theory (Becker, 1966) with Marxist political economy. Similar to the position defended by critical criminology within criminology, critical terrorism studies (CTS) stands as an unorthodox field within the corpus of terrorism studies, by its adoption of the social constructionist approach (Norris, Kern, & Just, 2003; Jackson, 2005; Altheide, 2007). Some of the key debates of CTS are the questioning of the nature and definition of terrorism, alongside the “terrorist” label and the exaggeration of the terrorism threat (Jackson, Introduction, 2016). These topics coincide with the call for the constructivist turn in terrorism studies that Hülse and

Spencer (2008) defend. In this perspective, not the “terrorist” actor but the discourse about it should be the starting point for research because the actor is the product of the discourse. The necessity of the shift to discourse-centered research in terrorism studies is emphasized in this call (Hülsse & Spencer, 2008, p. 571) with a slight divergence from CTS with their critique of state-centrism for CTS. It means that in studying the construction of the terrorist discourse, the agency of political elite should not be overestimated (2008, p. 579). I will reevaluate this critique after the discussion on the emphasis on power struggles in framing studies.

The theoretical journey from classical texts to subfields like critical terrorism studies exhibits the inclusiveness of the social constructionist approach to crime. Recognizing the social impact in the nature of crime is a common premise in social sciences shared by critical scholars for decades. However, the anchorage of this approach as a radical critique to mainstream studies of crime and criminology corresponds to the 1970s with the development of critical criminology. In the 2000s, with the global rise of the discourse on terrorism and cyber-threat, the return to the constructionist perspective is witnessed in the studies about crime. This contemporary rise also resulted in the summoning of the concepts of critical criminology, as the reference studies about the crime perception of hackers and analyses about the cyberterrorism discourse showed.

Return of critical criminology: Moral panics and folk devils

Critical criminology is one of the most established subfields advocating for a social constructionist perspective within the field of criminology. Within this perspective, crime and deviance are “doubly socially constructed” because the social is the producer of criminal attitudes, as well as the producer of the perception of criminality (Sumner, 2004, p. 6). Critical criminology offers a radical change in the determination of which problems and which solutions are significant and legitimate within criminology studies. They primarily focus on the exploitative nature of capitalist society in the formation and the perception of crime rather than the crime and the criminal. In this perspective, crime is considered to be formed through the practical or behavioral responses to social conditions. And its perception is the reflection of social censures based on emotions, ideologies, and

values of powerful social groups (p. 9). Therefore, the examination of crime is never limited with the crime. It is the exploration of “the historical milieu” (p. 13).

Critical criminology inherits this constructionist approach for crime from two important works from the 1960s: Goffman’s *Stigma* (1963) and Becker’s *Outsiders* (1966). Labelling theoreticians consider the interactional process of criminalization as a negotiation and an interpretation of meanings of crime (Tierney, 2009, p. 92). Critical criminologists deepen the cultural investigations of these works from the 1960s in the direction of the “social” element of crime within the larger framework of structural conflicts in the society (Sumner, 2004, pp. 15-17). This direction of the 1970s was settled by the influence of the Marxist political economy. In their analysis of crime, critical criminologists emphasized the economic and political context of capitalism and defended that capitalist society was unequal, unjust, and criminogenic because it was founded upon exploitative class relations (Tierney, 2009, p. 57).

The development of the concepts of *moral panics* (Young, 1971) and *folk devils* (Cohen, (1972) 2002) is the result of this intellectual context. Both concepts are coined in relation to how the position of deviant groups is altered by media at “the Age of Anxiety” (McLuhan, (1964) 1994, p. 5). In this conceptualization, moral panics begin with a concern about a potential or imagined threat. Then the hostility against specific responsible actors that will be labelled as the folk devils comes. The consensus shared by the elites of the society alongside the mass media follows this hostility. And the disproportionality by the exaggeration of the objective harm and the volatility of the panic are the characteristics of moral panics (Cohen, (1972) 2002, pp. xxvi-xxvii). Not just social psychological factors but also the role of the state authoritarianism and the crisis of capitalism in the 1970s in the creation of moral panics were emphasized by the perspective of critical criminology (Hall & Jefferson, (1976) 2003).

By the 1990s, *moral panics* was settled as an inclusive concept to define diverse phenomena from “juvenile delinquency” (Springhall, 1998) to “the Renaissance witch craze” (Goode & Ben-Yehuda, 1994, pp. 144-184) in historical perspectives. On the other side, as studies on crime frames for hackers (Yar, 2006; Wall, 2012) and works on the discourse about cyberterrorism (Bowman-Grieve, 2015) show, the concepts of moral panics

and folk devils were expanded to be explanatory tools for new social relations emerged with computer and network technologies.

This is how the concept of moral panics and folk devils were developed within the critical criminology subfield. As this review exhibits, social psychological factors and structural problems of capitalism merge in the construction of labelling processes and criminalize specific groups. The emphasis about the historicity of such processes is important to understand the continuity of this social phenomena. Meanwhile, analyses about these criminalization processes reveal social changes that trigger such fears, as the works on the discourse about hackers and cyberterrorists show. From here, I will pass to the last fundamental mechanism that would be used in the effort to contextualize hacktivism. This is the framing analysis that enables the exposure of labelling processes.

Framing analysis and studying power in meaning-making processes

Framing as a process of meaning-making refers directly to the construction of social reality. In a more concrete sense, framing means to select specific facts, images, or developments over others to prioritize the first ones. How crime is framed constitute a main topic in cultural criminology studies (Hayward & Presdee, 2010; Ferrell, Hayward, & Young, 2015). A focus on images created and consumed by criminals, control agents, media institutions, and audiences to understand how crime and crime control are constructed corresponds to a productive fusion of critical criminology with framing analysis. In that line, works that examine the framing of terrorism approximate framing analysis with the discourse-centered approach and the constructivist turn in critical terrorism studies, too (Norris, Kern, & Just, 2003; Reese, 2010).

Framing analysis takes its source from the work of Goffman ((1974) 1986). In its original usage, the analysis of individual cognitive structures is accentuated at the expense of the analysis of social structures. Yet the frame in Goffman's work refers to the inevitably relational dimension of meaning and implicates the meanings of background, setting, and context (Berger B. , (1974) 1986, p. xiii). In adopting framing analysis, I diverge slightly from the individual cognitive approach and approach this implicit denotation. Therefore, I benefit from framing analysis through its critical interpretation based upon an emphasis on

broader structural and ideological processes (Gitlin, 1980). In this sense, I consider framing as the meaning-making process deeply dependent to *politics of signification* (Snow & Benford, 1988, p. 198).

Coined by Hall ((1982) 2005), *politics of signification* is the crucial point that links framing to ideology because the power to signify events in a particular way is an ideological power shaped within the contextual power struggles (pp. 65-66). However, for a long time, ideology was neglected in framing studies. Scholars from social movement studies (SMS) (Snow & Benford, 1988; Oliver & Johnston, 2000) and from media studies (Carragee & Roefs, 2004) criticized this negligence based upon their different approaches to ideology, an already loaded concept especially within the Marxist corpus.

In the classical materialist approach for ideology from Marx, ideology is socially determined. It is the false consciousness that serves to universalize and eternalize the interests of the ruling class (Eagleton, 1991, p. 56). The new class has “to represent its interest as the common interest of all the members of the society” (Marx, 1978, p. 174). So, ideology represents these relations as “unchangeable, inevitable and natural” (Hall, (1982) 2005, p. 72). In that sense, the ideological naturalization of historical capitalism is represented as an objective fact (Downey, Titley, & Toynbee, 2014, p. 880). To understand how framing works within this ideological naturalization, it is important to emphasize the processual nature of ideology.

The semiotic theory of ideology is one way to understand ideological processes. In this approach, ideology is defined as “the struggle of antagonistic social interests at the level of the sign” (Eagleton, 1991, p. 195). Advocated by Voloshinov, this approach would be the procreator of discourse analysis with its emphasis on ideological power as the performance of social power within language during meaning-making processes (1991, p. 195). However, a constructionist emphasis on the discursive view results in the idea that there is no social reality apart from the signification in the discursive process. It also neglects the domination that ideological processes support (Downey, Titley, & Toynbee, 2014, p. 880). To overcome this negligence, the call for *ideology critique* in media studies enables the understanding of the processes of consent construction within structural inequality (Downey, Titley, & Toynbee, 2014). This call adopts another processual

conceptualization of ideology than the radical constructionist perspective of the semiotic theory. It is based upon the Gramscian concept of *hegemony*.

Antonio Gramsci ((1971) 1992) is one of the main figures from the Marxist corpus who adopts the processual conceptualization for ideology without adopting the constructionist perspective. In this conceptualization, hegemony is a renewed, recreated, defended and modified and also resisted, limited, altered, and challenged process (Williams, 1977, p. 112). For that reason, it is highly useful to understand the function of ideology, as the power struggle in the meaning-making. In all hegemonic processes, consent is secured by ruling elites through the production and diffusion of meanings and values. In line with that, frames have a central role in producing hegemonic meanings (Carragee & Roefs, 2004, pp. 221-222), as well as in developing the counterhegemonic stance (p. 227). Therefore, the call for an emphasis upon ideology – and hegemony – in framing studies is to enlighten how political and social contexts shape framing contests alongside how the construction and interpretation of the frames are shaped by the distribution of power (p. 215).

For scholars from social media studies, this critique of the negligence of ideology in framing studies has a longer history going back to the 1980s (Snow & Benford, 1988). Recent approaches to this call reviewed it with the warning of not substituting frames and ideology (Oliver & Johnston, 2000).

Ideologies are socially constructed, and their social construction involves framing processes, but trying to reduce ideology construction to a series of framing processes at the interactive level or frame alignment at the organizational level loses its social and political content.

(Oliver & Johnston, 2000, p. 51)

It is in this sense that I adopt the emphasis on ideology when studying crime frames developed during the criminalization of hacktivism. Social and political content of the criminalization needs such an elaborated theoretical structure to become explicit.

This is how framing analysis will be used as the last theoretical root in the examination of criminalization of hacktivism to overcome the problem of disembodiedness

within the hacktivism literature. Through a detailed discussion on the necessary examination of ideologies in framing studies, I outlined the approach to be adopted during the study of crime frames while examining the criminalization of hacktivism. In the former part on critical criminology, I had exhibited the theoretical development of the concepts of moral panics and folk devils. These two sources will be the theoretical instruments that I will use to contextualize hacktivism through its criminalization.

2.3. Conclusion

This theoretical chapter was designed as an inverted-funnel deepening towards theoretical roots. Beginning by the problem of disembeddedness within the hacktivism literature, I passed through the presentation of the problem, the initial steps to overcome this problem within the hacktivism literature, the investigation of reference studies beyond the hacktivism literature, and the examination of theoretical roots found from these reference studies to reach the necessary instruments to be used in the analysis of the case study.

The constructionist approach that I chose for this study has an intellectual involvement with all the three generations of hacktivism studies – as I categorize them. This is a critique to the first generation of hacktivism studies limited with the dichotomy between cyber disobedience and cyber-terrorism and a challenge to the second generation where the crime aspect is not challenged at all. Last, this approach is in dialogue with the third generation focused on the discourse of hacktivism with its intention to surpass these studies.

In consequence of this advance, I form the theoretical backbone of the case study from the social constructionist approach for crime, the adoption of the concepts of moral panics and folk devils from critical criminology literature, and the use of framing analysis with an emphasis on power struggles in meaning making processes. In the formation of this theoretical framework, I do not neglect the possibility of new theoretical requirements that can be born from the case study in line with the doctrine of grounded theory.

CHAPTER 3

HACKTIVISM IN MIRROR:

MEANINGS, PERCEPTIONS, EXPERIENCES

This chapter will exhibit how the meaning of hacktivism is changing historically through a close relation with its perception. However, this perception cannot be thought as a unified worldwide process. Different hacktivist experiences arise from different cultural, economic, and sociopolitical contexts. Alongside the global context, diverse local contexts also become constitutive for these experiences and their perception. Perceptions about hacktivism largely go parallel with its criminalization. For that reason, it is not just the hacktivist experiences and their perceptions but also the criminalization about hacktivism that shape the meaning of hacktivism. At the end, the changing meanings of hacktivism are the total result of this interactive historical process between perceptions and experiences.

In this chapter, I will trace the history of hacktivism through a periodical compartmentalization. This history will be shaped around the simplest definition of hacktivism as political hacking, to embrace different hacktivist experiences with diverse ideological motivations. For the definition of hacking, I acknowledge the more inclusive meaning of hacking as “the imaginative re-appropriation of technology’s potential within countercultural and oppositional communities” (Jordan & Taylor, 2004, p. 5). However, I narrow the meaning of hacking to the imaginative re-appropriation of computer and network technologies, relying upon two reasons. First is the reason related to hacktivist experiences: All the self-called hacktivist examples are the ones who engage politically with computer and network technologies. Second, the criminalization of hacktivism emphasizes computer and network technologies by defining hacking, as “illicit, illegal or unwanted *computer intrusion* [emphasis added]” (Jordan & Taylor, 2004, p. 5).

For these reasons, my historical inquiry begins with the development of computer and network technologies and the first actors that engaged politically with these technologies in the period before 1980. In the second section, I will look to the drastic change in the global political economy towards neoliberalism in the 1980s and how it created an anti-privatization oriented early hacktivism. Next section will be the 1990s, a crucial period for hacktivism both in the sense of experiences and also in the sense of perceptions. These years will be the peak point of its criminalization, as well as the period of the first attempts of stabilizing the meaning of hacktivism by the actors themselves. In the fourth section dedicated to the 2000s, the decisive incident will be 9/11, the attack on World Trade Center. This period is marked with the global diffusion of (cyber)terror frames that effect heavily the perception of hacktivism. The increase in nationalist hacktivist examples coincides with this proliferation of cyber-terror framings during this period. And the last part about the 2010s will focus on the context of global uprisings fueled by the global economic crises and the hacktivist experiences that had close relations with these uprisings.

3.1. Footsteps of hacktivism: Political engagement with computer and network technologies (1950-1980)

The roots of political hacking can be traced back to the 1950s in the elite university campuses in the US. In the 1930s and in the 1940s, the development of computer science was limited with code-making and code-breaking activities that would be used in World War II. In the 1950s, the U.S. Department of Defense turned to universities to develop cooperation for the research and development of computer science and engineering (Thomas, 2002, pp. 13-14). At this time, Soviet threats during the Cold War are considered as the reason of the governmental interest in computer technology. This interest was based on the need of a decentralized network, instead of a vulnerable center in case of attacks. Actually, alongside the pressure of the Cold War, government's interest in computer and network technologies lies also on the control capacity that these technologies provide on labor power (Hu, 2015, p. 18). For that reason, when the government developed

cooperation with universities, the interests of secrecy and national security of the World War II era was still alive but now both as an external and internal affair.

This political atmosphere gave rise to the first generation of computer hackers. Funded largely by the Department of Defense, computer scientists and engineers studied on computer and network technologies in the academic freedom of universities like Harvard, MIT, and Cornell. Computer enthusiasts of the 1950s were followed by the “hardware hackers” in the 1960s and by the “software hackers” in the 1970s (Jordan & Taylor, 2004, p. 10).

For example, ARPANET, one of the pioneers of what we know as internet now, was a military project funded by the Advanced Research Projects Agency (ARPA) of the Department of Defense to supply a secure communications system in case of a nuclear war (Thomas, 2002, pp. 14-16). It was developed with the collaboration of different universities and research centers in the US, including the University of Utah and the Stanford Research Institute that ARPANET linked for the first time as a digital network in 1969 (Hu, 2015, p. 5).

In a complete contradiction with the source of their military funding, these hackers founded the principles of *the Hacker Ethic*, a code that is followed by many hackers and hacktivists, even today:

Access to computers – and anything that might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!

All information should be free.

Mistrust Authority – Promote Decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.

(Levy, (1984) 2010, pp. 27-38)

This contradiction between the funding and the military/industrial usage of the technological results on one side, the political perspective of hackers on the other side can seem like an irony that Thomas expresses as, “while the ethic belonged to the hackers, the product belonged to the Department of Defense” (Thomas, 2002, p. 14). In this line, hackers with these liberal ideals fueled by left-wing anti-war protests of the 1960s constructed paradoxically the hardware and the software of the future military-industrial complex. Even though they possess a “fundamental anti-authoritarianism” (Lievrouw, 2011, p. 104), their works paved the way for the technologies of secrecy and surveillance. Actually, this contradictory relation between hackers and government is based on the dependency of hackers to their institutions for support and access to computers. Yet, these same hackers also gave birth to another tool that would break this dependency relation: the development of microcomputers, an early version of personal computers (PC). Next generations of hackers and hacktivists would rely on PCs and would act more independently from corporate and governmental institutions than their predecessors could have done (Thomas, 2002, pp. xi-x).

On the other side, alternative perspectives in the computer history warn against the fetishization of the role of the military in the development of computer and network technologies. For the reason that such an overestimation would necessitate to consider all digital networks with paranoia. Against this, Hu stresses that the “more utopian heritage” of the hackers who build these technologies is important to keep in mind (Hu, 2015, p. 34). The development of Usenet, called as the “poor man’s ARPANET,” in 1979 can be considered as one of the successors of such heritage. In practice, Usenet provided its users to post and to participate in the network, without political or financial connections that ARPANET required. In the political level, Usenet differentiated from ARPANET with its decentralized control system running by receivers. This system was in opposite with ARPANET’s system, a system based on a central control for all the material within the network (Hauben, 1996).

Even though this first generation of hackers had a political orientation that gave shape to their hacking activities, as *the Hacker Ethic* reveals and the development of Usenet concretizes, their hacking was not accompanied with an explicit political view. They mostly considered their hacking as an intellectual exercise to challenge the paradigms of

computer science. At this period, the public perception for hackers was in parallel with their self-consideration. Especially within the US, it was shaped with the success stories of these hackers, as many first generation hackers became important figures of Silicon Valley. At the end, not just *the Hacker Ethic* but even their hacker identity was lost in the public imaginary on behalf of “computer geniuses or nerds” (Thomas, 2002, p. ix).

This is how the roots of hacktivism were developed within the first generation of hackers in American universities. The technological development of computer and network technologies in the US was fueled by the threat perception of the American state from internal and external enemies gave rise to the formation of these actors. Even though they were funded by the military, anti-war movements and left-wing social movements in the 1960s shaped the liberal ideals of these hackers. These ideals would give birth to *the Hacker Ethic*, a manifesto based upon the freedom of information, a critical issue under neoliberal globalization that would be highly influential upon political hackers dating from the 1980s.

3.2. *Hacking against the neoliberal drive (the 1980s)*

The end of the 1970s is distinctive with the first attempts for the globalization marked with the neoliberal ideology. This process is defined with the reduction of national barriers in favor of the unconstrained movement of capital (Harvey, 2005, p. 11). Computer and network technologies have a central place in this new global political economy. They provided extraordinary increases in the capacity to process information in the sense of the volume, complexity and speed. Processing information became the main technological source of the economic, political, and social system to a degree that Castells would call this as the paradigm of “informationalism” (Castells, 2001). In this scheme, information technologies became the crucial intersection of global financial markets and global supply chain of production and consumption processes.⁴

In the early 1980s, ARPA’s Internet program created the common set of protocols TCP/IP (Transmission Control Protocol/Internet Protocol) that define how information

⁴ Detailed information about these aspects can be found in many important works. *Cyber-Proletariat* (2015) of Nick Dyer-Witheford is one of those works for those interested with the issue.

would be transmitted. These network connections would become “a de facto commercial standard in the 1980s” (Abbate, 1999, p. 147). TCP/IP, the basic of Internet technology, connected “noncommunicating islands of computer functionality” and facilitated “an increasingly supranational Internet community” (Schiller, 1999, p. xvi). This digital capacity to overcome national borders in favor of expansionary market logic gave rise to *digital capitalism*. This is a new political-economic epoch in which social and cultural range of the capitalist economy is unprecedentedly generalized by computer and network technologies (Schiller, xiv-xvii). The development of an “economywide network” that can support growing business processes can be seen as the main motivation of this digital construction (Schiller, 1999, p. 1). So, by the 1980s, new actors began to be added to the discussions about computer and network technologies. The controversy was transformed from whether it is a defense or academic research between governmental agents and academicians to an issue involving the arena of commerce and international politics. Conflicts between rival European and American business actors, as well as conflicts between computer manufacturers and telecommunications carriers would diversify the political aspect of computer and network technologies (Abbate, 1999, pp. 151-152).

On the other side, start-ups like Apple, Cisco Systems, Dell Computer, Oracle and Sun Microsystems that would become giant corporations became swiftly one of the most significant business components of this transformation. Actually, these corporations were founded with the contribution of the first generation of hackers. Therefore, the hacker culture was one of the fundamental components of informationalism (Castells, 2001, pp. 176-177).

The privatization of knowledge through the implementation of intellectual propriety (IP) rights was another characteristic of the global political economy of the 1980s. IP rights were lobbied heavily by new trade associations like the Intellectual Property Committee in the US and globally (Radikal, 2012, p. 71). In the US, IP rights were considered as a solution to the burgeoning trade deficit and to the inability of international competition against Japanese economic development (Sell, 2003, p. 99). This regime of IP rights aimed at creating a “knowledge scarcity” to commodify knowledge (May C. , 2010, p. 64). Yet, a new wave of political hacking challenged this political orientation based upon economic

needs of American capital in the 1980s. Free Software Foundation (FSF) is one of the early examples of this wave.

“Free software” means software that respects users’ freedom and community. Roughly, it means that the users have the freedom to run, copy, distribute, study, change and improve the software. Thus, “free software” is a matter of liberty, not price. To understand the concept, you should think of “free” as in “free speech,” not as in “free beer.”

(What is free software?, 2018)

This extract is from the website of the GNU project, a free software project that is the operating system designed by FSF. Founded in 1985 by Richard Stallman and other volunteers, the motivation behind FSF was to resist the proprietization of information. Even though IP rights regime was becoming one of the core aspects of the political economic system in the 1980s, hackers supporting free software were acting mostly “for the sake of affordable, better-built technology” rather than a radical challenge against capitalism (Radikal, 2012, pp. 70-71). In political sense, these hackers’ perspective can be framed as a liberal “critique of the neoliberal drive” with their “liberal themes and sensibilities” like “competitive mutual aid, avid free speech principles, and implementation of meritocracy” (Coleman, 2013, pp. 3-4). Still, their opposition to the IP rights regime would be the main reason of their criminalization in the 1990s (Dyer-Witheford, 2015, p. 65).

The 1990s would be the peak point of the wave of fear and fascination induced by the figure of the hacker in a global popular imaginary. This is a trend in fact born in the early 1980s. In *WarGames* (Badham, 1983), the earliest example of a hacker movie, hackers are represented as intrinsically dangerous in the sense that it is their knowledge and their skills what make them dangerous (Steinmetz, 2016, p. 180). In this sense, the danger of the hacker does not always come from the malicious intentions of hackers in the public imagery. The danger perception of hackers is closely related to the *risk* perception within computer and network technologies, as we will witness in the 1990s. However, in the 1990s, political hacking groups would be much more prepared to fight against this criminalization, too.

The *Cult of the Dead Cow (cDc)* is such a group that would lead the first attempts of deconstructing crime frames. Founded in the US in 1984 (Who We Be), the cDc is one of the oldest and most famous political hacking groups. Following the principles of *the Hacker Ethic*, the motivation of the cDc was in line with the motto of “the rights of all to information” (Jordan & Taylor, 2004, p. 98). The cDc is also an important group whose influence on the history of hacktivism cannot be restricted to the 1980s. They would be the one to coin the term hacktivism in 1994 and they would give rise to *Hacktivism* in 1999, one of the first self-claimed hacktivist groups that will be highly active in the 2000s.

However, it would be a mistake to think that this criminalization is a worldwide unified process. *The Chaos Computer Club (CCC)* from Germany is an important exception within hackers’ framing as criminals. Founded in 1981, CCC claims to be the largest hacker community in Europe (Chaos Computer Club). Since its foundation, the group actively opposes instruments of data collection by governmental bodies like data retention initiatives, biometric technologies and smart cards. In this line, they expose security breaches from German government related institutions (Bennett, 2008, pp. 52-53). These breaches show the vulnerabilities of central authorities. In this sense, this group relies on the principles of hacker ethic, too. This time, it is not the principle of “all information should be free” but another principle that they follow: “Mistrust authority [and] promote decentralization.” For example, to expose serious vulnerabilities in the computer systems that the German state uses, they hacked the German federal post and phone network Bildschirmtext (BTX) for a bank-robbery. Similar hacks that the group performed against the data retention centers of the German state created a positive perception in German public opinion for CCC. Quite different from the widespread criminal frames, CCC had a “Robin Hood-esque” perception. Many CCC members worked as ICT experts on issues like surveillance, IT legalization, and data retention in Germany (Cox, 2016). Even the espionage case on behalf of the Soviet Union in 1989 that some people in relation with the CCC were involved (Anderson, 2008, p. 5) did not change the positive perception of the CCC in Germany in the long term.

In sum, the global political economy shaped a political hacking experience struggling for the freedom of information in the 1980s. While some hackers became the founders or workers within the technology sector giants, others chose to follow the

principles of the *Hacker Ethic* by adjusting it to the needs of their time. For the 1980s, that adjustment meant an anti-IP rights advocacy based on the practice of developing free software. This confrontation provoked the construction of a crime perception for hackers, even though this generation of hackers was framing themselves within the liberal system. On the other hand, experiences like CCC from Germany showed that crime frames for hackers are not universally shared in every context. In the case of Germany, mistrusting central authorities became a principle shared both by hackers and by the public opinion that created a positive perception for hackers, to a point to understand the meaning of hacking as similar to ICT expertise. However, in the 1990s, the crime perception would be much more prevalent and it would become the turning point for the changing meaning of political hacking and the birth of the term *hactivism*.

3.3. Globalism is the enemy! Hactivism and anti-globalization (the 1990s)

The most important step of the 1990s for computer and network technologies is the development of a new Internet application, the World Wide Web, in the high-energy physics center CERN, Switzerland. Against the problems of locating and retrieving information in the earlier Internet, the Web provided a *hypertext*, a system of information organization that would link files located in different computers worldwide rather than a linear sending and receiving of information. Hacker culture was once again the impulse behind the development of the Web with the ideal of ensuring the participation of ordinary people to use computers. The Web was indeed a success to create an easy to access “pool of human knowledge” with the user-friendly hypertext organization and its enabling of multimedia information in Internet, as their developers wished it to be (Abbate, 1999, pp. 213-215).

On the other side, the success of the Web led to the popularization of internet. In 1992, approximately 4 million users were connected to Internet (Schiller, 1999, p. 12). Just within the three years between the first distribution of the Web by CERN in 1991 and 1994, more than a million copies of the first Web browser Mosaic was downloaded (Abbate, 1999, p. 217). Therefore, it resulted in an increasing interest from private sector to internet-related technologies. One example was the market-driven network development pushed by

the pressure from the American private corporate demand and supranational initiatives within the EU and the WTO (World Trade Organization) continued increasingly in the 1990s (Schiller, 1999, p. 203). In this perspective, the beginning of the 1990s was marked with a rapid restructuring of internet on “starkly neoliberal lines” (Schiller, 1999, p. 12). When information-oriented research and production processes were becoming the characteristic of all major businesses, the principle of “all information should be free” became to be considered as “subversive infringements on the rights of enterprise” (Schiller, 1999, p. 76). Following that, hackers’ framing as criminals was concretized via this opposition to corporate and governmental interests in the 1990s (Nissenbaum, 2004, p. 195).

In the mainstream media and culture, this opposition of the hacker culture against corporate and governmental power took the shape of a general fear from hackers based upon their ability to intervene in complexly networked communication technologies that the society has an increasing dependence upon. The antagonism between this dependence and social inabilities of controlling these technologies deepened the fear from hackers (Jordan & Taylor, 2004, p. 21). In the hacker imagery, a power that hacker/hactivist experience did not have was granted to the hackers in the 1990s. They were represented as some “omnipotent technological wizards” (Steinmetz, 2016, p. 181). This power imagery added to the crime frame transformed the meaning of hacker to something quite different from the initial meaning of hacking as the imaginative re-appropriation of technology’s potential. This is the period when the meaning of hacking became restricted to the illicit, illegal or unwanted computer intrusion. Movies like *Sneakers* (Robinson, 1992), *Hackers* (Softley, 1995), *the Net* (Winkler, 1995) are some of the hacker movies that reflect this crime perception.

Mentioned in the earlier part, the first self-claiming hactivist group Cult of the Dead Cow (cDc) had an explicit strategy to fight against this exaggerated and negative perception about hackers at this time. They were careful to humorously emphasize the divergence between crime frames about hackers and what they really do. Moreover, they prioritized to be visible in the mainstream media (Thomas, 2002, pp. 94-96). Even the coining of the term hactivism can be considered to be a tactic to fight against these prevalent crime framings of the 1990s. To invent a new category like hactivism is

instrumental to differentiate what they are doing from the negative hacker imagery circulated in the mainstream media.

Hacktivist experiences of the 1990s were also influential to feed the fear from hackers. It is not in the sense of being omnipotent internet villains but with their opposition to the neoliberal drive. These groups protested against national and international institutions within the larger struggle against neoliberal economic policies.

Electronic Disturbance Theater (EDT) is formed in 1998 to support EZLN (Zapatista National Liberation Army) and to protest violence against civilians in Mexico by using internet technologies. The EDT traces back its history to “Digital Zapatismo” emails sent to inform people all around the world about The First Declaration of the Lacandona Jungle on January 1, 1994, “one minute after midnight just as NAFTA⁵ went into effect” (Dominguez, 1999). In this way, the hacktivist group frames itself within the anti-globalization movement by supporting the Zapatista struggle (Jordan & Taylor, 2004, p. 72). The EDT became an influential group for the history of hacktivism with the tool that they developed for virtual sit-ins, the *FloodNet* software. The group describes FloodNet as “a symbolic gesture against an opponent’s website” by repeatedly sending browser reload commands (Wray, 1998). During 1998, the EDT targeted websites of Mexican presidency, the Pentagon, the White House, and the Frankfurt Stock Exchange with 18,000 participants for 13 hacking (Sauter, 2014, p. 111). The group’s motivations are mainly directed to create an international support for the Zapatistas and they target the Mexican government, the US military, and symbols of international capital (Wray, 1998). The EDT sought to arouse the media attention for the Zapatista cause. In this sense, the slowing or crashing of servers that was the result of their denial-of-service (DOS) attacks was not their main objectives but an instrument for that media attention (Samuel, 2004, p. 76). So when the New York Times framed them as “the first post-modern revolution,” it was a success for them (Dominguez, 1999). Even though they had this positive perception from the mainstream media, they felt the need to diverge themselves from the labels of cyber-crime and cyber-terrorism. For that reason, they self-framed as “net art performers,” in opposition to “the real cyber-terrorists”

⁵ Free Trade Agreement between Canada, U.S.A, and Mexico.

(Dominguez, 1999). The approach to the label of cyber-terrorism would be different for *Electrohippies Collective* from the UK.

Electrohippies, another hacktivist group of the 1990s, was also in line with the anti-globalization movement. They participated to the protests in 1999 against the World Trade Organization in Seattle and used the tactics that were developed by the EDT (Jordan, 2002, p. 8). Following the street protests in Seattle that aimed to physically block the conference, Electrohippies used distributed denial-of-service (DDOS) attacks to the WTO website. They declared that they acted “to prevent the most visible global neo-liberal organising institution from functioning” (Jordan & Taylor, 2004, p. 75), even it was for a temporary period. For the Seattle protest, the group claims to gather 450,000 protesters for the DDOS attack against the WTO with the aim to open a public dialogue about the organization itself (Electrohippies Collective, 2000a). For Electrohippies, anti-globalization was fueled with an anti-corporatism that was concretized with a strong protest against the commercialization of the internet (Samuel, 2004, p. 70). They cherished free and open-source software, the products of earlier hacker generations, as important tools for “a new hopeful future” (Electrohippies Collective, 2000b). Different from the EDT, Electrohippies Collective was perceived more negatively and was labelled as terrorists after their WTO protests (Electrohippies Collective, 2000a). This label would be an expending umbrella at the beginning of the 2000s with the World Trade Center attacks at September 11, 2001.

Briefly, in the 1990s, new computer and network technologies enabled changes in the global political economy, as well as inspiring new experiences of political hacking. In a very short time span, internet became a popular tool for large populations that would provoke the commercialization of the internet. This commercialization was also in line with the neoliberal restructuring of global economy. As the network of networks, internet became the tool *par excellence* for the unconstrained movement of capital. This centrality of the internet in the global political economy gave rise to hacking a meaning in accordance with its crime perception because of the potential that hackers are vested with and the risk that they pose. Popular culture products, especially movies, became the tool to popularize this criminalization of hackers. The coining of the term hacktivism is the fruit of this atmosphere, as an effort to differentiate political hacking from the pejorative connotations prevalent in the popular imagery. Parallel with that, hacktivist groups of the 1990s began to

struggle with crime frames against hackers that would soon transform to (cyber)terror frames by the beginning of the 2000s. The crime perception of political hackers increased also with the political inclination of hacktivist examples in the 1990s. Anti-globalization and anti-corporate tendencies of these groups nourished terrorist frames for political hackers even before the proliferation of such labels after 9/11. The oncoming decade would be distinctive with this labelling that would be influential on the perception of specific political hacker groups.

3.4. Globalism is still the enemy! The rise of patriotic hacking (the 2000s)

9/11 can be thought as the most influential event of the beginning of the 2000s for its power to establish a worldwide discourse on terrorism. That does not mean that the attacks on World Trade Center by Al-Qaeda created this discourse out of nothing but it fortified its effectiveness through legal and extra-legal (warfare) activities. The perception of political hacking and hacktivism was also affected by this terrorism discourse. They became to be less and less framed as activism or criminal activity and more like an issue of online security and terrorism after 9/11, especially within the American mainstream media (Vegh, 2005, p. 6). Mixed categories like “cyber-vandals, hackers, or potential cyberterrorists” produced a negative perception that enabled laws and regulations that consider hacktivism not as an alternative way of advocacy and political protest but as an act that should be prohibited by laws and regulations (Vegh, 2005, p. 10).

Electrohippies Collective challenged explicitly this discourse. First they emphasized that they are not cyber-terrorists. They did not do this by differentiating themselves from another group that they indicate as terrorist. They problematized the concept of terror itself. For them, the War against Terrorism (TWAT) was a pretext to militarize the control of undesirable activities by certain groups and justify this control by extreme measures (Electrohippies Collective, 2001). Talking from the British context, they considered new laws of their time – European Cybercrime Convention, the Terrorism Act, and the Regulation of Investigatory Powers (RIP) Act – as ways to criminalize collective action in the internet, especially anti-capitalist protests (Electrohippies Collective, 2001). However

not all hacktivist experiences of the 2000s were sharing the same critical attitude against terror framings against online action.

The 2000s were a fertile decade for different hacktivist experiences. For example, *Hactivismo*, the hacktivist organization founded in 1999 by the earlier famous the Cult of the Dead Cow (cDc), became highly active by the beginning of the 2000s. Targeting internet censorship in authoritarian regimes, they struggled against restrictions of free speech in non-Western contexts. In 2002, they developed a distributed network application named *peek-a-booty*, a tool – that they describe its function as – to allow users to “bypass firewalls, national or corporate, and access the free side of the Web from a host computer” (Ruffin, 2004). *Hactivismo*’s acts are in general against the censoring mechanisms – like firewalls – of national governments (Jordan & Taylor, 2004, p. 98). The main target of their acts is “the Great Firewall of China,” the censoring mechanism in China (Ruffin, 2004).

Hactivismo members framed themselves as “hackers and free speech advocates (...) developing technologies to challenge state-sponsored censorship of the Internet” (The *Hactivismo* Declaration, 2001). However, their targeting of national states fed another type of hacktivism that was already on rise; “patriotic hacking” (Denning, 2011).

3.4.1. Patriotic hacking experiences in different contexts

At the end of the 2010s, nationalism is a hot topic to be discussed based upon Western contexts. However, in the case of patriotic hacking, it takes its source from the nationalist wave of the 1990s. This period witnessed nationalist reactions from diverse contexts around the world. That was mostly the result of the neoliberal globalization that reduced national barriers. The aggressive marketization of previously public domains created a prevalent discontent among populations in the rest of the world. In specific contexts, this discontent was directed to foreign investment. China in the late 1990s and in the beginning of the 2000s is one of such contexts where nationalism is consciously triggered as a solution to ideological problems within the political system and fueled by the economic competition with the US-based capital.

Apart from the reaction to the neoliberal globalization, patriotic hacking has direct relations with much older international conflicts, as the ones between Israel and Palestine,

India and Pakistan, China and the US (Samuel, 2004, p. 52). This type of political hacking can be defined as attacks against the websites and email accounts that are considered threatening or harmful against the interests of the mother country – or the country of ethnic origin – of attacking hackers (Denning, 2011, p. 178). The beginning of the 2000s is marked with a considerable increase in patriotic hacking experiences (Anderson, 2008, p. 6).

An example is *World's Fantabulous Defacers (WFD)*, a pro-Palestinian hacker group reported to be from Pakistan. They defaced websites to draw attention to human rights violations of Muslim populations in Palestine, Kashmir, Chechnya and the former Yugoslavia (Samuel, 2004, pp. 55-56). This group defaced 349 websites between November 2000 and November 2002 (zone-h). Even though WFD frames its struggle in human rights discourse, the perception of this hacker group is oriented to see them as cyberterrorists. The reason of this perception is that their acts coincide with the islamophobia fueled with the terror discourse after 9/11.

In East Asia, the aggression of Chinese and Korean hackers against Japanese institutions and companies originates from the Second World War. This aggression is consolidated through economic rivalry of recent decades. The history of patriotic hacking in China goes back to the protests against anti-Chinese riots in Indonesia in 1998. The creation of *the Honker Union of China* was due to the union of two former Chinese hacker groups, *the Green Army* and *China Eagle Union*, both founded in 1997 (Denning, 2011, p. 178). Many independent websites where members are being educated on computer attacks constitute the larger unity named the Honker Union of China (Henderson, 2007, p. 7). This organization structure explains the incredibly high number of its participants, with an estimated 50,000 to 60,000 members in 2001, even though most members knew very little about computer networks and hacking (Denning, 2011, p. 179).

Between 1999 and 2004, the Honker Union of China was very active and led many attacks against Taiwanese, Japanese, and American websites with website defacements (Yip & Webber, 2011). This high activity of the group coincides with the timing of the protests of Hacktivism against the Chinese government. Chinese nationalist hackers' aggression can be thought as a reaction to this other hacktivist experience. In a globalized world, no experience is shaped separately from another.

Patriotic hacking did not come to an end in China by the end of the 2000s. In 2013, the Honker Union of China was still in the news, with their threats against Japanese institutions, including government and media websites, at the anniversary of the Manchurian Incident of 1931 ('Honker Union' sniffs 270 hacktivism targets, 2013).

In China, there was a strong relation between the Chinese state and patriotic hackers that can be explained with ideological affinity. Chinese government introduced a patriotic education campaign in 1991, as a remedy to the ideological crisis of Chinese Communist Party in the 1980s. Reflections of this campaign can be seen among Chinese hackers with their feelings of “national humiliation” and nationalist revenge against foreign pressures. The Chinese state has encouraged this nationalist digital activism that they believed less harmless than offline protests (Yip & Webber, 2011). Chinese state’s positive perception of Chinese patriotic hackers is a regular example for governments’ sponsoring of patriotic hacking when it is in their favor. However, patriotic hacking is still illegal in many jurisdictions worldwide, including governments sponsoring patriotic hackers (Samuel, 2004, p. 52).

While WFD was emphasizing the human rights framing for Muslim populations, the nationalism of the Honker Union of China was much more aggressive, as it is explicit in their website defacements with slogans like “blood for blood” when they were protesting the assaults against ethnic Chinese population in Indonesia in 1998 (Dahong, 2005). This ideological difference that is reflected in their framings can be explained by the difference between the perceptions – active support or passive non-intervention – of relevant governments.

3.4.2. Patriotic hacking experiences in Turkey

In Turkey, patriotic hacking was very popular among hackers, too. Many groups and individuals attacked websites with nationalist motivations since the 1990s (Eriş, 2009). Similar to the attacks of the Honker Union of China against activists and dissidents within China, Turkish patriotic hackers target the websites of political groups – mostly leftists, Kurdish, and identity-based advocacy groups.

One of the earliest examples of patriotic hacking is the defacement of the website of DHKP-C – a leftist radical and illegal organization in Turkey – in 2000. *Digital Angels Team* who performed the hack left a message saying that they carried out this hack “in the name of the Turkish people” (Hürriyet, 2000). In 2003, *Cyber-WARRIOR Hack Team* hacked American websites to protest Süleymaniye attack, known as the Hood Event in which Turkish military officers were questioned by American army in Iraq (Milliyet, 2003). This event had been perceived as an insult by the Turkish state, as well as by the mainstream media. So, this hack originated from a vengeance feeling against this perceived insult.

Another nationalist hacker experience is not a group but a hacker named *Iskorpitx*. She defaced 21,549 websites in one shot and put the Turkish flag to the targeted websites, alongside insults against Greece, PKK, Armenians and France. First three are the common enemies of Turkish nationalism. In this case, French websites – not a frequent target for Turkish patriotic hackers – were also hacked because this hack was a protest against the draft law on the Armenian Genocide, as the hacker reveals in an interview (Hürriyet, 2006). According to the Zone-H, hacks like this made Turkey “the new defacers kingdom” (Zone-h, 2006). By October 2018, the number of the defaced websites by *Iskorpitx* is 471,573 (*iskorpitx*). This patriotic hacker frames her motivation as “protest” by “replying to what is done to Turks in the digital realm” (Hürriyet, 2006). Offensive language framed as a response to what others have done to *us*, this verbal violence framed as a necessity is a frequent feature of offline nationalism.

Another example is *Ayyıldız Tim*, one of the largest and well-known patriotic hacking groups of Turkey. Founded in 2002, they define their mission as “lobbying voluntary against cyber-attacks targeting Turkey” and their ideology as “statism,” with an explicit reference to one of the six official principles of Kemalism. The group aims to protect state institutions, statesman, and “our” moral values and is strictly against “political topics” neither in their website nor in their social media accounts. This point may seem paradoxical for a highly politicized group but here “political” means all that is excluded by the kemalist ideology (Ayyıldız Tim, n.d.). Within this nationalist mission, Ayyıldız Tim attacked many websites. For example, in 2009, they attacked the official link of Armenia under the website of the United Nations, to protest the ethnic violence of China against

Uyghurs in Xinjiang. The reason of this hacking is said to protest the passive attitude of the United Nations about this issue (Türkiye Gazetesi, Türk hackerlar BM'nin sitesini çökertti, 2009). More complicated reason of the choice of the Armenian link lies in a pure racism, most probably through an indirect reaction to the attention given by “Western countries” to the Armenian genocide but not to the problems of Turkics. At the first glance, protecting Uyghurs motivation of Ayyıldız Tim seems like the human rights discourse that pro-Palestinian groups use performing their patriotic hacking. However, targeting Armenian websites reminds the aggressive framing of Chinese patriotic hackers’ nationalism.

Ayyıldız Tim has an ideological affinity with the Turkish state, through its nationalism and statism. Many privileges accompany this affinity. Even though it is a hacker organization that performs website attacks, illegal acts according to the Turkish Penal Code (TPC) no. 244 (Eralp, 2011), they can make calls for recruits through its website and twitter accounts (Ayyıldız Tim, n.d.). From national TV channels, one of its members, claiming to be a high ranking member of the group, can make the propaganda of the group without hiding his identity, and he does not undergo any judicial process (Ayyıldız Tim, 2016). Patriotic hacking in Turkey has a privileged place within the political system even though its deeds are outlaw, according to TPC. But in the mainstream media, these patriotic hackers are not framed as cybercriminals in Turkey. In the 2010s, experiences like Ayyıldız Tim would continue to exist. However, this time, another hacktivist experience would be much more popular: leak hacktivism.

Even though the concept of hacktivism was born in the 1990s, the 2000s exhibited the richness of hacktivism by hosting so many different hacktivist experiences from diverse contexts, including but not limited to China, Pakistan, and Turkey. This richness comes undeniably from the popularization of patriotic hacking. Apart from them, hacktivist experiences following the traditions, ideologies and methods of earlier hacktivist examples from the 1990s were also significant to criticize the perceptions of hacktivism and influence new hacktivist experiences. In sum, the widespread terrorism discourse fueled by 9/11 and the prevalence of patriotic hacker groups emerged in accordance with the aggressive globalization of neoliberal politics created a new meaning for political hacking. In parallel with the crime framing for hacking in the 1990s, hacktivism gained the meaning of (cyber)terrorism by the 2000s.

3.5. Time of crises, time of uprisings (the 2010s)

The 1990s was a period when computer and network technologies were popularized and then privatized in a very short time. Almost twenty years after that, the globally networked economic system was totally dependent to these technologies. During the financial crisis of 2007-2008, we witnessed how this worldwide system arose thanks to these technologies created a destructive domino effect in all national economies worldwide. With this global crisis, the discourses on stability, equilibrium, and security of capitalism that the motto “there is no alternative”⁶ emblemized has vanished to be substituted with an emphasis on “chaotic volatility” (Dyer-Witheford, 2015, p. 21). In parallel, the crisis deepened the vulnerability felt from network technologies upon which neoliberal globalism heavily depends. This crisis atmosphere nourished the fear from hackers, too, as the unpredictable specialists of the vulnerable technologies. In parallel, it strengthened the label of cyberterrorism for hackers and hacktivists.

Other economic crises followed the financial crisis. 2007-2008 World Food Price Crisis and European Debt Crisis that began with the Greek Crisis in 2009 were the most important ones. The accumulation of those global economic crises resulted in decreasing life standards for populations living in different contexts. Following that, anti-austerity movements and anti-governmental uprisings became widespread in many countries at the first half of the 2010s, including Greece (2010), Tunisia (2010), Egypt (2011), Bahrain (2011), Spain (2011), the US (2011), Turkey (2013), and Brazil (2013).

Alongside economic, political, and social reasons of these uprisings, technological tools used by the protesters during these uprisings became a huge topic. Network technologies had undoubtedly a central role in sharing the information and in gathering people together during these events gone as far as to be called as *Twitter Revolution*. The rising star of the 2010s was a peculiar technological development of network technologies: social network sites (SNSs). SNSs are “web-based services that allow individuals to construct a public or semi-public profile within a bound system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections

⁶ The famous slogan used by British Prime Minister Margaret Thatcher in the 1980s to promote neoliberalism.

and those made by others within the system” (Boyd & Ellison, 2007). First SNSs emerged at the end of the 1990s and they became popular by the middle of the 2000s with millions of users (Ellison & Boyd, 2013, p. 151). In 2018, Facebook, as the most popular SNS worldwide by user numbers, has approximately 2.5 billion users (Internet Live Stats). From 2005 to 2018, individuals using the internet escalated from 1 billion to more than 3.5 billion with more than the half of the world population (International Telecommunication Union, 2018, p. 13). That means that in 2018, more than 70% of worldwide internet users use one SNS at least. About daily activity of SNSs, Twitter’s popularity is significant. From 2007 to 2013, tweets per day escalated from 5,000 to 500 million (Internet Live Stats).

Through this popularity of SNSs and its widespread usage within global uprisings, a new hacktivist experience began to be shaped. I call this experience leak hacktivism. Similar to leak journalism, the main purpose of these groups is to leak information from hierarchical power structures, nation-states and corporations to create a public opinion.

3.5.1. Leak hacktivism: WikiLeaks and Tunisian uprising

Anonymous can be considered as the most famous hacktivist group of our time. Its history can be traced back the “popular, iconic, and opprobrious imageboard” (Coleman, 2014, p. 41) *4chan* launched in 2003. As early as 2006, the idea of *Anonymous* began to be concretized with online political raids conducted by the users of *4chan*, as in the example of radio host Hal Turner who was targeted by anonymous trolls because he was racist (Coleman, 2014, p. 65). In February 2008, *Anonymous* attacked the Church of Scientology. This time the attack was not just on the digital; it was accompanied with a call to protest in street that thousands of *Anons* and supporters followed with Guy Fawkes masks (Coleman, 2014, pp. 63-64). With *Project Chanology* – the name given to the attacks against the Church of Scientology, *Anonymous* began to act more like a group organized through specific IRC channels than raider-trolls of the internet (Coleman, 2014, p. 75). In Fall 2010, the IRC network named *AnonOps* – “a new direct action-oriented wing” (Coleman, 2014, p. 95) – began to use the name *Anonymous* for several DDOS attacks on pro-copyright groups to protest the corporate attacks against copyright infringer websites like the Pirate

Bay. Within this *Operation Payback*, the name *Anonymous* became a banner for their activism and the media attention fueled and solidified this formation (pp. 105-106).

When *Anonymous* began to be interested to WikiLeaks, first steps to leak hacktivism were taken. In November 2010, after the immense release of US diplomatic cables by WikiLeaks and the examination of these cables in distinguished newspapers in worldwide, Amazon, MasterCard, and PayPal interrupted all their commercial services to WikiLeaks. This included transferring of donations and providing website hosting (Coleman, 2014, pp. 118-119). In December 2010, AnonOps engaged to perform a DDOS campaign against these financial corporations under the name *Operation Avenge Assange* (p. 3). It was the largest single digital direct action campaign in the internet with over seven thousand individuals logging to the IRC channel where this operation were discussed (p. 120) and with the boosting of botnets – “an army of zombie computers” (p. 137).

After *Operation Avenge Assange*, the most remarkable deed of Anonymous was *Operation Tunisia*. In January 2011, Anonymous officially declared its Operation Tunisia with a press release that warns the Tunisian government, especially on the issue of its regime of heavy censorship (2014, p. 148). In fact, when Wikileaks released the cables, they had decided to be in contact with some local initiatives. Tunisia and Nawaat Wikileaks were one of this contact points. So, *Tunileaks* about the corruption of the government were known to Tunisians right after the release was effectuated. Three weeks after the release of translated cables by Nawaat Wikileaks, the protests began by enraged people by the death of Bouazizi.⁷ During Operation Tunisia, Anonymous provided technical assistance to protestors by “acting like digital courier pigeons to get word and videos out Tunisia,” launching DDOS attacks against official websites of the government, and by ensuring anonymous connection between protestors (Coleman, 2014, pp. 149-153). Through its involvement with Tunisian uprising, Anonymous gave the first example of how a hacktivist group can effectively share information leak about governmental corruptions to trigger widespread protest. Moreover, they followed the tradition of hacktivists struggling against internet censorship in authoritarian regimes by providing technical assistance for safe internet connection.

⁷ Mohamed Bouazizi is the Tunisian street vendor who became the trigger and the symbol of Tunisian uprising by his self-immolation.

Until its involvement with WikiLeaks, the perception of Anonymous was in line with the popular imagery of hackers from the 1990s. They were labelled as “a hacker gang,” “Internet hate machine,” and “domestic terrorists” (Fox News, 2007). Yet these labels were not sophisticated ones and they soon became a fertile source for internet trolls of Anonymous. Trolls ridiculed these labels by their lack of internet culture and Anonymous used this gap to frame themselves as fighters of human rights and freedom of speech. They also used this media labelling to attract new participants as well as the attention of international media (Cavelty & Jaeger, 2015, p. 186). However, with their inclination to leak hacktivism, Anonymous became the object of a securitization process conducted by the US state (Cavelty & Jaeger, 2015, p. 177). Leak hacktivism of Anonymous took the meaning of “a national security issue” based on how the group’s attacks endangered critical infrastructures – the financial sector – during *Operation Avenge Assange* (p. 189). In 2012, not just the populist Fox news but also the US state framed Anonymous members as “possible terrorist organisation members” (Pilkington, 2015). Using labels like “terrorist sleeper cells” for Anonymous is another version of what political power did in the 1990s against the risk of political hackers struggling for the freedom of information and against the privatization of internet. The terrorist perception of hacktivism became an instrument for more surveillance power in internet through the construction of fear from digital protest and from loss of power (Cavelty & Jaeger, 2015, pp. 190-191). Yet, different from their antecedents, Anonymous could use the popularity of SNSs to circulate their propaganda videos to create a positive public opinion about their deeds. For that reason, they had a power that none other hacktivist groups had about their self-perception. The popularity of hacktivism and its positive perception in the media can be traced to the new wave of interest for hacker movies in the mainstream media, as *Who am I?* (bo Odar, 2014), *Mr. Robot* (Esmail, Golin, & Hamilton, 2015-2018), and *Hacker* (Satayev, 2016).

3.5.2. Leak hacktivism in Turkey

Influenced by the global economic crises and increasing authoritarianism, Turkey also witnessed a mass popular uprising in May-June 2013, Gezi protests. Redhack, a hacktivist

organization founded in 1997, became highly popular in this year of crises and uprisings of 2013. As a self-identified Marxist-Leninist hacktivist group (RedHack ODTU'de!, 2013), Redhack diverges clearly from other hacktivist groups in Turkey, most of whom are patriotic hackers.

Website defacements, DDOS attacks and information leaks are the principal tools that they use. They defaced hundreds of public websites (and few company websites) to protest an event, to support offline protests, or to commemorate the martyrs of the revolution, a notion borrowed from leftist culture. The group's popularity began to arise with their first known leak from the Ankara Police Directorate website in February 2012 to publicize the information about the citizen informants who had sent emails to the police directorate (Radikal, 2012).

Redhack had already had an attraction at the beginning of 2013 through their many hacks up until then and their successful interaction with their audience in SNSs. However, it was actually the Gezi protests that put the hacktivist group under spotlight. Part of a larger protest cycle in Turkey (Yörük & Yüksel, 2014, p. 121) and also of the global wave of uprisings in some of the Mediterranean countries, Gezi uprising was “a resistance against the commodification of urban space, nature and everyday life for the reproduction of capital, as well as the conservative authoritarianism of the party in power, the AKP” triggered by an urban regeneration project (Ercan & Oğuz, 2014, p. 114). According to the estimations, approximately 2.5 million people participated in the protests during that time in 79 cities of Turkey (Ercan & Oğuz, 2014, p. 114). 1.5 of them were in Istanbul, corresponding to 16% of the city's population (Yörük & Yüksel, 2014, p. 105).

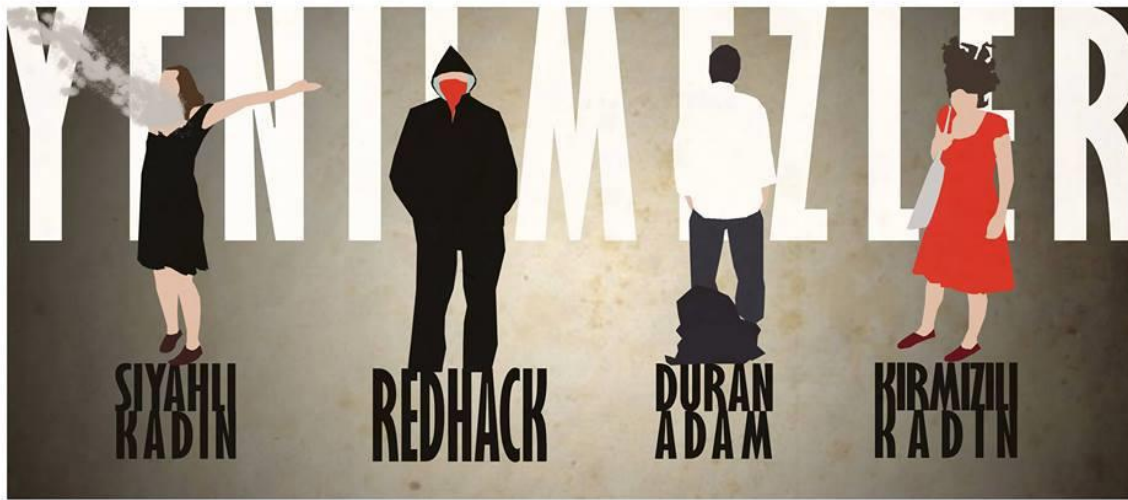


Figure 3.1: Title in white: Avengers [Invincibles]; Titles in black: Girl in Black, Redhack, Standing Man, Lady in Red (Resistart 2013, translated by Resistart).

Redhack quickly became one of the main spokesmen of the Gezi protests, as far as becoming a symbol. By a reference to the Turkish translation of the Hollywood movie *The Avengers* (Whedon, 2012), a dozen individuals and few organizations became part of the Gezi imagery by being called “Invincibles.” Among these figures, Redhack was the only group possessing a leftist ideology. Actually Redhack shared many characteristics with other leftist groups that participated to the heterogeneous whole of the Gezi protests. Similar to these groups, Redhack defined their aim as to propagate the idea of revolution (Redhack, 2012). This similarity was met positively by leftist circles to the degree of defining Redhack as a “cyber armed propaganda organization” (Yıldırım, 2014) while for the protesters in the Gezi uprising, the group soon became an object of the nostalgia for the romantic revolutionary ideal through their frequent reference to the Golden Age of the Turkish left, the 1970s. The fact that this nostalgia was fulfilled through a hacker group was the peculiarity of the Turkish context.

Undoubtedly, the group’s satirical and confident tone that emphasized persistently the technological incompetence of their targets in opposition to their competence also helped to create an aura around the group. In that line, famous slogans used by Redhack as “Hak yiyen hack yer [Those who act unjust would be hacked]” and “Nush ile uslanmayanı etmeli tekdir, tekdir ile uslanmayanın hakkı Redhack’tir [those who cannot be disciplined

with advice should be scolded, those who cannot be disciplined with scolding deserve Redhack]” would be embraced by the audience of the group in SNSs as well as protesters in the streets. This aura would excite the masses participating to the Gezi protests and would last as long as the group kept being active.



Figure 3.2: The banner says “those who cannot be disciplined with advice should be scolded, those who cannot be disciplined with scolding deserve Redhack (this is an adaptation from a famous aphorism through a vocal wordplay between kötek [stick that can be used for beating] and Redhack. This adapted aphorism was first used by the group in their Twitter account.

After the passive period between 2014 and 2016 during which the group had to deal with inner problems, Redhack came to the fore once again with a sensational data leak. In September 2016, Redhack declared that they had hacked the email account of the contemporary Minister of Energy Albayrak, also the son-in-law of President Erdogan. They said that they would publicize the content if the leftist dissidents who were taken into custody during the state of emergency were not released (Birgün, 2016). Albayrak’s emails included information about the formation of Twitter troll armies dating back to the Gezi protests (Sozeri, 2016). The most politically delicate issue involved emails that showed the close relationship between Albayrak and Powertrans, an oil company implicated in deals with oil produced by ISIS (Islamic State of Iraq and the Levant) (Independent, 2016). Similar to earlier data leaks performed by the group, this leak would also trigger judicial processes about Redhack in which charges of terrorism would appear.

Similar to how Anonymous was framed as terrorist and as a national security issue, Redhack was perceived mostly as terrorist by the Turkish state. Yet, as Anonymous,

Redhack also used SNSs to propagate about their own self-perception. Their Twitter accounts became the central place of communication for the hacktivist group. In this framework, the perception of Redhack in mainstream media, social media, and even in the changing nature of the state discourse were not that clear about how to perceive and how to give a meaning to this leak hacktivism experience of Redhack. This peculiarity was closely related to the Turkish context, about larger issues concerning meanings of political protest, digital action, cybercrime, terrorism that need to be discovered to understand the implications of the meaning of hacktivism in Turkey in the 2010s.

3.6. Conclusion

In this chapter, hacktivist experiences were exhibited in relation with their perceptions and changing meanings. Leak hacktivism – as I call it – that will be the topic of this study from now on was born from this historical context. This hacktivist experience of the 2010 demonstrated how hacktivist groups' involvement with popular uprisings of the 2010s influenced changing perceptions about these hacktivist experiences. Influenced heavily by global economic crises, large populations in different contexts chose to protest collectively against diverse economic, political and social problems. Emerging technologies like SNSs enabled these gatherings by providing affordances of information sharing and organization. Hacktivism of the 2010s emphasized the necessity to publicize the information kept secret from populations. In line with the *All information should be free* motto of the first generation of political hackers, leak hacktivists adapted political hacking to the needs of the 2010s. This experience brought new perceptions about hacktivism, alongside strengthening criminalization of it through terrorism labels. Yet, that does not mean that all perceptions about hacktivist experiences are constructed in a clear-cut way to nourish unified criminalization processes. Especially the development of new network technologies increased the visibility of different perspectives about how to perceive hacktivism and how to give a meaning to contemporary hacktivist experiences. Following that, changing meanings of hacktivism can be understood just through a deep contextualization of these diverse perceptions that would shape new meanings to hacktivism.

CHAPTER 4

HACKTIVIST EXPERIENCE IN TURKEY:

THE CASE STUDY OF REDHACK

The historical chapter about different hacktivist experiences and diverse perceptions exhibited the changing meanings of hacktivism dependent on the context. Redhack, the hacktivist group from Turkey, was included in the wave of leak hacktivism of the 2010s. Influenced by the popular uprisings in many different countries at the beginning of the 2010s, as well as influencing them, leak hacktivism aimed for the creation of public opinion through the leaked information from nation-states and corporations. Now, beginning with this chapter, I will focus on the case of Redhack and in this way, I will aim to uncover the criminalization of the group with a detailed examination of the crime frames surrounding the group. Thus, the contextual meaning of hacktivism in Turkey in the 2010s can be understood.

For this purpose, the chapter will be constructed in the following way. First, I will exhibit the acts of Redhack by a binary classification. In the first table, information leaks of Redhack will be demonstrated. In the second one, I will present data interference⁸ acts of Redhack, in which several website defacements of the group will be included, too. A discussion about the techniques and another one about the motivations of Redhack will emerge based upon these acts. After that part, judicial processes related to these acts will be shown. I will feature two discussions based upon these processes: the oscillation of the judicial perspective between cybercrime and terror and the change in the target of judicial processes. This chapter will be a reference for the following chapters about the crime

⁸ Data interference is used as the umbrella term to indicate diverse acts of the group, including website defacement, website crash, unauthorized access, data alteration and other acts.

frames of Redhack where the construction and the perception of the framing will be analyzed.

4.1. The acts of Redhack

Redhack became a known hacktivist group in the national scale with their major data leaks between 2012 and 2016. It was these acts that made them one of the important experiences of leak hacktivism in the 2010s. Between their first known leak from the Ankara Police Directorate website in February 2012 and their last leak from the email account of then Minister of Energy and Natural Resources Berat Albayrak in September 2016, they hacked many other governmental websites and the email accounts of political actors for information leaks.

The acts of Redhack are studied by different researchers (Gökdemir, 2013; Yaman U. , 2013; Uçkan, 2013; Polat, Tokgöz Bakıroğlu, & Demirhan Sayın, 2013; Yegen, 2014; Akin & Zıraman, 2015; Akser, 2015; Tatar & Çelik, 2015). Some of these works are not purely academic studies. Especially earlier works reflect the enthusiasm about the presence of a dissident hacktivist group in Turkey (Gökdemir, 2013; Yaman U. , 2013; Uçkan, 2013). The academic focus became more visible in later works. Alongside studies on the perception about Redhack (Polat, Tokgöz Bakıroğlu, & Demirhan Sayın, 2013), descriptive studies (Yegen, 2014; Akser, 2015), and mainstream criminology studies examining Redhack as a case in point with the aim of preventing the cyber threat (Tatar & Çelik, 2015), elaborated works in which Redhack is examined within larger theoretical discussions also appeared in recent years (Akin & Zıraman, 2015).

Methodologically, while the works of Uçkan (2013) and Tatar & Çelik (2015) presented the acts of Redhack based on news media sources, Yegen (2014) referred to the Wikipedia article about Redhack. In other works, there was no reference about the acts of the group. For that reason, I preferred to refer not just to news media but also use primary sources, as the group's own declarations, to exhibit more systematically the acts of Redhack.⁹

⁹ I must notice that the acts of Redhack, especially the leaks that are cited in the first table are the acts alleged by the group Redhack and not all of them are admitted officially by their alleged sources. Similarly, the

In the case of Redhack, the richest source of data is Twitter, as the group used this social media platform intensely for their propaganda. Twitter was first launched in 2006 as a friend-following and messaging platform. However, Twitter soon became a “real-time information and a place for debate in news, politics, business, and entertainment” (Weller, Bruns, Burgess, Mahrt, & Puschmann, 2014, p. xxx). During the time the group Redhack was an active user, Twitter was a quite popular platform with its worldwide users escalating from 138 million in the first quarter of 2012 to 336 million in the first quarter of 2018¹⁰ (Statista, 2019). For Turkey, the number of Twitter users increased from 1.8 million to 9.5 million during the Gezi uprising (Yaman A. , 2014, p. 21). In 2015, it had 10.3 million users in Turkey (Doğu, 2017, p. 4). Since the mass popular uprising of the Gezi protests in 2013, Twitter is considered as an alternative political platform in Turkey (Doğu, 2017, p. 4) and it can be seen as a key to Turkey’s politics (Bulut & Yörük, 2017, p. 4097).

Redhack’s use of Twitter is part of this larger significance of the platform in the nation-scale context. The group’s popularity in Twitter, their excessive use during their high activity, and their repeated exclusion from the platform with suspended and withheld accounts, all are the reflections of the political tensions in Turkey. Especially during 2012-2014, Redhack used the success of Twitter to be a flexible “platform for public communication at various levels of public-ness” (Bruns & Moe, 2014, p. 21). This publicness is created through different levels of communication offered by the platform, as macro (public level of hashtags), meso (personal public level of follower networks), and micro levels (interpersonal level of replies) (Bruns & Moe, 2014, p. 20). In this period, Redhack became highly popular in Twitter through their Twitter accounts and these accounts became the source of information for news media in their news about the group.

motivations category exhibits the explicit motivations declared by the group. Still, the acts figuring in the tables are the ones that were mentioned by external sources than the tweets from the accounts mentioning Redhack and the official account of Redhack (@TheRedHack). I excluded a small amount of the acts mentioned in the collected tweets, about which I could not find any news media or archive source mentioning these acts.

¹⁰ March 2018 is the end date when the account of Redhack (@TheRedHack) was accessed from outside the borders of Turkey. The account is inaccessible within Turkey in response to a legal demand. For that reason, I determined this date as my end date of Twitter data. This time period is large enough to exhibit the declining use of Twitter by the group.

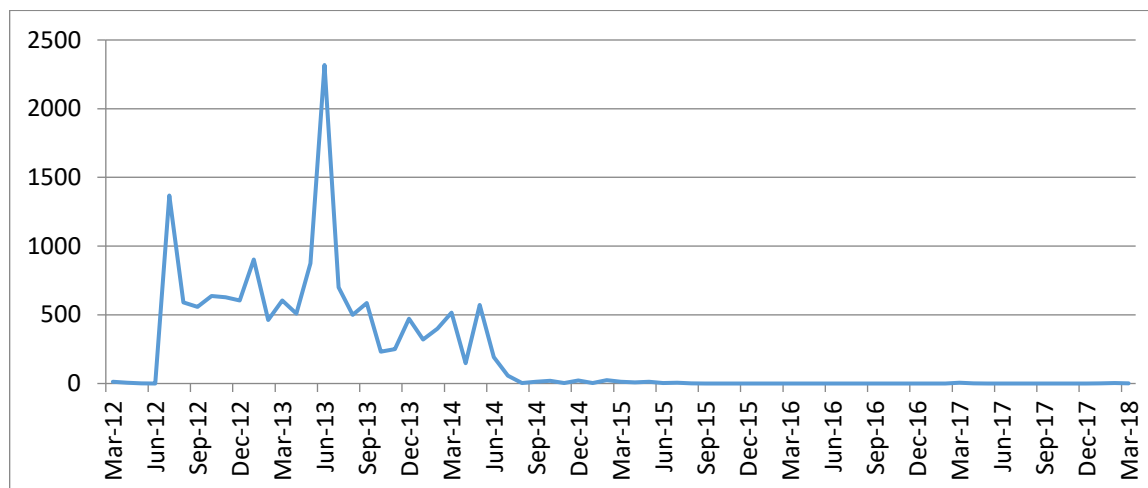


Figure 4.1: Number of (latest) tweets by the account @TheRedHack by month (March 2012-March 2018).

The first figure that I created based upon the tweets from the account @TheRedHack between March 2012 and March 2018 shows the activity of Redhack in Twitter. Due to several suspensions and withholdings, many accounts of Redhack cannot be used as data collection source for the acts of the group. The most reliable account that is also referred often by news media is the account @TheRedHack. This account is the only account that is not suspended by Twitter, mostly due to its withheld status within Turkey. In March 2018, @TheRedHack had 528k followers with its 24.9k tweets since its opening in March 2012. These high numbers support the reliability of the account.

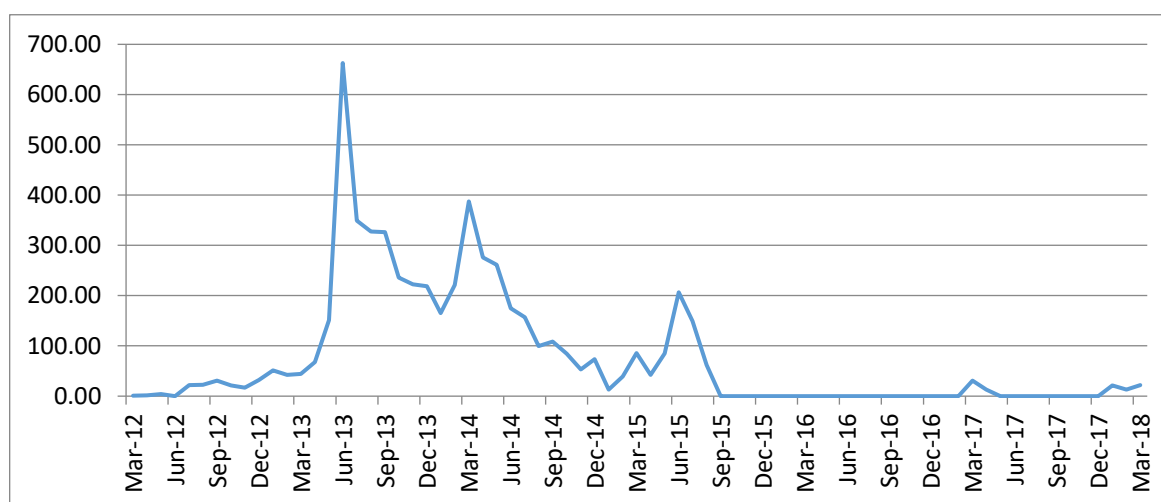


Figure 4.2: Number of retweets per number of tweets by the account @TheRedHack by month (March 2012-March 2018)

Figure 4.2 shows how other users in Twitter interacted with the tweets of the account @TheRedHack. Even though this figure is based upon just one account of the group and the act of interaction is retweeting, the high numbers in 2013 and 2014 compared to other years are significant to understand the popularity of Redhack in Twitter. The increase of interactivity coincides also with the increase of social movements in 2013 and in 2014, including the Gezi protests. Another relatively small rise of interaction in 2015 is based upon the high number of retweeting of the low number of tweets by the account; a political interest emerged from the general elections of June 2015. This election had resulted in the first hung parliament since the coming to power of AKP, especially due to the high voting rate of HDP.¹¹ In sum, not just the acts of the group, or the usage of Twitter by the group, but also the political atmosphere of the country influenced the interactivity related to the political tweets of Redhack in Twitter.

Redhack was a highly active hacktivist group between 2012 and 2014. More than 100 acts that the group claimed responsibility for are indicators of the nature of the group, as well as the crime frames that are constructed about them. In consequence of the centrality of data leaks in the judicial process related to Redhack, data leaks of the group are collected in a separate table than their other acts. These other acts will be exhibited in a second table under the title of data interference. Tweets collected from Twitter Advanced Search engine with the keyword “redhack” among all top tweets¹² in Twitter constitute the main dataset for these tables.

Information about the leaks of Redhack is found within this dataset through another search in Notepad ++ with the keyword “belge [document].” Found data is controlled with news portal links given in the tweets. The findings are also compared with all the tweets from @TheRedHack, once again via Twitter Advanced Search engine. In the data

¹¹ This result was due to the surpassing of the election threshold by HDP, which resulted in the change of the distribution of chairs in the Assembly to the detriment of the party in power.

¹² Twitter describes top tweets as “an algorithm-powered feed organized by ranking signals” (Sehl, 2019). New portals and influential people are the main accounts that this algorithm chooses in the case of tweets containing the keyword “redhack.”

collection, Twitter Advanced Search engine collected 15.124k tweets with the option “latest” from the 24.9k tweets posted by this account.¹³

Table 4.1: Data leaks by Redhack

Date	Source	Highlights	Motivation
February 2012	Ankara Police Directorate	Information about the citizen informants in Turkey	Reaction “against imperialism and its ‘green’ army that made the country a prison” (Cnn Türk, 2012)
June 2012	Turkish Land Forces, 2nd Commando Brigade Command	Information about the personnel of the Turkish Armed Forces	Exhibition of the vulnerability of armed forces (Hürriyet, Redhack bu tez TSK'ya saldırdı, 2012)
July 2012	Ministry of Foreign Affairs	Information about foreign diplomats in Turkey	Commemoration of Sivas Massacre and reaction against the Turkish foreign policy in the Middle East, especially about Syria (Ntv, Redhack Dışişleri Bakanlığı'nı hackledi, 2012)
July 2012	Ankara Police Directorate	Information about the citizen informants	Reaction against the threatening of academicians and journalists supporting Redhack (Odatv, 2012)
August 2012	Ministry of Foreign Affairs	Information about Turkish diplomats in foreign countries	Reaction against the people arrested within the scope of the Redhack case (Hürriyet, 2012a)
January 2013	Council of Higher Education	Information about corruption at Turkish universities	Support for the protests of ODTU students (Odatv, 2013)
February 2013	President of Ankara Commodity Exchange and President of	Information about corruption in Ankara Metropolitan Municipality	Reaction against the accusations in the judicial processes of Odatv , KCK, GrupYorum, DHF, D.Karargah, Balyoz, Ergenekon and etc., commemoration of

¹³ Different from its “top tweets” algorithm, no further information is found about how Twitter engine selects “latest tweets.” However, as the result shows, there is an algorithm that excludes almost half of the tweets with 15.124k from 24.9k tweets. Still, the dataset is accepted as representative.

Chapter 4: Hacktivist experience in Turkey

	Credit Guarantee Fund Faik Yavuz		Deniz Gezmiş, polemic with Melih Gökçek (SoL, 2013)
March 2013	MOSSAD, National Intelligence Agency of Israel	Information about 35,000 Israeli intelligence personnel	Support for Palestine, together with Anonymous (En Son Haber, 2013)
April 2013	Council of Higher Education	Information about illegal profiling in universities	Reaction against the arrest of journalists, dedication to the youngest arrested journalist Sami Menteş (Medya Tava, 2013; SoL, 2013a)
May 2013	Gendarmerie Intelligence Department	Information about the intelligence on Reyhanlı explosion	Exhibition of the state's responsibility in Reyhanlı explosion with the recall of the murder of civilians in Roboski by the state (Hürriyet, 2013; Milliyet, 2013)
May 2013	State Minister and Chief Negotiator for the EU Egemen Bağış	Information about corruption and misrepresentation of political actors	Reaction against the arrest of a private for Redhack's leaks about Reyhanlı explosion (Odatv, 2013a)
June 2013	N/A	Phone numbers of deputies and their partners	Support for the Gezi uprising (SoL, 2013b)
June 2013	Istanbul Police Directorate	Phone numbers of high ranked officers in Istanbul Police Directorate	Support for the Gezi uprising, reaction against the police violence, commemoration of Mehmet Ayvalıtaş ve Abdullah Cömert (Haberler, 2013)
September 2013	N/A	Information about corruption in prime ministry	Exhibition of the corruption (T24, Times: Barış Atay'ın gözaltına alınması Gezi eylemlerine misilleme, 2013)
September 2013	N/A	Information about the police officers who were on active duty on the spot where a protester, Abdullah Cömert was murdered by the police	Reaction against the police violence (Odatv, 2013b)

Chapter 4: Hacktivist experience in Turkey

October 2013	State Minister and Chief Negotiator for the EU Egemen Bağış	Information about the income and expenses of Egemen Bağış	Exhibition of the corruption (SoL, 2013c)
November 2013	Gendarmerie Intelligence Department	Information about the intelligence on Reyhanlı explosion	Reaction against the accusation of the private Utku Kali for leaking information about Reyhanlı explosion (SoL, 2013d)
November 2013	N/A	Information about corruption in Police	Exhibition of the corruption at the Police Department of Training (Vatan, 2013)
December 2013	Governorship of Amasya	Information about misuse	Exhibition of the misuse in the governorship (Cumhuriyet, 2013)
January 2014	Ministry of Transport	Information about corruption in TCDD	Exhibition of the corruption in TCDD (SoL, 2014)
January 2014	Ankara Metropolitan Municipality	Information about misuse in Ankara Metropolitan Municipality	Exhibition of the misuse in Ankara Metropolitan Municipality (Odatv, Nedir bu Melih Gökçek'in RedHack'ten çektiği, 2014)
February 2014	N/A	Phone numbers of ministers and deputies	Reaction against the censorship in the internet via the promulgation of Law 5651 (Hürriyet Daily News, 2014; Ege'nin Sesi, 2014)
February 2014	One of the biggest mobile phone operator of Turkey, Turkcell	Phone numbers of Turkcell workers	Reaction against the support of Turkcell for leaked phone numbers of deputies (Hürriyet Daily News, 2014; Ege'nin Sesi, 2014)
May 2014	AKP Group Deputy Chair Nurettin Canikli	Information about patronage relations, one between Yeni Akit newspaper and the AKP deputy	Exhibition of corruption between AKP and news media (Odatv, 2014a)
May 2014	AKP Manisa Deputy Muzaffer Yurttaş	Information about corporate misuse and information hiding related to Soma work accident	Exhibition of corporate misuse and information hiding related to Soma work accident (Diken, 2014; Cumhuriyet, 2014)

May 2014	AKP Düzce Deputy Osman Çakır	Information about patronage system, corruption, relations with Fethullah Gülen	Exhibition of the patronage system and of the corruption (Cumhuriyet, 2014a; Odatv, 2014b)
September 2016	Minister of Energy and Natural Resources Berat Albayrak	Information about media dependency of DHA to AKP government, the formation of Twitter troll armies, the relationship between Albayrak and Powertrans, an oil company implicated in deals with oil produced by ISIS	Reaction against the arrest of leftist dissidents (İleri Haber, 2016), exhibition of media dependency (Cumhuriyet, 2016), formation of illegal propaganda units, exhibition of ministry misuse and corruption (Yolculuk, Sansüre karşı yeniden yayınlıyoruz: İşte #RedHack'in Berat'ın mailinden paylaştıkları, 2016), exhibition of war crimes (Siyasi Haber, Redhack'ten yeni mailler: Kürt petrolünü usulsüzce taşıyan şirkette söz sahibi Albayrak'mış, 2016)

Alongside these data leaks from e-mail accounts and websites, Redhack have a recorded history of data interference since the end of the 2000s. Information about the acts of data interference by Redhack is found within the same dataset as data leaks by Redhack. This time it is done through another search in Notepad ++ with the keyword “hackledi [hacked].” Found data is controlled once again with news portal links given in the tweets and they are also compared with all the tweets from the Twitter account @TheRedHack.

Many website defacements of Redhack appear in *Zone-h*, a worldwide known and highly acknowledged web archive among hackers for website defacements (Zone-h). Zone-h archive was also used as a source in the indictment prepared by Ankara Chief Public Prosecutor's Office (2012) and the reasoned decision prepared by Ankara Heavy Penal Court No. 7 (2015).

Zone-h shows that Redhack notified 10,003 defaced websites to the web archive between December 2008 and March 2018. 9,277 of them are mass defacements. 73 of the defacements are labelled as “special defacements” by the archive because “important websites” were targeted. When these defacements are examined, they reveal that this qualification corresponds to websites with “gov.tr” url, which means websites belonging to the Turkish government (Zone-h). Not all the website defacement notifications appear in

the collected tweets posted by @TheRedHack or within the top tweets including the keyword “redhack.” In return, not all the mentioned website defacements are notified to the Zone-h archive. Information about website defacements in the following table grounds on the collected tweets and on the news links found in these tweets rather than Zone-h notifications because tweets and news links provided more information about the motivations of the group than Zone-h mirrors.¹⁴ When more than one website link are accessible from the tweets, the one containing more information about the act – especially the mirror of the defaced website – is preferred to be cited as the source. In few cases where there is no information or very little information about the act in the news websites, the web archive Zone-h is used as the complementary source.

This second table about the acts of Redhack gathers diverse acts under the umbrella of data interference. In this way, it provides the link between the acts of the group and the judicial processes related to these acts. Data interference is a legal conceptualization that would appear often in judicial processes. Nor techniques like DDOS attacks neither outcome like website defacements are covered in the Turkish Penal Code.

Table 4.2: Data Interference by Redhack

Date	Target	Act	Motivation
September 2007	Istanbul Police Department Traffic Services	Data alteration, erasing of fines (BirGün, 2007)	N/A
2 July 2011	More than 1000 websites with Turanist and Turkist ideologies, including the websites of Adnan Oktar	Website defacement (SoL, 2011)	Commemoration of the Sivas massacre in 2 July 1993
30 March 2012	Police directorates	Website defacement (Odatv, 2012a)	Reaction against the police brutality against KESK

¹⁴ Mirrors in Zone-h reflect the view of the defaced website at the time of the defacement.

Chapter 4: Hacktivist experience in Turkey

			members in the TEKEL protests, commemoration of a revolutionary murdered by the state, Mahir Çayan
13 April 2012	Gülen Community	Website defacement (Odatv, 2012b)	Reaction against the arrests in the Redhack investigation
13 May 2012	Ministry of Family and Social Policy	Website defacement (Zone-h, hizmet.aile.gov.tr hacked, 2012)	Mother's day, reaction against war, support for Saturday Mothers
20 April 2012	Ministry of Interior	Website defacement (T24, 2012)	Reaction against the mistreatment of Minister of Interior İdris Naim Şahin towards a citizen, reaction against the arrests in the Redhack investigation
3 May 2012	Milk companies, Yörükoğlu Gıda, Gülsan Gıda and Pınar Süt	Website defacement (SoL, 2012)	Reaction against the poisoning of elementary school students and the corruption within the campaign "okul sütü akıl küpü"
3 May 2012	Ministry of Health	Website crash, together with Anonymous (SoL, 2012a)	Reaction against the poisoning of elementary school students and the corruption within the campaign "okul sütü akıl küpü"
3 May 2012	TÜBİTAK	Website crash, together with Anonymous (SoL, 2012a)	Reaction against the technical support provided by TÜBİTAK to state institutions against Redhack
3 May 2012	Melih Gökçek, TTNET, Zaman newspaper	Website crash, together with Anonymous (SoL, 2012a)	Reaction against Gülen Cemaati
2 July 2012	Ministry of Foreign Affairs	Website defacement (Zone-h, 2012a)	Reaction against the war in Syria, against imperialism,

Chapter 4: Hacktivist experience in Turkey

			against Gülen Community, Commemoration of the Sivas massacre
13 July 2012	Ministry of National Education	Website crash (SoL, 2012b)	Reaction against the KPSS (Public Personnel Selection Examination) scandal
17 July 2012	Turkish Football Federation	Website crash (Hürriyet, 2012b)	Reaction against corruption in the football industry
31 August 2012	Court of Appeal, Ministry of Transport, Constitutional Court of Turkey	Website crash (Cnn Türk, 2012a)	Reaction against the judicial decision in the case of child sexual abuse
11 September 2012	Urfa and Siverek State Hospitals	Website crash (Milliyet, 2012)	Reaction against the claims of child sexual abuse
12 September 2012	Siverek District Governorship	Website defacement (Hürriyet, 2012c)	Reaction against the claims of child sexual abuse
17 September 2012	Governorship of Hatay	Website crash (Sözcü, 2012)	Support for the “Brotherhood Meeting” in Hatay
25 September 2012	Governorship of Sinop	Website defacement (Yeşil Gazete, 2012)	Reaction against the construction of the nuclear power plant
6 October 2012	Ministry of Interior	Unauthorized access, sharing access information (Sözcü, 2012a)	Exhibition of state vulnerability, reaction against war in Syria, reaction against the formation of cyber-army
27 October 2012	Ministry of Justice	Website defacement (SoL, 2012c)	Support the hunger strike by Kurdish prisoners, reaction against the civil war, reaction against the accusations in the Redhack case

Chapter 4: Hacktivist experience in Turkey

29 October 2012	Presidency of Religious Affairs	Website defacement (Bianet, 2012)	Republic day message, reaction against AKP and Gülen Community, against the corruption, against the denial of Armenian genocide and the denial of social rights of Kurds
9 November 2012	ODTÜ	Unauthorized access (Sözcü, 2012b)	Support the protest of ODTÜ students for hunger strikes, reaction against the support of ODTÜ administration to the police
23 November 2012	Constitutional Court of Turkey	Website crash (Haber 24, 2012)	Reaction against the trial related to the Redhack case
6 December 2012	Ministry of Finance	Data alteration, wage increase for civil servants (Hürriyet, 2012d)	N/A
22 December 2012	Ministry of Transport	Website crash (Evrensel, 2012)	Support the commemoration in Maraş for the Maraş Massacre in 1978, reaction against the blocking of the roads to Maraş by the ministry
8 January 2013	Council of Higher Education	Website defacement (Zone-h, 2013)	Support for protesting students in universities, reaction against YÖK, reaction against AKP
17 January 2013	Court of Appeal	Website crash (SoL, 2013e)	Reaction against the judicial decision in the case of child sexual abuse
7 April 2013	Ice cream company MADO	Website crash (SoL, 2013f)	Support for the protesters of Emek Cinema Theater, reaction against the mistreatment by the

Chapter 4: Hacktivist experience in Turkey

			company towards the protesters
15 April 2013	Ministry Of Environment And Urbanization	Website crash (T24, 2013a)	Reaction against the citizen mistreatment of Minister by Environment And Urbanization Erdoğan Bayraktar
5 May 2013	Governorship of Istanbul	Website defacement (Hürriyet, 2013a)	Support for the May Day protests
5 May 2013	Medical Park Hospital	Website crash (SoL, 2013g)	Reaction against the mistreatment of a citizen who was hurt during the May Day protests by the hospital
11 May 2013	Governorship of Hatay	Website crash (Aydınlık, 2013)	Reaction against the misbehavior of political figures and the disregard for the Reyhanlı explosion
30 May 2013	Beyoğlu District Police Department	Website crash (Sendika, 2013)	Support for the Gezi protests, reaction against the police violence against the protesters
2 June 2013	Presidency of the Republic, Istanbul Police Directorate and AKP	Website crash, together with Anonymous (T24, 2013b)	Support for the Gezi protests
4 June 2013	Governorship of Hatay	Website crash (Mynet, 2013)	Reaction against the hiding of police responsibility about the death of a protester, Abdullah Cömert during the Gezi protests in Hatay
12 June 2013	RTÜK	Website crash, together with Anonymous (Finans Gündem, 2013)	Support the news media reporting about the Gezi protests, reaction against the sanctions towards these media organizations

Chapter 4: Hacktivist experience in Turkey

12 June 2013	Ankara Police Directorate, Governorship of Istanbul	Website crash (Sözcü, 2013)	Reaction against the murder of a protester, Ethem Sarısülük by the police during the Gezi protests in Ankara
27 June 2013	Istanbul Special Provincial Administration	Data alteration, erasing of public institutions' fines to the state (Hürriyet, 2013b)	N/A
28 June 2013	Lice District Governorship	Website crash (Evrensel, 2013)	Support of the protests against the construction of high security police checkpoints [kalekol], reaction against the information hiding about the murder of a protester by soldiers
2 July 2013	Sivas Special Provincial Administration	Website crash (Haberler, 2013a)	Commemoration of the Sivas massacre
2 July 2013	Presidency of Religious Affairs	Data alteration, sharing access information (Vatan, 2013a)	Commemoration of the Sivas massacre
15 August 2013	ASKİ (Adana Water and Sewerage Services)	Data alteration, erasing of fines, sharing access information (Sözcü, 2013a)	N/A
23 August 2013	TBB (Union of Municipalities of Turkey)	Unauthorized access, website crash, sharing access information (Sözcü, 2013b)	Commemoration of the martyrs of the Gezi protests, Ali İsmail Korkmaz, reaction against the arrest of Utku Kalı
24 August 2013	OPET	Unauthorized access (Türkiye Gazetesi, 2013)	Reaction against the oil price rise
3 September 2013	AKP Edirne Provincial and Sub-Provincial Organizations	Website defacement (Medya Keşan, 2013)	Reaction against the claims of the president of AKP Edirne Provincial Organization about Redhack

Chapter 4: Hacktivist experience in Turkey

5 September 2013	Turkish National Police	Website crash (Sözcü, 2013c)	Support the protesters who were murdered and were injured during the Gezi protests, reaction against the police violence
15 October 2013	TKİB (Turkish Public Enterprises Association)	Website defacement (Sendika, 2013a)	Festival of Sacrifice message, commemoration of children and young people died in the Van earthquake, murdered in Roboski, during the Gezi protests, and in Rojova. Support for their mothers, for the peace, reaction against fascism
12 November 2013	Yeni Akit newspaper	Website crash (Medya Tava, 2013a)	Reaction against the reaction of the newspaper for the release of Utku Kalı
25 November 2013	AKP	Website defacement (Sözcü, 2013d)	Reaction against the arrests related to the Redhack case
28 December 2013	GASKİ (Gaziantep Water and Sewerage Services)	Unauthorized access (Kızıl Bayrak, 2013)	For the right to water, reaction against citizen informants
10 January 2014	TBMM	Website defacement (Odatv, 2014c)	Exhibition of vulnerability
16 January 2014	Central Bank of the Republic of Turkey	Website crash (Finans Gündem, 2014)	Reaction against the rise of the exchange rate of dollar
4 February 2014	Telecommunication Companies, TTNET and Vodafone	Unauthorized access (Cumhuriyet, 2014b)	Exhibition of vulnerability about the users' information of ministries, MIT, police directorates
8 February 2014	Kars Municipality	Website defacement (Diken, 2014a)	Support for the protests against the new internet law,

Chapter 4: Hacktivist experience in Turkey

			reaction against the censorship in the internet
8 February 2014	Sakarya Natural Gas Company, AGDAŞ	Data alteration, erasing of fines (Diken, 2014a)	N/A
8 March 2014	Konya Commodity Exchange	Unauthorized access, sharing access information (Ege'nin Sesi, 2014a)	Support Berkin Elvan, the young protester injured by the police during the Gezi protests
28 March 2014	Presidency of Telecommunication and Communication	Website crash (Hürriyet, 2014)	Reaction against the YouTube ban
17 April 2014	Aktif Bank, the seller of Passolig	Unauthorized access, website crash (Cumhuriyet, 2014c)	Support for the football supporter groups protesting against Passolig, the e-ticket application for football matches, exhibition of vulnerability
10 May 2014	Council of State	Website crash (Sendika, 2014)	Reaction against the dependent attitude of the president of the Council of State towards Erdoğan
13 May 2014	Soma Municipality	Website defacement (Sözcü, 2014)	Reaction against the murder of mine workers in the mine accident
18 May 2014	TIKA (Turkish Cooperation and Coordination Agency)	Unauthorized access, sharing access information (Hürriyet, 2014a)	Reaction against Erdoğan, commemoration of a revolutionary murdered by the state, İbrahim Kaypakkaya
1 June 2014	(ASO) Ankara Chamber of Industry	Website defacement (Cnn Türk, 2014)	Reaction against the nuclear power plant, commemoration of the Gezi protests, commemoration of a protester murdered during

Chapter 4: Hacktivist experience in Turkey

			the anti-nuclear protests, Metin Lokumcu
10 June 2014	Minister of Interior during the Gezi protests and Lice protests, Muammer Güler	Unauthorized access, sharing access information (Cumhuriyet, 2014d)	Commemoration of the Gezi protests and of the protests against the construction of high security police checkpoints [kalekol] in Lice, for the brotherhood of people
21 June 2014	Glass container manufacturing company, Anadolu Cam	Website defacement (Evrensel, 2014)	Support for the workers striking in the company
5 September 2014	Architectural company, Özyurt A.Ş.	Website defacement (Diken, 2014b)	Reaction against the overpass collapse, reaction against the patronage relations between the company and AKP
8 September 2014	Construction company, Torunlar Holding	Website defacement, website crash (BirGün, 2014)	Reaction against the murder of workers in the work accident, support for the union of workers, support for the brotherhood of people
25 September 2014	Power company, IZ-ENERJI	Web defacement (BirGün, 2014a)	Support for the workers protesting against the subcontractorization
14 October 2014	Communication Workers Union, BIRLIK BIR- SEN	Website defacement (BirGün, 2014b)	Support for the Kurdish resistance in Kobani, reaction against the patronage relations in news media
22 October 2014	Turkey Human Rights Foundation	Website defacement (Radikal, 2014)	Support for Saturday Mothers
29 October 2014	Istanbul Metropolitan Municipality,	Website defacement (Siyasi Haber, 2014)	Support for the people protesting against the

Chapter 4: Hacktivist experience in Turkey

	Parks and Gardens Department		mosque construction in the Validebağ grove
14 November 2014	Power company, TEİAŞ	Data alteration, erasing of fines (Diken, 2014c)	Support for the Yırca villagers protesting against the uprooting of olive trees and for the Validebağ protesters, exhibition of vulnerability
30 November 2014	Retired Police Commissioners Social Aid and Solidarity Association	Website crash (BirGün, 2014c)	Reaction against the injury of a protester by the police in Kobani protests
4 December 2014	Yatağan Municipality	Website defacement (Odatv, 2014d)	Support for the workers in Yatağan protesting against the privatization
5 December 2014	Mobese (City surveillance camera system)	Website defacement (SoL, 2014a)	Reaction against the incompetency in the Berkin Elvan case, commemoration of children and young people murdered by the state, during the Gezi protests, in Roboski and others
8 December 2014	Şırnak Special Provincial Administration	Unauthorized access, sharing access information (Kızıl Bayrak, 2014)	Reaction against the murder of a protester in Yüksekova and the injury of a child in Cizre by the police
15 December 2014	Istanbul Police Association	Website defacement (Odatv, 2014e)	Reaction against the trial of the Redhack case
28 December 2014	Ankara Metropolitan Municipality Sport Club, Melih Gökçek	Website defacement (Cumhuriyet, 2014e)	Support the family of Ethem Sarısülük, reaction against the defense of the police who murdered Ethem Sarısülük, reaction against the misuse

Chapter 4: Hacktivist experience in Turkey

			and corruption in the municipality
29 December 2014	GAP Administration, Ministry of Development	Website defacement (Kızıl Bayrak, 2014a)	Commemoration of people murdered in the Roboski airstrike
7 January 2015	Travel company, Oruç Travel, Ramazan Oruç	Website defacement (İleri Haber, 2015)	Support for the people protesting against the privatization of İztuzu Beach, reaction against the pillage of natural sources
11 March 2015	Istanbul Police Association	Website defacement (Diken, 2015)	Commemoration of Berkin Elvan, reaction against the police violence
19 August 2016	Çanakkale Municipality	Unauthorized access, sending SMS message (Cumhuriyet, 2016a)	Reaction against the military coup and against the state of emergency
23 September 2016	Sözcü Newspaper	Website defacement (Cumhuriyet, 2016b)	Reaction against the autocensorship of the newspaper about the leaks of Redhack, support for Saturday Mothers, exhibition of vulnerability
20 June 2017	Ministry of Defense	Website defacement (Yolculuk, 2017)	Reaction against the poisoning of soldiers, against the war, against the military coup
24 March 2018	Conglomerate company, Demirören Holding	Website defacement (Cumhuriyet, 2018)	Commemoration of protesters murdered during the Gezi protests, Kurdish people murdered by the state violence, leftists murdered by ISIS bombings, reaction against the patronage relations between the media and AKP

4.1.1. Techniques of hacktivism: Shall we hack together?

In this part, departing from the two tables about the hacktivist acts of Redhack, I will exhibit different categories of the acts of Redhack and discuss the most favored category of act. The discussion will reveal how the techniques of hacktivism are overshadowed and what can the implications of that explicit overshadowing be.

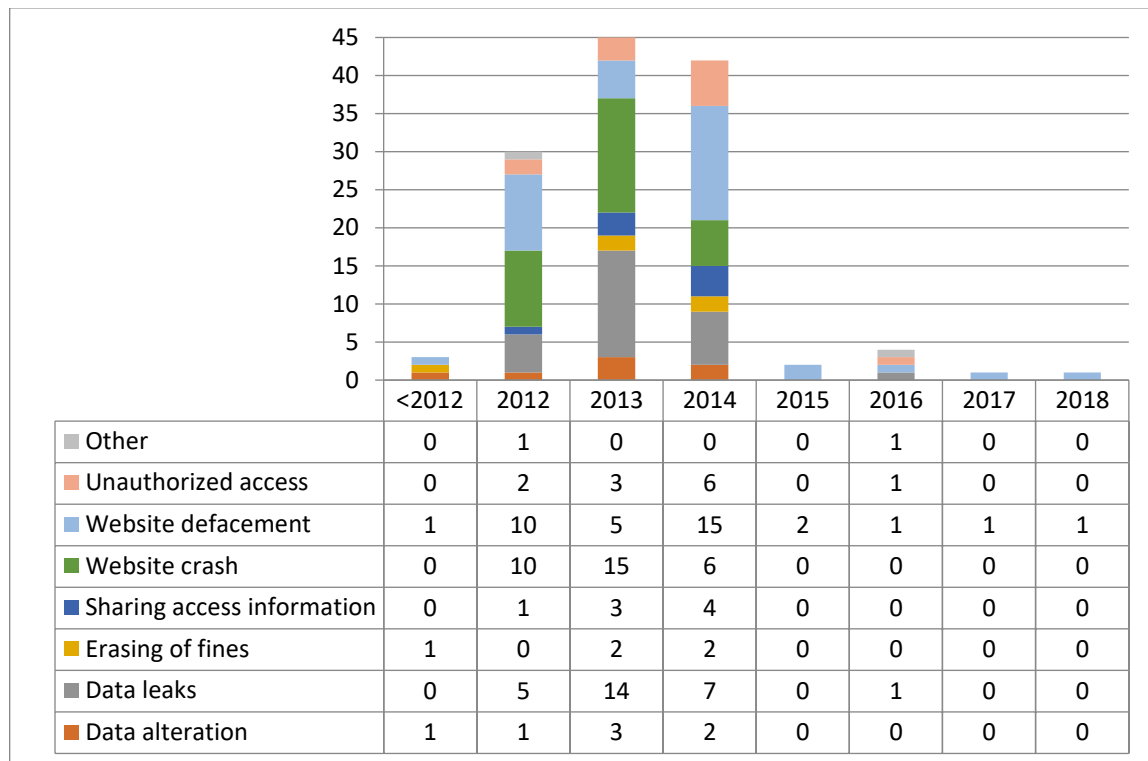


Figure 4.3: Acts of Redhack by years¹⁵

As Figure 4.3 shows, website defacement is one of the most favored data interference acts by Redhack. This category containing 36 acts is followed by website crashes (31 acts) and data leaks (27 acts). Website defacement is the replacement of a webpage with a new page containing specific messages. Some website defacements can be apolitical and can include

¹⁵ In some incidents, different acts coincide. Yet in the figure, acts are given as separate categories. For that reason, number of acts seen in the figure is higher than the real number of incident. As there are 14 incidents where two acts and 1 incident where three acts coincide among all 112 incidents (28 data leaks and 84 data interference acts), it is considered negligible. The “other” category includes two discrete acts: an act of unauthorized access to increase wages of civil servants and another one in which the group sent an SMS message through the hacking of Çanakkale Municipality system.

just the nickname of the hacker and/or some images (Samuel, 2004, p. 8). In these cases, the defacement is done mostly for the exhibition of prowess. However, the most outstanding website defacements are the ones that include political messages. Many hactivist groups use this technique to propagate their political views, to provide support for what they are defending or to make news about incidents that they are reacting against. Different from data leaks that are a characteristic of leak hacktivism of the 2010s, website defacement is a technique shared with different hactivist experiences from diverse contexts. Especially, for the patriotic hacking born within the context of anti-globalization in the 2000s, website defacement is frequently used to criticize the organization whose website is hacked or which it is associated, mostly based on the website's nationality (Samuel, 2004, p. 8).

In none of the tables, hacking techniques of Redhack are included. In the literature of hacktivism, techniques used by hactivists can appear as important signifiers of hactivist acts. For example, client-side distributed denial-of-service (DDoS) is considered as the distinctive sign of mass action hactivist groups (Jordan & Taylor, 2004, p. 75). In its original form, DDOS attacks were automatically conducted through the control of computers without the consent of computer owners. These computers were called zombies or bots. Different from that automated technique, in 1999, client-side DDOS attacks were used as a conscious choice by the hactivist group Electrohippies Collective during the Seattle protests. With this technique, the hacking depends on many people to initiate a mass action (Jordan & Taylor, 2004, p. 77) Using client-side DDOS attacks is one of the core characteristics that differentiate mass action hacktivism from other hactivist experiences. This technique creates a conscious refusal of the amplification of individual power that is supplied by computer technologies and it prefers mass solidarity for the sake of popular legitimacy (Jordan & Taylor, 2004, p. 85). According to Electrohippies, they reached this popular legitimacy with their use of this “democratically based protest-related DoS action” (Electrohippies Collective, Electrohippies Occasional Paper No.1, 2000a).

In the case of Redhack, hacking techniques of data interference are not used as part of the propaganda of their acts, neither directly linked to their political view. For data interference, Redhack mostly uses common techniques shared by apolitical groups and political groups with different ideologies. Moreover, Redhack does not prefer performing

mass action hacktivism in any of their acts - preferring mass solidarity against hacking skills. In few incidents where the group calls for collective action, there are nuances that dissociate their acts from the acts of mass action hacktivist groups.

In October 2012, when the group obtained the access information for the system of the Ministry of Interior, they shared this knowledge with their Twitter followers (Sözcü, 2012a). In one their tweets about the incident, Redhack claimed that 43,590 people accessed the system – in other words, joined their hacking (@TheRedHack, 2012).

In June 2013, Redhack made a similar call through its Twitter account. After hacking the databank of the Presidency of Religious Affairs and sharing the usernames and passwords, the group invited their followers to data alteration by saying “Shall we hack together?” (@TheRedHack, 2013).

In August 2013, Redhack shared the information to alter the data within Adana Water and Sewerage Services with the call “Friends from Adana, are we ready? ;)” (@TheRedHack, 2013a). This time, the alteration offer was not just about leaving messages or just having access to publicly inaccessible information. People were invited to change their own information in the system – in other words, to erase their bills, if they wished. Different from the earlier mass hackings where curiosity and/or political motivation could be more stimulating, now, seeking benefit was involved as a new stimulation.

These three instances where Redhack calls for mass action, these calls do not carry the same political meaning, as the hacking of WTO by the Electrohippies Collective had carried. In the case of Electrohippies, the participation of masses was the prerequisite for the hacking. When the hacker group decided to not use botnets¹⁶, it meant that without an immense number of participants, the hacking would not be successful to crash the targeted website. While in the case of Redhack, the acts of followers are not prerequisite. The unauthorized access is performed whether or not other people participated. From a very different perspective, the participation of followers provided legitimacy. However, it is not in the sense of masses participating to a democratic protest but in the sense of sharing responsibility in an act that is openly illicit. It was through becoming complicit that

¹⁶ Botnet is the network of bots, automated software applications that allow performing repetitive tasks. Botnets can be acting under one command, against the will of computer owners. For that reason, they are called as zombie programs.

Redhack created legitimacy in the eyes of masses. In that sense, Redhack did not refuse the amplification of individual power, as Electrohippies had done. On the contrary, they shared the amplified power that they had, with many people following them. For that reason, hacking techniques do not possess a political meaning by themselves for Redhack. Different from how mass action hacktivists claim, Redhack bestow their hacking with their followers, rather than hack together with them.

Following that, their techniques of hacking are not disputable. The group mentions their techniques just in a few instances with the aim of verifying their hacking skills against the underestimation of state authorities and other hackers in general with opposite ideologies (Cumhuriyet, 2016c). This verification effort results from the importance attributed by hackers/hactivists to be qualified as *real hackers* instead of being considered as *lamers*.¹⁷ That is also the reason why hacking techniques can become a controversial topic among different actors in the field. While Redhack claims to leak information or to change data through sophisticated hacking techniques, other actors can argue against it and defend that these acts are just the products of whistleblowers (Bianet, 2013). In this line, the government argues that what Redhack does is not hacking but a classic case of whistleblowing through the “treason” of a private (Hürriyet, 2013).¹⁸ Based upon the lack of public information about technical issues, techniques are not used in categorizing the acts of Redhack. However, they will have a crucial place within the discussions about the framing of Redhack.

4.1.2. Motivations of hacktivism: Reactive fusion of humor and leftist legacy

Four general categories are visible when Redhack’s acts are examined according to their explicit motivations. These are commemorative, exhibitivite, reactive, and supportive motivations. Commemorative acts are the ones where one incident from the past is recalled, as the message of the act. Exhibitivite acts aim directly for the state. They comprise acts exhibiting the vulnerability of cybersecurity, the incompetence in judicial decisions, the

¹⁷ *Lamer* is a pseudo-category that hackers use as an insult to incompetent hackers.

¹⁸ It should be also noted that in a research conducted within the scope of social sciences, the researcher cannot have the necessary expertise to defend one position against the other.

corruption and misuse in ministries and in municipalities, and the responsibility of violence and the mistreatment towards citizens. Reactive acts are the ones that are most dependent to the immediate context. Reaction against state violence, corruption, and judicial decisions that are found unjust by the group constitute the main motivations under this category. As the discussion of this part will exhibit, there are two secant lines in almost all of these acts with diverse motivations: humor and leftist legacy.

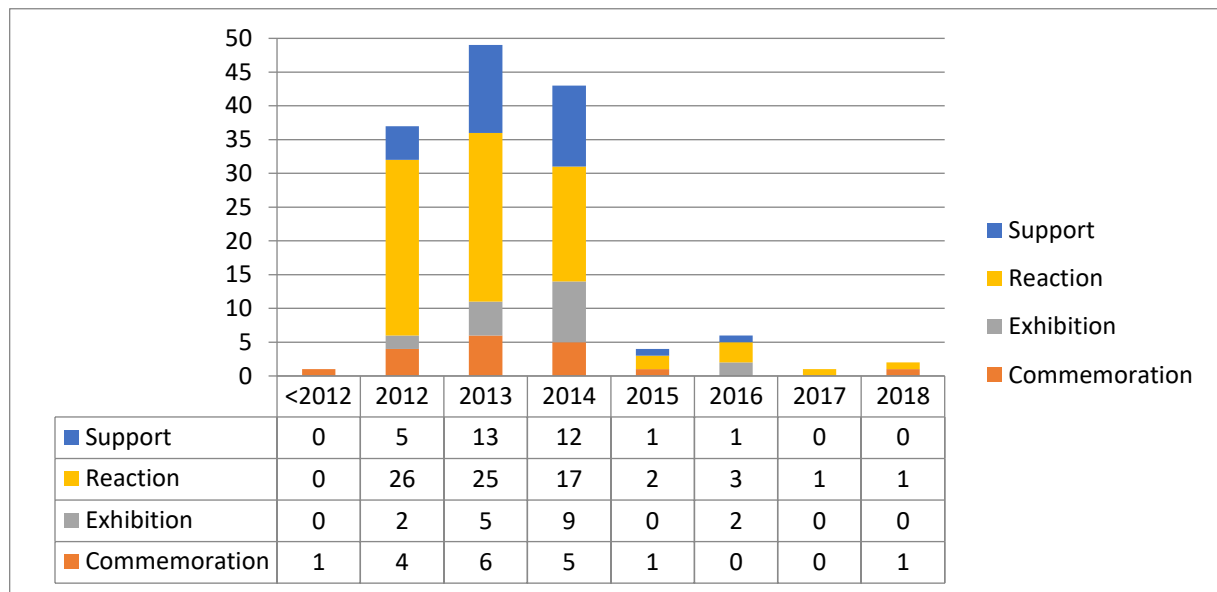


Figure 4.4: Acts categorized according to their explicit motivations by years¹⁹

As Figure 4.4 exhibits, reactionary motivations lead among other motivations of Redhack with 75 acts. This is more than twice of the second coming category of supportive acts (32 acts). Reactionary acts reveal that the group does not react just to the social and political issues that they find important. They also actively react to the judicial processes related to

¹⁹ As it was the case in the acts of Redhack figure, in this figure, too, different motivations coincide in same incidents. In this table, there are some acts for which no information can be found about the motivation of the act, too (5 acts). At the end, the number of motivations seen in the figure is higher than the real number of incident. Among all 112 incidents (28 data leaks and 84 data interference acts), there are 30 incidents where two motivation categories and 3 incidents where three motivation categories coincide. Different motivations that can be categorized under the same general motivation are counted as one. For example, in the act of website defacement of the website of the Ministry of Justice in 27 October 2012, Redhack mentions three motivations: support the hunger strike by Kurdish prisoners, reaction against the civil war, and reaction against the accusations in the Redhack case. They are counted as one supportive motivation and one reactive motivation.

them. 10 of 75 of their reactionary acts are performed as a response to the judicial acts against the group, especially in cases of arrests. It should also be emphasized that many supportive acts of the group are accompanied with reactionary motivations, as state violence mentioned in the incidents is in general towards the protesters of a specific event. When supportive and reactive motivations coexist in one incident, they may point at the same topic. For example, when Redhack performed an unauthorized access to the system of ODTÜ (Middle East Technical University) (9 November 2012), they supported the protest of the students and they reacted against the attitude of ODTÜ administration. Similarly, when the group crashed the website of Beyoğlu District Police Department (30 May 2013), they supported the Gezi protests and reacted against the police violence against the protesters. In that perspective, one of the reasons of the high numbers of reactive and supportive acts in 2012, 2013, and 2014 is the rise in the social movements and the support of Redhack for these movements, alongside the reaction of the group against the violence of police and army towards the participants of these movements. Not just the well-known Gezi protests but also the protests of workers (construction, thermal plant, glass, etc.), ODTÜ students, and Yırca villagers in this time period shape deeply the acts of Redhack, as the table of their acts shows.

Commemorative motivations also change slightly after 2013. While the group regularly commemorate the Sivas massacre²⁰ and sporadically commemorate youth activist leaders of the 1970s, they add the commemoration of the young people killed during the Gezi protests to their motivations. In that sense, the Gezi protests are an important source of motivation for Redhack. However, their activity is not limited with the Gezi protests. In total, just 17 incidents of their total 112 incidents have any motivations related to the Gezi protests, including commemorations of the Gezi *martyrs* in the following years.

However, there is not just one object of interest in the acts of Redhack. In some cases, the group prefers to mention different motivations within one act. This is the case especially in acts with exhibitive motivations. When Redhack accesses and share the access information of the system of the Ministry of Interior for a collective hacking (6 October 2012), they present their motivations as the exhibition of state vulnerability, the reaction

²⁰ Sivas massacre is the lynching of socialist intellectuals in 2 July 1993, during the cultural festival held by an Alevi organization.

against the war in Syria, and the reaction against the formation of cyber-army. These three acts do not have any common ground, yet they can appear together within the motivations of the act.

Exhibition of state vulnerability is a motivation that is often performed with humor. These acts provide a platform for the group to manifest their prowess against the incompetency of the state authorities. In the act against the Ministry of Interior, Redhack invites its followers to comment this act with the hashtag #RedHackBiziz [#WeAreRedhack] and they retweet this tweet that adopts a love poem to the collective hacking of Redhack:



Figure 4.3: [We felt about ;) -> “I liked the possibility to drink tea with you one day at <http://icisleri.gov.tr> #WeAreRedhack” RT @YalchinAkdeniz]

Humorous exposition of the state’s incompetence can be considered as a counter-hegemonic stance against the capitalist hegemony propagated actively by the Turkish state. Burrowing the perspective of Castells ((1996) 2010) in which he compares the origin of the internet to “Maoist tactics of dispersal of guerrilla forces” (p. 6), Akin and Zıraman (2015) frame hackers and – in the context of Turkey – Redhack as “the counter-hegemonic guerillas of the Internet sphere” (p. 15).

Not just in acts with exhibitive motivations but in other acts against the state, the humorous side of Redhack is visible, too. On 25 November 2013, Redhack defaced the official website of AKP with a pseudo news article about the apology of the Prime Minister Erdoğan for the arrests related to the Redhack case (Sözcü, 2013d). In another website crash from January 2014 performed against the rise of the exchange rate of dollar, Redhack tweeted:



Figure 4.4: [Aww Central Bank, did you get an owie at <http://www.tcmb.gov.tr/>; (]

Humor appears also in their acts of erasing fines. Actually the group does not mention any explicit motivation for the case of erasing fines and of one incident of wage increase. Implicit motivation of these populist²¹ acts can be creating legitimacy through benefit, as was discussed in the previous part about the techniques of hacktivism. On 8 February 2014, when Redhack defaced Sakarya Natural Gas Company and erased fines, they assembled the humor with their socialist ideology once again.

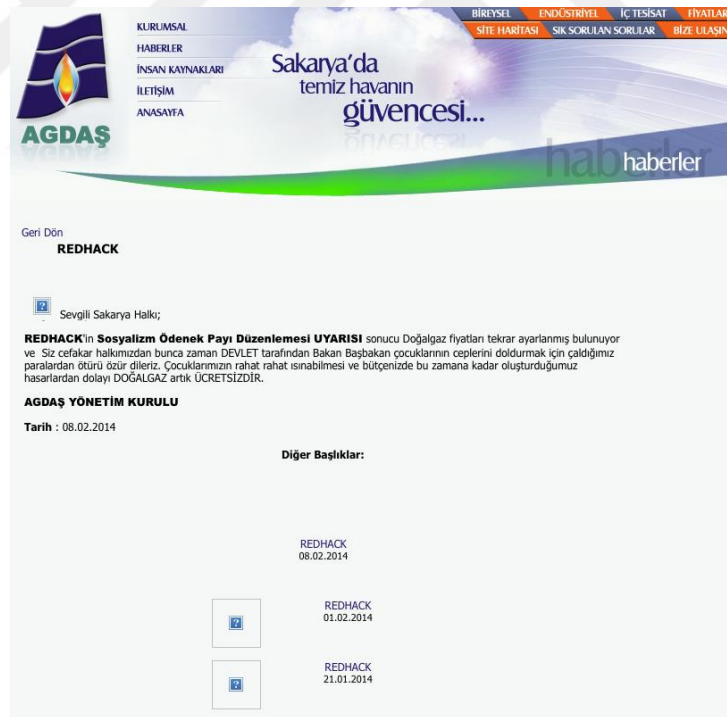


Figure 4.6: ‘Sosyalizm Ödenek Payı Düzenlemesi: Halkımız için bütün ödemeler yapılmıştır!

[Allotment rules of Socialism: All payments are done in the name of our people!] (Diken, 2014a)

²¹ Here populism is taken as “an ideology which pits a virtuous and homogeneous people against a set of elites and dangerous ‘others’ who are together depicted as depriving (or attempting to deprive) the sovereign people of their rights, values, prosperity, identity and voice” (Albertazzi & McDonnell, 2008, p. 3). This approach is in the same line as how Ernest Laclau conceptualizes populism as a “political logic” (Laclau, 2005, p. 117).

Satirical performance is quite central for hacktivist experiences (Jordan & Taylor, 2004, p. 85). This aspect comes from the hacking culture, as humor is central in the social world of hacking (Coleman, 2013, p. 7). For some groups like Anonymous, it takes the shape of “a spirit of humorous deviance” (Coleman, 2014, p. 17). Not just for the famous hacktivist group Anonymous, but for many hackers and hacker groups, *lulz*²² is the core stone of their acts. Lulz is a kind of “politically incorrect humor” that can be defined as the “carnavalesque celebration of free speech” (Goode, 2015, p. 76). In hacktivist acts, humor can also be used as a political weapon to criticize political opponents, as well as to arouse public attention (Fuchs, 2013, p. 372). Redhack’s case fits mostly the perspective of Fuchs where humor is a political weapon to criticize and attract attention, rather than politically incorrect humor. That is because Redhack adopts a strong leftist legacy, a characteristic that not many hacktivist groups possess.

Humor of Redhack is often mixed with the leftist culture, as the “Allotment Rules of Socialism” message shows. In many of their messages and posts, the group uses a jargon belonging to the Turkish left and they share the same interest for specific topics, as other leftist groups in Turkey. In many of their acts, they react for workplace issues, like occupational homicides, and they support the struggle of workers (Evrensel, 2014). As a reaction to the mass killing of Soma mine workers, the group defaced the website of Soma municipality with the message “iş kazası değil cinayet [not work accident, occupational homicide]” (Sözcü, 2014). This framing refers to the leftist struggle to enforce responsibility to employers and to the state by the frame of homicide, rather than accepting the incidents as accidents that cannot be controlled and foreseen (Bianet, 2014). In these acts in line with the labor movement, Redhack often uses expressions from the Marxist jargon like “the union of workers” and “for a classless world” (BirGün, 2014). They even use the famous quote from Marx and say “we have nothing to lose but our chains” (Odatv, 2014d).

²² According to Encyclopedia Dramatica, lulz is “a corruption of LOL, which stands for “Laugh Out Loud,” signifying laughter at someone else’s expense.” Coleman interprets lulz as an example of argot in the sense of “specialized and esoteric terminology used by a subcultural group” (Coleman, 2014, p. 31). Trolls and hackers are the main actors of this subculture.

Another topic in which they follow the leftist agenda is their support for the brotherhood of people with a focus on the 40 years old civil war between the Turkish State and The Kurdistan Workers' Party (PKK) and the Kurdish question in Turkey. In these tweets, they frame their support for the Kurdish struggle in a unity between that struggle and the Gezi protests:



Figure 4.7: [We dedicate this act to those who grow the resistance for Gezi to Lice, to those who fight for the fraternity of people...]

Redhack also emphasizes “the war against imperialism,” especially on issues related to foreign policy and wars in the Middle East (Cnn Türk, 2012).

The struggle against imperialism is one of the core topics in the leftist politics since the 1960s. When Redhack reacts against the police violence towards ODTU students that wanted to support hunger strike of Kurdish prisoners, the group recalls this past by quoting:



Figure 4.8: [We learnt three English words in ODTU, “Yankee Go Home” Sinan Cemgil²³ #AKPKeepYourHandsOffODTU]

Redhack is careful to commemorate all youth leaders of the 1970s without favoring one leftist fraction for another.

²³ Sinan Cemgil was an ODTU student and a famous youth leader of this period from the Marxist-Leninist organization THKO (People's Liberation Army of Turkey).



Figure 4.9: [We dedicate today's act to our beloved brother, teacher, and comrade Deniz Gezmiş. Happy birthday Deniz Gezmiş!]



Figure 4.10: ["Their power and their opportunities that seem immense today are nothing to us. They are few, we are millions." Mahir Çayan #30march1972]



Figure 4.11: [#İbrahimKaypakkaya, the brave one who did not breathe a word under torture, the castle of the revolution, the fighter of the oppressed peoples and the working class]

Deniz Gezmiş, Mahir Çayan, and İbrahim Kaypakkaya are three fundamental figures that gave rise to different factions of the contemporary leftist politics.²⁴ In that sense, Redhack follows a leftist unifying politics not just between the Kurdish struggle and the left but also between different leftist fractions in Turkey.

In sum, Redhack's acts reflect a reactionary agenda-setting bouncing between humor and the leftist legacy. This fusion between the two component materials – humor and the leftist legacy – is the one that distinguishes Redhack from other hacktivist groups.

²⁴ Deniz Gezmiş from THKO, Mahir Çayan from THKP-C (People's Liberation Party-Front of Turkey), and İbrahim Kaypakkaya from TKP/ML (Communist Party of Turkey/Marxist-Leninist) are all youth leaders killed by the state whether in armed conflict, by execution, or during torture.

It is also this characteristic that makes difficult the crime framing of Redhack. An Anon, a member of the hacktivist group Anonymous, says:

It's that idea of humor and irreverence which is at the heart of this [Anonymous].

It's what will stop it ever being able to be labeled terrorist.

(Coleman, 2014, p. 15)

In this correlation, humor and label of terrorism are positioned in inverse proportion. However, judicial processes related to Redhack would exhibit that this correlation does not work well in the case of Redhack and that humor does not guarantee a safe passage free from terror framings.

4.2. Judicial processes of Redhack

Judicial processes related to Redhack are not very easy to follow. First reason is that there are multiple simultaneously ongoing operations about the group. Before the end of a lawsuit about one hacktivist act, another operation begins. The other reason is that after the first lawsuit (2012-2015), investigations of Redhack are conducted under confidentiality order, which prevents access to investigation materials. For that reason, the table below is prepared not just based on tweets or news articles but also through documents provided by the judicial actors related to the cases during the field study.

The table of judicial processes contains the acts of detention, arrest, indictment, trial, release, court decision, and acquittal. Several transfers of the investigation between different prosecutor's offices, especially the ones between the office specializing cybercrime and the office specializing in anti-terror are also exhibited in the table.

Table 4.3: Judicial Processes related to Redhack

Date	Judicial process	Related act
20 March 2012	Operation of the prosecutor's office specializing in cybercrime, detention of 17 people, 7 people arrested (Bianet, 2012a)	Data leaks from Ankara Police Directorate

Chapter 4: Hacktivist experience in Turkey

4 July 2012	Transfer of the investigation from the prosecutor's office specializing in cybercrime to the prosecutor's office specializing in anti-terror (Hürriyet Daily News, 2012)	Data leaks from Ankara Police Directorate
7-9 August 2012	Release of 4 people (Ankara Heavy Penal Court No. 7, 2015)	Data leaks from Ankara Police Directorate
25 September 2012	Indictment of Ankara Chief Public Prosecutor's Office against 10 people (Ankara Chief Public Prosecutor's Office, 2012)	Data leaks from Ankara Police Directorate
26 November 2012	First trial, release of 3 arrested people, one arrest (T24, 2012a)	Data leaks from Ankara Police Directorate
27 November 2012	Release of the arrested (Odatv, 2012c)	Data leaks from Ankara Police Directorate
9 May 2013	Declaration of mistrial by the anti-terror prosecutors probing Redhack and transfer of the prosecution to the prosecutor's office specializing in cybercrime (Cumhuriyet, 2013a)	Unspecified data interference and data leaks from Ministry of Foreign Affairs, Ministry of Interior, Council of Higher Education, etc. (upon complaint of plaintiff state institutions)
23 May 2013	Operation of military prosecutor's office, one private (Utku Kalı) arrested (Cnn türk, 2013)	Data leaks of Reyhanlı
3 July 2013	Istanbul Police Directorate's investigation report about Redhack as a cyber-terror organization with the charge of provocation in the Gezi Protests (Sabah, 2013)	The Gezi Protests
17 July 2013	Indictment of military prosecutor's office, the decision of lack of jurisdiction, and the transfer from the military prosecution to the Heavy Criminal Court specialized by Anti-Terror Law Article no. 10 (Sivas no. 5 Military Prosecutor's Office, 2013)	Data leaks of Reyhanlı
21 October 2013	First trial (Odatv, 2013c)	Data leaks of Reyhanlı
11 November 2013	Release of Utku Kalı (Hürriyet, 2013d)	Data leaks of Reyhanlı
22 November 2013	Operation of the prosecutor's office specializing in cybercrime, detention of 13 people (one person added afterwards) including Taylan Kulaçoğlu, popular actor Barış Atay and some of the same	Unspecified data interference and data leaks from Ministry of

	arrested people from the Ankara Police Directorate case (Cumhuriyet, 2013b)	Foreign Affairs, Ministry of Interior, Council of Higher Education, etc. (upon complaint of plaintiff state institutions)
25 November 2013	Transfer of the investigation from the prosecutor's office specializing in cybercrime to the prosecutor's office specializing in anti-terror (Hürriyet, 2013e)	Unspecified data interference and data leaks from Ministry of Foreign Affairs, Ministry of Interior, Council of Higher Education, etc. (upon complaint of plaintiff state institutions)
25 November 2013	Release of 14 detainees (Bbc News Türkçe, 2013)	Unspecified data interference and data leaks from Ministry of Foreign Affairs, Ministry of Interior, Council of Higher Education, etc. (upon complaint of plaintiff state institutions)
28 November 2013	Operation, second detention and arrest of Taylan Kulaçoğlu (SoL, 2013h)	Unspecified data interference and data leaks from Ministry of Foreign Affairs, Ministry of Interior, Council of Higher Education, etc. (upon complaint of plaintiff state institutions)
12 December 2013	Release of Taylan Kulaçoğlu (Haber Türk, 2013)	Unspecified data interference and data leaks from Ministry of Foreign Affairs, Ministry of Interior, Council of Higher Education, etc. (upon complaint of plaintiff state institutions)

Chapter 4: Hacktivist experience in Turkey

16 March 2015	Court decision, acquittal of all accused (Ankara Heavy Penal Court no. 7, 2015)	Data leaks from Ankara Police Directorate
4 February 2016	Acquittal of Utku Kalı (Amasya Heavy Penal Court, 2016)	Data leaks of Reyhanlı
25 September 2016	Operation of the prosecutor's office specializing in crimes against the constitutional order, ²⁵ six people detained, three of them were acquitted from the previous Redhack case, third detention of Taylan Kulaçoğlu (Cumhuriyet, 2016d)	Data leaks from Berat Albayrak
6 October 2016	Release of all detainees (SoL, 2016)	Data leaks from Berat Albayrak
25 December 2016	Operation of the prosecutor's office specializing in organized crime, detention of five journalists (Sabah, 2016)	Data leaks from Berat Albayrak
3 January 2017	Operation of the prosecutor's office specializing in crimes against the constitutional order, detention of one person (Tunay Şentürk) (Ntv, 2017)	Data leaks from Berat Albayrak
11 January 2017	Release of the detainee (Tunay Şentürk) (Etha, 2017)	Data leaks from Berat Albayrak
18 January 2017	Arrest of three journalists (Cnn Türk, 2017)	Data leaks from Berat Albayrak
14 February 2017	Detention of one journalist (Deniz Yücel) (Bbc News Türkçe, 2018)	Data leaks from Berat Albayrak
16 February 2017	Arrest of Tunay Şentürk (Yolculuk, 2017a)	N/A
27 February 2017	Arrest of Deniz Yücel (Deutsche Welle Türkiye, 2017)	Data leaks from Berat Albayrak
21 April 2017	Operation of the prosecutor's office specializing in organized crime and MİT, detention of one person (Hünkar Alican Duman) (Sputnik Türkiye, 2017)	Data leaks from Berat Albayrak
24 April 2017	Release of the detainee (Hünkar Alican Duman) (Duvar, 2017)	Data leaks from Berat Albayrak
23 June 2017	Indictment of Istanbul Chief Public Prosecutor's Office against 6 people (Istanbul Chief Public Prosecutor's Office, 2017)	Data leaks from Berat Albayrak

²⁵ Prosecutor's offices specializing in crimes against the constitutional order is constituted in March 2014, in the place of prosecutor's offices specializing in anti-terror abolished after the political conflict between AKP and the Gülen Cemaati in December 2013. Crimes related to terror and military coup are under the responsibility of these offices (Cumhuriyet, AKP'den yeni 'operasyonel' büro, 2014).

4 July 2017	Separation of the investigation between other journalists and Deniz Yücel (T24, 2017)	N/A
24 October 2017	First trial, release of one journalist (Ömer Çelik) (Deutsche Welle Türkiye, 2017a)	Data leaks from Berat Albayrak
6 December 2017	Second trial, release of two journalists (Tunca Öğreten ve Mahir Kanaat) (Diken, 2017)	Data leaks from Berat Albayrak
16 April 2019	Last trial, ongoing lawsuit (Evrensel, 2019)	Data leaks from Berat Albayrak

As the table shows, there are five different judicial processes related to Redhack. These are called as “Redhack’s operation” and “Redhack’s case” in the news media. First one is the case related to the data leaks from Ankara Police Directorate (2012-2015). In this lawsuit, suspects were charged with being terrorist offender (Turkish Anti-Terror Law, Article no. 2, 1991)²⁶ and being part of a terrorist organization (Turkish Anti-Terror Law, Article no.7), as well as with establishing organisations for the purpose of committing crimes or committing an offence on behalf of an organisation, although not being a member of that organization (Turkish Penal Code, Article no. 220, 2004), illegally obtaining data (Turkish Penal Code, Article no. 136), unlawfully accessing a data processing system (Turkish Penal Code, Article no. 243), preventing the functioning of a system and deletion, alteration or corrupting of data (Turkish Penal Code, Article no. 244) and with securing prohibited information (Turkish Penal Code, Article no. 334). From this first judicial process, there is a wide range of applicable articles of TPC, as from parts on crimes against person, crimes against the public, and crimes against nation and state. Alongside, Anti-terror law (TMK) is mentioned in the indictment (Ankara Chief Public Prosecutor's Office, 2012). This diversity exhibits that from the beginning, acts of Redhack were perceived as a fusion of different crimes from the perspective of the state: obviously cybercrimes, but also as terror offences.

Second judicial process resulted from the data leaks of Reyhanlı (2013-2016). The private who allegedly leaked the gendarmerie intelligence to Redhack was charged with securing information relating to state security (Turkish Penal Code, Article no. 327) and disclosure of information relating to the security and political interests of the state (Turkish Penal Code, Article no. 329) during this lawsuit (Hürriyet, 2013d). This lawsuit was known

²⁶ The official name is Law on Fight against Terrorism of Turkey (Act No. 3713, 1991).

as an espionage case in the news media (Radikal, 2013), as the charges against the private were classified as “Offences against State Confidentiality and Espionage” (Turkish Penal Code, 2004). Actually in the first trial, one of the applicable articles (Turkish Penal Code, Article no. 334) was also an article from this part of TPC. Most probably because of the demography of the accused, espionage was not brought to agenda. Different from the private Utku Kalı who can be easily charged for a classical example of espionage based upon his profession and competence to have access to such information, accused of the first trial were very young people, mostly students who cannot be related to espionage in the classical sense.

Third (2013-) and fourth (2016-) judicial processes are not lawsuits but ongoing investigations. There is a high possibility that these investigations are related to the ongoing investigation opened upon complaint of state institutions about which the transfer of the file from the prosecutor’s office specializing in anti-terror to the prosecutor’s office specializing in anti-terror was on the news in May 2013 (Cumhuriyet, 2013a). These investigations are the most ambiguous ones because there are no indictments prepared in consequence of these investigations and for that reason, there are no lawsuits. Plus, they are conducted under confidentiality orders. In these investigations, accusations are not directly linked to specific acts of Redhack, as the indictments in other processes show. Even there are no mentions of specific acts of Redhack. During these investigations, the detainees were accused with the same charges as the ones in earlier lawsuits. These were the disclosure of information relating to the security and political interests of the state (Turkish Penal Code, Article no. 329), establishing organizations for the purpose of committing crimes – including becoming a member of an organization established to commit offences (Turkish Penal Code, Article no. 220), unlawfully accessing a data processing system (Turkish Penal Code, Article no. 243) and securing information relating to state security (Turkish Penal Code, Article no. 327), according to the written statement of the accused (Ankara Heavy Criminal Court no. 2, 2013). Putting aside the crime that is referred, the charges of the judicial power against Redhack was the same in this investigation. Within the investigation becoming manifest in 2016, the detainees are charged with illegally obtaining data (Turkish Penal Code, Article no. 136) and being member of an armed organization (Turkish Penal Code, Article no. 314), which is defined as a terrorist offence (Turkish Anti-Terror Law,

Article no. 3), as the statement prepared by the police shows (Ankara Police Dep. Organized Crime Control Bureau, 2016). The decision about the confidentiality order about this investigation refers also to the violation of the constitution (Turkish Penal Code, Article no. 309), which is also a terrorist offense according to Anti-Terror Law, Article no. 3 (Ankara Criminal Courts of Peace no. 7, 2016).

Prosecutors did not give any decisions of non-prosecution for these investigations. If these are separate investigations or parts of one investigation is not a public knowledge, either. However, the statements and the decision of confidentiality order show that the tendency to consider the charges of Redhack as a mix of cybercrime and terror continues in these investigations.

In the last judicial process arising from the leaks of the e-mail account of Berat Albayrak (2016-), the suspects were charged with making propaganda for a terrorist organization (Turkish Anti-Terror Law, Article no.7) and preventing the functioning of a system and deletion, alteration or corrupting of data (Turkish Penal Code, Article no. 244), according to the (Istanbul Chief Public Prosecutor's Office, 2017). Once again, we see the coexistence of terrorist offence and cybercrime within the charges towards Redhack.

4.2.1. Oscillations: Cybercrime or terror?

As the judicial documents exhibit, two major bodies of legislation appear: cybercrimes and terror offences. Information and Communication Technologies Authority (BİK) defines cybercrime as “illegal, unethical, or unauthorized acts within systems that automatically process or transfer data” (Bilgi Teknolojileri ve İletişim Kurumu, 2016). With a crucial *or*, “crimes through the use of computer and communication technologies” are added as a second and much larger definition for cybercrimes (Bilgi Teknolojileri ve İletişim Kurumu, 2016).

Articles under the part entitled “Offences Related to Data Processing Systems” of the TPC, articles no.243, 244, and 245, are the ones that regulate explicitly cybercrime acts in the Turkish legal system (Bilgi Teknolojileri ve İletişim Kurumu, 2016a). Article 243 about accessing unlawfully a data processing system and Article 244 about preventing the functioning of a system and deletion, alteration or corrupting of data are often referred in

the judicial processes of Redhack. Article 245 about the misuse of bank or credit cards is never referred as a charge against the group. These articles correspond to the first definition of cybercrimes. I also prefer to focus on this definition for now, rather than the ambiguous second definition. Yet, it should be stressed that this dual definition will be manifest within the discourse of crime framing.

On the side of crimes of terror, as the Reasoned Decision of the first Redhack lawsuit (Ankara Heavy Penal Court no. 7, 2015) reveals once again, Anti-Terror Law of Turkey no. 3713 First Article defines what terror is for the Turkish legal system:

Any criminal action conducted by one or more persons belonging to an organisation with the aim of changing the attributes of the Republic as specified in the Constitution, the political, legal, social, secular or economic system, damaging the indivisible unity of the State with its territory and nation, jeopardizing the existence of the Turkish State and the Republic, enfeebling, destroying or seizing the State authority, eliminating basic rights and freedoms, damaging the internal and external security of the State, the public order or general health, is defined as terrorism.

(Turkish Anti-Terror Law, Article no. 1, 1991)

Aforementioned reasoned decision refers also to a decision by the Constitutional Court to cite three conditions to define an act as a terrorist act:

- Methods of oppression, force, and violence, terrorization, intimidation, suppression, or threatening,
- Aims cited in Article no.1 of Anti-Terror Law,
- Agency of members of a terrorist organization or of persons who, not being a member of a terrorist organisation, commit a crime in the name of the organization

(Ankara Heavy Penal Court no. 7, 2015, p. 12)

Alongside the coexistence of these two major bodies of cybercrimes and terrorist offenses, there is an indecision manifesting in several transfers of the judicial files between different

prosecutors' offices. During the first Redhack investigation in 2012, the prosecutor specializing in cybercrime decided that this was outside of his jurisdiction and the investigation was transferred to the prosecutor specializing in anti-terrorism (Hürriyet Daily News, 2012). In May 2013, this time, in another investigation that had begun with the complaint of plaintiff state institutions, anti-terrorism prosecutors looking to the investigation in Ankara declared mistrial by claiming that Redhack was not a terrorist organization but an illegal organization because it was not an armed organization, nor its actions involve violence (Cumhuriyet, 2013a). Even so, this decision made in the scope of another investigation did not influence the first judicial process related to Ankara Police Directorate leaks. The charges of terrorism still appeared in the reasoned decision in 2015. This charge is based upon the support of Redhack for "Marxist-Leninist-Maoist leftist and separatist groups." In this line, prosecutor declares that Redhack's members are committing a crime in the name of terrorist organizations without being members. The judge of the lawsuit declared Redhack as an illegal organization, without claiming it as a terrorist organization (Ankara Heavy Penal Court no. 7, 2015). That decision exhibits that terror offences related to Redhack resulted not from its acts but from its alleged relation with organizations that the Turkish judiciary acknowledges as terrorist.

In the lawsuit in which Utku Kalı was charged for Reyhanlı leaks, the file was also conveyed from the military court to Samsun Heavy Penal Court specializing in anti-terrorism, once again with the declaration that the file was outside of the military prosecutor's jurisdiction (Radikal, 2013). Utku Kalı was acquitted based on lack of evidence, as the suspects of the first lawsuit of Redhack were acquitted (Sputnik Türkiye, 2016). The reasoned decision exhibits that the suspects were acquitted based on the lack of evidence (Amasya Heavy Penal Court, 2016). In the plea of defense prepared by the lawyer of Kalı (Kalı, 2016), the charges of securing information relating to state security (Turkish Penal Code, Article no. 327) and of disclosure of information relating to the security and political interests of the state (Turkish Penal Code, Article no. 329) were objected based upon a very crucial issue: the lack of a specific definition on state's secrets within the Turkish legislation (Kalı, 2016). However, as the court decided on acquittal without discussing the alleged crimes, this point of whether the act of data leaks in the case of the

Reyhanlı explosion were considered as espionage – as these articles of TPC are under the category of espionage, or as terrorism, we do not know.

In July 2013, Istanbul Police Directorate prepared an investigation report in which they categorized Redhack as a cyber-terrorist organization and charged them with provoking masses during the Gezi protests (Sabah, 2013). The short-period of time between this report and the earlier decision by the prosecutors in Ankara is significant to understand the non-negligible nature of the oscillation between two frames – terror and cybercrime – used by the state for Redhack.

During the investigation of Redhack in November 2013, like in earlier judicial processes, the prosecutor specializing in cybercrime decided once again that this was outside of his jurisdiction and the investigation was transferred to the prosecutor specializing in anti-terrorism (Hürriyet, 2013e). This ongoing investigation has been probed by the prosecutor specializing in anti-terrorism since that time.

In the last lawsuit about the leaks from Berat Albayrak's e-mail account, charges about the terrorist offences are clear since the beginning. In that sense, there is not an oscillation, as it was seen during earlier processes. However, now there is a change in the perception of the judicial perspective about terror offences. Here what is judged is not the act of Redhack, the leaks of Berat Albayrak, but the usage of the leaks by the journalists. In the indictment, Redhack is once again framed as a supporter of "Marxist leftist" terrorist organizations. Besides, the charges against the journalists are framed not through this terror framing of Redhack but based upon their individual positions as terrorist organization supporters [*terör örgütlerine müzahir*]. Names of many ideologically diverse organizations are mentioned in the indictment as the suspects are allegedly supporting are far-leftist DHKP-C (Revolutionary People's Liberation Party/Front) and MLKP (Marxist–Leninist Communist Party), Kurdish democratic confederalist PKK/KCK (Kurdistan Workers' Party/Kurdistan Communities Union), and FETÖ/PDY²⁷ (Istanbul Chief Public Prosecutor's Office, 2017, pp. 4-9). Alongside these names, ISIS appears as the main crime of this indictment is to operate a perception about the relation between "Republic of Turkey

²⁷ First abbreviations (DHKP-C, MLKP, and PKK/KCK) are the names that the organizations use for themselves. However FETÖ/PDY (Fethullahçı Terror Organization/Parallel State Structure) is the name given to the religion-based Gülen Cemaati after their military coup attempt in 2016.

Minister of Energy and Natural Resources and DAEŞ terrorist organization” (Istanbul Chief Public Prosecutor’s Office, 2017, p. 4).

Here the oscillation is not between cybercrimes and terror offences. This time, the coexistence of many different organizations already framed as terrorist by the Turkish state appears in the indictment of the lawsuit about Redhack. The frame of terrorism becomes blurry, as ideologically different – even opposite – organizations come together within the same indictment. This bundling of terror offences will constitute one of the main critiques of terror frames within the crime framing of Redhack.

4.2.2. *A Game of targets: Punishing the periphery*

There is not a person sentenced to penalty resulting from any judicial processes about Redhack.²⁸ However, in every process – especially in lawsuits, suspects spent long periods of arrest in prison. During the first lawsuit about the leaks from Ankara Police Directorate, three accused stayed arrested for more than nine months (Cumhuriyet, 2015). In the second lawsuit about the leaks of Reyhanlı, Utku Kalı stayed arrested for more than five months (Sputnik Türkiye, 2016). As said before, in both lawsuits, all the suspects were acquitted for the lack of evidence. Within the scope of the last lawsuit where journalists were charged, three of them released after spending almost one year in prison (Diken, 2017).

During the investigations, one of the suspects of the 2013 investigation – Taylan Kulaçoğlu – is detained three times in total: two times within the scope of the 2013 investigation in which second detention resulted in an arrest of less than a month (Haber Türk, 2013), and one time within the scope of the 2016 investigation (Cumhuriyet, 2016d). Another suspect of the 2012-2015 lawsuit was arrested for eight months in 2012 and acquitted in 2015. He was detained again in each of the investigations, one in 2013, the

²⁸ Tunay Şentürk that was once detained during the Redhack investigation of 2016 stayed arrested for 22 months. However related to which investigation or lawsuit he stayed arrested is not a public knowledge. This confidentiality can be the result of his witness position in another important lawsuit related to the 2014 National Intelligence Organization scandal in Turkey. In his statements, he admits owning the account *lazepam*, an account name appearing often in charges against Redhack, yet Şentürk denies to have any relation with Redhack (Ajans Türk). Other newspapers claim that Şentürk is a member of Redhack (Sabah, 2018). In sum, we do not know if Şentürk was sentenced to penalty for being a member of Redhack. For that reason, he is not counted as a sentenced of a Redhack related lawsuit.

other in 2016. There are also allegations of torture against this suspect during his detention (Cumhuriyet, 2016e).

Long periods of arrests and repetitive detentions with mistreatment allegations exhibit that these preventive judicial measures are used as punishment tactics by the Turkish judiciary. This reaction can be the manifestation of an impasse about how to react against the acts of Redhack. Another indicator of this feeling of impasse can be distinguished through the changing targets of the judicial processes about the acts of Redhack. In this line, the last lawsuit about the leaks from Berat Albayrak stands in a dissimilar position compared to other processes. In the first lawsuit, the target of the judicial power was the primary perpetrators – hackers. Accused were the members of Redhack, people alleged to hack the police directorate. In the second lawsuit, the target was the private who allegedly shared the leaked information with Redhack. The accused private was not charged with being a member of Redhack, even though he was considered a primary perpetrator. In the last lawsuit, the judiciary power was not targeting the people who performed the leaks from the beginning. The target was the journalists who circulated the news about the leaks – secondary perpetrators of the hacking act. In that sense, it can be argued that as the Turkish judiciary confronted the impasse of *finding* Redhack, it changed its target and changed its direction towards the periphery of the hacktivist group, as to minimize the effects of the hacktivist acts.

4.3. Conclusion

Complicated history of Redhack's acts and their judicial processes exhibits an impasse and indecision of judicial actors about how to react to the group's acts. Especially the years of Redhack's high activity between 2012 and 2014 result in a high activity of judicial processes, too. However, not just during this period but even after 2014, Turkish judiciary continues to react to the acts of Redhack. Judicial processes mentioned above show that data leaks are the main reason of the reaction of the state against Redhack. In lawsuits and also in investigations, important charges²⁹ are mostly resulting from the acts of leaking data belonging to the state. The explicit judicial reaction indicates as if Redhack did not perform

²⁹ By important charges, I mean charges with heavier penalties.

data leaks, the group would not be faced with crime accusations. Yet, such a deduction would be too superficial to ignore the popular aura of the hacktivist group. For example, the impact of Redhack's fusion of humor and leftist legacy that the group used to react against agenda topics is an issue that cannot be observable through written documents of judicial processes. Similarly, we cannot know if the exhibition of hacking prowess and state vulnerability that Redhack was often performing has any influence on the crime frames about the group, either. These nuances stand for the necessity to enlarge the examination of judicial processes in two directions. One direction will follow external links of judicial processes. An investigation about crime framings outside the scope of the judiciary is necessary to understand the significance of judicial processes. The other direction will deepen the judicial processes through internal links. That means an examination of the discourse of judicial actors to unearth individual crime framings of Redhack.

CHAPTER 5

USUAL SUSPECTS OF THE CRIME FRAMING:

SPONSORING AND EMPLOYMENT OF THE OFFICIAL FRAMES

After the referential chapter about the acts of Redhack and the judicial processes related to the group, from this chapter on, I will focus on the construction of the crime frames of Redhack within discursive practices with an interpretive, qualitative approach stressing the cultural and political content of framing processes. Following that, I will consider frames as “specific and explicit agents of ideological processes” in line with the critical paradigm of framing research (Reese, 2010, pp. 18-19).

Following that, this first chapter about the construction of crime frames will discuss the usual suspects of the crime framing. These are political actors and journalists, as the literature of framing proposes. Based upon selective news analysis, this chapter will exhibit their quasi-absence as active agents within the crime framing of Redhack. The aim of this chapter is to identify the preference of these actors based upon general aspects rather than a detailed analysis of their framing.

In the theoretical chapter, a tripod research model was given as the method to follow in the examination of crime frames for the case study. This model focuses on the sponsoring of frames by political actors, the employment of these frames by journalists, and the interpretation of the frames by the audience (Carragee & Roefs, 2004, p. 215). Another approach in which the framing process centers on social movements, a slightly different multidimensional perspective is followed. This time, the study on frames aims at explaining an entire episode of contention, including the organizers of a movement, the media, significant third parties and the state. It is the examination of interactively constructed frames and their opposing nature, in other words, framing contests (Tarrow, (1994) 2011, p. 144).

In the study of crime frames about Redhack, I intend to unit these two approaches. In that line, for the construction of frames, different sources of framing appear as potential constructors. They can be categorized as political actors and actors from news media. However, when we try to apply this schema to the framing of Redhack, there are two incompatibilities. First, in the level of political actors, we witness a quasi-silence about the sponsoring of crime frames for Redhack. The other is the passive employment of the frames by actors from news media.

5.1. The quasi-silence of political actors

In the literature of framing analysis, the category of official frames is constituted of frames sponsored by political actors; politicians connected to systemic political parties. Yet the examination of this sponsoring is actually an undervalued research area of that literature. Especially when it comes to the mobilization of official frames to interpret political dissent, few works appear (Zuo & Benford, 1995; Noakes, 2000; Noakes & Wilkins, 2002). With the awareness of this blind spot about the construction and the promotion of official frames (Noakes, 2000, p. 659) and following the perspective of Carragee and Roefs (2004), I begin my examination with the frames constructed by political actors for Redhack, as the first step of the crime construction.

During 2012-2018, the period in which Redhack was on the national agenda with its acts and the judicial processes related to the group, few instances of official crime frames are explicit, as Twitter and news archives show. Among all the top tweets in Turkish that contain the keyword “redhack” since 2009, the first time that “redhack” was mentioned in Twitter – according to Twitter Advanced Search, there is just one speech of then Prime Minister Recep Tayyip Erdoğan in which he commented about the hacktivist group (Hürriyet, 2013f).

This finding is supported with another search within the news archive of Milliyet, one of the mainstream national newspapers with highest circulation. The mentioned speech is about the hacked and leaked documents allegedly belonging to the Gendarmerie Intelligence Department about the Reyhanlı explosion in May 2013. Redhack claimed to leak documents proving that Al-Qaeda was the responsible of this explosion in the border

town and that Gendarmerie Intelligence had knowledge about the incident before it had happened. In his response to the question of a journalist, Erdogan mentions Redhack as “these hackers” without using a specific crime frame for the group but *acknowledging* them as hackers. Yet, he does not refrain to activate another more familiar crime frame, a terror frame, as he says:

Assumptions [about the perpetrators of the explosion] would mean making propaganda and it should not be done. Otherwise, it would mean *unwitting support* to terror and terrorist organizations.

(Milliyet, 2013b)

In this speech, Erdoğan uses a very light and indirect terror frame related to the hacktivist group. “Unwitting support to terror” is a conceptualization that became apparent at the beginning of the 2000s. This logic of supporting terrorist organizations not on purpose considers a type of citizen who can be easily deceived and who constantly needs to be protected (Üstel, (2004) 2008, p. 304). Here, the terror discourse frames not only the active agents – terrorist – but also the potential audience. This citizen type who is unwittingly instrumentalized by terrorist organizations is part of “the menace and danger discourse” (Üstel, (2004) 2008, p. 299) of the 1990s. In this perspective, first signals of the later criminalization of Redhack’s periphery are apparent in this speech of Erdoğan from 2013. This criminalization would be witnessed in the lawsuit against the journalists in 2016 related to the data leaks of Berat Albayrak.

Compared to the terror frames that Erdoğan would use actively in following years, Redhack’s framing of terror can be considered as a quite passive one. Different from the light terror frame used for Redhack, Erdoğan would often use terror frames as enlarged and influential labels to include incrementally HDP³⁰, Gülen Community³¹, and many leftist

³⁰ The active framing of HDP as a terrorist organization coincides with the creation of the first hung parliament since the coming to power of AKP in June 2015, especially due to the high voting rate of HDP, and with the collapse of the Solution Process between the Turkish state and PKK following this election.

³¹ FETÖ/PDY (Fethullahçı Terror Organization/Parallel State Structure) is the name given to the religion-based Gülen Community after their failed military coup attempt in 2016. This community was the former political ally of AKP, before their conflict peaked in the alleged Corruption Leaks in December 2013. Known

dissidents³² under the umbrella term of “unarmed terrorists” by the beginning of 2016 (Diken, 2016). The transformation of the “unwitting support to terror” framing to this “unarmed terrorists” corresponds to a change in the official framing. Within this new discourse, the official framing would convert the ones at risk (citizens who can be easily deceived, constantly in the need of protection, and therefore, who can unwittingly support terror) to the responsible ones (terrorist organization propagandists). With this new and active framing of terrorism, Erdoğan would declare:

There is no difference between terrorists and those who gave order to [influence] the terrorists by using its position, its pen and its title. An academic, a journalist, the director of an NGO are also terrorists.

(Diken, 2016)

This apparent contrast between the light terror framing of Redhack and the more severe framing that is much more prevalent can be explained by the time lag. Erdoğan’s only framing of Redhack with terror is from 2013 and the beginning of the active terror frames including “unarmed terrorists” is 2016. Three years between 2013 and 2016 were actually a crucial period, even within the fast-changing political agenda of Turkey. The comment of Erdoğan about Redhack related to the Reyhanlı explosion was before the mass uprising of Gezi Protests against the government beginning in May 2013 and before the conflict in December 2013 fueled by the rivalry between two powerful centers within the power bloc: AKP and Gülen Community. This rivalry would result in the failed military coup of July 2016.

The political atmosphere in Turkey would become heavier in 2015, with the hung parliament in June 2015 and the end of the Solution Process following this election. The regular usage of violence as a political tool by ideologically diverse groups like ISIS and TAK³³, and also by the state, especially in summer and autumn 2015 would identify the

as the *Tape Scandal*, 2013 Corruption Scandal based upon leaked tapes allegedly belonging to top political figures from AKP brought into view the political dispute between two powerful former allies and now rivals.

³² Academicians for Peace is an example where the terror label was used actively by the state. In this incident, thousands of academicians in Turkey had signed the Petition for Peace, a call for action to the Turkish state to stop the violence against the civilians in Kurdish regions.

³³ Kurdistan Freedom Hawks (TAK) is an armed, Kurdish ultra-nationalist organization.

politics in Turkey for the next few years and would peak with the military coup attempt in July 2016 and the state of emergency declaration following this attempt that would last until January 2018. The proliferation of terror frames by political actors and the criminalization of dissent are parts of this political context than can be described as “a process of rapid democratic retrenchment” and “growing authoritarianism” (Baser, Akgönül, & Öztürk, 2017).

There would be no other crime or terror frames for Redhack used by Erdoğan again. Different from how one could expect to observe, there is not an increment in the usage of terror frames in the case of Redhack, in proportion to the general usage of terror frames.

Apart from Erdoğan, the crime framing by other political actors is also quite weak. Then Foreign Minister Ahmet Davutoğlu and AKP’s then Vice President Hüseyin Çelik, alongside then Deputy Prime Minister Beşir Atalay were the other political actors who gave public speeches about Redhack’s alleged leaks of Reyhanlı documents. While Davutoğlu (Milliyet, 2013a) and Atalay (Milliyet, 2013c) do not use any active crime frames for Redhack in their responses, Çelik emphasizes that the act of Redhack is not hacking but a physical information leak (Hürriyet, 2013). In his speech, he says:

The incident is *not hacking but physical information leak*. The image of aforementioned documents was taken by a gendarmerie private and sent to Redhack when the documents were going to be lodged to commanders. The private who did this is confirmed and arrested. In the report, there is the mention of another terrorist organization. *Redhack confused the name of the terrorist organization and then, they published incorrectly* [emphasis added].

(Akşam, 2013)

There are two crucial points in this speech. First is the emphasis on framing this deed of Redhack as a non-hacking, instead of a crime framing. In many cases, social control is implemented through a process of labelling and treating dissenters as deviants, in other words, through criminalization, with revenge, restitution, and/or deterrence needs. Yet, it does not mean that control agents consider all political protest in all circumstances as deviant attitude (Wilson, 1977, p. 470). This act of Redhack that allegedly exhibited the

state's responsibility in the Reyhanlı explosion did not provoke such needs from the official perspective. The official discourse of the period does not reflect any counter-framing tactics, the ordinary reactions of states in many different contexts. Framing effort aimed at discrediting the claim of Redhack is not fueled by the criminalization of the group, but through their lack of prowess. While Çelik implicitly frames Redhack as a group that cannot be qualified as a hacker group and displays it as an example of *spying*, compatible with the charges against the arrested private. This frame is derived from the conventional war scenarios, rather than a cybercrime and hacking frame.

On the other hand, this reaction of discrediting the group reminds of the official frames constituted for paramilitary groups fighting against states. States refer to their legitimate monopoly of violence with a stress to the military deficiency and incapacity of these opposite groups, as an added element of their negative framing in official frames. In that line, hacking becomes an indicator of cyberwar in which these political actors did not want to be seen as vulnerable against the attacks of a possible enemy, in the perspective of the political actors in Turkey in 2013. Then, the critical difference is between the war frame explicitly declared by the minister – physical leaks – and the cyberwar frame implicitly avoided – data leaks through hacking.

Such framing is quite different from the usual official frames that states form against social movements with references to “turmoil,” “upheaval,” “a violation of the constitution,” and “a plotted conspiracy” (Zuo & Benford, 1995, p. 143). The framing against hacking slightly constructs the act of Redhack as a threat within a war framing. Even though when this hacking aims the exhibition of state's responsibility, a demand for the accountability of the state within the democratic scope, instead of facing directly the state.

Initial signals about this war framing were actually given in December 2012, when Redhack crashed the website of the Ministry of Transport because the ministry had blocked the roads to Maraş to restrain the protesters from commemorating the Maraş Massacre³⁴ at the place of the event, Maraş. Related to this act of Redhack, then Minister of Transport

³⁴ In December 1978, more than hundred local Alevites and left-wingers were killed in Maraş in an organized event by fascist and Islamist groups leaded by *Ülkü Ocakları*. The passivity of the law enforcement forces resulted in the aggravation of the events. After the events, a state of stage was declared in many cities of Turkey.

Binali Yıldırım declared that “cybersecurity became the synonym of national security” (Evrensel, 2012). We cannot follow a persistent framing of Redhack because of the scarcity of the official frames about Redhack. However, judicial processes about Redhack in which the charges are centered around the terror crimes and the crimes against the state exhibit how Redhack is framed as an enemy of the state, similar to an armed enemy, by the Turkish State. This negative perception is just one part of the complex framing of Redhack.

When we return once again to the framing of the Reyhanlı leaks in 2013 and to the declaration of AKP’s then Vice President Çelik, on the opposite of the war framing for hacking, another and a much more positive framing of Redhack manifests itself. This is the second crucial point. In his speech, Çelik said: “Redhack confused the name of the terrorist organization and then, they published incorrectly” (Akşam, 2013). This presumption about the confusion of Redhack frames the group as a *guiltless and confused* actor, who acted on the basis of a mistake. Such a framing is quite unusual for a group perceived as an enemy of the state. In that sense, it can be argued that contradictory frames about Redhack – war framing and a more legitimate addressee framing – were visible together at that period.

The side of the dissident political actors is less fruitful than the governmental actors when it comes to framing Redhack. In general, Redhack is framed as a “red hacker group,” (Milliyet, 2013e) a framing in line with how Redhack self-frames, as it is apparent in its name.³⁵ It can be argued that this is a compatible framing that reflects a kind of acceptance of the group by dissident actors. This framing of addressee is emphasized with the acts of the actor from the dissidence; CHP’s (Republican People’s Party) then Vice President Erdoğan Toprak asked about the Reyhanlı leaks of Redhack as a parliamentary question towards the Prime Minister after the act.

The scarcity of official frames about Redhack can also be related to the novelty of the given acts. Considered as a new type of acts and a new type of actor, especially at the early period of Redhack’s popularity, political actors experienced difficulty to interpret the hacktivist group. When Redhack was on the agenda in May 2013 with the Reyhanlı leaks,

³⁵ Self-frames of Redhack constitute an encountered reference in the frames constructed by other actors. In the totality of this research, the construction of frames is considered as a circular process influenced by and influencing frames of other actors. As such circularity cannot be applied to the linear logic of a written document, I preferred to place the self-frames of the group after the frames constructed by other actors.

different frames were used among political actors who did not know how to categorize the group. Redhack used this confusion as a source of humor in their tweet:

The Assembly discusses yesterday: Dilek Yılmaz from CHP said a website called RedHack, Alim Işık from MHP [Nationalist Movement Party] said a media outlet called RedHack. ;)

(@TheRedHack, 2013b)

Even in the discourse of the political actors who entered into online arguments with the group and who were allegedly hacked by Redhack, no crime frames can be seen against the group. Neither then Mayor of Ankara Metropolitan Municipality Melih Gökçek (Milliyet, 2012a), nor then State Minister and Chief Negotiator for the EU Egemen Bağış (Milliyet, 2013d) do not use any crime frames against the group when they respond to the claims of their being hacked. Melih Gökçek's further polemics with the group in the following years continue to not construct any crime frames even though he uses an abusive language against Redhack (Ulusal Kanal, 2013).

One of the few crime frames of Redhack is activated at the end of 2013 with a speech by then Minister of Interior Muammer Güler. Güler gives that speech right after the detention of a famous actor, as a suspect during the Redhack investigation. Here, he frames Redhack as “a network or an organization” (Milliyet Tv, 2013) and in that way, he guides the audience to an explicit crime frame, as these wordings connote crime networks and crime organizations.

In this part dedicated to the potential constructors of the crime framing about Redhack, I examined the construction of criminalization by official frames. Adopting the power bloc perspective of Poulantzas ((1968) 1978, p. 141), I did not limit official frames with the frames of the governmental agents. I also added the few framing examples constructed by the actors from CHP and MHP, other constituents of the power bloc in the contemporary Turkish state.

Official discourse exhibited a quasi-silence about the criminalization of Redhack, especially when Redhack's framing is compared to other contemporary terror frames.³⁶ Few frames and fewer crime frames attest to the lack of certitude about how to frame and to react discursively against this group that the Turkish state had not been used to face with. From one side, official frames indicate a light framing of terror and war. However, at the same time, they reveal an almost positive framing of an addressee, quite unfamiliar for actors acknowledged as terrorist or enemy.

The apparent confusion about how to frame the group results also from the lack of knowledge about internet and computer technologies. This confusion is reflected in describing the group as website and as media outlet, an effort to engrave Redhack to more conventional and familiar shapes. However, when this silence is thought together with the quite aggressive and active framing from judicial processes with explicit terror charges, another connotation comes forward. Then the question of whether this silence is a deliberate tactic of the state to contain a fact that is uncontrollable with the conventional discursive tools remains unanswered for now.

5.2. Passive framing of news media

Journalistic strategies to frame events are largely used and discussed within the field of political communication since the canonical works of the sub-field (Gitlin, 1980; Entman, 1993) to recent ones entitled "media framing" (Scheufele, 1999; Scheufele, 2000; Carragee & Roefs, 2004) and "news framing" (D'Angelo, 2002; D'Angelo & Kuypers, 2010). This corpus has many other branches within itself, based upon *which types of events* are analyzed within news media frames.

To be able to analyze news frames of Redhack, we should first decide in *which types of events* the acts of Redhack can be included. Based upon the declarations of Redhack about their acts, whether they react against the acts of the state/corporate power, they support other protests, they exhibit state-related deficiencies, or they commemorate

³⁶ In a detailed analysis about the construction of official terror frames, I acknowledge that all contemporary terror frames should be examined in order to define the position of one specific terror frame. Yet the limits of that research do not allow such examination. For that reason, just some examples from this totality were mentioned to catch a glimpse of the general trend.

historical events, their explicit purpose is to protest. For that reason, the related acts can be considered under the category of *social movements*. Actors from media outlets can play roles as important as official actors when it is about the construction of frames for social movements (Tarrow, (1994) 2011, p. 144). On the other hand, based upon the terror accusations during the judicial processes, acts of Redhack can be considered as terror acts and following that, news framing of terrorism can be enlightening, too.

The common feature of these two categories of news frames – protests and terror events – is their reliance on official sources. In the case of protests and protesters, official interpretations of protests have greater volume and ubiquity compared to other interpretations in news media (Noakes & Wilkins, 2002, pp. 651-652). In the case of the events interpreted as terrorist events, news frames are shaped by the facts about the event, the interpretation by official sources, and by the self-frames of the related group (Norris, Kern, & Just, 2003, pp. 12-13). In some cases, news frames can become much more dependent to official frames, so far as echoing the official frames. In the literature about terror frames, there is an assumed distinction between the frames of “one-sided” and “two-sided conflicts.” In that line, a sociopolitical division constructed through long-standing political violence is the distinguishing feature that makes the framing of a terror event as one-sided or two-sided in news media. The framing of 9/11 in the US falls into the one-sided coverage with a relatively uncontroversial media coverage, while the cases in Northern Ireland or in Israel and the West Bank fall into two-sided coverage based on the lack of a broad consensus about the interpretation of events (Norris, Kern, & Just, 2003, p. 5 and p. 12).

In the case of Redhack, the diverging line from both research areas – social movement frames and terror frames – originates from the silence of political actors and the lack of official frames to rely on. The absence of official frames and the silence of political actors about Redhack were vocalized just by few non-mainstream news media outlets.

5.2.1. Frame diversity: Many ways to define Redhack

After the data leaks of Redhack from the Council of Higher Education (YÖK) in January 2013, then Minister of Transport, Maritime Affairs and Communication Binali Yıldırım

foregrounded the issue of cybersecurity rather than the content of the leaks in his declaration about the leaks. Left-wing news portals framed this declaration of Yıldırım as the neglect of the corruption in universities exhibited by the data leaks in question (SoL, 2013i).

After Reyhanlı leaks, the only incident that was included in the scope of official frames, Odatv captioned the omission of then Vice Prime Minister Beşir Atalay about the leaks: “Redhack’s leaks were asked to Beşir Atalay. Response: These are confidential issues” (Odatv, 2013d). However, such news about the silence of political actors does not constitute a widespread reaction among mainstream actors of news media in Turkey. Left-wing news outlets like SoL correspond to a small part of the news media in Turkey. Other actors known with their anti-AKP stance like Odatv are not highly influential ones either. Moreover, after the period of 2005-2013 during which news media environment in Turkey was transformed heavily with the rise of AKP-friendly partisan media companies, many news media outlets were targeted either with charges of military coup attempts – Ergenekon operations mostly against Kemalist, secularist journalists – or with terrorist propaganda – KCK operations against Kurdish journalists (Yesil, 2016, p. 88). Odatv was one of the political news websites that were targeted with Ergenekon charges in 2011 (Yesil, 2016, p. 99). In that sense, this emphasis on the neglect of Redhack’s acts by governmental actors was not on the agenda of news media, apart from non-mainstream political media outlets.

In the absence of the influence of official frames about Redhack, a variety of definitions appears within news frames, sometimes dependent on the ideological stance of the news outlets, and sometimes surpassing ideological boundaries. Here, the purpose is not to embark on a detailed analysis of news frames in every aspect. It is mostly to gain insight about the preference of news media actors about the crime framing of Redhack based upon the use of specific words through which frames can be manifested (Entman, 1993). To this end, definitive sentences from the news about Redhack are selected and categorized as “specific keywords that constitute the concepts underlying frames” (Reese, 2010, p. 20). These describing keywords are collected from the content analysis of news collected for the examination of the acts and judicial processes of Redhack.

Table 5.1: Examples of the frame elements about Redhack in news outlets

Keywords	Frames in sentence level
Group (Sabah, 2012a; Ntv, 2012a)	-
Socialist hacker platform (Sözcü, 2012)	Activism frame
Group known as the Turkish WikiLeaks (T24, 2012)	Activism frame
Digital activism collective (T24, 2013)	Activism frame
Famous hacktivist group (Radikal, 2013a)	Activism frame
Socialist hacktivist group (Siyasi Haber, 2014a)	Activism frame
Hacker group (Milliyet, 2012a; Hürriyet, 2013a; Sabah, 2013a; Diken, 2016a; T24, 2016)	Cybercrime frame
Turkish computer pirates group (Haber 24, 2012)	Cybercrime frame
Computer pirates group known as red hackers (Akşam, 2013a)	Cybercrime frame
Hacker group known with their attacks on public institutions during the Gezi protests (Türkiye Gazetesi, 2013)	Cybercrime frame
A Turkey based hacker group (Bianet English, 2013)	Cybercrime frame
Turkish hacker group (Hürriyet Daily News, 2013)	Cybercrime frame
Socialist hacker group (Cumhuriyet, 2012; SoL, 2013; Sendika, 2013; BirGün, 2014)	Cybercrime frame
Known as the red hackers (Cumhuriyet, 2013)	Cybercrime frame
Group of internet pirates (Cantürk, 2013; Sabah, 2014)	Cybercrime frame
Cyber pirates (Sabah, 2013)	Cybercrime frame
Famous cyber pirate group (Ege'nin Sesi, 2014)	Cybercrime frame
Red hacker group (Milliyet, 2013f; Sözcü, 2014)	Cybercrime frame
Communist, Marxist, Leninist hacker group (Yeni Akit, 2014)	Cybercrime frame
Marxist, socialist hacker group (Yeni Akit, Redhack grubu kimdir?, 2016)	Cybercrime frame

Illegal hacker group (Sabah, 2016; Milliyet, 2016; Yeni Akit, 2016; Sabah, 2017)	Cybercrime frame
Cyber-terror organization who played an active role during the Gezi protests (Sabah, 2014a; Takvim, 2014)	(Cyber-)terror frame
Qualified as the first virtual terror organization of Turkey (Hürriyet, 2015)	(Cyber-)terror frame
Terror supporter (Yeni Akit, 2016)	(Cyber-)terror frame
Structuring [yapılanma] (Sabah, 2015)	Crime frame
Illegal group (Sabah, 2017; Ntv, 2017)	Crime frame

In the initial period of Redhack's popularity, diverse definitions were apparent in news media. "Socialist hacker platform" (Sözcü, 2012), "group known as the Turkish WikiLeaks" (T24, 2012), "digital activism collective" (T24, 2013), and "hacktivist group" (Radikal, 2013a; Siyasi Haber, 2014a) were some early examples implying activism frames. "Computer pirates" (Haber 24, 2012; Akşam, 2013a), "internet pirates" (Cantürk, 2013; Sabah, 2014) and "cyber pirates" (Sabah, 2013; Ege'nin Sesi, 2014a) were cybercrime frame elements centered upon the word *pirate*, a popular allusion for hackers. Some outlets also preferred to use just "the group" (Ntv, 2012a) at this period. This diversity reminds the diversity of the definitions used by political actors, as "website" and "media outlet" to define Redhack. However, these different usages would give their places to the variations of the settled phrase *hacker group* in a quite short time. The consolidation on defining Redhack with "hacker group" is the adaptation of the actors from news outlets to their first encounter with a suddenly popularized group, acting with different tools than they were used to see, aka computer and internet technologies. Technology fetishism of the popular media is undoubtedly the first reason of this adaptation. The other reason seems to be related to the absence of official frames about Redhack.

5.2.2. Emergence of self-frames

In their own website, Redhack defined itself as the "only socialist revolutionary hacker group" (Redhack, 2012). Apparently, in the silence of political actors, news frames about

Redhack reflect the self-frames of the group. The basic “hacker group” is enormously used in news media to frame Redhack, as the table above shows a part of it. I claim that this widespread usage results from the self-framing of Redhack, as a hacker group.

The question of under what conditions social movements frames gain access to the media is a debate developed by frame analysis researchers. In their analysis about the access and the positive coverage of Palestinian injustice claims to US news media, Noakes & Wilkins (2002) claim that the milestone was when Palestinian movement framed their insurgence as “grassroots resistance to an oppressive power” (p. 665) during the intifada. The consistence of this self-framing with the civil rights master frame created a familiarity among the American audience and following that, gained access to news media. In the case of Redhack, the reason of the positive coverage is not the consistence with a familiar master frame. On the opposite, this time, the unfamiliarity of the frame becomes attractive for news media actors, especially when it is related to *cyber* issues, with a techno-fetishism.

Not just the phrase hacker group, but also the ideological self-description of the group is also repeated by ideologically diverse and even opposite news outlets. Left-wing socialist, communist BirGün, Sendika.org, and SoL, social democrat Cumhuriyet, Kemalist Sözcü, and right-wing Islamist Yeni Akit use the same frame of “socialist hacker group” for Redhack. This common usage of frames between ideologically diverse news outlets shows how a divide in the underlying ideologies does not imply a divide in framing. Here, based on the defining keywords used for Redhack in these news outlets, the common framing of the group exhibits the “fascinating instance of the same frame being tied to diametrically opposed ideologies” (Oliver & Johnston, 2000, p. 39).³⁷ This is also why ideologies and framings cannot be reduced one to the other and that they imply to different issues.

Another repetitive element of the framing for Redhack is the imagery used in news about the group. The usage of visual elements – like photographs, cartoons, and maps – is a non-negligible part of the frame construction (Entman, 1991). Images from the

³⁷ At the risk of repeating myself, I should declare that as all other arguments of this part, this argument is based on the keywords used to define Redhack and not to the integrality of the news. For that reason, I cannot propose that all frame elements are tied to the same frame between aforementioned news outlets with diametrically opposed ideologies.

documentary produced by a left-wing film production center about Redhack would become the representative image of the group (RED!, 2013).



Figure 5.1: (Sabah, 2015)



Figure 5.2: (SoL, 2012)

These images would repeatedly be used by the news media and by the group itself in their social media platforms, right after the shooting of the documentary. Mainstream news outlets like Hürriyet (2012b; 2013; 2015), Hürriyet Daily News (2013; 2014), Milliyet (2012; 2013; 2014; 2016; 2017), and NTV (2012; 2013; 2015; 2017); AKP-friendly right-wing news outlets Sabah (Ilıcak, 2013; Sabah, 2015) and Yeni Akit (2014; 2016); and anti-AKP left-wing news outlets Bianet (2013a), BirGün (2014), İleri Haber (2016a; 2018), Siyasi Haber (2014a; 2015; 2016a), SoL (SoL, 2012b; SoL, 2013; SoL, 2014), Yolculuk (2016), Kemalist news portal Odatv (2014b), and social democrat newspaper Cumhuriyet (2016f) prefer to use the same images from the documentary for a large amount of the news about Redhack. With the increase of the judicial processes about Redhack, the imagery of people taken into custody is also used in the news. However, especially in the acts of Redhack and also in some of the judicial processes news, the imagery from the documentary has the first place.

None of these elements, neither the description of the group in line with the self-framing nor the images borrowed from the same source determine whether the framing is positive or negative for Redhack. The distinctive line between positive and negative framing of Redhack appears in the including of the images of the Redhack's acts in the news. In many instances, mainstream news outlets and news outlets with an anti-AKP stance include the documents leaked by Redhack or show the images of the websites defaced by Redhack (Milliyet, 2013; Odatv, 2013b; SoL, 2014; Siyasi Haber, 2016). In this

way, these outlets play an important role of “co-producing” (Walgrave & Manssens, 2000) protest events (Tarrow, (1994) 2011, p. 134) of Redhack, as the protests of the group are based upon the circulation of their hacking performances. The inclusion of documents belonging to social movement actors is a tactic used by alternative media outlets in Turkey for positive coverage of the related protest movements. The case of the framing of TEKEL workers’ struggle³⁸ in alternative media constitutes an example in which alternative media outlets identify with the related struggle (Doğu, 2013, p. 353). Especially when the movements are in the same ideological line as the outlets, this framing becomes much more apparent.

On the other hand, AKP-friendly partisan news outlets would avoid using such documents related to the acts of Redhack. In some instances, especially about data leaks, these outlets would also begin to remain silent about the acts of Redhack by the Reyhanlı leaks event in 2013. This silence of partisan news outlets would be criticized by dissident news outlets (SoL, 2013k). However, the silence of news outlets would enlarge by time.

5.2.3. Increasing silence about framing Redhack

In 2016, when Redhack would leak the e-mails of Berat Albayrak, fewer news outlets would make news of this act. While some anti-AKP stance news outlets would continue to make news, most of their webpages about this news would be censored by the government through denied access without notice (Diken, 2016b; Diken, 2016a; Sendika, 2016; SoL, 2016a; T24, 2016). As Redhack shared the information that they leaked in Dropbox and Google Drive, the government denied access to these global cloud storage services, too (Sputnik Türkiye, 2016a). At the same time, many other outlets would abstain from making news with a mechanism of self-censorship, not just partisan outlets but also mainstream and some anti-AKP outlets. A search with the keyword “Redhack” in the online news archives of mainstream and partisan news outlets like Akşam, Hürriyet, Milliyet, Ntv, Sabah, and Yeni Akit shows that apart for Hürriyet, none of these news outlets reported about Berat Albayrak leaks. In Hürriyet newspaper, an indirect mention of “documents allegedly leaked

³⁸ More information about this strike (December 2009-February 2010) against the neoliberal privatization politics can be found in Doğu’s thesis (Doğu, 2013, pp. 164-166).

by Redhack” in reporting the access denial of cloud storage services is about this incidence (Hürriyet, 2016) and a direct mention of the leaks – without the content – in the news about the lawsuit related to the journalists are the only references to the event (Hürriyet, 2017). In the total opposition to that silence related to Berat Albayrak leaks, all these news outlets – apart from Yeni Akit – had reported largely the previous acts of Redhack in earlier years. According to their online archives, between 2012 and 2018, there are 41 news containing the keyword Redhack in Akşam newspaper (Akşam), 224 news in Hürriyet newspaper (Hürriyet), 194 news in Milliyet newspaper (Milliyet), 38 news in NTV news channel (NTV), and 103 news in Sabah newspaper (Sabah). Redhack would criticize this silence of the news outlets by hacking anti-AKP Kemalist newspaper Sözcü and by making their own news with a satirical language, in which they warn the newspaper for security gaps and they write: “PS: Well done, you had us do our own news” (Yolculuk, 2016a).

5.2.4. Positive and negative frames

Another peculiarity of the news framing of Redhack is the indirect exaltation of the group based upon their prowess in cyber issues, even when these issues are crime-related. The cyberwar frame is used widespread by diverse news outlets in reporting the acts of the group. “Brought down” and “hit” are some of the most used verbs to define the acts of Redhack after the popular verb “hacked”. The effort of discrediting Redhack through their lack of prowess, as in official frames, cannot be seen in news framing of the group, as much as in official frames. In one interview in which cyber-attacks on Anadolu News Agency during the local elections in March 2014 are reported, the president of the agency declared: “They attacked but they could not bring down” (Sabah, 2014b). Sabah newspaper used this phrase as the title.

In other incidents, news outlets prefer to exalt the cyberattacks by making additions emphasizing the nation-state, like “a Turkey-based hacker group” (Bianet English, 2013) and “Turkish hacker group” (Hürriyet Daily News, 2013). Without going too far to interpret these additions as a symptom of the nationalist ideology, we can say that this is a populist tactic to highlight the uniqueness of the group, through representing it as the national representative of an international phenomenon. Nation-state emphasis is added to

other crime frames than *hacker*, too. “Turkish computer pirates group” (Haber 24, 2012) is in the same line of exaltation. Another example from 2015 is much more expressive. In this news of *Hürriyet* newspaper about the acquittal of the suspects from the first Redhack case in March 2015, they define Redhack with “qualified as the first virtual terror organization of Turkey” (*Hürriyet*, 2015). Even Redhack is defined as a terror organization – a negative frame, the emphasis on *Turkey* and on being the *first* one stands out as positive frame elements with the presence of the attributive *virtual*.

While definitions related to terror are explicitly negative frames for Redhack, it is hard to say the same thing for cybercrime frames. As mentioned, hacker group is heavily used for Redhack’s framing in news media but this usage was closely related to their self-framing. From the other side, *hacker* does not possess a negative connotation for the Turkish news media. The fear of and the fascination with the figure of the hacker had already begun to expend in the 1990s through the global popular imaginary – fueled mostly through Anglo-American movies. This fear and fascination echo in the Turkish popular imaginary, too.

Movies about hackers fuel the hacker imagery in the Turkish media since the 1990s. Not just for the ordinary people interested in this imagery, even for the hackers in Turkey, these movies and translated books are a source of knowledge about the hacker culture (Eriş, 2009).³⁹ However, this fear and fascination did not become a source for the criminal framing of hackers. Following the argument of Nissenbaum (2004) according to which the criminalization of hackers is based upon the anti-governmental and anti-corporate stances of hackers (p. 195), the non-criminalization of hackers in Turkey is related to the absence of such local experiences until Redhack. For that reason, the framing of Redhack becomes crucial to follow that change of news framing and the criminalization of hacker/hacktivist experience.

In the Anglo-American context, September 11 was a milestone for the decrease of activism and criminal activity frames used for hacking and hacktivism. Instead of these frames, security and terrorism perspective would become prevalent for framing hacking and hacktivism after September 11 (Vegh, 2005, p. 6).

³⁹ This argument would be exemplified in the next chapter, based on the in-depth interviews conducted with judicial actors.

5.2.5. Political economy of news framing

In the case of Redhack in Turkey, the criminalization of the group through the changes from activism frames to cybercrime frames and then to cyber-terror frames neither follow such a linear line, nor are these changes traceable in every news outlet. With very basic guidelines, activism frames are characteristic of anti-AKP news outlets – regardless of their ideologies, terror and cyber-terror frames are mostly peculiar to AKP friendly news outlets, and cybercrime frames are widespread without ideological or political differentiations. Nevertheless, these vulgar category lines endanger to obscure the complicated political context of the Turkish news media with its increasing dependency to the central power of AKP.

In Turkey, commercial media outlets had an implicit dependency to the state through the necessity of informal ties since their origin in the 1980s. Under the AKP's single-party rule, this dependency became much more apparent. Beginning by the mid-2000s, capital groups loyal to AKP began to enter the media sector with the aims of strengthening their political positions and demonstrating their political commitments to the government (Yesil, 2016, pp. 105-106). AKP-friendly partisan media companies like Çalık (Turkuvaz Media Group), Feza, Samanyolu and Ipek-Koza gained strength by the elimination of older actors of the sector, which were major media conglomerates (Bilgin, Uzan, and İhlas) (Yesil, 2016, p. 88). This “reshuffling of media ownership structure” (Yesil, 2016, p. 88) continued with the gradual elimination of Doğan Holding in favor of Demirören Holding through economic and political pressures. All the political crises of the 2010s – Gezi protests, the alleged Corruption Leaks of December 17-25, the military coup attempt, and the state of emergency – influenced directly the media landscape in Turkey. Aforementioned witch hunts against dissident journalists and the waves of seizing and selling of media outlets through direct pressures towards older actors of media sector peaked with the elimination of *Cemaat*-related [Gülen Community related] media outlets in 2015-2016 and the suppression of oppositional media under the state of emergency, as the final blows to media critical of AKP (Bulut & Yörük, 2017, p. 4098).

The active involvement of the government to the media sector created a news media shaped with censor and self-censorship mechanisms. In that sense, even though there is an absence of official frames for the criminalization of Redhack, we cannot assume an independent news media that can construct frames apart from the official discourse. Examples from Sabah newspaper can be a significant example to understand the changing framing of Redhack.

Sabah is a right-wing newspaper since its foundation. In 2007, the state had seized the newspaper through the Savings Deposit Insurance Fund of Turkey (TMSF) due to its debts and then sold it to Turkuvaz Media Group, an AKP-controlled capital group. After this selling, the newspaper became explicitly pro-government. Its circulation rates are quite high and it stands as one of the top selling newspapers in Turkey, if it is not the best-selling (Gazeteciler, 2019). Sabah's first news about Redhack is from the beginning of 2013. In the very first news about the detention of 16 people in the first investigation of Redhack, Sabah abstains from any framing and uses just the neutral description "group" (Sabah, 2012a). With the second news, the newspaper begins to search for a framing for the group. In this second one about the website defacement of the Ministry of Interior, the act of Redhack is framed as a protesting act and the motivation of the group – reaction against the mistreatment of Minister of Interior İdris Naim Şahin towards a citizen – is also mentioned. Within the text, the group is defined as "Redhack who identifies oneself as the cyber-army of the proletariat" (Sabah, 2012). All these elements show that the self-frames of the group can find a place in the news framing, even when it is a right-wing AKP-friendly news outlet. In 2013, the well-known "hacker group" (Sabah, 2013a) is used to define Redhack. In 2013 and 2014, there are news in which different attractive phrases like "cyber pirates" (Sabah, 2013) and "internet pirates" (Sabah, 2014) are also used. In 2014, Sabah uses for the first and the only time the phrase "cyber-terror organization" and this is to define Redhack. The newspaper uses two different contexts to amplify the effect of the *terror* related definition: "cyber-terrorist organization who played an active role during the Gezi protests" – a reference to the Gezi protests that became to be constructed as a conspiracy against the Turkish state in the official frames and a content about the relation of Redhack

with *Cemaat*, which is defined as the “parallel structuring” (Sabah, 2014a).⁴⁰ At that time, neither the Gezi protests nor the Gülen Community was framed as terror organizations per se. Yet it seems like the presence of both references provides persuasiveness for the claim of cyber-terror.

5.2.6. Reflection of judicial processes in the terror framing

Actually, terror framing of Redhack was already a discussion during the judicial processes at an early date like 2012, compared to the comparatively late emergence of terror frames of Redhack in news media. The indecision of the Turkish judiciary about whether Redhack’s acts constitute cybercrime or terror crime was manifest since the transfer of the file between cybercrime prosecutor and prosecutor specializing in anti-terrorism in July 2012 (Hürriyet Daily News, 2012). This indecision became the source of satirical polemics about the terror attribution of Redhack in social media, among constitutional and non-constitutional accounts, as well as in conventional news media. Cnn Türk, a mainstream news channel belonging to Doğan Media Group, part of Doğan Conglomerate at that time, tweeted this news about the transfer of the file during the Redhack case with a humorist expression:



Figure 5.3: [Prosecutor’s office declared Redhack terrorist organization. Reason is farcical...] (@cnnurk, 2012)

⁴⁰ This news is doubled by the newspaper. As the time and the content of the second news are the same, I count them as one source.

In the related news published in CNN Türk's website, the news channel reported that the prosecutor's office specializing in cybercrime considered Redhack as a terrorist organization based upon their hammer and sickle logo and their possession of a manifesto (Cnn Türk, 2012b). Many news outlets would report the decision with the same reasons on the basis of a report prepared by the prosecutor's office (Odatv, 2012; Radikal, 2012; Sabah, 2012; SoL, 2012), even though the reason written in the final indictment is the support of Redhack for "Marxist-Leninist-Maoist leftist and separatist groups." In this line, prosecutor specializing in anti-terrorism accuses Redhack's members of committing a crime in the name of terrorist organizations without being members (Ankara Chief Public Prosecutor's Office, 2012, p. 46).

After that transfer, there would be many other transfers of the Redhack related judicial files between prosecutors specializing in anti-terror and others specializing in cybercrime. Yet, these transfers would no longer be a source of satire for news media. This gradual decrease in the satirical tone is closely related to the dense political atmosphere of Turkey, as this was apparent in the tone of official frames. The reflection of this context upon the framing of Redhack is first the usage of terror frames. Like the news of Sabah newspaper from 2014 (Sabah, 2014a), Takvim, another right-wing AKP partisan newspaper of the same Turkuvaz Media Group, also framed Redhack as a cyber-terror organization in their news about the same incident (Takvim, 2014). Hürriyet, owned by Doğan Media Group at that time, also emphasized that Redhack is considered as a "virtual terror organization," without the satirical tone that once Cnn Türk had about that claim (Hürriyet, 2015). In 2016, terror frame of Redhack would slightly change for the right-wing news outlet Yeni Akit and they would define the group as "terror supporter" (Yeni Akit, 2016). As mentioned in the official frames related to terror charges, being a terror supporter is a passive criminalization used heavily for larger public categories. In that sense, it can be argued that even the partisan news outlets do not construct Redhack as a pivotal target of criminalization centered on terror.

In earlier news from Yeni Akit in December 2014, Redhack was defined with the accusation of "causing the death of Berkin Elvan [a young boy shot by the police with a tear-gas canister] by supporting the provocations during the Gezi events." The irrelevance

of this definition with the content of the news about the hacking of Mobese, the city surveillance camera system exhibits the indirect and even remotely constructed criminalization of the group (Yeni Akit, 2014). Phrases like “so-called anarchist” in the same news (Yeni Akit, 2014) are quite different from the dense terror frames and related criminalization processes that would be prevalent by 2016.

Table 5.2: Hürriyet newspaper online news archive

Years	Number of news with “terror” keyword	Number of news with “terror” and “Redhack” keywords
2012	4272	11
2013	3130	10
2014	4232	1
2015	13857	4
2016	30091	1
2017	22209	1
2018	16672	0

The table above shows the number of news containing the keywords “terör [terror]” and the number of news containing the keywords “Redhack + terör [terror]” within the online news archive of Hürriyet newspaper, the top selling newspaper of Turkey in 2019 (Gazeteciler, 2019). The immense gap between the numbers indicates how small is the terror relevant news of Redhack compared to the general terror news in the national context. Yet, it does not mean that there is not at all any labelling of terror for Redhack. By the beginning of 2017, the terror framing of Redhack would be supported with new claims. Now, different from the ideological relation of the group with far-left illegal organizations, the relation of the group to “FETÖ [Fethullah Gülen Terrorist Organization]” would be alleged (Ntv, 2017; Sabah, 2017; Sabah, 2018; Yeni Şafak, 2018). Such associations of terror organizations with diverse – even opposite – ideological tendencies would be an ordinary characteristic of terror labels during the state of emergency after the attempted military coup of 2016.

Espionage charges constitute another part of the criminalization of Redhack in news media. Disclosure of information relating to the security and political interests of the state

(Turkish Penal Code, Article no. 329), which is classified as an offence against state confidentiality and espionage was a charge in the Reyhanlı leaks case and also in the investigation about the leaks from Berat Albayrak's e-mails. Even though the lawsuit about the Reyhanlı leaks was known as an espionage case in the news media (Radikal, 2013), we could not see an active criminalization of Redhack as a spy organization at that time. In the news about the private accused with espionage, Redhack was defined as a “computer pirates group” (Akşam, 2013a). However in 2017, the same newspaper would use “Spy hacker is captured” as the title of the detention of one person during the investigation related to Berat Albayrak leaks (Akşam, 2017). Actually even with this crime framing based on espionage, some distance from terror frames becomes apparent.

The other indicator of the divergence from the terror framing for Redhack is the substitution of terror frames with accentuated crime and cybercrime frames. In the same news of Yeni Akit, Redhack is described as a “terror supporter” in the title of the news. However, within the text, the group is defined as an “illegal hacker group” (Yeni Akit, 2016). This definitive frame element would be apparent in other mainstream news outlets, too (Sabah, 2016; Milliyet, 2016). Adding *illegal* to the phrase *hacker group* gives the impression to recognize the non-criminalization of hacking in the Turkish context. As if without accentuating *illegal*, *hacking* would mean a legal activity. Earlier, I had argued that this lack of criminalization in Turkey, in opposition to global trends, was based on the absence of anti-governmental and anti-corporate hacker and hacktivist experiences in Turkey. Yet now, this implicitly positive news framing of hacking comes right after such an experience, within the news about the acts of a group who has an anti-governmental and anti-corporate stance. It means that the actors of news media think that hacking has a positive/non-crime connotation in public opinion, even after the acts of Redhack. Following that, a prefix is needed to make explicit the criminal aspect of hacking.

The wave of criminalizing Redhack without terror labels is also seen in the usage of “structuring” (Sabah, 2015) and “illegal group” (Sabah, 2017; Ntv, 2017) to define the group in the news media. This return to the absence of terror labels is quite significant. It signals a non-consolidation of the terror label for Redhack in the news media. The table below presents this changing pattern through the news about Redhack in Sabah newspaper. Beginning with the non-crime frame element “group,” Sabah passes through cybercrime

frame elements “hacker group,” “cyber pirates” and “internet pirates” to reach “cyber-terrorist organization” after the political crises of Gezi protests and the alleged Corruption Leaks of 2013. By 2015, the cyber-terror label is abandoned for “structuring,” a notion used sometimes for terror groups but not always. In 2016, when “hacker group” is back, its “illegal” extension diverges from the earlier usage of it in 2013. It is as if there is a reduction of the *cyber* attribute of the crime framing for Redhack. For cyber-terrorism and also terrorism, even when there are references to FETÖ, a direct frame element of cyber-terrorism or terrorism is no longer used by the newspaper.

Table 5.3: Changing crime frames for Redhack in Sabah newspaper

2012	2013	2013/2014	2014	2015	2016/2017	2017	2018
-	Cybercrime	Cybercrime	Cyber-terror	Crime	Crime emphasized cybercrime	Crime	Terror related crime
Group	Hacker group	Cyber pirates / internet pirates	Cyber-terrorist organization (relation to Gezi protests and to Gülen Community)	Structuring	Illegal hacker group	Illegal group	Part of the treason network (relation to FETÖ)

5.3. Conclusion

Compared to other criminalization processes centered on terror frames in the contemporary Turkish political discourse, Redhack’s passive criminalization positions in a distinct place within the crime frames constructed by political actors and news media outlets. Concerning media frames, divergences between ideologically opposite news outlets are not always explicit for the crime framing of Redhack. Diverse media actors – regardless of their ideological positions, political tendencies and capital relations – echo the self-frames of the group and construct cybercrime frames with a rather positive coverage accentuated with

techno-fetishism. The hacker label – the one that is heavily used in cybercrime frames – does not always possess a negative connotation in the Turkish context, even though it is not precise to say that there is a positive connotation either. The positive coverage becomes more apparent in news outlets possessing an anti-AKP stance. In these outlets, in addition to cybercrime frames, activism frames appear within news reporting the acts of Redhack and the judicial processes related to the group.

The peculiarity of media framing of Redhack manifests itself within the news of AKP-friendly conservative and mainstream media outlets. First, similar to dissident media outlets, these outlets echo the self-frames of Redhack, too. The silence of political actors seems like the main reason of this echoing. Under a media landscape heavily dependent to the government, the lack of official frames engenders a gap that media outlets would fill with the self-frames of the group.

Another reason of the appearance of Redhack's self-frames in AKP-friendly news outlets can be the dramatic characteristic of Redhack's acts. Data interference and data leaks acts are sensational events. In that sense, they are highly compatible with the episodic news coverage – the shadowing of the broader issues – that news media tends to incline (Noakes & Wilkins, 2002, p. 652). For that reason, the episodic news coverage of Redhack's protests becomes a peculiar advantage for the group to be able to appear in AKP partisan news outlets in total opposition with the group's ideological stance.

About the changing trends of Redhack's crime framing in news media, cyber-terror and terror frames for Redhack are not actively performed by the actors from news media outlets. In addition, the terror framing gives its place to a regular crime framing in news media, even though terror charges continue to be a crucial part of the judicial processes related to the group.

When this changing pattern of news frames of Redhack is compared to the coverage of hacking in American and British news media, an inconsistency immediately appears. In American and British news media, hacking's framing changes dramatically after September 11 towards a negative treatment (Vegh, 2005, p. 6). Following that, activism and criminal activity frames would decrease in favor of an increase on security and terror frames. It is true that for Redhack, political crises like Gezi protests and Corruption Leaks stand as reasons of the enlarged terror frames and therefore, they stand for the terror framing of

Redhack in the scope of AKP-friendly news outlets, similarly to how September 11 stood in American and British news media. The issue of the alleged Corruption Leaks can have an extra effect on the terror labelling of Redhack, through intensifying the criminalization of data leaks, a favorite method of protest for Redhack.

However, the terror framing of Redhack in Turkish news outlets is not as widespread or continuous as the terror framing of hacking and hacktivism in the Anglo-American media. Even in the AKP-friendly news outlets, the criminal activity frames rise again after the short appearance of terror frames for the criminalization of Redhack. In parallel with the decrease of terror frames, there is a decrease in cybercrime frames, too. News outlets prefer to frame Redhack as a criminal organization, without any specific attribution added.

Another point to emphasize is that the acts of Redhack do not stand as powerful sources in the construction of crime frames for Redhack. Reyhanlı leaks (2013) about which almost all explicit official frames were constructed do not constitute a milestone for an emphasized crime framing in news media. Moreover, as Berat Albayrak leaks (2016) exhibited, it can be argued that the acts of Redhack stand as the reason for the negligence of news outlets – in that sense, the non-framing of the group, as a tactic of self-censorship. In sum, the usual suspects of crime framings, political actors and actors from news media, do not play an active role in the criminalization of Redhack. Even though this passivity indicates a lot about the positioning of the state and the media landscape in Turkey, their quasi-absence creates a need to a search for a different source to understand the construction of crime frames for Redhack.

In the next chapter, I will advance towards the details of the framing preferences identified in this chapter using a totally different methodology. In the middle of the quasi-absence of official frames and the passive crime framing of the news media, personal narratives of the actors who worked within the judicial processes would become a valuable source to interpret how the construction of crime frames is implemented for Redhack.

CHAPTER 6

UNOFFICIAL CRIME FRAMES FOR REDHACK:

ANALYZING THE CONSTRUCTION OF THE CRIMINALIZATION

In the previous chapter, official frames about the criminalization of Redhack were presented through the discourse of political actors and of news media. However, this criminalization was considered as a passive one, due to the quasi-absence of official frames and the light criminalization reaching the absence of crime frames with an explicit censure and auto-censure. Following that, in this sixth chapter, I rely on a different source to discover the characteristics of criminalization, as well as the underlying reasons of this process. Calling as unofficial crime frames, I refer to the personal frames constructed for Redhack in relation with the more general frames about hacking, cybercrime, cyber-terror and terror.

Through this analysis, personal frames would present sometimes compatibility and sometimes resistance with the framing preferences designated by official frames. Furthermore, they would give elaborated meanings to the crime frames expressed within the official discourse and the news media discourse.

6.1. Digging a hidden source: Methodological notes on the analysis of unofficial frames

Judicial processes always play a central role in the construction of criminalization. In the absence of active official frames, this role becomes much more critical, as Redhack's case exhibits. Judicial processes related to Redhack draw a considerable amount of public attention via conventional news media and social media. Yet, they are limited sources to

understand the crime frames of Redhack.⁴¹ For that reason, I turn towards the actors who have direct or indirect relations with these judicial processes. An attempted analysis for the discourse of judicial actors is to dig a hidden source because frames of these actors are not always explicit, even when they have high impact on the formation of judicial decisions. These are the frames lying behind the surface.

For that purpose, I analyzed 25 semi-constructed in depth interviews that I conducted during Summer 2017 and Winter 2018-2019 with actors interested/worked in cybercrime related judicial processes in Turkey. 5 experts, 7 law enforcement agents (LEAs), 10 lawyers, and 3 prosecutors constitute the sampling. Interviewed actors had specialization in cybercrime but that did not necessarily coincide with active duty.⁴² Some were retired; some had quitted their work at the time of the interview. Among the sampling, 8 of 25 interviewees are actors who work/worked directly in Redhack related judicial processes. Experts were added to the sampling after initial interviews from which the essentiality of cybercrime expertise in judicial processes became apparent.⁴³

During the interviews, how they define specific concepts was asked to the interviewees. As the interviews were not totally structured, idiosyncratic questions appeared in each interviews. However, in general, main questions were mostly about definitions (*What is cybercrime? What is hacking? What is cyber-terror? What is terror? What about Redhack? – Is Redhack hacker? Is Redhack cyber-terrorist? Is Redhack terrorist?*). Questions about moral evaluation (*Are there good hackers? Who are good hackers? Who are bad hackers?*) and questions related to the reaction of the state, especially related to the judicial reaction to emerge causal interpretation and treatment recommendation (*Do the state perform well? What the state should do?*) followed

⁴¹ Acknowledging the importance of judicial processes as an important starting point, the limitedness of judicial processes originates from two reasons. First is the technical limit. One judicial process is about one single act. For that reason, it cannot provide more inclusive frames. The other reason is epistemological. As a judicial process is expected to decide according to the law system in force, it cannot surpass the limits of that system. In that line, it is hard for the relevant judicial actors to express their frames beyond crime frames within official documents of judicial processes.

⁴² The position of 3 criminal lawyers who did not participate to any cybercrime examination is an exception. They were added to the sampling because two of them had publicly known interest in Redhack related judicial processes or one was a known expert in terror related charge – a central charge against Redhack.

⁴³ All of the interviewed experts have reputation in the cybersecurity community. For most of the time, these experts were referred more than a one time by different interviewees and their names facilitated my access to other interviewees. One of the experts is added to the sampling because of his knowledge, network, and reputation; even though she never worked in a judicial process.

questions about definitions. Through these questions, I aimed to identify frame elements of problem definition, causal interpretation, moral evaluation, and treatment recommendation (Entman, 1993, p. 52).

For the analysis of these frame elements, I followed the suggestion of Van Gorp (2010) to construct *frame matrix* by means of three coding procedures – open coding, axial coding, and selective coding (Strauss & Corbin, 1990). Through this coding, I designated framing devices – “specific linguistic structures such as metaphors, visual icons, and catchphrases that communicate frames” (Reese, 2010, p. 19) – and reasoning devices “demonstrating how the frame functions to represent a certain issue” (Van Gorp, 2010, p. 91). At the result of this analysis, specific frames emerge for Redhack in the discourse of judicial actors: as a result of the widespread positive framing of cybercrime and hacking, interviewees tend to frame Redhack as cybercriminal and/or hacker if they want to frame positively the group. On the contrary, if the framing of Redhack is negative, interviewees recede from these frames and incline towards framing Redhack by cyber-terror and terror frames. Here, my aim is not just to understand how Redhack is framed with each of these notions. I also examine how these notions – frames – are framed by the actors interviewed. In that line, first, I look to the framing of cybercrime and hacking.

6.2. Cybercrime and hacking frames: Imagining the threat

In this part, I will examine cybercrime and hacking frames through six interrelated discussions developed from the analysis of the interviews conducted with judicial actors. First, the anxiety resulting from the opposition between the threat perception of technological developments and the concerns of incompetency in relation to these developments will be presented. Then, I will begin to exhibit the definitive lines of cybercrime according to interviewees. The first discussion about it will be whether motivations should be taken into consideration to designate cybercriminals. The second one will discuss the notions of permission, reporting the deficits, serving the state and the public good, as divergence lines between criminal and non-criminal acts. After these sub-parts, following the discussions of serving the state and how to define the public good, the question of framing cybercrime will turn to the state itself and alleged illegal activities of

the state would be put on the table. The next sub-part will return to the question of designating cybercriminals, this time through the divergence between good and bad hackers. Beginning with the widespread acknowledgement of the relativity of good hackers, this discussion will develop into a dichotomy in the self-positioning of the interviewees as insiders and outsiders of the hacker community. As the last discussion, this positioning of the interviewees will be crucial in their stance about the criminalization of hackers. At the end of this part, a sub-part will be dedicated to the implications of framing Redhack as cybercriminal and as hacker, in line with the discussions elaborated before.

6.2.1. Unavoidable technological threats and deep concerns of incompetency

Everyone using a cell phone is under cyber-threat.

(LEA 6, 2019)

In framing cybercrime, a large part of the energy is consumed to emphasize its criticality. For some, it is “a bullet train coming towards us” (Expert 2, 2018). The ubiquity of technologies and limitlessness of their development are the most used arguments for the construction of cyber-threat. Technological devices are acclaimed for facilitating the human life but also they are held responsible for being the instruments of widespread surveillance. Working for many years in an engineering program within a well-respected university, Expert 2 is a person who has knowledge about information and communication technologies (ICTs) as well as her⁴⁴ accessibility to these technologies more than an average person in Turkey.⁴⁵

Expert 2’s concern about technology could be seen as the result of the central position of ICTs in her professional life. However, this concern would be shared by other interviewees, too. This time, these would be people having comparatively lower degrees of knowledge about ICTs with limited accessibility to ICTs. One of the middle-aged

⁴⁴ Mentioned before, just two of the 25 interviewees are women. However, for anonymity concerns, all interviewees would be mentioned with she/her pronouns.

⁴⁵ Providing anonymity is central for the security of the interviewees. I will give some personal aspects about interviewed experts and lawyers in case such information can enlighten the discussions. However, for LEAs and prosecutors, I will restrain myself from giving personal information that can reveal the identity of the interviewees.

prosecutors would describe her concern about ICTs as: “Nobody has a personal life. Cell phones are chips. There is a system controlling every one of them” (Prosecutor 1, 2019). The Orwellian fear of a system controlling everything does not have to coincide always with the deeds of the nation-state under which power the interviewee lives. Sometimes the controlling agency can become corporations, sometimes other nation-states. Moreover, in some cases, the absence of a controlling source becomes the fuel of anxieties. With an emphasis to *the technology era* in which we live, communication technologies become directly the agents of that threat. With an attitude to make jealous the most devoted Latourian scholars, artificial intelligence, bitcoin, and – to my surprise, a relatively older technology – cell phones (LEA 6, 2019; Prosecutor 1, 2019) appear as threatening and unavoidable sources of danger.

The threat perception of digital technologies and the excessive emphasis on cybercrime are undoubtedly related to the incompetency felt by almost all of the judicial actors. Global perception trends about hacking and hacktivism have already shown how these threat perceptions were deeply influenced by the globally networked economic system dependent to ICTs. This dependence to ICTs is amplified with the feeling of incompetency about these technologies in institutional and/or personal levels. For many of the interviewees, especially for the ones entirely specialized in ICTs related judicial processes like Lawyer 3, ICTs always precede states (Lawyer 3, 2017). “You cannot prevent it,” an expert would declare implying cybercrime. She asks: “What would you do? Banning bitcoin?” and uses a metaphor to emphasize the duality of ICTs – its necessity and its danger in our lives: “You can use knives to cook or to save lives, but you can use it to kill someone, too” (Expert 2, 2018). Law enforcement is one of the frequent addresses that interviewees mention to blame for the incompetency about ICTs (Expert 1, 2018; Lawyer 10, 2019; Prosecutor 1, 2019). A law enforcement agent describes her frustration about their institutional incompetency with this metaphor:

We are drivers, we drive cars, but we do not have driving license.

(LEA 4, 2017)

Actually, the lack of expertise and education are counted as the main reasons of the incompetency to fight against cybercrime not just for laws enforcement agencies but for many different actors of the judicial processes (Expert 1, 2018). Moreover, this incompetency feeling nourished also the anxiety of falling behind vis-à-vis rapidly developing technologies. In that line, the lack of adaptation emerged often during the interviews: “Compared to the rapid development of ICTs, the law cannot adapt itself to it” (LEA 6, 2019). For others, it was not an issue of ability to adapt but an unwillingness: “The state do not lean towards ICTs, but it comes loudly [bangır bangır geliyor]” (LEA 4, 2017). Differences in age, position, and ICT related knowledge of the interviewed LEAs did not prevent them to share this anxiety of falling behind felt for the state.

According to other actors, the unwillingness of the state was emphasized with an aggressive attitude: “About the issue of hacking, the state does not like those who know the issue” (Expert 5, 2019). As an ambitious lawyer working also as an expert in ICTs related judicial processes, Expert 5 did not show an explicit political ideology during her interview. Yet, she felt free to criticize the state. Here, she framed the state’s position towards ICTs as reactionary because of its incompetency to govern it.

Alongside the rapid development of ICTs, another issue emerged during the interviews as a reason of the judicial bodies’ incompetency in ICTs. Interviewees from different positions declared that the power struggle between AKP and Gülen Community became a catalyzer for the lack of expertise in law enforcement agencies, prosecutor’s offices, and in magistracy. This general context of the Turkish judicial body influenced heavily cybercrime related institutions and resulted in the expelling of many experts from these institutions through an anxiety based upon the expertise of now unwanted actors – members from Gülen Community. Politically decided reassignments and dismissals worsened the reaction potential of the state against cybercrime by eliminating specialized personals. In the current situation, some interviewees emphasized that these agencies try to deal with the excessive workload with few and unexperienced personals (Prosecutor 1, 2019).

However, for other interviewees, the excess of the workload is not the only problem of the law enforcement agents. Lawyers are much more critical about the incompetency of law enforcement agencies, as well as the lack of expertise of prosecutors and judges.

Lawyer 2 who had an interest in the judicial process of Redhack even though she was not specialized in cybercrime said harshly that there was not a single competent prosecutor or judge about ICTs (Lawyer 2, 2017). Others expressed their critique with reference to their experiences:

One client said this: Policeman just knows to turn on and turn off a computer. They know nothing about the hacking. The client tries to tell something technical, judge does not know, prosecutor does not know. Policeman does not know either, yet she is credited. Experts know the issue. We all do not know: police, we – lawyers, prosecutors, and judges.

(Lawyer 10, 2019)

Both Lawyer 2 and Lawyer 10 were actively leftist lawyers and their harsh criticism was fueled with the overreliance of prosecutors and judges to the decisions coming from law enforcement agencies. Including herself, Lawyer 10 was aware of the general incompetency about cybercrime related issues among judicial actors and she was explicit to talk about it. Considering that these are lawyers who worked/working in cybercrime related judicial processes, this incompetency feeling is non-negligible. The lack of the knowledge of prosecutors and judges is also mentioned many times during the interviews by lawyers, LEAs, and experts. Except from one expert who defined judges as: “Those who know nothing but have to decide” (Expert 1, 2018), the incompetency of prosecutors and judges was framed as the most critical problem responsible for the cybercrime *threat*. The exceptional approach of Expert 1 results from her strong belief in the liberal principles of the state of law and also from her modesty, which was quite unusual for a highly reputable expert like her within the ICTs community.

The official perspective of the state was framed quite clearly by LEA 5 about why this incompetency about cybercrime is critical: “You cannot govern what you do not know, you would get harm from what you cannot govern” (LEA 5, 2018). In a different perspective, the same incompetency was considered critical because it resulted in victimizations through inaccurate evidence (Expert 1, 2018). Both perspectives – governance and justice – converged in the necessity of the specialization of the judicial

actors, as the solution of the problem of the incompetency about cybercrime (Expert 1, 2018; Expert 2, 2018; Lawyer 4 & Lawyer 5, 2018; Lawyer 8, 2018; Lawyer 10, 2019).

Actually, prosecutors working in cyber-crime related judicial processes complain about the technical impossibilities of finding cybercriminals in the given circumstances, too. Through the example of a case that she was charged with, one interviewee declares that she cannot finish the case in 10,000 years because of the large number of suspects sent from the IP pool of the internet service providers (ISPs). One of the reasons of the large number of suspects is the lack of accuracy in the information sent by ISPs, due to their use of Carrier Grade NAT (CGN) technologies that permit sharing the same IP addresses. The other reason of the large number is the presence of *curious users* that should be separated from other suspects (Prosecutor 2, 2019).

Curious users constitute an interesting category that implies a specific perspective about how cybercrime should be defined. In this perspective, curious users are people who perform a criminal act just with curiosity in opposition to people who perform it for other reasons. Following that, we arrive at another important issue: Whether motivations should be taken into account when an act is judged to be criminal or not.

6.2.2. Motivations matter, or not: How to designate cybercriminals?

Motivations as a reference to define crime is a diverging point between interviewees when their perceptions about cybercrime are asked. Actually, in a perspective strictly loyal to legal texts, motivations cannot be taken into account to differentiate criminal and non-criminal acts, as two interviewees emphasized (LEA 6, 2019; Prosecutor 2, 2019). If a person broke the law, it does not matter why she broke it. In that perspective, articles of TPC should be the only reference to define crime – thus, cybercrime. In TPC, Article no. 243 and Article no. 244 are the main articles that regulate punishments for cybercrime. In these articles, not *motivations* but *deeds* are identified as unlawful acts. Respectively, these acts are unlawfully accessing a data processing system (Turkish Penal Code, Article no. 243) and preventing the functioning of a system and deletion, alteration or corrupting of data (Turkish Penal Code, Article no. 244). As one of the LEAs said: “If you entered, you

are guilty. It does not look to your motivation” (LEA 6, 2019). Thus, the perspective considered all cybercriminals equal, no matter what their motivations were.

The perspective about motivations become quite crucial not just for cybercrime but also when it comes to define hacking and how one can differentiate good hackers from bad hackers. The boundaries between cybercrime and hacking were easily transgressed during the interviews. Two notions interchange quite often in the discourse of judicial actors. In the absence of active crime frames for hackers in the national context, this interchangeability between cybercrime and hacking seems to be the product of the criminalization of hackers in the 1990s within the global context. As they appear in some of the interviews, Hollywood movies stand as an instrument for the adjustment of that crime perception for hackers in the Turkish context. Interviewees mentioned movies like *The Matrix* (The Wachowskis, 1999), *Live Free or Die Hard* (Wiseman, 2007), *Blackhat* (Mann, 2015), and *Hacker* (Satayev, 2016) to respond to the questions of what is cybercrime, what is hacking, and sometimes what is cyber-terror. This imagination of cybercriminals and hackers through movies is part of a global trend of the criminalization of hackers in worldwide (Steinmetz, 2016, pp. 180-182).

If you do not watch it, your dissertation would be deficient.

(Expert 3, 2018)

That and similar warnings showed how cultural products were essential in the cybercrime and hacking constructions of interviewees. Age did not matter in the importance attributed to the movies, as I had imagined it would matter. As a middle-aged well-known expert in the ICTs community, Expert 3’s suggestion for me to watch a movie about cyber-terrorism was in an instructive tone. The reference to cultural products and this kind of warnings were not specific to just one interviewee category, either. The importance given to cultural references appeared in the discourse of experts, LEAs, and prosecutors. The mention of *The Matrix* came even from the lips of a prosecutor, a figure mostly imagined as the sullen face of the Turkish state (Prosecutor 1, 2019). This is significant to understand once again that the widespread influence of hacker movies is not limited with the hacker community nor with young people aspiring to become hackers.

Other than cyber-related movies, older movies were mentioned, too. About the popular nicknames of good and bad hackers as white hat and black hat, one expert recalled that these nicknames were created from the Western movies in which good cowboys had always white hats and bad ones had black hats (Expert 4, 2018).

However, for interviewees following the fundamentalist perspective, loyal to legal documents, all hackers are considered cybercriminals and the distinctions between white, black, and grey hats are considered insignificant – just a jargon between the hacker community (Prosecutor 2, 2019). Yet for many others, the motivation blindness of legal documents created an incompetent framework to understand the nature of hacking. In that view, actors defended that the cybercriminals should have the right to speak about their motivations (LEA 2, 2018).

To illustrate the importance of the motivation in hacking, an expert gives the example of a young boy who hacks a website to test its security. Through the technical evidence from the hacking act of the boy, the expert concludes that what the boy did was a non-profit act. He tried to detect deficits and reported these deficits to the webmaster without exploiting the deficits that he found. Following that, the expert declares that this act is not a cybercrime. “The true cybercrime is to exploit the vulnerability,” she claims (Expert 1, 2018).

The question of what cybercrime *really* is could become quite relative for some of the interviewees. Interviews demonstrated two different levels of relativity about the motivations of cybercrime. One level is about what are the motivations of the act. Another level is about which motivations should be categorized as cybercrime. Child pornography issue is a perfect example to see clearly the divergence of these two levels of relativity.

In line with the worldwide moral panics of child pornography (Jenkins, 2001), the discourse of judicial actors, especially of LEAs, reflects the moral panics about child pornography by considering it as one of the worst cybercrime types (LEA 3, 2018) and seeing its perpetrators as *monsters* (LEA 6, 2019). One interviewee interprets the proliferation of this crime as “the normalization of perversion” (LEA 7, 2019), while another suggest to enlarge the terror label to include child abuse (LEA 6, 2019). An expert would claim that the society has very strict rules about child pornography because it is a *cursed* crime (Expert 5, 2019). In that line, we can say that a consensus exists in the

perception of child pornography among judicial actors. It does not possess at all a relativity constructed on which motivations should be categorized as cybercrime. Abusive motivations are considered as the fundament of the crime of child pornography. However, the other level of the relativity of motivations, the *what motivation* question remains intact for child pornography. It is not the deed itself but the motivation that defines the criminal nature of the act. To concretize the issue, let's take this example given by a LEA:

There are [child] photos shared for humor [in social media]. Photos of circumcision come [to law enforcement agencies]. First job is *to decide whether it is for humor or for abuse*. We watch, divide, report, and send them to the prosecutor's office.

(LEA 3, 2018)

When the two incidents are compared – the boy who unlawfully access a website with the motivation of detecting deficits and the family member who share the photo of circumcision belonging to a boy, it is quite interesting that the second scenario receives much more tolerance about being identified as non-crime than the first one. As an early diagnosis, it seems as if more an act is considered as moral panics, more interpretation power is given to the actors of social control to differentiate normal people from *monsters*. However, when it is about a *not-cursed* crime, as hacking, loyalty to legal texts can become an easier choice for judicial actors as the criminalization brought together with this loyalty is not as deep as the demonization of child pornography perpetrators.

6.2.3. Other lines of divergence: *Permission, reporting, state service, public good*

For many judicial actors, the crime nature of hacking was deeply dependent to the motivation of the actor. For others, *permission* became the diverging point between a good and a bad hacker (Expert 4, 2018). In a similar framing, *reporting the deficits to the related corporation or to the state* could appear as the line between white hat and black hat (LEA 4, 2017). In this perspective, the figure of the cybersecurity expert stands as the good hacker (Lawyer 8, 2018). In some interviews, this figure would even become the example *par excellence* of what a hacker is (LEA 2, 2018; LEA 4, 2017).

Some others saw the service to the state as the distinctive sign of the good hacker. “The hacker of the state is the good hacker,” one LEA would say explicitly (LEA 1, 2017). In that line, pursuing *the wellbeing of the state* is what defines the good hacker, while *the harm to the state* is the characteristic of the bad hacker.

We cannot qualify the acts performed for the wellbeing of the state as attacks. It is to embrace what should be done [iş sahiplenme].

(LEA 2, 2018)

If you infiltrate a *state* agency, then publish it online or share it with *foreign* hacker groups, it is not *public good* [emphasis added].

(LEA 4, 2017)

This response implies the framing of Redhack as a bad hacker group. In another interview, the name of Redhack is explicitly mentioned as a bad hacker group, based upon their attacks on *public institutions* (LEA 1, 2017). The overlapping of *state* and *public* appears many times in the crime framing of bad hackers. In Turkish language, *kamu* [public] has two definitions. One is “all the state bodies working for the public service” and the other is “all the people in a country” (TDK [Turkish Language Association]/*kamu*). These two definitions in TDK referring to quite different interpretations – public as state and public as people – form an interpretative political space. Thus, this ambiguity becomes the point of divergence among judicial actors about how to frame *public good* as a motivation that a good hacker should possess.

The earlier extract demonstrates that public good means not harming state agencies in the perspective of LEA 4. In the case of Expert 1, a recognized expert working in many cybercrime related judicial processes, public good is the act performed for the benefit of the society and it is what defines a good hacker (Expert 1, 2018). Among lawyers, Redhack was in general framed as a good hacker group in the sense of seeking public good. Lawyer 3, a recognized cybercrime lawyer, framed this public good as “creating awareness for the state about cyber-security,” (Lawyer 3, 2017). In her perspective, public good is not always

about the people, it can be about the state, too. However, its relatedness with the state does not imply an immediately supportive act for the state.

Mocking with the state is actually quite beneficial. Why? That is because when Redhack attacked, when the group infiltrated, they realized that most of the passwords are 123456. The system in use is a very old trash system. Or they are using a security standard that is long abandoned. Of course, they will mock them. At the end, the state is not something that we cannot mock. *The state is not sacred; it is there to serve us.* If that state cannot protect my data, if it tries to protect it with trash security systems and with silly passwords, of course, it deserves to be mocked. We should consider this mocking as a positive act. What happened then? Good thing that was done. [The state] took precautions, it took measures. It boosted [the cyber-security]. Here, I look after my own interest as a citizen [emphasis added].

(Lawyer 3, 2017)

This interesting extract does not show a position opposite to the state, neither a position defending the state in all conditions. It is a “pragmatist” approach, as the interviewee interprets herself (Lawyer 3, 2017). It is not framing the good hacker as the hacker of the state, as some LEAs do. However, this perspective is supportive of the state in the sense of considering the state’s good performance important for the wellbeing of its citizens.

It is a little bit ambiguous to trace the line distinguishing being supportive or being opposite to the state, especially when being critical of the state is considered as a tool to ameliorate the state.

If they leak the *crimes of the state*, then they are good hackers. It is political.

(Lawyer 10, 2019)

Here, by an incremental divergence from “the hacker of the state” perspective, the good hacker is framed as the one who struggles against the crimes of the state with an unvoiced motivation of public good. As an openly leftist lawyer, she considers the state as an entity that commits crime against its citizens. For that reason, public good cannot be framed as

non-harm to the state in her perspective. From how Redhack is framed as a criminal, we arrived to the crime frame of hacking, then to the frame of public good. Now, the question reaches the crime framing of the state.

6.2.4. A Change in the perspective: State (cyber)crimes and ghosts of counter-guerilla

Actually the lawlessness of the state agents was a quite common topic for many of the interviewees when they talked about the performance of the state against cybercrime. From the preferential treatment to the purchasing of unnecessary and useless technical devices, from warrantless wiretapping to illegal digital tracking, from manufacturing of the evidence to the use of social media bots⁴⁶ and trolls,⁴⁷ many reactive acts of the state that do not fit in the legal framework appeared during many interviews (LEA 2, 2018; LEA 5, 2018; Prosecutor 2, 2019; Expert 2, 2018; Lawyer 3, 2017; Lawyer 4 & Lawyer 5, 2018; Lawyer 6, 2018; Lawyer 10, 2019). Even though all interviewees who talked about these issues considered these incidences as lawlessness acts of the state, many abstained from framing them directly as crime. They preferred to stay in the safe lands of beyond law, between categorizing these acts as lawful or criminal.

The conceptualization of “state crimes” is discussed widely in the literature of critical criminology (Chambliss, 1989; Barak, 1991; Green & Ward, 2000; Ross, 2000; Kramer & Michalowski, 2005). About the issue of cybercrimes committed by the states, the critical perspective in internet policy studies focuses on the “informal and indirect practices of suppression” on the internet (Yesil, Sözeri, & Khazraee, 2017, p. 26) and names these illegal acts of the state as “third generation controls” (Deibert, Palfrey, Rohozinski, & Zittrain, 2010).

In that line, the usage of hackers by the Turkish state as one of the illegal methods to control internet was alleged (Yesil, Sözeri, & Khazraee, 2017, p. 10). During the interviews, to the question of whether the state uses hackers, many responded with “possible” (LEA 3, 2018). The name of the National Intelligence Organization (MIT)

⁴⁶ “A computer program that works automatically” (Cambridge Dictionary/english/bot).

⁴⁷ “Someone who leaves an intentionally annoying message on the internet, in order to get attention or cause trouble” (Cambridge Dictionary/english/troll).

appeared more than once during the interviews about this issue of the hackers working within/for the state. MIT is framed like a black box in the discourse of judicial actors. While some claimed that “MIT has a very qualified cyber staff” (Expert 5, 2019), others said: “few people work for MIT but there are many supportive ones” (Expert 1, 2018). Following that “supportive people” argument, the possible relation between patriotic hacker groups in Turkey – like Ayyıldız Tim – and MIT is one of the raised allegations (Prosecutor 1, 2019). Turkey was quite deeply influenced by the wave of the patriotic hacking in the 2000s. Ayyıldız Tim constituted one of the outstanding experiences with its explicit nationalist ideology and its close stance to the state discourse. This kind of supportive actors working for the state’s perpetuity without standing officially within the state has a long history going back to the era before the cyber issues. In the case of Turkey, this refers to the counter-guerilla activities – the illegal use of paramilitary groups by the state against leftist, Kurdish, and dissident groups, with a peak in the 1990s.

90’s, there were counter-terror structures in Turkey, the deep state, Abdullah Çatlı, *Green*.⁴⁸ The state used them. Now [about hackers], I do not know.

(LEA 5, 2018)

Even in the cautious response of this LEA to the question of whether the state uses hackers, the ghosts of the counter-terror / counter-guerilla come forward. In some interviews, this characteristic of the state is legitimized with the feeling of falling behind. Another LEA would say: “Criminals are always one step ahead. Like counter-guerilla. Defense pursuant to the attack” (LEA 6, 2019). Alongside the explicit usage of counter-guerilla, Lawyer 3 would say more implicitly: “The state responded to every new method with an anti-method or a counter-method” (Lawyer 3, 2017). According to one of the interviewed experts, counter-guerilla tactics are all about suppression.

⁴⁸ Abdullah Çatlı and Green nicknamed Mahmut Yıldırım are infamous names from the 1990s. The Turkish state allegedly used both names to perform illegal acts, up to the point of massacring civilians.

[The state] It uses hackers. The counter-guerilla issue, it tries to suppress. The state stands aside sometimes. Sedat Peker.⁴⁹ A man like you, like me. Yet, it works with fear.

(Expert 5, 2019)

The next question is who the state and patriotic hackers try to suppress with fear. The answer is similar to how the state answered this question in the classical counter-guerilla: The target is “the websites of leftists, socialists, dissidents, and belonging to the people struggling for ethnic issues” (Lawyer 10, 2019). According to Lawyer 10, the state frames the good hacker with patriotic hackers who inform the state in case of detecting deficits and who attack above mentioned websites with propagandist messages (Lawyer 10, 2019).

In line with the nationalist ideology of patriotic hackers, an emphasis on *the harm to the country* is added to the figure of bad hackers in defining the motivation of groups like Redhack and Anonymous: “They do not want the country to develop” (LEA 2, 2018).

Together with the modernization myth, the developmentalist ideal is one of the cornerstones of the Turkish official discourse through the narrative of *the modernization of Turkey* (Özbek, 2003, p. 235). As an actor performing within the neoliberal period fueled by populist ideologies, AKP revitalized the economic development myth. In this myth, domestic and foreign enemies [*iç ve dış mihraklar*] appear as the scapegoats in the absence of all that are promised but cannot be provided. It is because of these enemies that the country could not reach the foreseen development level (Cinar, 2017, p. 62). Here, Redhack and Anonymous stand as the perfect examples of domestic and foreign enemies. Harm to the country is not a side-product of their hacking deeds. These groups are framed as agents actively harming the country with this exact motivation. Yet in other instances, the harm to the country by leftist hackers is framed less aggressively:

There are leftist hackers, those who disrupt the system. Still, they have right on their own side. The ideology that they adopt requires it: communism. They harm their

⁴⁹ Sedat Peker is also a name known for his mafiatric business and his close relation with the state. Allegedly, he is the ideological successor of Abdullah Çatlı in counter-guerilla.

states. They suppose [acting] to make the state serve the people. However, *the harm to the state brings harm to the citizen.*

(LEA 4, 2017)

Here, compared to the previous framing in which Redhack was considered as a criminal group acting with the motivation of harming the state/the country, this second framing can be considered lighter with the infantilization of the actors. Criminals are not to blame severely because they are unable to understand the truth about their crime: it is through the construction of the direct connection between the harm to the state and the harm to the people.

This positive framing of patriotic hackers would lead to a request of differential treatment towards these actors. Reacting against the motivation blindness of legal framework for cybercrime, this perspective defended “the necessity of *different* punishments for those patriotic hackers in jail, for their service to the state” (LEA 4, 2017). In more moderate articulations, the appraisal was expressed as a wish to not oppose patriotic hackers (LEA 6, 2019). However, even when the motivation related to the state is considered as the main distinction between good and bad hackers, the harm to the country/the state does not result in an undisputed *goodness* of hackers.

6.2.5. Relativity of good hackers: Positionality, motivation, skills

A patriotic hacker is good or bad depending on which side one is looking to her. “Right-wing hackers are black hat for opposite countries, white hat for their own country” (LEA 4, 2017). Another one would emphasize this relativity through the attacks of Ayyıldız Time against Israeli websites: “They are black hackers for them [Israel], white hackers for me” (LEA 7, 2019). Even though, these interviewees considered patriotic hackers as good hackers, they were aware of the relativity of this attribution.

Reference to figures from historical narratives came up to emphasize this relativity of patriotic hackers as good hackers. *Robin Hood* (Prosecutor 2, 2019) and *Barbaros Kheireddin Pasha* (Expert 4, 2018) were mentioned during the interviews. Both references were used to problematize the boundaries between good and bad hackers:

Robin Hood was good or bad? If you are rich, he draws sword against you. Hacker is the same, similarly created names. If they are narrated romantically or tragically, it is different.

(Prosecutor 2, 2019)

Who is Barbaros Kheireddin Pasha? A pirate. Europeans know him as the Redbeard. A pirate. Who is for us? A pasha.

(Expert 4, 2018)

Not just the position of the hacker concerning the state, but other motivations are also considered critical while framing the good hacker. For Lawyer 10, the good hacker is framed in the negative of what would the bad hacker do:

Is there harm to persons? Is there harm to people? Is there a personal *profit*? If these are missing, then it is a good hacker.

(Lawyer 10, 2019)

Alongside the harm to the country, personal profit or economic gains is often cited as a characteristic of bad hackers. The bad hacker is the one who uses her skills for “the exploitation of information, the fraud” (LEA 1, 2017). “Bad ones are those who interfere in the system for personal profits” (Prosecutor 3, 2019). Cultural references appear again in this issue. Expert 4 gives the example of Lucky Luke to demonstrate the difference between good and bad hackers, based on the lack of economic profit motivation for good hackers.

White hat is *Lucky Luke*. He is good with guns. Yet, he does not use it to rob a bank, to have an easy life. Black hat, it is *The Daltons*.

(Expert 4, 2018)

From this extract, another important point emphasized by many interviewees appear. This is the skill of hackers that the interviewee indicated by narrating how proficient is Lucky

Luke with fire arms. In this perspective, first of all, a good hacker has to be a skilled hacker. Actually the emphasis on the skill of the hacker is such a central issue that in some interviews, it appeared not just as the characteristic of good hackers but as the fundamental aspect of being hacker. Components of the technical expertise like the knowledge about computer, software, software engineering, and software language are the absolute musts of being hacker for many interviewees (LEA 2, 2018; LEA 3, 2018; Expert 1, 2018; Expert 4, 2018; Lawyer 10, 2019). This expertise should be reflected in their acts of hacking, too. Even for agents of law enforcement, it is what distinguishes hackers from ordinary cybercriminals who do not develop their own tools and who just imitate hackers.

Using thousands of bots is not hacking for me. Hacking is a different skill.

(LEA 3, 2018)

They [Hackers] should write their own viruses. If they cannot, these are *lamers*.

(LEA 2, 2018)

Lamer is an insulting pseudo-category largely used within the hacker community to define incompetent hackers. As it appears in the discourse of LEAs during the interviews, during the trial against a less known hacktivist organization called *Cold Hackers*,⁵⁰ a very long paragraph is reserved by the prosecutor in charge to define lamers, too. According to the prosecutor, lamers are “unskillful people who aspire to be hacker. They try to show off by memorizing parlor tricks” (Diyarbakır Heavy Penal Court no. 2, 2016). It is as if state agents share the jargon of the hacker community, as an insider of the community. Such convergence between state agents and the hacker community is in total opposition with the perspective of one of the interviewed prosecutors who did not accept the distinctions between good and bad hackers. According to her, such distinctions were just a jargon between the hacker community (Prosecutor 2, 2019). However, following the mention of *lamer* in the state discourse, the emphasis of the prosecutor about how the state should see

⁵⁰ Cold Hackers is a Pro-Kurdish hacker group. During the lawsuit about them, the group was charged with having relations with PKK.

hackers as *outsiders* becomes the indirect admission of the tendency within some state agents to consider themselves as *insiders* of the hacker community.

6.2.6. *Insiders and outsiders: Against the criminalization of hackers*

The insider perspective is stronger within the interviewed experts to the degree of considering hackers equal to themselves. Some defined hackers “as a kind of experts [bilirkişi]” (Expert 1, 2018). They were also quite protective about who should be named hacker and who should be not. One expert warned: “One should distinguish hackers from imposters” and following that, she defined hackers as “the ones who find the deficits of the system” (Expert 5, 2019). Almost all of the experts were quite critical of the criminalization of hackers. In this critic, a feeling of intimacy can be sensed through an explicit nostalgia about the time of the first generations of hackers who followed the *hacker ethic*. The hacker ethic is the famous anti-statist manifesto in which ideals like the freedom of information, the merit system between hackers, and the use of ICTs for public good are introduced (Levy, (1984) 2010, pp. 27-38). In that line, Expert 4 claims that the concept of the white hat hackers is developed against the criminalization of hackers and to substitute the notion of hacker, in its original meaning compatible with the hacker ethic.

If someone called me hacker 30 years ago, I would be proud. It meant to know it [ICTs] very well, it did not mean criminal. Then, there were crackers, cybercriminals. American press and a little bit English press should have found them too long that the word hacker degenerated. It turned to negative. I denied [that I was hacker]. The [ICTs] sector restored it a little bit with the white hat.

(Expert 4, 2018)

This “30 years ago” is the implication of the period before the criminalization of hackers in the 1990s and the allusion of the hacker ethic. Like almost all interviewed experts, Expert 4 had an engineering education, too. Even though she described herself as “lay [alaylı] security expert,” she is an important figure within the ICTs community. Expert 3 is another interviewee who preferred to evoke the history of hacking to define hacking. Similar to

other experts, hacking is not something *new* for her and to explain it, she mentions the book of Julian Assange – no doubt, *Cypherpunks*⁵¹ – as the source from which one can see how hacking was meant to be political hacking against the financial system in the 1980s (Expert 3, 2018). Indeed, the resistance against the proprietization of information was a central characteristic of the global trend of political hacking in the 1980s and at the beginning of the 1990s. In that way, she makes an indirect link to the freedom of information ideal from the hacker ethic. Expert 1 is also explicit about the importance of the first generation hackers in defining hacking. She emphasizes the contribution of hackers to the software development – most probably referring to the “software hackers” of the 1970s (Jordan & Taylor, 2004, p. 10).

Expert 5 refers to an older mentality than the hacker ethic, to the birth of hacking in the 1960s and in the 1970s when hacking was considered as an intellectual exercise to challenge the paradigms of computer science. Through this primitive definition, she emphasizes the necessity to diverge hacking from fraud.

We should diverge hacking from fraud. Hacking is the shortcut. In English. For example, this is a glass, but you use the glass in different ways. For example, you hack the cassette tape. Shortcut, a different method, for example, if the battery was low, you rewound manually. (...) Now, they consider credit card fraud as hacking.

(Expert 5, 2019)

Expert 1 would also emphasize that the starting point of hacking was “to use your mind and to develop quick solutions” (Expert 1, 2018). In these definitions, not just the recalling of the hacking history but also the enlarging of the hacker definition beyond the limits of crime and beyond the limits of ICTs is visible. Alongside experts, lawyers mentioned that issue, too: “Hacking is to find an easy way, to find a method for something” (Lawyer 3, 2017).

⁵¹ Founded in the early 1990s, Cypherpunk movement is distinguishable with its emphasis on cryptography to achieve societal and political change. These hackers advocate for the privacy for the weak – the protection of private information or data – and struggle for the transparency of the powerful – the usage of public information. Anti-statist and anti-corporatist ideologies are quite explicit among Cypherpunks. For more information, the mentioned book is quite useful (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2012).

However, defining hacking beyond the limits of ICTs did not always coincide with considering hacking beyond the limits of crime. It is apparent in how interviewees often give the example of *social engineering* to concretize hacking beyond technical (LEA 2, 2018; LEA 4, 2017; LEA 7, 2019; Expert 3, 2018; Lawyer 3, 2017). Social engineering is the psychological manipulation to obtain information from system users and operators (Anderson, 2008, p. 18). The name of Kevin Mitnick is mentioned more than one time during the interviews. Mitnick is “not the best but the most famous hacker” – as one interviewee carefully emphasizes (Expert 4, 2018) – and he is known with his skills in social engineering. One interviewee would describe social engineering as “giving your confidential data yourself” (LEA 4, 2017). That is related to this type of hacking that one LEA would defend individual responsibility and vigilance as a solution for the problem of cybercrime (LEA 7, 2019). In this frame, ordinary citizens are framed as vulnerable against “vigilant” hackers “who exploit people’s foolishness” (Expert 2, 2018).

In line with that dichotomy between ordinary citizens and vigilant hackers, many intellectual capabilities are attributed to the image of hackers in the discourse of judicial actors. The intelligence of cybercriminals is a topic that especially the prosecutors expressed during the interviews.

Children commit cybercrime, too. Very intelligent children. First thing they see is their phones. They start by committing frauds. (...) There is no way for ordinary, simple people to commit [cyber]crime.

(Prosecutor 1, 2019)

Since the global trends of the 1990s, cybercriminals – and hackers, as these two are used in an interchangeable way by the interviewees – are considered as the masters of information and communication technologies (ICTs). In this perception, their craft is assumed to be related to their familiarity with ICTs thanks to their young ages. As the digital natives of the technological era (Barlow, 1996), young generations are always attributed with an advantage to be more familiar with developing technologies. Actually, the notion of young generations does not refer to a specific generation. It is a perpetual relation between developing technologies and younger generations. In interviews, the mention of *children*

appears a lot to define who the cybercriminal is and who the hacker is. The age of who these children are differ widely, in line with the unspecific reference of digital natives. For some, these are 12-13 years old children who develop curiosity for hacking through video games to find game tricks (LEA 2, 2018). For others, 18-20 years old who want showing-off and/or learning new things are the main population of hackers (Prosecutor 2, 2019). Age range of the imagined cybercriminal can increase to 25-30 years, an age where the curious gamer children of once become disappointed with not being recognized and being jobless (Prosecutor 3, 2019).

Intelligent children. If they are directed towards positive acts, they would be quite helpful. They want to make money. At a young age, they want to make money through selling characters in gaming websites. I do not think that most of them are bad people, harmful to the society. They expect to be recognized by the state or by the sector.

(Prosecutor 3, 2019)

As this extract shows, the intelligence attributed to the young hacker image does not become a source of anxiety, as it becomes in the global trends of the criminalized hacker perception. As one expert would express: “The judicial system sympathizes with them [hackers], yet they do not understand and they arrest based upon the misdirection of the law enforcement” (Expert 5, 2019). In this perspective, prosecutors do not consider hackers as an “irreducible systemic threat of digital media” (Krapp, 2005, p. 71). The image of the “talented nerd” having profitable yet innocent hobbies (Krapp, 2005, p. 71) is still acceptable within the discourse of prosecutors.

The interest for cybercriminals is like at the edge of an implicit exaltation in many interviews. The adaptation ability of these actors to the novelty of ICTs while the state and its agents suffer heavily from the feeling of falling behind creates an appraisal even from the most distant actors to ICTs. “Criminals update themselves, as the internet system updates. (...) It is interesting. Types are interesting, both the offender and the victim” (Prosecutor 1, 2019). The novelty of cyber-related issues is indeed a source of anxiety for judicial actors. Yet, in the same time, it is a fascination.

As many interviewees stress over and over, “cybercrime is a new issue” (Expert 2, 2018). It is indeed new in Turkey, compared to other crime categories. Cybercrime is regulated for the first time by the new Turkish Penal Code in 1991. The broadest regulation was promulgated by the new Turkish Penal Code no. 5237 in 2004 (Bilgi Teknolojileri ve İletişim Kurumu, 2016a). The novelty accompanying the technological development constructs a kind of interest and curiosity for crimes related to these technologies from the perspective of judicial actors. “A new type of crime every day,” a prosecutor would say and she would add: “Working on cybercrime takes you somewhere. It is like eating a new meal in a new table everyday” (Prosecutor 1, 2019). One of the LEAs shares this positive framing of cybercrime by emphasizing her curiosity for novelty in cybercrime (LEA 3, 2018). Expert 3 expresses her motivation to do her job by defining “expertise as the means to follow the latest developments” (Expert 3, 2018). In that sense, the overemphasis on cybercrime does not always imply a negative framing. It is following that perspective that the positive framing of the agents of cybercrime surfaces within the discourse of judicial actors.

While the positive perception of prosecutors is implicit for hackers, the advocacy of experts is much more explicit. Within this embrace of the hacker ethic and the consideration of the hacking culture as something more than just a criminal act, experts accuse the popular media and the news media – mostly Anglo-American sources – for the negative change in the meaning of hacking (Expert 1, 2018; Expert 4, 2018). In the discourse of the experts, media actors become the scapegoats of the criminalization of hackers, independently from the context that gave rise to that negative perception. In sum, for almost all of the experts and for few other actors, “hacker is something beyond the guy who breaks the system” (Lawyer 3, 2017). However, not everyone is so critical of the crime framing of hackers. For some interviewees, the hacker is exactly *that* guy who breaks the system.

A cybersecurity expert cannot be a hacker. Hacker is someone who finds and who exploits the deficits of the system data. It is an *aggressive* word. Hacking and security cannot exist together. Hacking is a crime notion [emphasis added].

(LEA 7, 2019)

The responses that the interviewees gave to the questions about how to define hackers and how to define good hackers were critical instances in which the critical positioning about the criminalization of hackers manifested – as with most of the experts – or it did not manifest – as the case of LEA 7. For LEA 7, the non-existence of an intimacy with the hacker community prevented such a critical positioning about the criminalization of hackers. However, for some other LEAs, the closeness with the hacker community appeared through the figure of the cybersecurity expert. According to one LEA who also works as an expert for judicial processes, “for hacking, one should be a cybersecurity expert” (LEA 2, 2018). This equalization of hackers with cybersecurity experts or directly with experts exposes an interesting element of intimacy between some interviewees and the hacker community. In that sense, the question of who is the (good) hacker was responded with an implicit *me*. The definition of hackers as experts [bilirkişi] by one of the experts was the crystallization of that appropriation. This becomes apparent especially when considering hacking as a craft and hacker as a craftsman who has high skills in ICTs. In that sense, the positive perception of the hackers was prevalent among interviewed judicial actors from two sides: from the actors who embrace the hacker culture in the form of an appropriation of the hacker identity and from the actors who perceive hackers as interested outsiders. Not a single interviewee among 25 actors was disinterested totally with hackers, based upon hacker’s skills, intellect and craft or upon their motivations, like seeking public good or pursuing the wellbeing of the state.

6.2.7. Implications of framing Redhack as cybercriminal

Following these discussions, the framing of Redhack as cybercriminals was changing depending upon the perception of its hacking skills and whether this group should be included in this category of cybercriminal/hacker that is endowed with such a positive perception from different judicial actors. For that reason, the perception of Redhack as a hacker group was quite ambiguous during the interviews. The first interviews with LEAs had shown that Redhack was not considered as a good hacker group not just because of its motivation to harm the state, the country, the public – according to the interviewees’

perspective – but also because an alleged absence of their hacking skills (LEA 1, 2017). On the other side, for lawyers specialized in cybercrime, Redhack's acts were in the scope of cybercrime without doubt, even these acts were considered legitimate in the eyes of the public (Lawyer 3, 2017). If the interviews were left at that point, it would be easy to link the positive framing of Redhack with its hacker/cybercriminal framing. However, following interviews complicated the schema of frames. One of the interviewed lawyers who was ideologically very close to Redhack claimed that what the group did was not hacking but a simple information leaks thanks to the security deficit, when she talked about the first Redhack case related to the data leaks from Ankara Police Directorate (Lawyer 10, 2019). On the other hand, different from the first interviewed LEAs, the last LEA who was quite negative about the group claimed that Redhack's acts are based sometimes on the information provided by people in the field, and sometimes they are performed through their hacking (LEA 7, 2019). This seemingly neutral explanation of LEA 7 is actually a significant acknowledgement because many LEAs avoided using the word hacker while talking about Redhack. It was as if the absence of the hacker frame would be instrumental to discredit the group. The reason of the indifference of LEA 7 to qualify Redhack as a hacker group without any concern is linked to its distance to the hacker culture and to its crime perception of hackers. Yet, LEA 7 constitutes a small part of the total interviewee sample who – by a majority – endows hackers with a positive perception. In the avoidance of the cybercrime/hacker framing, another frame is operated. In concordance with judicial processes and news media, (cyber-)terror frames activate for the criminalization of Redhack.

6.3. Cyber-terror and terror frames: Containment of the dissidence

In this second part, I will examine cyber-terror and terror frames based on five discussions. First, narrow frames of political hacking and hacktivism will be demonstrated through their opposition to the paranoias of cyber-terror, cyber threat, and cyberwar. Second, following the ambiguities of designating the cyber-terrorists, the notion of harm will be once again discussed in the scope of cyber-terrorism. Third, following the unclear and changing definitions of harm, anxieties of defining cyber-terror will be presented through the

discourse of judicial actors. Then, the summoning of older frames of terror by the state will be put on the table through the use of moral panics and folk devils. As the last discussion, I will look to the critics about this terror label based on folk devils of terror and to the limits of that critic. At the end, the implications of framing Redhack as terrorist based will be examined upon former discussions.

6.3.1. *Narrow frames of political hacking vs. Unchained paranoias of cyber-terror*

Redhack's act is totally *hacktivism*, and *cybercrime*. A cybercrime is committed. It is clear-cut. Doing a supportive act in the eyes of the public cannot legitimize that deed. *Crime is crime. However, it is not terror* [emphasis added].

(Lawyer 3, 2017)

The interviews with the actors from the Turkish judicial field concretized how *hacktivism* is a politically loaded concept that indicates a specific – and mostly positive – framing for information and communication technologies (ICTs) related political acts. The history of the changing perceptions on hacktivism had exhibited how this concept is constructed in opposition to specific crime frames like the label of cyber-terror. In that sense, the use of the concept signifies a positive framing critical of the criminalization of political acts. Seldom appearance of the hacktivism concept during the interviews (Expert 4, 2018; Lawyer 3, 2017) indicates two possibilities about the perception of cybercrime in the Turkish judicial field: Hacktivism is not a known concept for judicial actors and/or hacktivism does not answer to their perception of cybercrime. In one of these few appearances, Lawyer 3 creates an opposition between two crime frames: She puts hacktivism within the cybercrime frame and diverges it from the terror frame. Following that, in this part, one of the main problematics will be based on the lines distinguishing political hacking – as a more familiar synonym for hacktivism – and cyber-terror.

Political hacking is framed quite narrow compared to the imagined cyber-terror in the discourse of judicial actors. This disproportionality is especially striking in the response of a prosecutor who worked on one of the Redhack related cases. When she is asked to define political hacking, she responded:

I hardly saw political hacking. Probably, it is insulting a politician that they do not like.

(Prosecutor 3, 2019)

The reference to harm politicians appear in the response of another prosecutor, too. This time, political hacking is framed as “the deed with the motivation of harming a political campaign, a simple data interference” (Prosecutor 1, 2019). The coexistence of hacking and politics rarely refer to activism but mostly to cyberwar scenarios in the international level. During the interviews, when political is mentioned, it is understood related to the deeds of the nation-states. In an imagination fueled with movies – similar to how cybercrime was imagined, cyberwar and cyber-terror are considered as the characteristics of our era.

It is not the time of cannons and rifles anymore. Our era is the time of cutting the electricity of a city with cyber tools from where you sit.

(Expert 3, 2018)

As one of the interviewees remarked it, actually there is not a single event acknowledged as cyber-terror neither in Turkey nor worldwide (Prosecutor 1, 2019). In the absence of real events to refer to, judicial actors referred to imagined threats to define cyber-terror. Attacks to the infrastructure of the country, disabling its power plants and structures, demolishing its communication and transportation networks, and damaging airline companies and hospitals emerge as cyber-paranoias of the judicial actors during the interviews (LEA 5, 2018; Prosecutor 1, 2019; Prosecutor 3, 2019; Expert 2, 2018; Expert 3, 2018; Lawyer 8, 2018). In these paranoias, the critical line that separates the cyberwar from cyber-terror is not the type of acts but the identity of actors. For many interviewees, cyberwar is a game between the states, while cyber-terror is the acts performed by extra-state actors against the states (Expert 5, 2019). Even in the discourse of actors who are most rigid about the definition of cyber-terror based upon the motivations of terrorists, the exclusion of states from the cyber-terror definitions is apparent.

Of course, we would not call the US a terrorist organization just because now, we are on bad terms with them.

(LEA 2, 2018)

Not the nature of the deeds but the actors defining whether an act is cyber-terror or not would remain as a critical point not just for the crime frames of Redhack but also, it will be one the main sources of the general anxiety felt about cyber-terror. When we are talking about cyber-attacks, it is never easy to identify the agents. “We do not have a clue about who is doing what in the cyber realm,” as one expert would express (Expert 4, 2018). Actually, even identifying between cyberwar and cyber-terror is not always accurate, as states sponsor patriotic hackers behind the scenes. For some interviewees, the difference between individual and state powers is still in force in the ICTs related realm (Lawyer 8, 2018). For that reason, important attacks should be performed within the knowledge of nation-states, if it is not their direct action. In that line, when there is a hacking act against an institution that can be identified with a state, this act is easily framed as the attack of a country. *Stuxnet*, the cyber-attack on the nuclear program of Iran, is cited several times when interviewees were asked to define what is cybercrime, cyberwar, and cyber-terror (LEA 5, 2018; Prosecutor 2, 2019; Expert 3, 2018; Lawyer 8, 2018). The confusion between whether to define it as cyberwar or cyber-terror was based upon the unclear nature of the American and Israeli support behind the hackers who performed this act. Another common example was the Russian intervention to the American elections (LEA 5, 2018; Lawyer 8, 2018) and to the electricity cut in Ukraine (LEA 5, 2018; Expert 4, 2018). As these acts are illegal acts that cannot be acknowledged explicitly by the state, the ambiguity of the actors in the cyber realm is doubled by these unclear relations between the states and the hackers.

These ambiguity reflects in the framing of Redhack, too. For some interviewees, Redhack is sponsored by nation-states – similar to the patriotic hacker groups, but this time, they are not sponsored by the states of their own countries but by *foreign* states.

Redhack is not just in Turkey. Greece, Germany, Great Britain, France support them. All states against Turkey support them.

(LEA 4, 2017)

Framing protest and activism as the acts supported by foreign states is not a recent reaction of governments. The history of Turkey, as well as many other nation-states, is full of defamation campaigns directed by the official discourse to frame domestic protest movements as a foreign states involved issue. In some instances, official frames can also exhibit the opposite reaction, like framing a foreign threat as a domestic issue to increase its relevance for the public opinion (Noakes, 2000, p. 661). However, the framing of Redhack as the deed of foreign states is to externalize a domestic issue, a distraction from the acts of Redhack that are mostly about domestic problems to the threat of foreign enemies. In that sense, once again, this is part of the larger “domestic and foreign enemies” rhetoric.

The appearance of nation-states as central actors within the discourse of state agents is a kind of surprising. While the discourse of neoliberal globalism was already erasing the image of nation-states as primary actors, the cyber realm was supposed to be less influenceable to their acts. In that sense, the perception of the judicial actors expresses a strong presence of the states – real or imagined – within the ICTs related conflicts in the global scale. This perception empowers the critique of considering states as passive victims of – digital – globalization. In this perspective, rather than victims, states are the authors and enforcers of that new global system (Panitch & Gindin, 2005, p. 101).

The reflection of that state-centered perception on the framing of Redhack is the interrogatability of its activism. Alongside its alleged relation with foreign states, one interviewee claimed that Redhack had done hacking on behalf of the Turkish state, too (Expert 4, 2018). On the other side, the collaboration with the state is not always framed negatively. Lawyer 10 mentioned how the state took support of the group about the issue of child pornography. She added: “The guy solves what the state, what the police cannot solve” (Lawyer 10, 2019). Here, there is a highly positive framing of Redhack. First, a positive framing based on its motivation to struggle against an issue of moral panics, child pornography. Second, a positive framing based on its craft as a skilled hacker, compared to the state and to its agents.

However, during the questions about defining political hacking, few interviewees who responded with activism – rather than cyberwar – had actually hesitant responses to

give Redhack, as an example. For one expert, “Redhack introduces itself as a political hacker” (Expert 3, 2018). According to one LEA, Redhack says “we are doing it [hacking] for the struggle” (LEA 5, 2018). Right after giving the examples of “Anonymous in the international arena and Redhack in Turkey” for political hackers, Lawyer 8 quickly added her indecision about how to categorize political hackers like Assange, whether as cybercrime or as cyber-terror (Lawyer 8, 2018). Lawyer 8 was cautious to talk about issues of cyber-terror. Specialized more in courts of peace than criminal courts and interested in the theoretical discussions about cybercrime, Lawyer 8 shared the unwillingness to talk about cyber-terror with Expert 2 and Expert 4. However, I cannot say that this unwillingness corresponds to their specialization area. In other words, those specialized in cybercrime do not wish to talk about cybercrime would be a wrong implication, as Expert 3 and Lawyer 3, both specialized in cybercrime had strict views that they wanted to share willingly during the interviews.

After the difficulty to diverge cyberwar and cyber-terror based on the shady relation of hackers with the states, another ambiguity comes about the identity of political hackers. How to diverge cyber-terrorist and political hacker?

6.3.2. Shaping harm to find out cyber-terrorists: From bad intentions to data theft

We are living in a wicked atmosphere. There are those who have *bad intentions*. It is an atmosphere we cannot understand who is what. (...) Some of them *exploit* activism [emphasis added].

(Expert 3, 2018)

The mention of “bad intentions” brings us once again to the issue of motivations. Motivations constitute another fundamental theme in framing cyber-terror. Similar to the framing of bad hackers, cyber-terrorists are framed mostly through their motivations to intentionally harm the country (LEA 2, 2018; Prosecutor 3, 2019), the state (LEA 2, 2018; LEA 4, 2017; Prosecutor 3, 2019; Expert 1, 2018; Expert 5, 2019), the public institutions (LEA 4, 2017; Prosecutor 1, 2019; Expert 3, 2018), the social order (LEA 2, 2018), or the people (LEA 4, 2017; Prosecutor 1, 2019; Prosecutor 3, 2019).

These categories are not totally separate ones. Many interviewees used more than one categories to define cyber-terror. For example, for LEA 4, cyber-terror could be against a person, a public institution, or against the state. Here, how interviewees frame the notion of *harm* becomes important, too. When we were talking about the harm against a person, it was mostly a murder or physical damage. In the case of institutions, *harm* was used equal to disabling. “Placing a bomb in a bank and bringing down the system is the same. Disabling the bank,” a prosecutor would say (Prosecutor 1, 2019). Yet for harming the state, things become much more complicated. How would you harm the state?

Those who attack Pentagon is a cyber-terrorist organization. Using ICTs to steal documents (...) Anonymous is a cyber-terrorist organization.

(LEA 2, 2018)

How the experience molds the definition of the act that it would be qualified is quite clear in this extract. It is through the acts of data theft performed by Anonymous – and also of Redhack – that the interviewee defines cyber-terror and the harm to the state. “Stealing documents” appears in the responses of other interviewees, too. One of the prosecutors would say: “You can obtain all the data of a country. You can obtain weapons” (Prosecutor 3, 2019). Another interviewee would speculate about the state’s perspective about cyber-terror: “It [cyber-terror] may be the content that can harm the states, information about clandestine works of the sub-units of the state or information about the functioning of the state” (Expert 1, 2018). It is not a physical harm nor disabling that emerges in the discourse of judicial actors. It is the critical possession of data that harms the state.

E-state structure, data. It is the most valuable thing, data. That means the cause [dava] of a country.

(LEA 5, 2018)

Obtaining information without permission. For the state, it is home, it is private [mahrem].

(LEA 7, 2019)

The importance for the states of possessing data and information that no other actor possesses under its sovereignty reflects on framing data theft as a critical harm to the state. The attributed centrality of data by the interviewees reminds the informationalism argument of Castells related to which he claims that processing information became the main technological source of the economic, political, and social system (Castells, 2001).

The incompatibility between different framings of harm – to the person, to the institution, and to the state – in defining cyber-terror crystallizes in comparing cyber-terror to terror.

They hacked directly the prefecture, they threw a molotov cocktail to the office of the sub-governor. The table is burnt. The other hacked, took data, shared it with terrorist organizations. Would not we call them terrorist organization? There are armed man, hackers can help, too.

(Prosecutor 3, 2019)

The interrogative form of the response expresses the need of approval in an issue that the interviewee is not confident either. The ambiguity of cyber-terror comes from the absence of a description for the notion in legal texts (LEA 7, 2019; Lawyer 10, 2019). Lawyer 10 declares that she does not think that there is a description for cyber-terror and therefore, the state can see everything as terror. She speculates that maybe, acts involving data leaks or password cracking can be considered as cyber-terror according to the state (Lawyer 10, 2019). Expert 1 also questions whether cyber tools are weapons or not and in which conditions crimes committed with these tools can be categorized as terror (Expert 1, 2018).

6.3.3. Chronic anxieties of defining cyber-terror

The absence of the legal definition for cyber-terror distresses many interviewees. They externalized their distress during the interviews with questions like “Why you ask me these issues?” and with an unwillingness to respond like “I am not an expert on these issues” (Expert 2, 2018; Expert 4, 2018). Expert 2 expressed openly his annoyance with defining

cyber-terror because for her, there is an ambiguity that she is not used to deal with, as a person coming from an engineering background. On the other hand, Expert 4 reacted more authoritatively as if these questions had other specific addressees and the interviewer made a mistake to ask these questions to her, rather than to ask these to these other *correct* addressees.

LEAs were the most confident actors to talk about cyber-terror. For them, the ambiguity about cyber-terror was about to find out who are cyber-terrorists, rather than an inherent ambiguity to the notion of cyber-terror.

Do not think like PKK. You cannot find them. (...) They would not declare: “We are from this terrorist organization.” They would say: “I follow an ideology.” They would say: “Leninist, Stalinist, Maoist,” they would say: “We are revolutionary.”

(LEA 2, 2018)

Irony of the interviewee was quite explicit in that response to display her perspective according to which ideologies are just masks hiding cyber-terrorists. LEAs also used interesting comparisons to concretize clear-cut definitions about cyber-terror. During one interview, the interviewee explained cyber-terror with an equation of killing somebody with harming the state.

You just add cyber to normal crimes, like cyberattack, cyberterrorism. An attack on public institutions as cyberterrorism and the attacks of the terrorist organization DAES because they attack human rights.

(LEA 4, 2017)

In this extract, she frames cyberterrorism as a mere appendix to the word terrorism and through this, she synchronizes these two acts – the attacks of DAES and the hacking of public institutions. Actually considering cybercrime equal to offline crime was quite prevalent among LAEs and experts.

Even though the environment is virtual, the crime is real.

(LEA 2, 2018; LEA 5, 2018)

Abovementioned motto was quite popular in the discourse of law enforcement agencies. The framing of cybercrime as real crime is undoubtedly an instrument to emphasize the criticality of cybercrime and to construct the criminalization of cyberspace. Following that, the legal framework in other countries is an argument that the interviewees like to refer to consolidate their perspective. “In other countries, all crimes have a cyber-version,” one LEA would defend in a reaction against the lack of legal framing in Turkey (LEA 4, 2017). The equalization of cybercrime to crime is also useful to highlight diverse types of cybercrime in comparison with their offline versions: child abuse through physical contact and child abuse through internet (LEA 3, 2018), theft and cyber-theft (Expert 2, 2018; Expert 3, 2018) – also hacking as qualified theft (LEA 6, 2019), and of course, terror and cyber-terror (Prosecutor 3, 2019; Expert 2, 2018; Expert 3, 2018).

Considering cyber-terror equal to terror is a difficult analogy to construct for the reasons cited above, as the changing nature of the notion of harm when it transfers from offline to online realm. For that reason, another relation is established to define cyber-terror. That is the summoning of those labelled as terrorists to designate cyber-terrorists. The ambiguity of defining cyber-terror is overcome with hypothetical relations formed between cyber-terrorists with *agreed-upon* terrorists.

6.3.4. Anxieties alleviated: Moral panics of terror, agreed-upon terrorists as folk devils

If they have connections with terrorist organizations that would harm the system of the state, then the law considers this notion as terror.

(LEA 6, 2019)

Reference to terror is fed by moral panics about specific groups and organizations in Turkey. One part of this moral panic is about leftist and identity rights groups. The consensus about their terror labelling is constructed through the decades long official ideology of the state through an explicit state policy. Other part is about FETÖ [Fethullah

Gülen Terrorist Organization], a new candidate of moral panics about terror after the failed military coup against the AKP government. Interviewees use both categories to designate cyber-terrorists.

Leftist terrorist organization, DHKP-C, MLKP, they do propaganda through ICTs, they collect militants to their organizations. Fuat Avni, he is right-wing terrorist.

(LEA 7, 2019)

Names of the leftist organizations and also of FETÖ/PDY had appeared in the indictments prepared during the judicial processes about Redhack. In the perception of the crime framing of Redhack, these alleged relations with the old folk devils will be also quite central to determine the positive or the negative perception of the group. Whether Redhack has relations with agreed-upon terrorists would be the turnsole of its terror framing. The reason was clearly declared by one interviewee:

Once you mention terror, most people beware. Nobody would like to be related to terror and terrorism. They would not like to be inside that issue or be its supporter.

(Lawyer 3, 2017)

Even if the enlargement of the terror charge towards diverse groups in the society resulted in a weakening in the moral panics of terror and gave rise to a process of its criticism, the terror charge still has an influence on third actors – those who are not the constructors of the terror label neither the actors labelled as terrorists. The discourse of cyber-terror actually possesses some elements of moral panics like the concern about the imagined threat and the disproportionality reflected in the exaggeration of its objective harm. However, in the moral panics about terror, central elements like the hostility towards the actors and the consensus about the moral outrage are added to the concern, the disproportionality, and the volatility elements of the moral panic (Cohen, (1972) 2011, pp. xxvi-xxvii). In that sense, not cyber-terror but terror is a source of moral panics in the discourse of judicial actors. Following that, subjecting cyber-terror to terror aggravates the

criminalization of cyber-terror and brings forward the question of how terror is framed as a moral panic.

In the framing of terror, two tendencies emerge among judicial actors: an official framing and an ethical framing. The official framing is the framing constructed in relation with official discourse and judicial decisions. For some interviewees, this means loyalty to the official framework without adding any ethical perspective. In another one of her interrogatively formulated responses, Prosecutor 3 emphasizes this official framing of terror.

If they support organizations that *the state accepts as* terrorist organizations, then, would not we call them terrorist organization? [emphasis added]

(Prosecutor 3, 2019)

Official framing of terror relies heavily on older folk devils of terror rather than a written legal definition. Even though Article 1 of the Anti-Terror Law defines terrorism, the interpretable nature of the article suggests a non-framing.

Any criminal action conducted by one or more persons belonging to an organisation with the aim of changing the attributes of the Republic as specified in the Constitution, the political, legal, social, secular or economic system, *damaging the indivisible unity of the State* with its territory and nation, *jeopardizing the existence of the Turkish State* and the Republic, *enfeebling, destroying or seizing the State authority*, eliminating basic rights and freedoms, *damaging the internal and external security of the State*, the public order or general health, is defined as terrorism [emphasis added].

(Turkish Anti-Terror Law, Article no. 1, 1991)

For some interviewees, this article was the source of considering terror as the harm to the state. Moreover she added that, according to this official framing, it was only natural for prosecutors and judges to consider Redhack as a terrorist organization, even though for him, Redhack's acts should have been included to cybercrime (Lawyer 1, 2017). As a leftist

advocate, Lawyer 1 was quite critical of the state's framing of terror. However, she did not see this framing as some recent issue peculiar to the AKP government. For her, it was part of a historical trend going back to the military coup of 1980 and to the promulgation of the Anti-Terror Law (TMK) in 1991 as a fruit of that post-coup context. It was in this context that the political crimes were transformed to terrorism in the Turkish crime discourse (Lawyer 1, 2017).

A milestone for neoliberal conservative policies, the coup discursively and physically erased the leftist political presence in the Turkish context. The 1980s witnessed the rise of the civil war in the Kurdish regions of Turkey and the political violence by leftist groups adopting illegal methods. The Anti-Terror Law of 1991 was indeed the embodiment of this political context. Another interviewee added that alongside "armed students' and people's terror," "the mafia terror" was another issue of the 1980s and the 1990s (Lawyer 7, 2018). For Lawyer 7, the mafia terror was the real reason behind the promulgation of the Anti-Terror Law.

In the promulgation of TMK, the mafia terror was the movement that Turkey did not want to exist. Those who somehow worked as agents for MIT, people from right-wing organizations who played roles for the state's interest in preventing the assassinations executed by Armenians in Europe, they had become gangsters. The state suppressed that terror. Like Alaaddin Çakıcı, Sedat Peker, Dündar Kılıç. Drug traffic.

(Lawyer 7, 2018)

For Lawyer 1, the Anti-Terror Law was strictly related to the labelling of political crimes as terrorist acts. For Lawyer 7, the inclusion of the terror crime into the Turkish law was related to political crimes – that she mentions as students' terror – and also, to the terror created by the state through the counter-guerilla actors getting out of the state control.

The category of political crimes has faded from the political discourse and also, from the judicial processes after the Anti-Terror Law. Whether political crimes should be included in terror charges or not was already an academic discussion among legal scholars (Bayraktar, 1982; Alpaslan, 1983). After the Anti-Terror Law, the total ignorance of

political crimes in favor of an enlarged terror frame was also criticized based upon the neglect of motivations between two crime types within the legal and judicial perspectives (Bayraktar, 2015, p. 149). However, in that critique, the potential terrorists are considered as people acting without any motivations than to bring the society into disorder.

In political crimes, *the political motivation is predominant*. Seizing or influencing the political power is the main issue. In other words, the political criminal is the one who executes acts against the political order of the state. Whereas in terror crimes, such motivations do not exist. In terror crimes, a terrorist organization member creates violence, terror, and intimidation against people *with the motivation of bringing the society into disorder* [emphasis added].

(Bayraktar, 2015, p. 149)

Framing terrorists as bad people deprived of any specific object-oriented motivation is in accordance with the formation of folk devils. Obscuring the background, motivation, and context of the actors makes it easier to demonize related actors (Cohen, (1972) 2011, p. xxx). That was also the problem of social movements about their news framing. Episodic coverage was a disadvantage resulting in the shadowing of the broader context from which social movement actors speak (Noakes & Wilkins, 2002, p. 652). When we adapt this perspective to our subject about the relation between political crimes and terror, the decontextualizing effort seems like the distinctive of the transformation of political crimes to terrorism. Since the 1990s, public opinion in Turkey largely accepted this transformation through the mainstream news media's widespread circulation. The absence of political hacking in the discourse of judicial actors can be interpreted in this legacy. Within the larger fading of political crimes, cybercrime with political motivations has no other choice than to be considered as cyber-terror rather than being framed as political hacking or hacktivism.

The summoning of agreed-upon terrorists from the political history of Turkey is to draw on the existing terrorism “master frame” (Snow & Benford, 1992) that had never been in abeyance for the Turkish state. In this way, the discussion about harm that was present both in the discussions about cybercrime and cyber-terror gains deeper meaning, too. By

calling the terrorism master frame to interpret cyber-terrorism, the Turkish state reminds of all the political struggle against the state as a violence against the public. The statist ideology is strengthened through equalizing state's harm with public harm and correspondingly, state's benefits with public benefits. Such reminder is deemed necessary, especially in the case of a hacktivist experience declaring to adopt the ideological line of these political struggles.

6.3.5. Limits of being critical: Relative opposition to terror labels

Resulting from the contextual formation and development of the terror label from the 1990s to the 2010s, many judicial actors prefer to construct their own ethical framings of cyber-terror and terror. In most cases, interviewees recognized the relativity of their terror framings that do not rely on specific sources.

When she was asked about cyber-terror, Prosecutor 2 would confirm once again the close relation between terror and cyber-terror: She would declare that to define cyber-terror, one should look to the definition of terror. Then, after declaring that “there is no definition of terror,” she questioned: “Is terror the deed? Is it destructive deed?” and declared its relativity and its contextuality by comparing it to the issue of visa liberation (Prosecutor 2, 2019). The relativity of terror – and relatedly, the relativity of cyber-terror – is expressed by LEA 6 with concrete examples:

PKK and DAES want to make propaganda and gather members through internet.
[That is] a terrorist act. If you do it for ÇYDD⁵², it is not crime. If you do it for
PKK, it is crime.

(LEA 6, 2019)

⁵² ÇYDD (Association for the Support of Contemporary Living) is a non-governmental organization with an explicit secular and Kemalist ideology. The organization is known especially with its educational projects. In 2009, during the Ergenekon case, the managers of this organization were accused of being allies with those who allegedly organized military coup attempt. They were acquitted in 2015. In this interview, ÇYDD is given as an example of non-criminal and opposite to terrorist organizations, just few years later of the accusations about the organization. This expresses the quickly changing political context in Turkey and the contextuality of the terror label through an off-topic example.

Once again, it is not the nature of the deeds but the actors who are defining whether an act is terror or not. In this definition, the use of agreed-upon terrorists is a beneficial instrument to construct ethical framings of terrorism. For Lawyer 7 who was the oldest interviewee, “Kurdish separatist event” was the milestone of terrorism in Turkey and that before that, we could not say “terror” for student movements (Lawyer 7, 2018). “In principle,” Lawyer 7 determined “violence” and “creating fear” as the defining aspects of terrorism in divergence from political crime and she relied on historical actors to define the lines diverging political criminals and terrorists (Lawyer 7, 2018). Her perspective was in line to define terror as “a serious harm to the human life and to its physical integrity” (Bayraktar, 1982, p. 173). Yet, diverging the student movement of the 1970s and the Kurdish movement does not correspond to a historically accurate interpretation, as both movements used violence as a political instrument in their protests. In that sense, her theoretical definition and her example-based definition did not coincide. When she was asked to give an example of a contemporary political crime, she gave “burning all the ballot boxes in Ankara during an election, without killing anyone” (Lawyer 7, 2018). An act that can easily fall into the terror category within the current legal framework, Lawyer 7 was also aware of her contradictions, as she expressed that “we are in two minds about terrorism, even during our interview” (Lawyer 7, 2018).

On the other hand, possessing a liberal political stance, this lawyer found demagogical the contemporary discourse of “unarmed terrorist organization” and she was critical of “the consideration of every single Kurdish word as terrorist propaganda” (Lawyer 7, 2018). In line with its critical stance for the contemporary use of terror labels, for her, Redhack’s acts were not terror because there was no violence. Even though her critical attitude against the enlargement of the terror label was limited when it came to the old folk devils of Turkey like PKK, she did not agree with the contemporary labelling of terror for Redhack.

6.3.6. Implications of framing Redhack as terrorist

Discussing Redhack was a fruitful topic to clarify the reflection of the interviewees about framing cyber-terror and terror. For a majority of LEAs, Redhack was framed directly as a

terrorist organization while they had doubts about its cyber-terror framing. In that line, one of the LEAs declared: “The hacker group who takes a name is a terrorist organization” (LEA 2, 2018). Once again, we see how the experience of Redhack molds the definition of the act that it would be qualified, this time to define terrorism.

On the other side, as Lawyer 7, many other interviewees – especially lawyers – were against the framing of terror for Redhack and saw such framing as a tactical reaction of the state to contain dissidence (Expert 2, 2018; Lawyer 2, 2017; Lawyer 4 & Lawyer 5, 2018).

Being critical against the terror framing of Redhack was shared by other interviewees, too. This time, their opposition was based on framing terror as “the violence” aimed to “threaten, frighten, terrorize, and intimidate the people” (Lawyer 1, 2017; Lawyer 3, 2017). In all these responses, the implicit reference is the definition of terrorism as:

[T]he use of *violence to create fear* for political, religious, or ideological reasons. The terror is intentionally aimed at noncombatant targets, and the objective is to achieve the greatest attainable publicity for a group, cause, or individual. (...) the impact of terrorist violence and damage reaches more than the immediate target victims. It is also directed at targets consisting of a larger spectrum of society.

(Matusitz, 2013, p. 4)

Similarly, Expert 2 emphasized also that terror means fear. Then, she added that to designate an act as a terror act, it should be an organized act against a specific group. Switching between defining terror and cyber-terror, as it was frequent during many interviews, she declared: “Cyber-bullying cannot be included to the cyber-terror category. (...) However, if it is against Kurds, against a specific group, then it is cyber-terror” (Expert 2, 2018). Here, the ethical framing of terror takes a different direction towards framing discrimination as terrorism. In all these perspectives, the framing of Redhack as a terrorist organization was considered as a meaningless decision.

Only for the interviewees who acknowledged the framing of terrorism dependent on agreed-upon terrorists, the framing of terror for Redhack was logical – even though they were against it. In this critique, such framing was an instrument used by the state to label Redhack as a terrorist organization.

It is up to who did it. If PKK does, it is terror. If it is a hacker, it is not a terrorist act. For that reason, they tried to rely the case [to PKK].

(Lawyer 9, 2019)

In this extract, Lawyer 9 shares the perspective of LEA 6 and Prosecutor 3 to explain the state's framing of terror and cyber-terror as the relation of the actors in question to the agreed-upon terrorists with a critical approach. The designation of cyber-terrorists through their relation – named mostly as “support” – to terrorist organizations in the state's perspective was emphasized by different judicial actors, sometimes as the confirmation of that frame (LEA 2, 2018; LEA 3, 2018; LEA 6, 2019; LEA 7, 2019; Prosecutor 3, 2019) and sometimes as a critique (Prosecutor 1, 2019; Lawyer 9, 2019).

6.4. Conclusion

As one interviewee said: “The definition of terror is always a political interpretation” (Lawyer 8, 2018). We can adapt it to all the crime frames presented by mentioned judicial actors during the interviews. In this part dedicated to the detailed analysis of the interviews with judicial actors related to cyber-crime cases in Turkey, diverse frames of cybercrime, hacking, cyber-terror, and terror were expressed around the hacktivist experience of Redhack.

Within cybercrime and hacking frames, the ubiquity of technologies and the limitlessness of their development became as source of anxiety for the actors through the concern of falling behind vis-à-vis these rapidly developing technologies. The anxiety was also accentuated by the incompetency that many actors felt for almost all of the judicial actors, included law enforcement agents, judges, lawyers, and prosecutors. Law enforcement agencies were often referred as the place to blame for the incompetency of the state about issues related to information and communication technologies (ICTs). Moreover, the incompetency of prosecutors and judges was considered as the most essential problem responsible for the cybercrime threat. The excessive workload with few

and unexperienced personals were cited as the reasons of that incompetency, alongside the general hostile attitude of the state towards ICTs.

Opposite to that incompetency, cybercriminals and hackers were seen as the masters of these technologies. Cybercriminals and hackers were used interchangeably by the judicial actors during the interviews. This interchangeability was related to the criminalization of hackers in the 1990s within the global context. This global trend influenced the local actors through movies about hackers, as the frequent presence of references to movies given by interviewees demonstrate. Alongside cybercrime themed movies, other cultural products were used to concretize interviewees' perceptions about hackers and cybercriminals. In that line, Western movies were mentioned to clarify the divergence between good and bad hackers.

The difference between good and bad hackers was a double-headed discussion: an ethical divergence and a craft-based divergence.

From one side, this difference was constructed upon the motivations of the hackers. Personal profit and economic gains are motivations that fit mostly bad hackers and cybercriminals. In that line, acting without the permission of the system administrator was the diverging line between good and bad hackers. The harm to the country or to the state was also presented as a characteristic of bad hackers. However, this perspective did not exclude the relativity of goodness either. Through references to figures from historical narratives, the boundaries between good and bad hackers were problematized.

Another perspective defended that motivations cannot be taken into account to judge an act as a criminal act, or to categorize a hacker as good or bad. Following that, all hackers should be considered as cybercriminals, as their acts were included as cybercrime in the Turkish law. This motivation blindness was condemned by the defendants of the first perspective on the grounds of creating an incompetent framework to understand the nature of hacking. By the nature of hacking, the hacker ethic was referred with the aim of enlarging the definition of hacking beyond the limits of crime and beyond the limits of ICTs.

On the other side, the goodness of a hacker was related to the hacking skill of the hacker. A good hacker should be a competent expert of ICTs. In that sense, the overemphasis on cybercrime and the dangerousness of the cybercriminal do not always

imply a negative framing. Curiosity for novelty was the positive sentiment shared by many interviewees alongside the anxiety felt from the rapid development of ICTs. Following that, hackers received a positive framing from the actors who perceived hackers as interested outsiders. Another positive framing came from those who embraced the hacker culture up to appropriating the hacker identity. The intimacy between some interviewees and the hacker community resulted in framing the good hacker as an implicit me during the interviews.

That positive framing was one of the main reasons of the critical position of many interviewees against the criminalization of hackers. In this opposition, one divergence that was expressed by more than one interviewee was significant: the difference of hacking from child pornography. Named as one of The Four Horsemen of the Info-pocalypse (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2012, p. 43), child pornography is indeed a source of moral panics for the judicial actors while hacking and cybercrime are not at all.

Following that positive framing of hacking, framing Redhack as a hacker or cybercriminal group implied a positive framing for the group, too. One split within the hacker framing towards a negative perception was the bad hacker framing constructed upon the motivation of harming the country and the state. In that line, Redhack and also Anonymous were considered either as agents actively harming the country or as infantilized actors acting on *wrong* ideologies. Some interviewees preferred to avoid the hacker framing for Redhack based upon the lack of their hacking skills, as an instrument to discredit the group. In the avoidance of the cybercriminal and hacker framing, another frame was operated. That was the second horsemen of the Info-pocalypse: terrorism (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2012, p. 43).

The usage of the terror and the cyber-terror frames for Redhack has different implications. First, why political hacking or hacktivism was not used as a frame for Redhack can be asked. One reason is the narrow definition of political hacking compared to the cyber-terror constructed with cyber-paranoias. In these paranoias, the coexistence of hacking and politics rarely refers to activism but mostly to cyberwar scenarios in the international level. The other reason was the transformation of political crimes to terrorism in the political context of Turkey in the 1990s. Within the larger fading of political crimes,

cybercrime with political motivations has no other choice than to be considered as cyber-terror rather than being framed as political hacking.

Cyber-terror framing brought along its own fears and anxieties. The general anxiety felt about cyber-terror results from the difficulty of identifying the related agents. The ambiguity of defining the actors in the cyber realm was doubled by the unclear relations between the states and the hackers. When cyber-terror is framed as an extra-state activity, if the states sponsor hackers behind closed doors, how we could diverge cyberwar and cyber-terror? Another ambiguity of cyber-terror was related to its definition based on motivations of the related actors. Similar to the framing of bad hackers, cyber-terrorists were framed mostly through their motivations to intentionally harm the country, the state, the public institutions, the social order, or the people by the interviewees. However, defining cyber-terror as harm created an incompatibility between different levels of harm between harming a person, an institution, and a state. Respectively, the harm meant physical damage against a person, disabling an institution, and surprisingly, stealing data from the state.

In the absence of a legal description for cyber-terror, this notion became a mere appendix to terror for some interviewees. Following that, the attacks of DAES and the hacking of public institutions could be equalized. Yet for others, the absence of the legal definition created another level of anxiety.

This anxiety was pronounced at most by interviewees who did not possess an explicit ideological stance. In that line, ideological differences became distinguishing in the construction of terror and cyber-terror frames while they were less decisive for cybercrime frames. Interviewees who possessed nationalist and statist ideologies and also those who had leftist inclinations were much more assertive about terror frames than those who did not explicitly defended a political ideology. Yet even for these assertive perspectives, framing cyber-terror could become a challenging load.

In that line, ambiguities of defining cyber-terror and designating cyber-terrorists were overcome through constructing hypothetical relations formed between cyber-terrorists with agreed-upon terrorists. In this construction, the critical point is that the relation is not formed between legal definitions of cyber-terror and terror, as the Turkish law does not offer sufficient material for such framing. Many interviews reflected the official framing of terror in Turkey, as a construction upon specific folk devils rather than written legal

definitions. In that sense, not the nature of the acts but the agents define the qualification of an act as a terrorist act. Even if the contemporary enlargement of the terror charge towards diverse groups in the society resulted in a weakening in the moral panics of terror and gave rise to a process of its criticism, the terror charge still has an influence in the society that cyber-terror does not possess. In that line, interviewees – some of them by confirmation, others with a critique – expressed that in the state's perspective, cyber-terrorists were framed mostly as supporters of terrorist organizations.

The terror framing of Redhack gains another meaning following these discussions emerged through the interviews with judicial actors. A charge present in judicial documents and also in news frames, terrorism was an irrelevant frame for many interviewees in the case of Redhack. However, the interpretable nature of the terror definition in the Turkish law, which is the product of the 1980 military coup and the ambiguity of cyber-terror result in the reliance on agreed-upon terrorists of Turkey to construct terror and cyber-terror frames. In framing Redhack as a terrorist organization, the alleged relations with the old folk devils were central to determine the perception of the group. During the interviews, most of the interviewees who were against the terror framing of Redhack actually did not oppose to the terror framings of the mentioned agreed-upon terrorists. Being critical about the terror label of Redhack and considering it as a tactical reaction of the state to contain dissidence did not result in an immediate resistance against all folk devils of terror. In that sense, it can be argued that the construction of the terror framing of Redhack through its relations with agreed-upon terrorists is a critical point in the framing contest about Redhack between the state and the actors themselves. Next chapter will depart from this issue of framing contest and will ask if the terror framing of Redhack resonates with the general perception.

CHAPTER 7

PERCEPTIONS OF THE CRIMINALIZATION: COUNTERFRAMING AND REFRAMING STRATEGIES

Sosyal medya er meydanıdır. Yani sizin sorduğunuz soruları sadece muhatapları değil, sizin takipçileriniz, onun takipçilerinin de görme şansı vardır [Social media is a field of contest. It means that not just the addressees of your questions see you. Your followers, their followers, all have the chance to see, too].
(Redhack, 2013b)

This chapter is about the perceptions of the criminalization about Redhack. Following the earlier chapter about the construction of the criminalization through official and unofficial⁵³ frames, in this chapter, we will change the angle and focus on the counterframing and reframing strategies on the trail of already constructed crime frames. The studies on social movement frames use the notions of counterframing and reframing for these strategies aimed to “rebut, undermine, or neutralize” the frames (Zuo & Benford, 1995, p. 139). In that sense, they are deeply connected to the notion of “framing contests” in the sense of interactively constructed frames in opposition (Tarrow, (1994) 2011, p. 144). This perspective follows the argument that all frames are embedded in a web of culture and for that reason, they cannot be thought as separate units (Reese, 2010, p. 18).

However, as the literature of framing contests suggests, state agencies’ frames possess advantages that no other frames benefit. In that line, while the *web* metaphor of framing contests is useful to emphasis the dynamism of interconnected frames, the

⁵³ The notion of unofficial frames is a conceptualization developed within the scope of this research. For that reason, when I refer to the literature, they are not present next to the notion of official frames. However, every time that I mention official frames in this chapter, unofficial frames are implicitly present along with them.

negligence of the inequality between contestants would be an inadequate interpretation of this *web*. This inequality results from the inequality in the access capacity to cultural resources between social movement actors and others, like state agents and the media (Tarrow, (1994) 2011, p. 145). This contest can be seen as a “struggle for cultural supremacy” (Noakes, 2000, p. 669). In that sense, framing contest is an issue of hegemony, too. Hegemonic meanings produced by official frames and the counterhegemonic stance against these frames (Carragee & Roefs, 2004, pp. 221-222) are indivisible parts of the framing contests.

On the other hand, “the fundamental unfairness of framing contests” in favor of official/state frames does not always guarantee the successful promotion of the frames constructed by the state agents against other frames, like collective action frames (Noakes, 2000, pp. 670-671). The conventional media was already playing an important role of “co-producing” protests events. Now, especially the digital media is considered as an important tool that allows the visibility of counter-frames, as well as providing the capacity to have more capacity of resonance on the audience. In some instances of social movements, this impact of the digital media on the audience is over-emphasized with the technological enthusiasm (Tarrow, (1994) 2011, pp. 134-138). This tendency of overlooking other social and political factors than the usage of technological devices was especially visible for the Zapatista rebellion (Tarrow, (1994) 2011, p. 138) and for the Arab Spring (Aouragh, 2012; Fuchs, 2013). Without neglecting these critiques, this chapter will consider the digital media as a central platform for framing contests because of its ability to create “a public social negotiation of the meaning of political events” (Maireder & Ausserhofer, 2014, p. 316). This will be one of the main reasons of why the social media platform Twitter is taken as the primary data source in this chapter.

Combining with the criminalization and moral panics perspective, we can say that the labelled ones – for our cases, social movement actors – have also some abilities to challenge the cultural supremacy of official frames (Welch, 2006, p. 190). This challenge is about frame resonance, about how the constructed frames resonate – are perceived – in the target community (Snow & Benford, 1992). For every actor promoting a frame – especially state actors and social movement actors, frame resonance is a crucial issue to be concerned about (Noakes, 2000, p. 672). Following that, the success in a framing contest – for our

case, in the contest about the crime framing – is the ability to alter and to deconstruct opposite frames, mostly the ones represented in the media (Noakes & Wilkins, 2002, p. 652).

The examination of the perception of the crime frames about Redhack is a study on its framing contest following this multidimensional approach. In the case of Redhack, the contest between opposing frames is striking, especially when we focus on one specific aspect of the crime frames constructed by the state: the terror framing.

In an intermingled structure, the chapter will examine the counterframing and reframing strategies of both the group itself – Redhack – and the strategies performed by the audience of the crime frames. Analysis about the self-frames of Redhack alongside its counterframing and reframing strategies will be based mostly upon the data collected from their audio and written interviews. This data source consists of eight audio interviews – conducted in 2012 and 2013 – lasting more than 18 hours in total⁵⁴ and seven written interviews published in different news portals from 2008 to 2016.

Besides, Twitter Advanced Search Engine will be once again one of the main tools of data collection. It will be used to analyze the self-frames through all the tweets collected from the account @TheRedHack because Twitter was the main outlet used by the group to communicate with its audience, as well as propagating their ideas. Moreover, another dataset is formed with the help of Twitter Advanced Search Engine to focus on the perception of the terror framing of Redhack. Using the keywords “terör [terror]” and “Redhack,” all tweets available between March 2012 and October 2017 from the search are collected and will be analyzed pursuant the discussions of this chapter.

First, the temporality of this perception will be discussed. In other words, then sociopolitical context that surrounds the crime frames related to Redhack will be put on the table. Second, I will examine the alterations in the use of the political satire as a way of counterframing the terror label. Third, the examination about the supportive reframes will focus on the perception of the relation between Redhack and agreed-upon terrorist groups of Turkey. And last, the counterframing strategies of the group in which they identify the

⁵⁴ Interviews given by Redhack in the context of the Gezi protests are exceptionally long. The peak is the interview of Halk TV in August 7, 2013. This one would last more than five hours. Such presence in the news media is the result of the popularity of Redhack, as well as the popularity of issues related to the Gezi protests.

state's acts as terrorist acts will be examined. Following these discussions, the question of how the terror framing of Redhack resonates within the audience, as well as who succeeds in the framing contest about the terror framing of Redhack will be responded as the conclusion of the chapter.

7.1. The Rise of the discussion: Temporality of the terror framing

The dataset formed by the keywords “terör [terror]” and “Redhack” collects all the tweets provided by Twitter Advanced Search Engine in October 2017. Yet, in the current working discipline of the search engine, the formation of its superset – all the tweets containing the keyword “Redhack” – is not possible. For that reason, I rely on the previously examined dataset formed with the top tweets containing the keyword “Redhack” to gain insight about the significance of the discussion about the terror framing of Redhack in the general discussion about Redhack in Twitter. While there are 2899 tweets found with these two keywords within the latest tweets category of Twitter Advanced Search Engine, among the 3555 top tweets with the keyword “Redhack” between March 2012 and March 2018, there are 109 tweets containing the additional keyword “terör [terror].” In other words, while the ratio of top tweets containing “terör [terror]” and “Redhack” in the superset of top tweets containing “Redhack” is known as 109/3555, the ratio of all tweets containing “terör [terror]” and “Redhack” in the superset of all tweets containing “Redhack” is unknown (2899/?).⁵⁵

Even though, the first ratio shows that the top tweets discussing the terror framing of Redhack correspond to approximately 3% of the top tweets.⁵⁶ In that line, even all the tweets do not have to follow the same pattern as the top tweets, it can give us an outlook about the positioning of the dataset that will be examined in this chapter. This proportion signifies that the terror framing of Redhack is not the most crucial issue in the totality of

⁵⁵ This is the result of the methodological problem with using the Twitter data for a retrospective study. Twitter Advanced Search Engine is a quasi-manual tool that do not permit the collection of big data.

⁵⁶ This low ratio implies that the discussion of the terror framing did not constitute a large part of the general discussion about Redhack. However, as my research does not include all discussions about the group, I cannot make assumptions about the significance of this discussion on the terror framing compared to other possible discussions about the group. On the other side, a low ratio does not make a discussion irrelevant or insignificant because it has diverse meanings inside and outside of the case study. For these reasons, the number is given just to place the discussion within a possible larger discussion about Redhack.

discussions about Redhack in Twitter. Yet the number of 2899 indicates that the discussion about the terror framing is not an ignored issue by Twitter users, either.

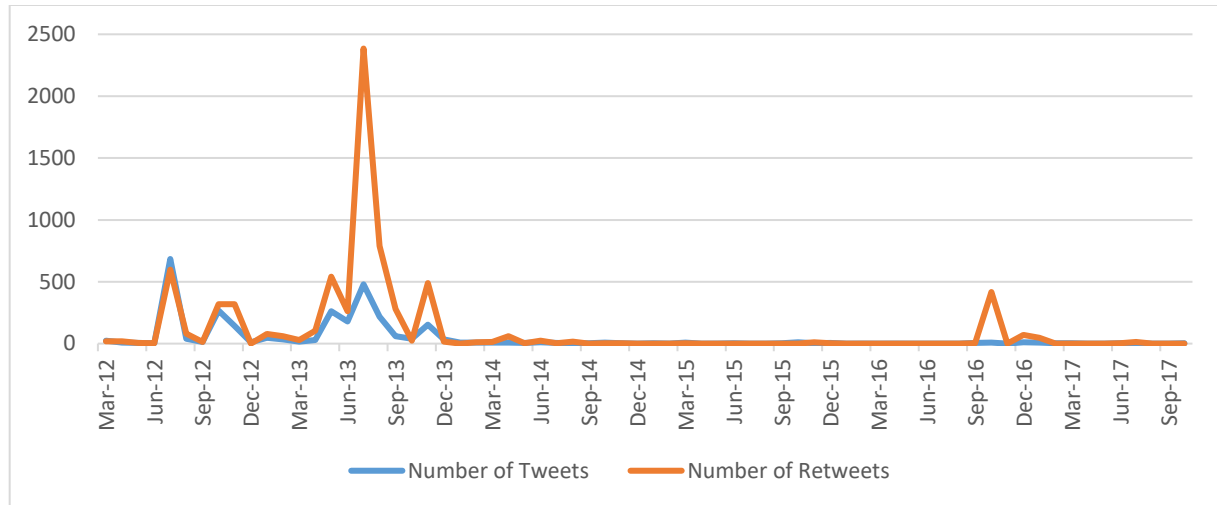


Figure 7.5: Number of tweets containing the keywords “terör [terror]” and “Redhack” and their retweet numbers by month (March 2012-October 2017)

The temporal trends analysis of the dataset formed through the keywords “terör [terror]” and “Redhack” points to specific periods in July 2012, October-November 2012, May-August 2013, November 2013, and October 2016, as upsurges in the number of tweets and their retweets. July 2012 is indeed a month of high activity of Redhack. Two data leaks and three data interference acts performed by the group can stand as the reason of their visible presence. However, most of the tweets sent in that time is about another act. It is the decision of the prosecutor’s office specializing in cybercrime to transfer the investigation about the data leaks from Ankara Police Directorate to the prosecutor’s office specializing in anti-terror (Hürriyet Daily News, 2012). In that sense, it is not the acts of the group nor the declarations of politicians nor some news about Redhack that trigger the discussion of the terror label in the social media platform. It is a judicial act that becomes the source of the discussion with 684 tweets discussing the terror framing of Redhack. This number is the highest number of tweets per month related to the discussion about the terror framing of the group.

The period October-November 2012 exhibits another instance when two judicial acts heat again the discussions about the terror framing of Redhack. First one is the

completion of the indictment against Redhack about the data leaks from Ankara Police Directorate at the end of September 2012. This indictment was in the news as the framing of Redhack as a terrorist organization by the prosecutor's office (SoL, 2012) and resonated in the social media with an almost completely total counterframing. Second incident of this period was the first trial of the lawsuit in November 2012, following the acceptance of the indictment. That trial would result with the release of the arrested people. All the 411 tweets containing the keywords “terör [terror]” and “Redhack” collected in this period are about these two judicial acts, without any exception.

Next noticeable period is the one between May and August 2013. This is the longest period in which there is a continuous discussion about the terror framing of Redhack. Numbers of tweets per month shuttle between the range of 178 and 479 tweets per month during this period. Three judicial moments and one audio interview of Redhack stand as crucial moments that trigger the discussions in Twitter during this period.

The declaration of mistrial by the anti-terror prosecutors probing Redhack and the transfer of the prosecution to the prosecutor's office specializing in cybercrime about an ongoing investigation upon the complaint of plaintiff state institutions at the beginning of May is the first instance of that period. This instance was in the news as “the prosecutor's office changes mind” with an allusion to the indictment of October 2012 (Cumhuriyet, 2013a).

Towards the end of the same month, the perception about terror frames is influenced this time by a dual-event: data leaks of Redhack from Gendarmerie Intelligence Department about the intelligence on the Reyhanlı explosion and the operation of military prosecutor's office, which would result with the arrest of one private right after that act of the group. This time, the discussion about the terror framing is triggered with an act of Redhack and with a judicial act successively. The act of Redhack is important about discussions about the terror label because it adds other actors labelled as terrorists because the leaked documents allegedly showed the involvement of El Nusra in the Reyhanlı explosion. These documents stratified the terror framing of Redhack: a group framed as terrorist – Redhack – claims to expose the responsibility of the state to not prevent an act framed as terror – the Reyhanlı bombing – by neglecting the acts of another group framed as a terrorist group – El Nusra.

At the beginning of July 2013, another act appears as the topic of discussions about the terror label of Redhack. This is the investigation report prepared by Istanbul Police Directorate in which Redhack is categorized as a cyber-terrorist organization charged with provoking the masses in the Gezi protests. Different from the perception of the terror framing in 2012, this time, supportive reframes of the terror frames constructed through judicial processes begin to be apparent alongside opposing counterframes.

In August 2013, not a judicial act but an act of Redhack became the center of attention for those who were discussing the terror frame of Redhack. It is the audio interview that the group gave to the news channel Halk TV, a Kemalist channel known with its anti-AKP stance. This channel became highly popular among participants and sympathizers of the Gezi protests – regardless of their ideological positions – due to its wide coverage of the events while many mainstream news channels lost legitimacy because of their decision to not report the protests. In this interview lasting five hours, Redhack counterframes the terror frame about itself with an active reframing strategy targeting the acts of the state (Redhack, 2013b).

While this interview influenced the discussions in Twitter so much, a judicial act in the same month had almost no influence, quite different from earlier judicial processes with high impact. This is the first trial of the lawsuit about data leaks of Reyhanlı. This trial resulted in the transfer of the case from the military prosecution to the Heavy Criminal Court specialized by Anti-Terror Law. In that sense, this judicial act was one of the important indicators of the oscillation between cybercrime and terror framings of Redhack. Yet, this time, it did not trigger discussions in the social media platform. Following that, it can be argued that hereafter, judicial acts began to have less influence on the perception of the crime frames, compared to the influence of the self-frames of the group.

Alongside being the longest period of high numbers of tweets with continual discussions about the terror frame through several instances influencing the perception, this period distinguishes with the outstanding numbers of retweets, too. The total numbers of tweets and retweets per month in this period are 263 to 541 for May, 178 to 263 for June, 479 to 2385 for July, and 217 to 790 for August. All the four retweet numbers are quite high in the average of all retweets of this dataset. However, the number of 2385 retweets compared to 479 tweets in July 2013 is exceptional in the totality of the dataset. To

understand this high number, we should put some emphasis on the temporality of this period.

The most important sociopolitical event of that period between May and August 2013 is undoubtedly the Gezi protests. Parallel to the politicization of the masses with the Gezi protests, the social media platform Twitter was popularized and politicized in this period, too, in the national scale. The sudden increase of Twitter users from 1.8 to 9.5 million during the protests (Yaman, 2014, p. 21) is the concrete indicator of this relation. Used as a central tool of organization and communication, Twitter became to be seen as an “alternative political platform” (Doğu, 2017, p. 4) for Turkey since the Gezi protests. In that sense, the high numbers of tweets and retweets in the period of the Gezi protests (May 28, 2013 – June 16, 2013) and in the active political atmosphere afterwards cannot be thought separately from that context. Moreover, as the terror framing of Redhack in that period is directly related to their position during the protests, the connection between the discussions about the terror frame and the context of the Gezi protests is much more direct.

The charge of provoking and abetting the masses during the Gezi protests constituted the main issue in the investigation report prepared by Istanbul Police Directorate to frame Redhack as a cyber-terrorist organization. Tweets containing call to action for protests sent from the account @TheRedHack in June 14 and June 15 were shown as the evidence of their cyber-terror activity, according to the news of Sabah newspaper in this report (Sabah, 2013). When these tweets from the news article are examined, it is seen that apart from their content, their high numbers of retweets are another common characteristic between them.



Figure 7.6: [Today, after 14 p.m., everywhere, in every square.. #ResistanceNews]



Figure 7.7: [While we focus to work, please write the protests, the announces, the declarations, the urgent needs under the hashtag #ResistanceNews..]



Figure 7.8: [The resistance keeps growing. Please write the protests, the announces, the declarations, the urgent needs under the hashtag #ResistanceNews and follow it!]



Figure 7.9: [For an equal, just, classless world, for fraternity, for liberty and independence, we march with all of our hearts. They can stop us, if they can!]



Figure 7.10: [Those who hand out buses, raincoats, lunch.. say TOMA, [pepper] gas, truncheon when it comes to us. Will you be quiet?]



Figure 7.11: [*Gazi, Sarigazi, Okmeydani, Nurtepe, Caglayan, 1 Mayıs, Kadikoy, Gulsuyu... Your home, your sister, your mother, they are waiting for you! #1MilliontoTaksimToday*]

These tweets show that Redhack frames itself as a spokesman of the Gezi uprising. Plus, to understand the perspective of the law enforcement, how the most retweeted tweets of Redhack are shown as evidence connotes the predictable importance attributed to actors having the capability to resonate with the audience rather than less influential actors.

This spokesman framing has concrete reasons behind it. As the group mentions in another tweet, the account @TheRedhack was one of the most influential accounts sending tweets about the Gezi protests. Moreover, the hashtag #Redhack was also among the top hashtags shared by Twitter users (Medyatava, 2013). The group claimed that in the first 15 days of the protests, 400,000 new people started following their account (Redhack, 2013c). In that sense, Redhack was part of the content, as well as being an actor of the Gezi protests. Even though the Gezi uprising had a leftist atmosphere explicit in slogans and graffiti with reference to the leftist tradition in Turkey, class-based political and leftist organizations were not highly influential in the organization of the uprising. For that reason, participants of the Gezi protests desired symbols that can unite their nostalgia for the leftist tradition without indicating a *concrete* political organization – concrete in the sense of material presence and precise political projects.

Being explicit about their participation to the Gezi protests in many of their interviews, Redhack praised the “resistance” for its ability to bring together diverse groups of people who were “constantly discriminated against, constantly “other”ed” (Redhack, 2013a). Through giving examples of how they learnt news issues from other participants during the protests, like those from the LGBTQ movement (Redhack, 2013a), they stood as one of the idealized political entities of the protests – a praise for those who affiliated with the larger Gezi community based upon the principle of the respect for diversity. Redhack reflected this inclusive political position to their reading and their adoption of the leftist,

socialist, and communist traditions of Turkey, too. In that line, they expressed their ideological stance in their declarations as being “Marxists who put up a struggle in a Leninist organization structure,” their mission as “opening a digital propaganda space to the opposition groups,” and their position as “an online self-defense movement of the oppressed” (Redhack, 2016). The group often commemorated important figures from the leftist tradition (Redhack, 2013; Redhack, 2013d). However, they were careful to diverge themselves from the Orthodox Marxism (Redhack, 2012b).

One of the critical divergence lines that they drew was their critique against the disunity of the leftist groups and the need to be unified (Redhack, 2012b; Redhack, 2013; Redhack, 2013a). A nostalgia for people sympathizing with the leftist culture, this framing of the problem by Redhack might resonate positively among the participants of the Gezi protests, too. Moreover, Redhack emphasized in many instances the importance of the offline struggle. “We did not forget how to throw rocks,” they would say to indicate their participation to street protests (Redhack, 2012b) and that the revolution they reach for would rise from streets, ghettos, factories, universities (Redhack, 2013). This emphasis on the revolutionary practice (Redhack, 2013a) would be in line with the masses who went out to protest during May-June 2013. Last, when they present their ultimate objective as building an “equal, fair world without exploitation, class divisions, and limits,” (Redhack, 2012a; Redhack, 2013a), they frame a large enough – and ambiguous – utopia that diverse participants of the Gezi protests can be able to mold according to their ideological stances and struggle perspectives. All these characteristics point to the deep connection between Redhack and the Gezi protests in the level of the self-framing of the group.

With the investigation report prepared in July 2013, it would not be wrong to claim that Istanbul Police Directorate connected the cyber-terror framing of Redhack with the criminalization of the Gezi protests. This dual criminalization of Redhack and the Gezi protests seems to be the reason of the high number of interaction by Twitter users in that period. People who struggled with the state in the streets felt the urge to struggle in this framing contest about the criminalization of Redhack because it was directly linked to their own acts just one month ago. This counterframing performed by Twitter users concretizes how contests over meaning are another aspect of the struggle between states and movements (Tarrow, (1994) 2011, p. 32).

After the long period of the discussions tangling around the Gezi protests, November 2013 witnesses another rise of the discussion about the terror framing of Redhack. In this month, there is one development in the lawsuit about the data leaks of Reyhanlı: the release of the private Utku Kalı. However, this did not become a trigger of discussions in Twitter. What was more influential was the operation of the prosecutor's office specializing in cybercrime towards the end of the month. In this operation, 13 people was detained, including Barış Atay, a popular actor known with its participation to the Gezi protests.⁵⁷ Even though this time the charges were not about the protests, many news outlets echoed the interpretation of the Times newspaper that this operation was a response to the Gezi protests (Radikal, 2013; T24, 2013; Hürriyet, 2013). A detail from that operation became quickly the hot topic of the discussions in Twitter: Another instance of the transfer of the investigation file, this time from the prosecutor's office specializing in cybercrime to the prosecutor's office specializing in anti-terror. While all 14 detainees were released before the end of November, three days later one of the detainees, Taylan Kulaçoğlu was detained and arrested for the second time. These indecisions of the judicial body were largely discussed in the social media platform.

The last period that manifests itself in the Figure 1 belongs to a relatively recent time, to October 2016. As this time indicates to an important period related to the data leaks performed by the group from the e-mail account of Minister of Energy and Natural Resources Berat Albayrak in the previous month. Another wave of detention and release was executed following that incident, too. However, when the data is examined, it shows that the high number of retweets is the result of one tweet retweeted 418 times. It is not about the terror framing of Redhack but an opposition to the terror framing of the Gülen Community. The reason of its appearance in the dataset is based on the usage of the hashtag Redhack and do not contribute to the discussion other than showing an example of the counterframing of the terror label about another group.⁵⁸ For that reason, it can be said that,

⁵⁷ Barış Atay would become a deputy in June 2018 from HDP (Peoples' Democratic Party), a party established after the Gezi protests as a collaboration between the Kurdish movement and some leftist organizations. Atay transferred later to the newly-established TİP (Workers' Party of Turkey). This detail that is unrelated to the events of 2013 is still important because it highlights the political identity of Barış Atay.

⁵⁸ Some conspiracy theories were expressed during the interviews about the relation between Redhack and the Gülen Community related to the data leaks of Berat Albayrak. However, as I analyze the discourse of judicial actors as elements of framing practices rather than intelligence, I do not open that discussion here.

after the atmosphere of the Gezi protests, the discussions about the terror framing of Redhack declined drastically. This decline indicated that the Gezi protests remained to be the center of the counterframing and reframing strategies.

7.2. Counterframing strategies: Using political satire to criticize the terror label

The Gezi protests was an outstanding movement in the political history of Turkey both with its quantitative and qualitative traits. The intensive use of the political satire was one of these qualitative characteristics of the movement that diverged it from most of the earlier protests. In the contemporary global context, political satire has been celebrated for a quite long time, especially in the context of the political dissidence visible through social media platforms. Actors who criticize the political oppression through the means of political satire became the subject of widespread affection among the users of social media platforms in many different contexts. In Turkey too, online political satire has become an indispensable aspect of online activism in the 2010s, almost simultaneously with the Gezi protests.

Online political satire fits in the larger category of internet humor. From its very beginning, humor has been a part of the digital culture. Hacker culture – thought together with trolling, pranking, and hoaxing – is a lively habitat in this respect (Jordan & Taylor, 2004; Coleman, 2013). Hacker culture's interest in political issues can generate examples of online political satire in two opposite senses: Politically motivated hackers can use satire in their political acts with “a spirit of humorous deviance,” called lulz (Coleman, 2014, p. 17). This “politically incorrect humor” (Goode, 2015, p. 76) is different from the second sense of political satire in which humor is used as a political weapon to criticize political opponents and to arouse public attention (Fuchs, 2013, p. 372). Examples given about the acts of Redhack already showed how the group uses the political satire in a fusion with its leftist legacy. This characteristic of the group resonated well among the Twitter users.



Figure 7.12: [Even we cannot decipher the encoded Necati Sasmaz speech, the global technology is not that much developed, we are sorry.. #RedHack ;)]

This is by far the most retweeted tweet sent by the account @TheRedHack between March 2012 and March 2018. The tweet is about the speech given by an actor known with his role in a nationalist mafia drama series, in the same day of the tweet. In June 12, during the Gezi protests, Sasmaz gave this speech in which he commented on the movement by phrases like “we are affected by evil eye” and “we need the guidance of academicians, sociologists, scientists to illuminate today’s events like a cat’s phosphorous eyes” (Sasmaz, 2013). Even though this speech was not in total opposition with the protests, nor an attempt to criminalize it, its explicit attitude to avoid to be part of it was perceived negatively among the protestants and the sympathizers of the protests. The lack of coherence in the speech became rapidly the source of satirical reactions in Twitter. Redhack’s tweet frames this reaction with a magnifying glass effect based upon creating an opposition between his lack of coherence and their skills on hacking, implicitly their mental abilities.

About their framing as a terrorist group, both Redhack and their followers used heavily political satire to construct counterframes about this labelling. Especially after the first oscillation of the investigation file from the prosecutor’s office specializing in cybercrime to the prosecutor’s office specializing in anti-terror in July 2012, humorous oppositions to the terror framing were performed both by Redhack and other Twitter users.



Figure 7.13: [You did everything, you would do this, too. Bring us whatever this prosecutor drinks]

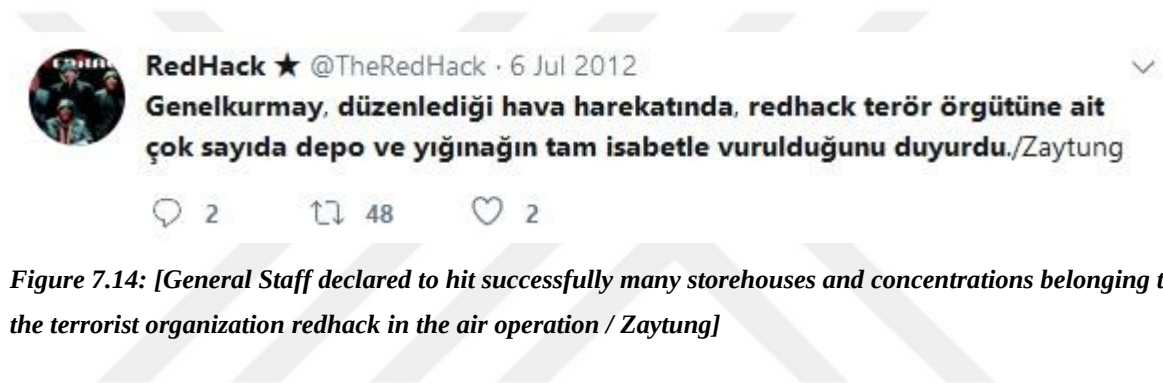


Figure 7.14: [General Staff declared to hit successfully many storehouses and concentrations belonging to the terrorist organization redhack in the air operation / Zaytung]



Figure 7.15: [After that moment, I do not know if we will do terror but we will make them give error a lot for sure ;) ->>]



Figure 7.16: *[We figured out why they declared us as terrorist.. The prosecutor who studied for 25 years thought this photo real ;)) ->>>]*



Figure 7.17: *[A brand new miracle to call our own: Redhack is our new terrorist organization!]*



Figure 7.18: *[The ones who declared Redhack a terrorist organization by the pretext of hammer and sickle would just as soon shut down hardware stores for being weapon providers]*



Figure 7.19: [RedHackers Redhack Did you submit a petition to become an official terrorist organization with a residency certificate from local authorities?]



Figure 7.20: [hammer and sickle + manifesto = terrorist organization || we will progress a lot with this equation. that's nice. it works. it is a mighty prosecutor, after all, right? #Redhack]

The literature on moral panics exhibits that the criminalization campaigns are more vulnerable in framing contests within a “multimediated” social world. The reason is that targets of moral panics are more competent to fight back against crime framings, especially by using media tools to challenge authority and legitimacy of those who label (Welch, 2006, p. 190). Above examples concretize how the criminalization of Redhack through its terror framing was opposed by Redhack and by the audience through the use of political satire. Another interesting example of political satire was the hashtag #coktatinn [whatever]. Different from the serious #HepimizRedhackiz [#WeAreAllRedhack] calling to solidarity, #coktatinn was a direct and explicit negligence of the terror framing of the group. Both hashtags were used as a reaction to the prosecutor’s office decision implying the terror frame in July 2012.



Figure 7.21: [*@allahcc, explain that to us. Did you create those who declared #Redhack a terrorist organization, too? Why did you create? Is it another exam for us? #whatever*]

However, the widespread usage of satire in counterframing the terror label of Redhack in 2012 will be diminished right from the next year. Now, the opposition would be more serious with comparisons to other sociopolitical events and even when the political satire is used, it is less humorous with the gravity of events, like the Reyhanlı bombings.



Figure 7.22: [*The judicial power who declares Redhack a terrorist organization do not consider those who killed Hrant Dink⁵⁹ a terrorist organization*]



Figure 7.23: [*They said Redhack was an armed terrorist organization. That was indeed true. They had a bomb and today, they dropped it with the truths about reyhanlı*]

⁵⁹ Hrant Dink was an Armenian journalist, a supporter of human and minority rights, a prominent figure in the Armenian community in Turkey, and the editor-in-chief of Agos newspaper. He was assassinated midday in 2007, as he was returning to his office in Agos. More than 100,000 people participated to its funeral. Every year, Dink is commemorated with large protests at the scene of murder. The lawsuit is still ongoing.

This second period of high discussion about the terror framing in May-August 2012 is different from the earlier period with the excessively high numbers of retweets rather than such high numbers of tweets compared to July 2012. During the political protests, the preference of retweeting rather than tweeting can be read as the enlargement of the political expression through a passive participation (Boyraz, Krishnan, & Catona, 2015). In our case, this corresponds to the passivation of opposing the terror framing in 2013, compared to the discussion in 2012. Another characteristic of this second period is that they begin to reflect the counter-framing strategies of the group more and more. The reason is undoubtedly the appearance of Redhack in the news channels Halk TV and Ulusal Tv during that period. This will be the subject of the last part of this chapter. Before that, an examination about the other side of the story: the supportive reframes of the terror framing of Redhack. Especially after June 2013, such frames would be more visible in Twitter. Almost all of these supportive tweets framed the terror label of Redhack based upon one issue, which is the relation of Redhack with agreed-upon terrorists of Turkey.

7.3. Supportive reframes: Agreed-upon terrorists, performativity, nationalism

Judicial processes and the unofficial frames of the judicial actors had already shown that the relation of Redhack with the groups already labelled as terrorists was the central point of their terror framing. The discussion about the terror framing of the group in Twitter reflects that point, too. The frequency analysis on the dataset formed by the keywords “terör [terror]” and “Redhack” exhibits that within 2899 tweets, 252 of them contain the keyword “pkk.” The second most frequent organization labelled as terrorist is “dhkp-c”⁶⁰ with 91 tweets. These tweets predominantly question the relation of Redhack with these organizations.

These organizations are ideological and illegal organizations challenging the violence monopoly of the Turkish state. PKK (Kurdistan Workers' Party) is the armed political organization struggling for the Kurdish movement for more than 30 years. DHKP-C (Revolutionary People's Liberation Party/Front) is a Marxist-Leninist organization using armed instruments since its formation in 1994. Both organizations are perfect examples of

⁶⁰ Modifications of the keyword “dhkp-c,” like “dhkpc” and “dhkp/c” are included to the count.

folk devils within the Turkish context. Decades long official ideology circulated by the state's official tools and the news media made these organizations firm sources of moral panics. However, the coincidence of the temporality of the dataset with the Solution Process, a negotiation period between the Turkish state and PKK (2012-2015) is an important detail. In that period, even though an alleged relation to PKK was used heavily as a source of terror framing of Redhack, it can be said that in the general context, the terror framing of PKK was lighter than the period before and after.



Figure 7.24: *[Redhack is a pro-DHKP-C, leftist terrorist organization. Those who do not believe can google Redhack DHKPC. This groups wants nothing but anarchy in Turkey]*



Figure 7.25: *[Redhack is terrorist. They did not deny their relation to DHKP/C, to PKK. Those who defend them should investigate first truthaboutredhack.blogspot.com #RedCakeisBestEverTerrorist]*

The changing pattern is explicit in these two tweets sent by the same Twitter user, alongside the radical increase in the number of retweets. In the first tweet, the user claims the relation of Redhack with DHKP-C. In the second one, she grounds her claim to the lack of denial by Redhack about its relation with the organization. Actually this claim is not true as the group declares to not have any relation with any organization in their interviews since 2008 (Redhack, 2008; Redhack, 2012; Redhack, 2012b; Redhack, 2013b). Being aware of this discussion, Redhack frames this questioning of their relation with other organizations as “an attempt to prevent the support of the people” (Redhack, 2012).

Without demonizing neither Kemalists nor PKK, they describe themselves as socialists following the Marxist-Leninist tradition and explicitly say that they are neither Kemalists nor from PKK (Redhack, 2013b). However, these declarations do not suppress the terror framing constructed upon the alleged relation with agreed-upon terrorists.



Figure 7.26: [Redhack is terrorist! If they say they are not, then they should tweet that dhkpc and pkk are terrorist organizations]



Figure 7.27: [Just one question to shameless Redhack. Why they block those who ask whether Pkk is a terrorist organization or not ;)]



Figure 7.28: [#ExplainRedhackWhetherPkkIsTerrorist is nonsense? Redhack is a terrorist organization by itself]



Figure 7.29: *[Redhack's inability to not declare Pkk as a terrorist organization is so meaningful! They talk around it :)) #ExplainRedhackWhetherPkkIsTerrorist]*

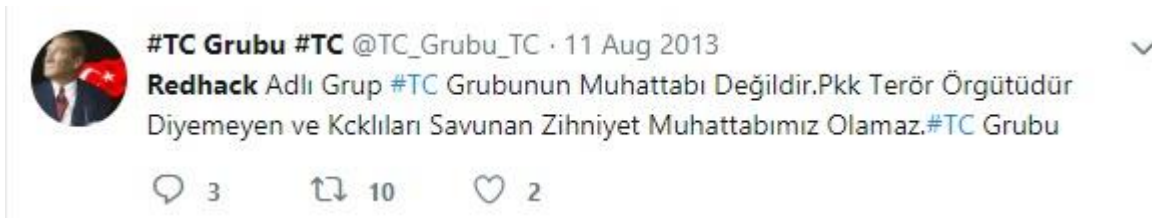


Figure 7.30: *[The group called Redhack is not an addressee of #TC group. A mentality who cannot say Pkk is a terrorist organization and who defends Kck people cannot be an addressee to us. #TC Group]*

As tweets above show, the alleged relation of Redhack with PKK – and also with DHKP-C, in a lower level – will be framed mainly around this polemic during the context right after the Gezi protests. Even the hashtag #ExplainRedhackWhetherPkkIsTerrorist is created to unify the supporters of the terror framing. Even though in this analysis, we do not examine in detail the users who created the content of framing, in the case of supportive tweets, one account attracts the attention. The tweet of the account @Turkguvenligi is the most retweeted tweet of the all dataset from March 2012 to October 2017. As a patriotic hacking group – according to their twitter account, Türk Güvenliği is in opposition to Redhack, based upon their ideological stances. Moreover, the popularity of Redhack during the Gezi protests undoubtedly created a challenge for the patriotic group whose audience is also sympathetic to the protests. All these reasons result in a feeling of necessity for a manageable frame for this new⁶¹ rival.

The Gezi protests became a pressure not just for nationalist actors. For all actors – including Redhack, this heterogeneous mass movement became a rich source of audience difficult to handle. Three main groups had Kemalist, leftist, and pro-Kurdish political

⁶¹ I say “new” not because Türk Güvenliği is an older group than Redhack but because the tradition in which it belongs – patriotic hackers in Turkey – has an established history.

positions. Redhack's self-framing as a spokesman of the Gezi protests necessitated a midway position reconciling these different political identities. In this line, insistent requests for declaring PKK as a terrorist group could not be part of this mediator position sought by Redhack. However, this emphasis on performativity is actually an indispensable aspect of nationalist ideology. Nationalism is almost always performed through symbols and rituals. Explicit declarations are also a part of these rituals. Similar to the religious rituals, explicit declarations are necessities for entrance, exit, and prove of belonging to a community. This request to recognize the political identity of a part of the Gezi protests as folk devils was a dead-end to the imagined community of the Gezi movement. For that reason, Redhack abstained from this polemic and deflected its counterframing strategy into the reframing of the terror label targeting the state itself.

7.4. Reframing strategies: Targeting the state with its own frame



Figure 7.31: [It is true that what we are doing is illegal but no one can say that we are doing a bad thing.]

Redhack is attentively framing their deeds as illegal but legitimate as the first step of its reframing strategy against the crime frames of the state. For this counterframing, they benefit both from leftist tradition (Redhack, 2013d) and from the hacker ethic (Redhack, 2012a). In that line, they emphasize that justice cannot be reduced to law (Redhack, 2013a). They would continue to frame their deeds in this way even when the political atmosphere in Turkey would become heavier after 2015, as the following quote from their interview from 2016:

Certainly we are not bound by the laws of thieves, murderers and fascists who burned people in basements. [Note: This refers to the 'Cizre Massacre']. We do not care about the decrees they issue about us, we do not even take Erdoğan and

his security forces seriously. Public interest and the history of the revolutionary struggle provide legitimacy to our actions.

(Redhack, 2016)

The disavowal of the legal framework as the source of justice opened the path to reframe radically the terror label. In this part, some examples of this reframing during the context of the Gezi protests will be examined.

Audio interviews of Redhack are crucial in the propagation of that reframing strategy in which the state's acts were framed as terrorist acts. The discussions in Twitter resonated highly to these interviews. The most influential was the five-hours interview in Halk TV. A long direct quote from this interview would illustrate this reframing strategy of the group:

First we should ask, who is terrorist, what is terror? Is terror not the oppression, the intimidation, the force? Does the addressee of terror not always live on a knife edge? Is terror not beating someone to death in darkened streets with woods? Is terror not the assault of the police against its citizens crying Allah Allah? Terror is actually the distrust between neighbors. And now, the people had to learn all the police vehicles – including *scorpion*,⁶² they know *scorpion*, TOMA (armored water cannon used for riot control) by heart now. Terror is actually the sexual harassment in the *scorpion*. Terror is to increase the frequency of naked body searches in prisons, in the entrance of prisons. There will be visits to prisons tomorrow, tomorrow is holiday, there will be body searches before and after, are these harassments not terror? Is terror not the protection of those who attack people with scimitar? This guy who goes to streets with a scimitar, is he not terrorist? Terror is actually not to be sure if your house will be invaded by the police one morning. Terror is invading houses by saying “open the gate, it is police.” For us, those who create illegal executions are terrorists. (...) On the other side, terror is to defame people – socially prominent people – by invading their houses at the morning, at 4 a.m., while they could be detained, interrogated during the day. Remember how Türkan Saylan who educated 40,000 girls was detained in her seriously ill condition. What would happen if she was detained during the day? Look, we are not saying “do not judge do not detain” but arbitrary arrest, arbitrary detention, these are against universal declaration of human rights, too. Now, what they do? They attempt to create a religious pressure through the pilot project of the district imam. Detecting the religious identities of people and to develop a culture of imposition through it, here what is terror! Terror is to put notice box for informants in newly-established neighborhoods and to intimidate

⁶² It is a small riot control vehicle, compared to TOMA.

people with concerns of “what I will do, if they inform on me.” What a miracle, there was a defamation operation towards artists who supported the Gezi resistance, before and after *Silivri*.⁶³ To paralyze with pressure and intimidation. It is an attempt to shackle people. It is the paralyzation. (...) Those who call us terrorist, provoker, that prosecutor or these servants of *Green Tsardom*,⁶⁴ they talk as if we are the ones who fired at those young resisters who would be martyred, who choked its own people with pepper gas as they were insects. If what they say [when they talk about terror] is to encourage people who chose the free life with their free will, for their freedom, to go to the streets with them, to take sides with the oppressed, then my friend, with this mentality, you can applaud and write heroic saga with the Israeli soldiers who fired at those who were in *Mavi Marmara*.⁶⁵

(Redhack, 2013b)

This interview and especially these phrases through which Redhack reframed the terror label with concrete examples in relation with the Gezi protests and beyond it would be highly influential in Twitter. 128 tweets sent in August 7-8 were directly related to this interview. All the tweets below are quotations containing elements of the reframing strategy that the group mentioned in the audio interview (Redhack, 2013b).



Figure 7.32: [*“Terror is the distrust between neighbors. It is to put notice box for informants!”*
#RedHackInHalkTV @TheRedHack]

⁶³ This is a reference to the earlier judicial processes of Ergenekon in which mostly Kemalist, secularist journalists were charged with military coup attempt.

⁶⁴ This is a conceptualization used by Redhack to define the Islamist oppression, with an indirect reference to the Gülen Community.

⁶⁵ In 2010, people from a non-governmental organization allegedly carrying humanitarian aid to Israeli occupied Gaza were shot by Israeli soldiers and ten of the passengers died in Mavi Marmara ship as the result of the assault of the Israeli army. Israel alleged that the NGO was supporting terrorist organizations. The Turkish government condemned this event, supported the related NGO and therefore, opposed actively the terror framing of Israel.



Figure 7.33: [*“Terror is the police invading your house at the morning.” [from the speech of Redhack in Halktv]*]



Figure 7.34: [*The Ministry of Foreign Affairs calls “our friends” international terrorist groups #Redhack*]



Figure 7.35: [*Terror is the detention of Türkan Saylan⁶⁶ who educated 40,000 children in her seriously ill condition! @TheRedHack #RedHackInHalkTV*]



Figure 7.36: [*“Terror is the assault of the police against its citizens crying Allah Allah” @RedHack*]

⁶⁶ Türkan Saylan was the president of ÇYDD (Association for the Support of Contemporary Living), a non-governmental organization with an explicit secular and Kemalist ideology. This organization had been mentioned within the interviews conducted with judicial actors, too. Even though ÇYDD was charged with terror, this organization had a high legitimacy to a large extent due to its educational projects. Moreover, Saylan was a patient with terminal cancer when she was detained. This action of the state met with quite negative reactions from different parts of the society.



Figure 7.37: [Terror is beating someone to death in darkened streets #RedHack #TodayIsRedHack]

The group explicitly defined the terror labelling of the state as “an attempt of frightening and intimidating people to nourish its own terror” (Redhack, 2013b). In that line, all these tweets counterframe the terror label of Redhack through reframing terror with references to the acts of the state. Especially, Figures 7.21, 7.24, and 7.25 show tweets about the violence against the protesters during the Gezi protests. Other examples refer to events for which the public opinion is highly disturbed against the act of the state, like the detention of Türkan Saylan mentioned in Figure 7.23. In this way, the group consolidated the counterframing of the terror label about itself by connecting it to the framing of violence against highly legitimate events – the Gezi protests as the most specific one.

7.5. Conclusion

In this chapter, the perceptions of the criminalization about Redhack were examined together with the counterframing and reframing strategies of the group. The analysis of temporal trends showed how judicial processes and self-frames of Redhack can become triggers of the discussions about the terror framing of Redhack. One crucial finding was that in the context of the Gezi protests, Istanbul Police Directorate connected the cyber-terror framing of Redhack with the criminalization of the protests, which would contribute to the self-identification of Redhack with the Gezi protests.

The part about the usage of political satire as a tool of counterframing exhibited that the positive resonance of the self-frames did not always indicate a better position than the counterframing of the audience independent from self-frames in the framing contest. The changing pattern from mostly independent frames constructed by the audience through the use of political satire in 2012 to high resonance of the self-frames of Redhack with the dominant usage of retweets in 2013 seems like the indicator of a regression in the support

of the group against the official frames not in quantitative terms but in qualitative terms – implying a passivity of the opposition.

The increasing presence of supportive frames by 2013 emphasized this fall of Redhack in the framing contest about the terror label. The persistence request for the labelling of agreed-upon terrorists as explicit declarations in supportive terror reframes exhibited how contrary to technology determinist approaches about Twitter, old patterns of political communication, like nationalist rituals, find their way in social media platforms.

Against these opposite frames, Redhack developed a reframing strategy that targeted the state by framing its acts as terrorist acts. In this part about the reframing strategy of Redhack, I claimed that the group built a contradiction between the problematic nature of its terror framing and the violence of the state against its citizens, especially during the Gezi protests.

At the end, it can be said that Redhack was highly aware of the cruciality of the framing contest built upon the resonance of crime frames. For that reason, they would be open to interaction with Twitter users and declare: “More than what they call us, what matters for us is how the people think about us. They are the criteria” (Redhack, 2013b). It is as if they considered the frame resonance as the real constructor of the terror framing. They succeeded to create that resonance, as the high numbers of interaction – tweets and retweets – about the terror framing of Redhack exhibit that many people acted to oppose the criminalization of the group. However, the rise in retweets rather than tweets, the quasi-disappearance of the political satire and the increasing presence of supportive terror frames within the audience indicated a changing pattern to the detriment of the group. In the period of the Gezi protests, self-frames of the group continued to resonate positively in general. However, after the fading of that politicized atmosphere, Redhack’s self-frames did not resonate that much and gave its place to the influence of judicial processes, once again. It is hard to claim that Redhack’s ability to alter and to deconstruct the terror frames about itself is as high as it was during the period prior to the Gezi protests.

CHAPTER 8

CONCLUSION

In this dissertation, I embarked upon the study of the criminalization of Redhack by defining a crucial problem of disembeddedness within the hacktivism literature that should be overcome with grounded studies about diverse hacktivist experiences. The case study of Redhack from Turkey is an attempt to initiate such literature. Based on this study, the dissertation problematized the ungrounded categories of cyber-activism and cyberterrorism used to define hacktivism in the hacktivism literature.

Following and moving beyond the wave of hacktivism studies focusing on the crime discourse of hackers and hacktivists, Chapter 2 explored the theoretical roots to problematize the concepts of terror and cyber-terror within the sociopolitical context that produces these labels. In this problematization, the chapter proposed the debates of whether Redhack is considered as a folk devil and hacktivism is a source of moral panics in Turkey and following that, it presented framing analysis as the analytical tool to examine this criminalization.

Chapter 3 contextualized the hacktivist experience of Redhack within the global and historical framework by positioning the group as an example of leak hacktivism. This specific hacktivism type is characterized through their involvement with popular uprisings of the 2010s and their emphasis on leaking the information kept secret by states and corporations from the masses. The global meaning of hacktivism is shaped with this interaction between hacktivists, states, corporations, and masses in the 2010s.

Following that, Chapter 4 exhibited how the acts of Redhack was in relation within the political agenda of Turkey, especially under the influence of the Gezi protests, a mass uprising in 2013 against the governmental policies that can be considered as a part of the global wave of popular uprisings of the 2010s. Redhack's reactionary agenda-setting

against the AKP government was formed by the fusion of humor and the leftist legacy that is no doubt closely related to the politicized atmosphere of 2012-2013 in which the Gezi protests outstand. In response to this, the complicated history of Redhack's judicial processes demonstrates that, contrary to the general belief shared both by hacktivism researchers and hacktivist actors, the activist self-identity and the use of humor that is so central in hacker communities do not guarantee a safe passage free from terror labels. The high activity of the judicial processes about Redhack is full of impasses and indecisions. Many oscillations of the judiciary in framing the activities of the group as cybercrime or terror and the change of the judicial gaze towards the periphery of the group are indicators of a need felt by the state to contain judicially the group and its changing tactics in response to the containment incapacity. Another important finding is that data leaks from the state performed by the group stand as the main reason of the state reaction against Redhack. This aspect would appear again within the unofficial crime frames developed by judicial actors in following chapters.

By Chapter 5, the development of the dissertation begins to exhibit that the criminalization of Redhack does not fit to the construction of a moral panic. Rather, it fits to a process of "transformative state simplifications" (Scott, 1998) with the aim of making legible the illegible phenomena of hacktivism. In that sense, I will review the discussions exhibited in Chapter 5, Chapter 6, and Chapter 7 within the lens provided by Scott about the state projects of standardization and legibility.

Chapter 5 explored the official crime frames produced by actors from *the power bloc* and the frames circulated by news media actors. The quasi-silence of the official discourse about Redhack attested to the lack of certitude about how to frame and how to react discursively against the group. Different from the judiciary reaction, in the discursive ground, the state abstains from reacting against the group rather than searching for different frames. The light framing of terror and war used for Redhack in official frames does not fit in the contemporary expanded terror labels used heavily within the official discourse against dissidents and political rivals. The apparent confusion about how to frame Redhack results from the lack of knowledge about internet and computer technologies (ICTs). Also, even though there were other hacker groups, the Turkish state had not been used to face with a hacker/hacktivist group before because these groups were mostly patriotic hacker

groups that were strictly aligned with the state's ideology and did not challenge its authority. Yet in the case of Redhack, the state had to frame for the first time a dissident hacker group. That is the reason why an almost positive framing of an addressee can be seen among official frames, an approach quite unfamiliar for actors that the states acknowledge as terrorists or enemies. One of the main reasons of this positive approach is the techno-fetishism that would be a central issue in the framing of the news media, too. The indirect exaltation of the group is based upon their prowess in ICTs related issues. This is what makes the group quite attractive for news media actors, even when it is about the criminal acts of the group.

The fascination with crime is an issue highly discussed within the studies focusing on the media representations of crime. Especially cultural criminology's interest with the issue reveals the duality of "the public's fascination with violence and crime via the mass media, and also the enactment of violence and crime as pleasure or spectacle" (Jewkes, 2004, p. 28). The fascination with crime is not at all peculiar to cybercrime. Public fascination with organized crime is most visible in the popularity of mafia-themed books, drama series, and movies for many decades (Albanese, 2015, p. 1). In the case of cybercrime, techno-fetishism taking its source from the fears and fascination from the 19th century with mechanical power (McCutcheon, 2007, p. 263) and consolidated by the centrality of information and communication technologies in the contemporary era accentuates the fascination with cybercrime.

This fascination results in the positive framing for hackers that seems to be the reason of the light usage of the terror label in the news media for Redhack. Regardless of their ideological positions, political tendencies and capital relations, news media actors echo the self-frames of the group – mostly as a result of the quasi-absence of official frames – and they construct cybercrime frames with a rather positive coverage accentuated with that techno-fetishism. It is as if the hacker label – the one that is heavily used in cybercrime frames – does not always possesses a negative connotation in the Turkish context.

On the other hand, even when the terror frame was activated for Redhack for a short period of time, there was an immense gap between the total number of news containing terror frames and the number of news framing Redhack. Under the heavy influence of the government, political crises like Gezi protests and the alleged Corruption Leaks indeed

influenced news outlets to use more enlarged terror frames. In that sense, at least in the scope of AKP-friendly news outlets, the terror framing of Redhack is similar to how September 11 stood in American and British news media for the terror framing of hacking and hacktivism.

In 2017, during the post-coup period, when terror labels were used intensively in the news media, Redhack would be framed as a terrorist organization via its alleged relation to “FETÖ [Fethullah Gülen Terrorist Organization].” Yet, this ideologically-blind terror framing was sweeping, as many groups and persons would be labelled based on such relations during the state of emergency after the attempted military coup of 2016. The difference of Redhack is the volatility of the terror and cyber-terror framings for the group in favor of a regular crime framing – not a cybercrime framing – in a period when the general terror labeling was as strong as ever in the national political discourse.

The contradiction between charges of terrorism in judicial processes and the passivity of official frames does not stand for a simple incompetency from the perspective of the state. This implies a deeper issue: a problem of illegibility for the state in the case of hacktivism, concretized in the example of Redhack.

When Scott (1998) elaborates the issue of legibility as a central issue of statecraft, he claims how legibility is *sine qua non* for a large-scale social engineering (pp. 2-5). Similar to societies in which modern states emerged, in societies influenced deeply with the rapidly changing ICTs, social realities become illegible to the state “in their raw form” (1998, p. 24). To be able to transform these realities into legible and controllable facts, states need to create fictions by administrative, judicial, and coercive powers even though these fictions would never fit exactly the realities (p. 24).

Remembering the high activity of the judicial processes about Redhack and the continual charges of terrorism in these processes, the quasi-absence, the passivity, and the silence of official frames and of the frames of news media appear as active tactics of containment for an illegible group by an effort to make it legible through familiar frames of terrorism. In that sense, the non-framing of the group in news media – especially in the period after 2016, also corresponds to a tactic of self-censorship, in a media landscape heavily dependent to the government – politically and economically.

Chapter 6 elaborated framing preferences exhibited in Chapter 5 through the examination of personal frames constructed by judicial actors interested and/or worked in cybercrime related cases – experts, law enforcement agents, lawyers, and prosecutors. Perspectives provided by the interviewees illuminated why the terror framing of Redhack by the judiciary was so central in the criminalization of the group. Interviews with these judicial actors demonstrated how the perceived opposition between hacking prowess and state vulnerability are crucial to inspire the positive framing of hackers and at the same time, to strengthen their danger perception. Different from that paradoxically positive and unfamiliar crime framing for hackers, the conventional terrorism frame constructed on the summoning of agreed upon terrorists from the political history of Turkey would be the more preferred in the case of Redhack. In this way, paranoias related to cybercrime – commonly shared anxieties of the ubiquity of technologies and concerns of falling behind vis-à-vis these rapidly developing technologies, as well as the feeling of incompetency – become issues unrelated to the hacktivist group.

The anxieties about ICTs is crucial to understand the abstention of the cybercrime/hacker frame for Redhack. This is once again related to the issue of illegibility. Redhack standing as a reality “lying outside the brackets” (Scott, 1998, p. 20) is haunting for the state. If the state cannot read – make legible the social reality in question, than it means political autonomy for these actors appearing outside of the legible area of the state (p. 54). The position of political hackers with their craft about ICTs corresponds to such a haunting imagery based upon the illegibility of ICTs and hackers for the state.

The anxiety born from the illegibility is strengthened with the fascination with cybercrime. The emphasis put on the ubiquity of cybercrime crystallized in the quote “everyone using a cell phone is under cyber-threat” (LEA 6, 2019) exhibits the hysteria of “potential victimness” that constitutes one of the main elements of “the postmodern fascination with crime” (Jewkes, 2004, p. 28).

Following that, to be able to differentiate Redhack from the illegible, fascinating and haunting hackers, one of the rare points of connection between Redhack and cybercrime is first, framing Redhack as a bad hacker group through their alleged lack of the hacking. Second, the “bad hacker” characteristic of Redhack is framed this time, through

their alleged motivation of harming the country and the state – as agents actively harming the country or as infantilized actors acting on wrong ideologies.

Similar to how bad hackers were framed, the framing of cyber-terrorists was constructed through the motivation to intentionally harm the country, the state, the public institutions, the social order, or the people. However, defining cyber-terror as harm created an incompatibility between different levels of harm between harming a person, an institution, and a state. Respectively, the harm meant physical damage against a person, disabling an institution, and surprisingly, stealing data from the state. Two levels of ambiguities increased the anxieties about the cyber-terror framing: the absence of a legal description for cyber-terror and the difficulty of designating what is cyber-terror and who are cyber-terrorists. This is from where the hypothetical relations constructed between cyber-terrorists and agreed-upon terrorists become instrumental to overcome the ambiguities of cyber-terror frames. In this relation, it is not the nature of the acts but the agents who define an act as a terrorist act. In this way, cyber-terrorists were framed mostly as supporters of terrorist organizations – as it was the case for Redhack.

Chapter 6 is a complicated chapter when it is reviewed with the discussion of legibility. From one side, findings from the interviews support how hacktivism is an illegible issue for the Turkish state and how it actively tries to transform it to a legible fact – terrorism and/or cyber-terrorism. From the other side, the ambiguity of the legal definition of terrorism and the absence of legal definition of cyber-terrorism create an illegibility this time about the law. As Das and Poole (2004) claim in their work about the anthropology of the state, “the state is continually both experienced and undone through the illegibility of its own practices, documents, and words” (p. 10). In the case of the illegibility of the legal framework for terrorism and cyber-terrorism, when the state oscillates between “the rational and the magical” (Das, 2004, p. 234), law – rules becomes illegible even to the persons charged with implementing the legal norms – rules (p. 238). The difficulty that judicial actors try to deal with when I asked them to define terror and cyber-terror exhibits this illegibility experienced by those who are bound by legal norms, as judicial actors. On the other side, the definite judgements of some of the interviewed law enforcement agents about defining terror and cyber-terror and accusing Redhack for these crimes also fit in this illegibility of the law schema, paradoxically. They stand as “direct embodiments of the

state” (Das, 2004, p. 235) in the margins of the state when representing and performing state’s law right in the middle of the ambiguity of legal definitions. The terror framing of Redhack fits in this dual illegibility: illegibility by the state and illegibility of the state.

Actually, this terror framing of Redhack says a lot about the political context of Turkey. First implication is its relation with the transformation of political crimes to terrorism, which is the product of the 1980 military coup. Within the larger fading of political crimes discourse, cybercrime with political motivations had no other choice than to be considered as cyber-terror rather than being framed as political hacking. However, the ambiguities of the cyber-terror framing required a return to the older framing of terrorism, a popular labelling used heavily in the hegemonic discourse against the political crises of the 2010s.

For Redhack, the terror framing intermingles old myths of left and cybercrime to form the ghostly figure of terror supporters, a master frame that had never been in abeyance in the Turkish context since the 1990s. In this framing, the supported terrorist organizations are the agreed-upon terrorists of Turkey – in other words, mainly the old folk devils of left – PKK and DHKP-C – and secondary, the newer ones from right – FETÖ.

The unexpected finding was the still influence of the terror framing in the society, despite the contemporary enlargement of the terror charge towards diverse groups in the society that seems to weaken the moral panic about terror and to give rise to its criticism. We should not neglect that for many interviewees – especially for lawyers and experts, framing Redhack as a terrorist organization is inaccurate. This criticism is important when it is thought together with the ongoing terror charges present in judicial documents. However, being critical about the terror label of Redhack and considering it as a tactical reaction of the state to contain dissidence do not result in a resistance against the totality of the moral panic about terrorism. Many interviewees who were against the terror framing of Redhack did not prefer to oppose the terror framing of the agreed-upon terrorists of Turkey. In the general perspective, this implies that terrorism is still a source of moral panics in Turkey and the terror framing is a useful instrument for the state to criminalize oppositional entities. And for Redhack, it implies that their alleged relation with the old folk devils is central to determine the perception of the group and in that sense, whether they would be framed as a source of moral panics or not.

Chapter 7 explored this question of perception on the basis of the framing contest between the state and the group itself by focusing on the terror framing. In this perception, judicial processes stand once again as a crucial trigger of the discussions about the terror framing of Redhack. Other than that, self-frames of Redhack appear as an important influencer of the discussions about the terror perception of the group, too. The reason of that influence is undoubtedly the emphasis put by the group to counterframe the terror label alongside reframing it by targeting the state.

The dual illegibility about Redhack – the illegibility of the group by the state and the illegibility of the legal norms used by the state to criminalize the group – becomes crucial in the acts of counterframing. As Scott (1998, p. 49) warns against, state simplifications aiming to make legible the illegible social realities can always be encountered with capacities coming from the society to “modify, subvert, block, and even overturn the categories imposed upon it” (p. 49). Active counterframing and reframing tactics in the case of the opposition to the criminalization of Redhack are examples demonstrating such capacities.

Moreover, burrowing the perspective of Das and Poole (2004) about the illegibility of the state, I claim that the counterframing of the terror label of Redhack owes much to the instance of the illegibility of the legal definitions of terror and cyber-terror both by judicial actors and by those who are subjected to these definitions. In that sense, the instances of resistance against the hegemony of the state are performed thanks to the illegibility created by the state, indeed.

Counterframing of the terror charges against Redhack was sweeping within the audience of the group as long as the perception of Redhack was highly positive in the social network site (SNS) Twitter until Summer 2013 – the period that coincides with the end of the Gezi protests. Mentioned within the acts of Redhack, the group’s fusion of humor and leftist legacy fits perfectly with the political atmosphere developed during the mass popular uprising of 2013. In that sense, the usage of political satire as a tool of counterframing by Redhack resonated well within the audience in Twitter. Redhack’s followers in Twitter used heavily satire and humor as an instrument to counterframe the terror labelling, too. Especially the oscillations of the investigation file between different prosecutor’s offices became a source of humor implying the incompetency of the state.

The main reason of the opposition coming from the audience to the terror and to the cyber-terror framings of Redhack was based on the relation constructed by the police between the criminalization of Redhack and the criminalization of those who participated to the Gezi protests. Redhack used this relation with the Gezi protests in two senses. First, this construction supported the self-identification of Redhack with the Gezi protests. Second, the group used it to build a contradiction between its terror framing and the violence of the state against its citizens during the Gezi protests. In that sense, they reframed terror with the acts of the state.

Participants and sympathizers of the protests also felt that their struggle against the state was not limited with the streets and with the acts of protest but should be pursued in the discursive level in the contest over meaning. The ongoing criminalization of the Gezi protests in 2019 through judicial processes and the counterframing efforts against this criminalization show the value attributed to this framing contest about the Gezi protests both by the state and by the participants of the mass uprising.

However, after the Gezi protests, a regression in the support of the group against the terror framing is observable. One indicator is the dominant usage of retweets instead of independent tweets. Second is the quasi-disappearance of the political satire. These two imply a passivity of the opposition to the terror framing. On the other hand, there is the increasing presence of supportive frames of the terror label with the persistent request from Redhack for explicit declarations about the labelling of agreed-upon terrorists. That framing reveals first, how old patterns of nationalist rituals – explicit declarations about designating enemies that would harm the unity of the nation – find their way in social media platforms. In that sense, this characteristic demonstrates how new actors – a hacktivist group – and new communicative platforms – social media platforms – do not mean a *tabula rasa* from the older discursive practices. Second, it concretizes how in the lack of a successful crime framing – the cyber-terror framing, the activation of older frames resonates well within the audience. Similar to the limited criticism of judicial actors revealed during the in-depth interviews, for the audience of the crime framing of Redhack in Twitter, the terror framing is not a purely constructed label that should be criticized totally when it comes to the agreed-upon terrorists of Turkey – in other words, to the old folk devils.

Here it should be emphasized that these folk devils that a part of the audience requests the explicit declaration about their terror framing are mainly PKK and DHKP-C. In Chapter 7, I claimed that this persistent request was also related to the Gezi protests as the protests became a pressure for all actors participating to the uprising because of its heterogeneous characteristic. Especially, Kemalist, leftist, and pro-Kurdish political positions had to make advances towards each other to constitute the imagined community of the Gezi protests. In this proximity, political tensions became apparent between diverse groups, too. Especially for the organizations participating to the protests, midway positions to handle this diversified totality and nuanced emphases to be distinguished among the heterogeneity intermingled in a complex way. The unstable political position of being against the government added another layer of complexity to the relations between different groups. The Gezi protests occurred in a relatively soft political atmosphere of Turkey. The Solution Process, the negotiation period between the Turkish state and PKK (2012-2015) was an important aspect of that atmosphere. In this framework, the labelling of terror for PKK became ambiguous as the state's official framing was lighter than the period before that process. On the opposite direction, for some parts of the society, the terror labeling became heavier and more inclusive towards the state – even though it contained within itself the germs of criticism – with an emphasis put on the opposition to the AKP government. After 2015, the terror labeling for PKK would return to its golden age. The use of violence as a political tool by the state in the Kurdish regions and the similar use of violence by Kurdish ultra-nationalist groups in the West of Turkey aggravated the political atmosphere and promoted the discourse of terror. While at the same time, the presence of ISIS and its high activity with suicide bombs was also a factor that cannot be ignored in the criticality of the terror framing and the increase of the moral panic about terrorism.

Consequently, in this dissertation, I have shown that Redhack is criminalized through the usage of older crime frames – terrorism – instead of new crime frames – cyberterrorism and cybercrime. The main reason of this criminalization is the containment, the control and therefore, the legibility needs of the Turkish state. Cybercrime framing provokes a positive perception based on the fascination with cybercrime for larger parts of the society in Turkey – including state agents. On the other hand, cyber-terror framing implies superiority resulting from fears, anxieties, and feelings of incompetence about

information and communication technologies. In that sense, terror framing is the most reassuring containment tool that can be used to label and to successfully contain Redhack. In this labelling, not just the leftist tradition that Redhack adopts but also contemporary instruments of terror label – the discourse of “terrorists without arms” and the widespread usage of alleged relations with FETÖ – are used to construct that criminalization. The political atmosphere of Turkey, the historical anxieties, and the international popularity of terror discourse fortify together this labelling. These macro-level and meso-level conditions result in limitations about counterframing efforts conducted by Redhack about the terror framing. The political satire used heavily by the hacktivist group resonates well in the society – in general and specifically, as a counterframing instrument against the terror framing. Moreover, it triggers criticism about the terror labelling of Redhack. However, it does not succeed to develop a larger criticism about the terror discourse in Turkey.

This dissertation also claims that Redhack is not considered as a source of moral panics. The main reason is because the labelling actors do not prefer to construct a hacker group as an explicit source of moral panics, as it would feed a discourse of incompetency of the state. That is why building indirect relations to older frames and older sources of moral panics instead of the construction of a new folk devil is more useful in the governmental logic. However, it should not be neglected that the criticism about the terror labeling of Redhack is also a reason of why the group was not constructed directly as a terrorist group but as a group having indirect relations with other “agreed-upon” terrorist groups. In that sense, Redhack is not framed as a new source of moral panics but it is constructed as an ordinary example of an older moral panics, the terrorism discourse. This framing diverges from the general tendency to consider hackers as new folk devils. This abstention of developing a new moral panic based upon cybercrime and cyberterrorism anxieties is striking. It implies that the peculiar importance attributed to the frames of cybercrime and cyberterrorism does not always result in the development of new moral panics. In that sense, negative correlations can exist between the criminalization processes and the development of new moral panics. The criminalization of Redhack exhibited such negative correlation in favor of the activation of the older moral panics of terrorism.

Thinking with the conceptualization of transformative state simplifications provides the explication needed in the absence of the construction of moral panics for hacktivism.

The Turkish state reactivates the familiar terror frame to criminalize Redhack to make the hacktivist group a legible reality that can be controlled, instead of constructing an illegible new folk devil. The fascination with cybercrime serves the hegemonic discourse needed for such transformative containment by the state with its emphasis on the threat of potential victimness from cybercrime. As hackers are crucial actors within ICTs dependent global political economy, their political autonomy is an issue that cannot escape the modern state's aspiration for a legible and hence manipulable society with productive "physical and human resources," as Scott (1998, p. 51) claims. It is in that sense that bureaucratic and commercial logic often go hand in hand in transformative state simplifications (p. 58).

As the consequence of these discussions, this dissertation possesses implications concerning larger issues, too. Considering the growing moral panic about terrorism worldwide, this study exhibits from one side that no actor is safe from being a part of this labeling as long as the discourse of moral panics develops. Master frames in abeyance and continual master frames can be used by the states to empower contemporary moral panics when it is felt necessary. However, from the other side, the study also showed that the need for social control through criminalization does not always require a construction of moral panics. Hackers and hacktivists are not considered as new folk devils in Turkey for now. Their criminalization is indirect through the reactivation of older terror frames with the aim of overcoming the problem of their illegibility. Hegemonic crime discourses coming dating from the 1980s, contemporary needs of the government, the peculiarity of the group with its fusion of leftist legacy and humor intermingled with its hacker skills and the influence of global trends construct altogether this criminalization for the hacktivist group Redhack within the Turkish context. This study reveals that despite the anxieties resulting from the imagination of cybercrime and cyber-terror, these *crimes* are not perceived as sources of moral panics. On the contrary, they produce feelings of excitement, curiosity, and the quest for power – a pure fascination. Redhack, as a hacktivist group concretizing the imagery of cyber, is no doubt a challenge for the containment capacity of the Turkish state. Even limited, the criticism developed by the opposition about its terror framing is significant for the general critical attitude against the growing terror discourse. As a group invalidating the ungrounded divergences between activism and terrorism, the criminalization of Redhack

concretizes how the labels of cyber-terrorism and terrorism are illegible, open to interpretation, and actually empty signifiers.

This dissertation about Redhack was constructed as a study on the discursive level. Further studies about how the discursive challenge of hacktivist groups lying outside the brackets of legibility against the transformative state simplifications have the possibility to influence the factual level – a capacity of resist these modern state projects – are important and necessary. In that sense, studying hacktivist groups like Redhack paves the way for discussing how hacking and hacktivism can open new political spaces within longstanding predispositions.



REFERENCES

Primary Sources

- (n.d.). Retrieved from Zone-h: <http://www.zone-h.org>
- (n.d.). Retrieved from Ayyıldız Tim: www.ayyildiz.org
- (n.d.). Retrieved from TDK [Turkish Language Association]/kamu:
http://www.tdk.gov.tr/index.php?option=com_bts&view=bts&kategori1=veritbn&kelimesec=179692
- (n.d.). Retrieved 10 25, 2018, from Chaos Computer Club: <https://www.ccc.de/en/>
- @TheRedHack. (n.d.). Retrieved from Twitter: <https://twitter.com/theredhack?lang=en>
- @TheRedHack. (2012, 10 06). *For those who did not hear: http://icisleri.gov.tr*. Retrieved from Twitter.
- @TheRedHack. (2013, 07 02). *Still, they did not become wiser*. Retrieved from Twitter.
- @TheRedHack. (2013a, 08 15). *Friends from Adana, are we ready?* Retrieved from Twitter.
- @TheRedHack. (2013b, 05 23). *The Assembly discusses yesterday*.
- Ajans Türk. (n.d.). Son Dakika: Eren Erdem hakkında yakalama kararı çıkarıldı.
- Akşam. (n.d.). Retrieved from
https://www.aksam.com.tr/arama/default.asp?anahtar_kelime=redhack
- Akşam. (2013, 05 23). Çelik'ten Redhack ve Reyhanlı belgesi açıklaması: 1 er gözaltında. Retrieved from <https://www.aksam.com.tr/siyaset/celikten-redhack-ve-reyhanli-belgesi-aciklamasi-1-er-gozaltinda/haber-208880>
- Akşam. (2013a, 08 06). Reyhanlı belgesini sızdıran asker görüntülendi. Retrieved from <https://www.aksam.com.tr/guncel/reyhanli-belgesini-sizdiran-asker-goruntulendi/haber-232941>
- Akşam. (2017, 04 21). Casus hacker yakalandı. Retrieved from <https://www.aksam.com.tr/guncel/casus-hacker-yakalandi/haber-616551>

References

- Amasya Heavy Penal Court. (2016). Gerekçeli karar [Reasoned decision].
- Ankara Chief Public Prosecutor's Office. (2012). İddianame [Indictment].
- Ankara Criminal Courts of Peace no. 7. (2016).
- Ankara Heavy Criminal Court no. 2. (2013, 11). İfade sorgu zaptı [Written statement].
- Ankara Heavy Penal Court no. 7. (2015). Gerekçeli Karar [Reasoned Decision].
- Ankara Police Dep. Organized Crime Control Bureau. (2016, 10 05). İfade tutanağı (şüpheliler için) [Written statement of suspects].
- Aydınlık. (2013, 05 12). 'Reyhanlı kan içinde AKP'liler düğünde' -(TAMAMI). Retrieved from <https://www.aydinlik.com.tr/arsiv/reghanli-kan-icinde-akpliler-dugunde>
- Ayyıldız Tim. (2016, 01 02). (Kanal A, Interviewer) Retrieved from Youtube: <https://www.youtube.com/watch?v=laBc-Yz8Gak>
- Badham, J. (Director). (1983). *WarGames* [Motion Picture].
- Bbc News Türkçe. (2013, 11 25). RedHack soruşturmasında 14 kişi de serbest. Retrieved from https://www.bbc.com/turkce/haberler/2013/11/131125_redhack_update
- Bbc News Türkçe. (2018, 02 16). Gazeteci Deniz Yücel tahliye edildi. Retrieved from <https://www.bbc.com/turkce/haberler-turkiye-43084331>
- Bianet. (2012, 10 29). RedHack Diyanet'i Hackledi. Retrieved from http://bianet.org/bianet/bilisim/141716-redhack-diyaneti-hackledi?utm_source=twitterfeed&utm_medium=twitter
- Bianet. (2012a, 03 21). RedHack "Örgütünden" Yedi Tutuklama. Retrieved from <https://m.bianet.org/bianet/ ifade-ozgurlugu/137088-redhack-orgutunden-yedi-tutuklama>
- Bianet. (2013, 05 29). "Reyhanlı Belgeleri Nöbet Saatine Denk Geldi" Diye Tutuklandı. Retrieved from <http://bianet.org/bianet/bianet/146995-reghanli-belgeleri-nobet-saatine-denkgeldi-diye-tutuklandi>
- Bianet. (2013a, 01 09). YÖK'ten Kendine Soruşturma, RedHack'e Suç Duyurusu. Retrieved from <http://bianet.org/bianet/bilisim/143407-yokten-kendine-sorusturma-redhacke-suc-duyurusu>
- Bianet. (2014, 05 14). Neden İş Cinayeti, Kaza Değil? Retrieved from <https://bianet.org/bianet/toplum/155658-neden-is-cinayeti-kaza-degil>
- Bianet English. (2013, 01 08). Hacker Group Cracks Higher Education Council Website. Retrieved from <http://m.bianet.org/english/other/143391-hacker-group-cracks-higher-education-council-website>

References

- Bilgi Teknolojileri ve İletişim Kurumu. (2016, 11 11). Bilişim Hukuku ve Bilişim Suçu. Retrieved from <http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html>
- Bilgi Teknolojileri ve İletişim Kurumu. (2016a, 11 26). Türkiye’de Bilişim Hukuku. Retrieved from <http://internet.btk.gov.tr/turkiye-de-bilisim-hukuku-detay-70.html>
- BirGün. (2007, 09 11). Hacker’lar ceza sildi. Retrieved from <https://www.birgun.net/haber-detay/hackerlar-ceza-sildi-35940.html>
- BirGün. (2014, 09 08). Redhack’ten Torunlar Holding’e katliam hack’i. Retrieved from <https://www.birgun.net/haber-detay/redhackten-torunlar-holdinge-katliam-hacki-68254.html>
- BirGün. (2014a, 09 25). RedHack İz-Enerji’nin sitesini hackledi. Retrieved from <https://www.birgun.net/haber-detay/redhack-iz-enerjinin-sitesini-hackledi-69121.html>
- BirGün. (2014b, 10 15). RedHack Kobane için hackledi! Retrieved from <https://www.birgun.net/haber-detay/redhack-kobane-icin-hackledi-70011.html>
- BirGün. (2014c, 12 01). RedHack başından vurulan Mustafa Solmaz için hackledi. Retrieved from <https://www.birgun.net/haber-detay/redhack-basindan-vurulan-mustafa-solmaz-icin-hackledi-71941.html>
- Birgün. (2016, 09 23). RedHack, Enerji Bakanı'nın Mail Hesabını 'Hack'lediğini Duyurdu. Retrieved from <https://www.birgun.net/haber-detay/redhack-enerji-bakani-nin-mail-hesabini-hack-ledigini-duyurdu-129163.html>
- bo Odar, B. (Director). (2014). *Who am I?* [Motion Picture].
- Cambridge Dictionary/english/bot. (n.d.). Retrieved from <https://dictionary.cambridge.org/dictionary/english/bot>
- Cambridge Dictionary/english/troll . (n.d.). Retrieved from <https://dictionary.cambridge.org/dictionary/english/troll>
- Cantürk, S. (2013, 01 09). *YÖK’ün yolsuzluk belgelerini yayınladılar*. Retrieved from Sabah: <https://www.sabah.com.tr/gundem/2013/01/09/yoku-hackleyip-belgeleri-yayinladilar>
- Cnn Türk. (2012, 02 27). Ankara Emniyet Müdürlüğü'nü hacklediler. Retrieved from <https://www.cnnturk.com/2012/guncel/02/27/ankara.emniyet.mudurlugunu.hacklediler/650932.0/index.html>
- Cnn Türk. (2012a, 08 31). Redhack Ö.C. için hackledi. Retrieved from <https://www.cnnturk.com/2012/bilim.teknoloji/teknoloji/08/31/redhack.o.c.icin.hackledi/674906.0/index.html>

References

- Cnn Türk. (2012b, 07 06). RedHack terör örgütüymüş! Retrieved from <https://www.cnnturk.com/2012/bilim.teknoloji/teknoloji/07/06/redhack.teror.orgutuyumus/667919.0/index.html>
- Cnn türk. (2013, 05 24). Redhack'e belge sızdıran asker tutuklandı. Retrieved from <https://www.cnnturk.com/2013/turkiye/05/24/redhacke.belge.sizdiran.asker.tutuklandi/709333.0/index.html>
- Cnn Türk. (2014, 06 01). RedHack Ankara Sanayi Odası'nı hackledi! Retrieved from <https://www.cnnturk.com/haber/turkiye/redhack-ankara-sanayi-odasini-hackledi>
- Cnn Türk. (2017, 01 18). 3 gazeteci Red Hack soruşturmasında tutuklandı. Retrieved from <https://www.cnnturk.com/turkiye/3-gazeteci-red-hack-sorusturmasinda-tutuklandi>
- Cumhuriyet. (2012, 08 30). RedHack, Ö.Ç. için Yargıtay ve AYM'yi hackledi! Retrieved from http://www.cumhuriyet.com.tr/haber/diger/367516/RedHack__O.C._icin_Yargitay_ve_AYM_yi_hackledi_.html
- Cumhuriyet. (2013, 12 27). Validen skandal sosyal medya genelgesi. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/23049/Validen_skandal_sosyal_medya_genelgesi.html
- Cumhuriyet. (2013a, 05 09). Savcılık fikir değiştirdi: RedHack terör örgütü değil. Retrieved from http://www.cumhuriyet.com.tr/haber/diger/420548/Savcilik_fikir_degistirdi__RedHack_teror_orgutu_degil.html
- Cumhuriyet. (2013b, 11 22). Barış Atay'a RedHack gözaltısı. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/12105/Baris_Atay_a_RedHack_gozaltisi.html
- Cumhuriyet. (2014, 05 28). Redhack, AKP'nin Soma raporunda şoke eden gerçekleri paylaştı. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/76457/Redhack__AKP_nin_Soma_raporunda_soke_eden_gercekleri_paylasti.html
- Cumhuriyet. (2014a, 05 28). Redhack'ten AKP'nin kadrolaşma belgeleri. Retrieved from http://www.cumhuriyet.com.tr/foto/foto_galeri/76565/1/Redhack_ten_AKP_nin_kadrolasma_belgeleri.html
- Cumhuriyet. (2014b, 02 04). RedHack yine hackledi. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/37347/RedHack_yine_hackledi....html
- Cumhuriyet. (2014c, 04 17). RedHack 'e-bilet'in sitesini hackledi. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/61895/RedHack__e-bilet_in_sitesini_hackledi.html

References

- Cumhuriyet. (2014d, 06 11). Redhack'ten Muammer Güler'e hack şoku. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/81433/Redhack_ten_Muammer_Guler_e_hack_soku.html
- Cumhuriyet. (2014e, 12 28). RedHack, Ethem Sarısülük ve ailesi için hackledi: Suçlusun fişkiyeci Gökçek! Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/175090/RedHack__Ethem_Sarisuluk_ve_ailesi_icin_hackledi__Suclusun_fiskiyeci_Gokcek_.html
- Cumhuriyet. (2015, 03 17). Redhack'te 9 ay hapis, 3 yıl dava: Sonuç beraat. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/231774/Redhack_te_9_ay_hapis__3_yil_dava__Sonuc_beraat.html
- Cumhuriyet. (2016, 09 30). Aydın Doğan'ın damadı Yalçındağ'dan, Erdoğan'ın damadı bakan Albayrak'a günlük rapor! Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/608496/Aydin_Dogan_in_damadi_Yal_cindag_dan__Erdogan_in_damadi_bakan_Albayrak_a_gunluk_rapor_.html
- Cumhuriyet. (2016a, 08 19). Çanakkale Belediyesi'nin SMS sistemi hacklendi. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/587396/Canakkale_Belediyesi_nin_SMS_sistemi_hacklendi.html
- Cumhuriyet. (2016b, 09 23). Redhack Sözcü'yü hackledi, haberi kendi yayınladı. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/604807/Redhack_Sozcu_yu_hackledi__haberi_kendi_yayinladi.html
- Cumhuriyet. (2016c, 09 30). RedHack madde madde anlattı: Damat Berat'ın hesabı nasıl ele geçirildi? Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/608331/RedHack_madde_madde_anlatti__Damat_Berat_in_hesabi_nasil_ele_gecirildi_.html
- Cumhuriyet. (2016d, 09 25). RedHack 'yazışmalar elimizde' dedi, polis Taylan Kulaçoğlu'nu gözaltına aldı. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/605421/RedHack__yazismalar_elimiz_de__dedi__polis_Taylan_Kulacoglu_nu_gozaltina_aldi.html
- Cumhuriyet. (2016e, 10 06). Taylan Kulaçoğlu gözaltında gördüğü işkenceyi anlattı: Tecavüzle tehdit ettiler. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/611114/Taylan_Kulacoglu_gozaltinda_gordugu_iskenceyi_anlatti__Tecavuzle_tehdit_ettiler.html
- Cumhuriyet. (2016f, 09 29). İnternetin tartışılan korsanları... RedHack kimdir? Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/607603/internetin_tartisilan_korsanlari__RedHack_kimdir_.html

References

- Cumhuriyet. (2018, 03 25). RedHack'ten Demirören'e 'Hoş geldin partisi'. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/948188/RedHack_ten_Demiroren_e_Hos_geldin_partisi_.html?platform=hootsuite
- Deutsche Welle Türkiye. (2017, 02 27). Gazeteci Deniz Yücel tutuklandı. Retrieved from <https://www.dw.com/cda/tr/gazeteci-deniz-y%C3%BCcel-tutukland%C4%B1/a-37740232>
- Deutsche Welle Türkiye. (2017a, 10 24). Redhack davası: Bir gazeteci tahliye edildi. Retrieved from <https://www.dw.com/tr/redhack-davas%C4%B1-bir-gazeteci-tahliye-edildi/a-41095733>
- Diken. (2014, 05 29). AKP'li vekilin gizlediği 'Soma raporu': Üretim aksamasını diye önlem alınmamış. Retrieved from <http://www.diken.com.tr/redhack-akpli-vekilin-gizledigi-soma-raporuna-ulasti-uretim-aksamasin-diye-onlem-alinmamis/>
- Diken. (2014a, 02 08). Red Hack'ten 'Sansüre dur de!' eylemi. Retrieved from <http://www.diken.com.tr/red-hackten-sansure-dur-de-eylemi/>
- Diken. (2014b, 09 05). RedHack Avcılar'da çöken üst geçidi yapan firmayı hackledi. Retrieved from <http://www.diken.com.tr/redhack-avcilarda-coken-ust-gecidi-yapan-firmayi-hackledi/>
- Diken. (2014c, 11 14). Validebağ ve Yırca için TEİAŞ'ı hackleyen RedHack, 1.5 milyon TL'lik elektrik borcunu 'sıfırladı'. Retrieved from <http://www.diken.com.tr/validebag-ve-yirca-icin-turkiye-elektrik-iletim-syi-hackleyen-redhack-1-5-milyar-tllik-elektrik-borcunu-sifirladi/>
- Diken. (2015, 03 11). RedHack, Berkin Elvan'ın ölüm yıldönümünde İstanbul Polis Derneği'nin sitesini hackledi. Retrieved from <http://www.diken.com.tr/redhack-berkin-elvanin-olum-yildonumunde-istanbul-polis-derneginin-sitesini-hackledi/>
- Diken. (2016, 03 14). Erdoğan muhaliflere çattı: Ya bizim yanımızda olacaklar ya teröristlerin. Retrieved from <http://www.diken.com.tr/erdogan-faturayi-akademisyenlere-kesti-ya-bizim-yanimizda-olacaklar-ya-teroristlerin/>
- Diken. (2016a, 09 30). Diken'in, 'RedHack Albayrak'ın maillerine nasıl sızdı' haberine de sansür. Retrieved from <http://www.diken.com.tr/dikenin-redhack-albayrakin-maillerine-nasil-sizdi-haberine-de-sansur/>
- Diken. (2016b, 09 29). Diken'in 'Yalçındağ'dan Albayrak'a mesajlar' haberine sansür. Retrieved from <http://www.diken.com.tr/dikenin-dogan-medya-ceosu-yalcindagdan-bakan-albayraka-mesajlar-haberine-sansur/>
- Diken. (2017, 12 06). RedHack davası: Tunca Öğreten ve Mahir Kanaat'e tahliye kararı. Retrieved from <http://www.diken.com.tr/redhack-davasi-tunca-ogreten-ve-mahir-kanaate-tahliye-karari/>
- Diyarbakır Heavy Penal Court no. 2. (2016, 01 28). Gerekçeli Karar [Reasoned Decision].

References

- Duvar. (2017, 04 29). 'Redhack gözaltısı hayatımı kararttı'. Retrieved from <https://www.gazeteduvar.com.tr/gundem/2017/04/29/radchak-gozaltisi-hayatimi-karartti/>
- Ege'nin Sesi. (2014, 01 16). RedHack Turkcell'in Merkezine Girdi. Retrieved from http://egeninsesi.com/haber/131544-redhack_turkcellin_merkezine_girdi
- Ege'nin Sesi. (2014a, 03 08). RedHack Berkin Elvan İçin Konya Ticaret Borsası'nın sitesini hackledi. Retrieved from http://www.egeninsesi.com/haber/67232-redhack_berkin_elvan_icin_konya_ticaret_borsasinin_sitesini_hackledi
- Electrohippies Collective. (2000a, 02). *Electrohippies Occasional Paper No.1*. Retrieved 10 29, 2018, from Free Range Activism Website: <http://www.fraw.org.uk/electrohippies/archive/op-01.html>
- Electrohippies Collective. (2000b, 12). *Electrohippies Occasional Paper No.2*. Retrieved 10 29, 2018, from Free Range Activism Website: <http://www.fraw.org.uk/electrohippies/archive/op-02.html>
- Electrohippies Collective. (2001, 11). *Electrohippies Occasional Paper No.4*. Retrieved from Free Range Activism Website: <http://www.fraw.org.uk/electrohippies/archive/op-04.html>
- En Son Haber. (2013, 03 24). Anonymous Mossad'ı çökertti. Retrieved from <https://www.ensonhaber.com/anonymous-mossadi-cokertti-2013-03-24.html>
- Esmail, S., Golin, S., & Hamilton, C. (Directors). (2015-2018). *Mr. Robot* [Motion Picture].
- Etha. (2017, 01 11). 'RedHack'ten gözaltına alınan Şentürk serbest bırakıldı. Retrieved from <http://www.etha.com.tr/Haber/2017/01/11/guncel/redhackten-gozaltina-alinan-senturk-serbest-biraki/>
- Evrensel. (2012, 12 24). Redhack, Ulaştırma Bakanlığını hackledi. Retrieved from <https://www.evrensel.net/haber/44507/redhack-ulasirma-bakanligini-hackledi>
- Evrensel. (2013, 06 28). Redhack Lice Kaymakamlığı sitesini hackledi. Retrieved from <https://www.evrensel.net/haber/60716/redhack-lice-kaymakamligi-sitesini-hackledi#.Uc3oqBSWN2k.twitter>
- Evrensel. (2014, 06 21). RedHack Anadolu Cam'ı hackledi. Retrieved from <https://www.evrensel.net/haber/86782/redhack-anadolu-cami-hackledi>
- Evrensel. (2019, 04 16). 6 gazetecinin yargılandığı RedHack davası 24 Eylül'e kaldı. Retrieved from <https://www.evrensel.net/haber/377592/6-gazetecinin-yargilandigi-redhack-davasi-24-eylule-kaldi>
- Expert 1. (2018, 10). Personal interview.
- Expert 2. (2018, 10). Personal interview.

References

- Expert 3. (2018, 12). Personal interview.
- Expert 4. (2018, 12). Personal interview.
- Expert 5. (2019, 01). Personal interview.
- Finans Gündem. (2013, 06 12). Önce RTÜK, sonra emniyet şimdi de. Retrieved from <https://www.finansgundem.com/haber/once-rtuk-sonra-emniyet-simdi-de/384974>
- Finans Gündem. (2014, 01 16). Merkez Bankası'na Redhack saldırısı. Retrieved from <https://www.finansgundem.com/haber/merkez-bankasina-redhack-saldirisi/405828>
- Fox News. (2007). FOX 11 News Report on Anonymous. Retrieved 11 01, 2018, from <https://www.youtube.com/watch?v=kkAngvkWVkk>
- Gazeteciler. (2019, 02 26). Geçtiğimiz hafta en çok tiraj kaybını hangi gazeteler yaşadı? Retrieved from <http://www.gazeteciler.com/haber/gectigimiz-hafta-en-cok-tiraj-kaybini-hangi-gazeteler-yasadi/327427>
- Haber 24. (2012, 11 24). Redhack Anayasa Mahkemesi'ni vurdu. Retrieved from <https://www.haber24.com/ozel-haber/redhack-anayasa-mahkemesini-vurdu-h52581.html>
- Haber Türk. (2013, 12 12). O isim serbest bırakıldı! Retrieved from <https://www.haberturk.com/gundem/haber/902956-o-isim-serbest-birakildi>
- Haberler. (2013, 06 07). Redhack, Polislerin Telefon Numaralarını Yayınladı. Retrieved from <https://www.haberler.com/redhack-polislerin-telefon-numaralarini-yayinladi-4709248-haberi/>
- Haberler. (2013a, 07 03). Sivas İl Özel İdare Sitesi Hacklendi. Retrieved from <https://www.haberler.com/sivas-il-ozel-idare-sitesi-madimak-icin-hacklendi-4792882-haberi/>
- 'Honker Union' sniffs 270 hacktivism targets. (2013, 09 18). Retrieved from The Register: http://www.theregister.co.uk/2013/09/18/honker_union_270_japan_targets_manchurian_incident/
- Hürriyet. (n.d.). Retrieved from <http://www.hurriyet.com.tr/arama/#/?page=1&key=redhack&where=/&how=Article,NewsVideo,NewsPhotoGallery,Column,Recipe&firstPage=firstPage&platform=/&isDetail=false>
- Hürriyet. (2000, 12 25). Türk hacker'lar sanal DHKPC'yi çökertti. Retrieved from Hurriyet: <http://www.hurriyet.com.tr/turk-hackerlar-sanal-dhkp-cyi-cokertti-39210287>
- Hürriyet. (2006, 06 04). Tavla oynarken puanlarımı çaldılar kurcalarken hacker oldum. Retrieved from Hürriyet: <http://www.hurriyet.com.tr/kelebek/tavla-oynarken-puanlarimi-caldilar-kurcalarken-hacker-oldum-4520370>

References

- Hürriyet. (2012, 06 13). Redhack bu tez TSK'ya saldırdı. Retrieved from <http://www.hurriyet.com.tr/gundem/redhack-bu-kez-tskya-saldiridi-20747846>
- Hürriyet. (2012a, 08 26). Redhack Dışişleri'nin belgelerini yayınladı. Retrieved from <http://www.hurriyet.com.tr/gundem/redhack-disislerinin-belgelerini-yayimladi-21304300>
- Hürriyet. (2012b, 07 18). TFF'yi hacklediklerini duyurdu. Retrieved from <http://www.hurriyet.com.tr/gundem/tffyi-hacklediklerini-duyurdu-21009158>
- Hürriyet. (2012c, 09 12). RedHack, Dilan için Siverek Kaymakamlığı'nı hackledi. Retrieved from <http://www.hurriyet.com.tr/gundem/redhack-dilan-icin-siverek-kaymakamligini-hackledi-21445902>
- Hürriyet. (2012d, 12 07). RedHack, Maliye'yi hackledi iddiası. Retrieved from <http://www.hurriyet.com.tr/teknoloji/redhack-maliyeyi-hackledi-iddiasi-22092073>
- Hürriyet. (2013, 05 23). Bu kez 'bomba' mail'ler. Retrieved from <http://www.hurriyet.com.tr/gundem/bu-kez-bomba-mail-ler-23342165>
- Hürriyet. (2013, 11 26). Times: Barış Atay'ın gözaltına alınması, Gezi'ye yanıt. Retrieved from <http://www.hurriyet.com.tr/dunya/times-baris-atayin-gozaltina-alinmasi-geziye-yanit-25206286>
- Hürriyet. (2013a, 05 06). Redhack İstanbul Valiliği'ni hackledi. Retrieved from <http://www.hurriyet.com.tr/gundem/redhack-istanbul-valiligini-hackledi-23213121>
- Hürriyet. (2013b, 06 30). RedHack, İl Özel İdare'yi hackledi. Retrieved from <http://www.hurriyet.com.tr/teknoloji/redhack-il-ozel-idareyi-hackledi-23604713>
- Hürriyet. (2013d, 11 11). Er Utku Kalı serbest bırakıldı. Retrieved from <http://www.hurriyet.com.tr/gundem/er-utku-kali-serbest-birakildi-25095685>
- Hürriyet. (2013e, 11 26). Redhack soruşturmasında 14 kişi serbest kaldı. Retrieved from <http://www.hurriyet.com.tr/gundem/redhack-sorusturmasinda-14-kisi-serbest-kaldi-25207036>
- Hürriyet. (2013f, 05 23). Erdoğan'dan Redhack cevabı. Retrieved from <http://www.hurriyet.com.tr/gundem/erdogandan-redhack-cevabi-23354546>
- Hürriyet. (2014, 03 28). YouTube yasağından sonra TİB'e büyük şok. Retrieved from <http://www.hurriyet.com.tr/teknoloji/youtube-yasagindan-sonra-tibe-buyuk-sok-26100763>
- Hürriyet. (2014a, 05 19). Redhack TİKA'yı hackledi. Retrieved from <http://www.hurriyet.com.tr/gundem/redhack-tikayi-hackledi-26444523>
- Hürriyet. (2015, 03 16). Redhack'e beraat. Retrieved from <http://www.hurriyet.com.tr/teknoloji/redhack-e-beraat-28464093>

References

- Hürriyet. (2016, 10 10). Dropbox, OneDrive, Google Drive, Github ve Archive.org Türkiye'de engellendi. Retrieved from <http://www.hurriyet.com.tr/gundem/google-drive-dropbox-onedrive-github-ve-archive-org-turkiyede-engellendi-40244298>
- Hürriyet. (2017, 12 06). Mahir Kanaat ve Tunca Öğreten'e tahliye kararı. Retrieved from <http://www.hurriyet.com.tr/gundem/mahir-kanaat-ve-tunca-ogretene-tahliye-karari-40669751>
- Hürriyet Daily News. (2012, 07 06). Prosecutor demands RedHack be declared 'terrorist' organization. Retrieved from <http://www.hurriyetaailynews.com/prosecutor-demands-redhack-be-declared-terrorist-organization-24891>
- Hürriyet Daily News. (2013, 01 10). Corruption runs deep in Turkish universities, hacker group shows. Retrieved from <http://www.hurriyetaailynews.com/corruption-runs-deep-in-turkish-universities-hacker-group-shows-38749>
- Hürriyet Daily News. (2014, 01 16). Redhack divulges Turkcell numbers after company changes disclosed ministers' phones. Retrieved from <http://www.hurriyetaailynews.com/redhack-divulges-turkcell-numbers-after-company-changes-disclosed-ministers-phones-61141>
- İleri Haber. (2015, 01 08). Redhack İztuzu için hackledi. Retrieved from <https://ilerihaber.org/icerik/redhack-iztuzu-icin-hackledi-8289.html>
- İleri Haber. (2016, 09 23). RedHack Berat Albayrak'ın mail hesabını 'hack'ledi! Retrieved from <https://ilerihaber.org/icerik/redhack-berat-albayrakin-mail-hesabini-hackledi-60374.html>
- İleri Haber. (2016a, 10 17). RedHack yayınlamaya devam ediyor: 'Fikri Işık Cemaat mensubu, Erdoğan ve Gülen arasında gizli anlaşma var'. Retrieved from <https://ilerihaber.org/icerik/redhack-yayinlamaya-devam-ediyor-fikri-isik-cemaat-mensubu-erdogan-ve-gulen-arasinda-gizli-anlasma-var-61660.html>
- İleri Haber. (2018, 03 25). RedHack Demirören'e ait tüm siteleri hackledi. Retrieved from <https://ilerihaber.org/icerik/redhack-demirorene-ait-tum-siteleri-hackledi-83354.html>
- İlicak, N. (2013, 05 24). *Redhack 2'inci belge*. Retrieved from Sabah: <https://www.sabah.com.tr/yazarlar/ilicak/2013/05/24/redhack-2nci-belge>
- Independent. (2016, 12 07). Email Cache Proves Turkish Oil Minister's Links to Isis Oil Trade, WikiLeaks Claims. Retrieved from <https://www.independent.co.uk/news/world/middle-east/wikileaks-turkey-isis-oil-minister-email-cache-leaks-claims-a7460736.html>
- Internet Live Stats. (n.d.). Internet Usage. Retrieved from <http://www.internetlivestats.com>
- iskorptx. (n.d.). Retrieved 10 24, 2018, from Zone-h: <http://www.zone-h.org/archive/notifier=iskorptx?hz=1>

References

- Istanbul Chief Public Prosecutor's Office. (2017). İddianame [Indictment].
- Kalı, C. (2016, 02 01). Savunma dilekçesi [Plea of defense].
- Kızıl Bayrak. (2013, 12 28). RedHack GASKİ'yi hackledi: İhbarcılığa alet olmayın! Retrieved from <http://kizilbayrak42.net/ana-sayfa/guendem/haber/-/redhack-gaskiyi-hackledi-ihbarciliga-alet-olmayin>
- Kızıl Bayrak. (2014, 12 08). RedHack Rojhat Özdel için hackledi. Retrieved from <http://kizilbayrak42.net/ana-sayfa/guendem/haber/-/redhac-rojhat-oezdel-icin-hackledi/>
- Kızıl Bayrak. (2014a, 12 29). RedHack Roboski için hackledi. Retrieved from <http://kizilbayrak42.net/ana-sayfa/guendem/haber/-/redhack-roboski-icin-hackledi/>
- Lawyer 1. (2017, 05). Personal interview.
- Lawyer 10. (2019, 01). Personal interview.
- Lawyer 2. (2017, 05). Personal interview.
- Lawyer 3. (2017, 05). Personal interview.
- Lawyer 4 & Lawyer 5. (2018, 10). Personal interview.
- Lawyer 6. (2018, 11). Personal interview.
- Lawyer 7. (2018, 11). Personal interview.
- Lawyer 8. (2018, 11). Personal interview.
- Lawyer 9. (2019, 01). Personal interview.
- LEA 1, 2. &. (2017). Personal interview.
- LEA 2. (2018, 09). Personal interview.
- LEA 3. (2018, 10). Personal interview.
- LEA 4. (2017, 08). Personal interview.
- LEA 5. (2018, 12). Personal interview.
- LEA 6. (2019, 01). Personal interview.
- LEA 7. (2019, 01). Personal interview.
- Mann, M. (Director). (2015). *Blackhat* [Motion Picture].
- Medya Keşan. (2013, 09 05). Yine hack'lediler. Retrieved from <http://www.medyakesan.com.tr/guendem/yine-hacklediler-h3403.html>
- Medya Tava. (2013, 04 17). Redhack: YÖK'ü yok etmeye kararlınız! Retrieved from http://www.medyatava.com/haber/redhack-yok-u-yok-etmeye-kararliyiz_88157

References

- Medya Tava. (2013a, 11 12). RedHack'ten Yeni Akit'e gece yarısı operasyonu! Retrieved from https://www.medyatava.com/haber/redhack-ten-yeni-akit-e-gece-yarisi-operasyonu_98791
- Milliyet. (n.d.). Retrieved from <http://www.milliyet.com.tr/haberler/redhack>
- Milliyet. (2003, 07 23). Türk korsanlar 1500 Amerikan sitesini çökertti. Retrieved from Milliyet: <http://gazetearsivi.milliyet.com.tr/Ara.aspx?&ilkTar=01.01.2003&sonTar=30.12.2007&ekYayin=&drpSayfaNo=&araKelime=&gelismisKelimeAynen=cyber%20warrior&gelismisKelimeHerhangi=&gelismisKelimeYakin=&gelismisKelimeHaric=&Siralama=RANK%20DESC&SayfaAdet=20&isAdv>
- Milliyet. (2012, 09 12). 3 yaşındaki Dilan'a tecavüz mü edildi? Retrieved from <http://www.milliyet.com.tr/3-yasindaki-dilan-a-tecavuz-mu-edildi--gundem-1595186>
- Milliyet. (2012a, 05 08). Melih Gökçek'ten şok eden 'Ray' cevabı. Retrieved from <http://www.milliyet.com.tr/melih-gokcek-ten-sok-eden-ray-cevabi-siyaset-1537771/>
- Milliyet. (2013, 05 22). Redhack'ten şok Reyhanlı belgeleri. Retrieved from <http://www.milliyet.com.tr/redhack-ten-sok-reyhanli/gundem/detay/1712423/default.htm>
- Milliyet. (2013a, 05 22). Redhack iddiasını Davutoğlu yalanladı. Retrieved from <http://www.milliyet.com.tr/redhack-iddiasini-davutoglu/gundem/detay/1712509/default.htm>
- Milliyet. (2013b, 05 23). 'Hakaret edebilecek babayığit göremiyorum'. Retrieved from <http://www.milliyet.com.tr/-hakaret-edebilecek-babayigit-siyaset-1713082/>
- Milliyet. (2013c, 05 23). Beşir Atalay: 'Bu istihbaratları zaten takip ettik'. Retrieved from <http://www.milliyet.com.tr/besir-atalay-bu-istihbaratlari-siyaset-1713044/>
- Milliyet. (2013d, 10 25). Bağış'tan RedHack'e 'Hz. Ali'li yanıt. Retrieved from <http://www.milliyet.com.tr/bagis-tan-redhack-e-hz-ali-li-siyaset-1782087/>
- Milliyet. (2013e, 05 23). CHP'li Toprak: 'Terör istihbaratı alındı'. Retrieved from <http://www.milliyet.com.tr/chp-li-toprak-teror-istihbarati-siyaset-1712810/>
- Milliyet. (2016, 12 25). RedHack'e operasyon! Gözaltılar var... Retrieved from <http://www.milliyet.com.tr/redhack-e-operasyon-gozaltilar-gundem-2367616/>
- Milliyet Tv. (2013, 11 23). Bakan Güler'den "Redhack" açıklaması. Retrieved from <http://www.milliyet.com.tr/Milliyet-Tv/video-izle/Bakan-Guler-den--Redhack--aciklamasi-952hxgIv40VS.html>
- Mynet. (2013, 06 04). RedHack, Hatay Valiliği'nin sitesini hackledi. Retrieved from <https://www.mynet.com/redhack-hatay-valiliginin-sitesini-hackledi-110100700314>

References

- Ntv. (n.d.). Retrieved from <https://www.ntv.com.tr/ara?q=redhack>
- Ntv. (2012, 07 03). Redhack Dışişleri Bakanlığı'nı hackledi. Retrieved from https://www.ntv.com.tr/turkiye/redhack-disisleri-bakanligini-hackledi,iECCMBunCE2i7A16_PkFVg
- Ntv. (2012a, 04 20). İçişleri Bakanlığı 'hack'lendi. Retrieved from <https://www.ntv.com.tr/turkiye/icisleri-bakanligi-hacklendi,3kdtZFzt00msI4WP1eiu4A>
- Ntv. (2013, 01 09). YÖK'ün gizli belgelerine RedHack! Retrieved from https://www.ntv.com.tr/turkiye/yokun-gizli-belgelerine-redhack,MQz_7DB1xk6UQUK7cnGnLg
- Ntv. (2015, 03 16). RedHack davasında karar. Retrieved from https://www.ntv.com.tr/turkiye/redhack-davasinda-karar,Kf5v23_320OGuBkrXmkFhA
- Ntv. (2017, 01 03). Ankara'da RedHack operasyonu: 1 gözaltı. Retrieved from <https://www.ntv.com.tr/turkiye/ankarada-redhack-operasyonu-1-gozalti,uG9aBNguqUy-sGcgjL3ECQ>
- Odatv. (2012, 07 16). Muhbirleri deşifre etti. Retrieved from <https://odatv.com/muhbirleri-desifre-etti-1607121200.html>
- Odatv. (2012, 07 07). Red Hack terör listesine alındı. Retrieved from <https://odatv.com/redhack-teror-listesine-alindi-0707121200.html>
- Odatv. (2012a, 03 30). Redhack bu eylemi hangi devrimciye atfetti. Retrieved from <https://odatv.com/redhack-bu-eylemi-hangi-devrimciye-atfetti-3003121200.html>
- Odatv. (2012b, 04 13). Redhack Fethullah Gülen'in sitesini hackledi. Retrieved from <https://odatv.com/redhack-fethullah-gulenin-sitesini-hackledi-1304121200.html>
- Odatv. (2012c, 11 27). Redhack davasında tutuklu kalmadı. Retrieved from <https://odatv.com/redhack-davasinda-tutuklu-kalmadi--2711121200.html>
- Odatv. (2013, 01 08). 60 Bin gizli belgeyi yayınlıyor. Retrieved from <https://odatv.com/60-bin-gizli-belgeyi-yayinliyor-0801131200.html>
- Odatv. (2013a, 05 26). Egemen Bağış RedHack'e çarptı. Retrieved from <https://odatv.com/egemen-bagis-redhacke-carpti-2605131200.html>
- Odatv. (2013b, 09 11). Abdullah Cömert'i bu polisler mi öldürdü. Retrieved from <https://odatv.com/iste-abdullah-comert-in-katilleri-1109131200.html>
- Odatv. (2013c, 10 21). Utku Kalı davasında şok detay: Bakan Güler: O belge gizli değil. Retrieved from <https://odatv.com/utku-kali-davasinda-sok-detay-bakan-guler-o-belge-gizli-degil-2110131200.html>

References

- Odatv. (2013d, 05 23). Beşir Atalay: Bunlar özel konular. Retrieved from <https://odatv.com/bunlar-ozel-konular-2305131200.html>
- Odatv. (2014, 01 13). Nedir bu Melih Gökçek'in RedHack'ten çektiği. Retrieved from <https://odatv.com/nedir-bu-melih-gokcekin-redhackten-cektigi-1301141200.html>
- Odatv. (2014a, 05 20). Akit AKP'den öyle bir şey istedi ki. Retrieved from <https://odatv.com/akit-akpden-oyle-bir-sey-istedi-ki...-2005141200.html>
- Odatv. (2014b, 06 06). Redhack Pensilvanya'dan hiç bilinmeyen fotoğrafları yayınladı. Retrieved from <https://odatv.com/redhack-pensilvanyadan-hic-bilinmeyen-fotograf-lari-yayin-ladi-0606141200.html>
- Odatv. (2014c, 01 10). Redhack bu kez TBMM'yi hackledi. Retrieved from <https://odatv.com/redhack-bu-kez-tbmm-yi-hackledi-1001141200.html>
- Odatv. (2014d, 12 04). Redhack: Madem sonsuza kadar yaşamayacağız, o vakit istediğimiz gibi yaşayacağız. Retrieved from <https://odatv.com/redhack-yatagana-destek-icin-hackledi-0412141200.html>
- Odatv. (2014e, 12 16). Redhcak, İstanbul Polis Derneği'nin internet sitesini hackledi. Retrieved from <https://odatv.com/polis-dernegine-saldiri-1612141200.html>
- Pilkington, E. (2015, 02 02). *FBI put Anonymous 'Hactivist' Jeremy Hammond on Terrorism Watchlist*. Retrieved 11 01, 2018, from The Guardian: <https://www.theguardian.com/us-news/2015/feb/02/fbi-anonymous-hactivist-jeremy-hammond-terrorism-watchlist>
- Prosecutor 1. (2019, 01). Personal interview.
- Prosecutor 2. (2019, 01). Personal interview.
- Prosecutor 3. (2019, 01). Personal interview.
- Radikal. (2012, 02 28). Ankara Emniyeti 'Çökertildi'. Retrieved from <http://www.radikal.com.tr/turkiye/ankara-emniyeti-cokertildi-1080108/>
- Radikal. (2012, 07 06). Redhack resmen terör örgütü ilan edildi. Retrieved from <http://www.radikal.com.tr/turkiye/redhack-resmen-teror-orgutu-ilan-edildi-1093352/>
- Radikal. (2013, 08 22). Casuslukla suçlanan er Utku Kalı 'terör mahkemesi'nde yargılanacak. Retrieved from <http://www.radikal.com.tr/turkiye/casuslukla-suclanan-er-utku-kali-teror-mahkemesinde-yargilanacak-1147259/>
- Radikal. (2013, 11 25). Times: Barış Atay'ın gözaltına alınması 'Gezi'ye' cevap. Retrieved from <http://www.radikal.com.tr/turkiye/times-baris-atayin-gozaltina-alinmasi-geziye-cevap-1162826/>

References

- Radikal. (2013a, 08 01). Şafak Sezer Twitter'da kendi kendini mi hack'ledi? Retrieved from <http://www.radikal.com.tr/turkiye/safak-sezer-twitterda-kendi-kendini-mi-hackledi-1144391/>
- Radikal. (2014, 10 23). RedHack, Cumartesi Anneleri için hackledi. Retrieved from <http://www.radikal.com.tr/turkiye/redhack-cumartesi-anneleri-icin-hackledi-1220780/>
- RED! (2013). [Motion Picture].
- Redhack. (n.d.). Retrieved from Zone-h: <http://www.zone-h.org/archive/filter=1/notifier=Redhack>
- Redhack. (2008, 09 02). Tempo Dergisi RedHack Röportajı. (Tempo, Interviewer) Retrieved from SODAP: <https://www.sodap2.org/cesitli-yazilar-roportajlar/tempo-dergisi-redhack-roportaj>
- Redhack. (2012, 04 26). RedHack'in lideri 'Şirin Baba' çıktı! (Radikal, Interviewer) Retrieved from <http://www.radikal.com.tr/turkiye/redhackin-lideri-sirin-baba-cikti-1086105/>
- Redhack. (2012a, 08 31). RedHack: “Dünyadaki tüm sınırları ortadan kaldırmak istiyoruz” [Röportaj]. (DigitalAge, Interviewer) Retrieved from <http://digitalage.com.tr/redhack-dunyadaki-tum-sinirlari-ortadan-kaldirmak-istiyoruz-roportaj/>
- Redhack. (2012b, 11 21). (Nor Radyo, Interviewer)
- Redhack. (2013, 03 07). (Sosyalist Düşünce Topluluğu, Interviewer)
- Redhack. (2013a, 06 07). (Halk Tv, Interviewer) Retrieved from <https://web.archive.org/web/20160403042602/https://redhack.tumblr.com/post/52597166692/exclusive-interview-with-redhack-on-halk>
- Redhack. (2013b, 08 07). (Halk Tv, Interviewer)
- Redhack. (2013c, 06 21). Redhack, devletin siber ordusundan memnun: Büyürüz! (Radikal, Interviewer) Retrieved from <http://www.radikal.com.tr/turkiye/redhack-devletin-siber-ordusundan-memnun-buyuruz-1138586/>
- Redhack. (2013d, 05 26). Ezber Bozanlar Programı. (Ulusal Kanal, Interviewer)
- Redhack. (2016, 10 13). Why RedHack challenges Turkey's political establishment. (E. Sozeri, Interviewer) Retrieved from <https://www.dailydot.com/layer8/redhack-interview-turkey-censorship/>
- RedHack ODTU'de! (2013, 03 08). Retrieved from YouTube: <https://www.youtube.com/watch?v=kCaItV2uYKA>
- Robinson, P. (Director). (1992). *Sneakers* [Motion Picture].

References

- Ruffin, O. (2004, 06 03). *Hactivism, From Here to There*. Retrieved from The Cult of the Dead Cow: http://www.cultdeadcow.com/cDc_files/cDc-0384.php
- Sabah. (n.d.). Retrieved from <https://www.sabah.com.tr/arama?query=redhack>
- Sabah. (2012, 04 20). Redhack grubu İçişleri Bakanlığı'nı hackledi. Retrieved from <https://www.sabah.com.tr/teknokulis/haberler//2012/04/20/icisleri-bakanliginin-dosya-paylasim-sitesi-hacklendi>
- Sabah. (2012, 07 05). Redhack terör listesine giriyor. Retrieved from <https://www.sabah.com.tr/gundem/2012/07/05/redhack-teror-listesine-giriyor>
- Sabah. (2012a, 03 20). Kızıl hackerlara 8 ilde operasyon. Retrieved from <https://www.sabah.com.tr/teknokulis/haberler//2012/03/20/kizil-hackerlara-8-ilde-operasyon>
- Sabah. (2013, 07 04). 'Redhack'e sanal terör örgütü işlemi. Retrieved from <https://www.sabah.com.tr/gundem/2013/07/04/redhacke-sanal-teror-orgutu-islemi>
- Sabah. (2013a, 11 11). Er Utku Kalı, suçlamayı kabul etmedi. Retrieved from <https://www.sabah.com.tr/gundem/2013/11/11/er-utku-kali-suclamayi-kabul-etmedi>
- Sabah. (2014, 08 14). Redhack'in FBI bağlantısı ifşa oldu. Retrieved from <https://www.sabah.com.tr/amerika/2014/08/14/gezici-redhackin-fbi-baglantisi-ifsa-oldu>
- Sabah. (2014a, 04 23). Redhack'in ucu da paralel yapıya çıktı. Retrieved from <https://www.sabah.com.tr/gundem/2014/04/23/redhackin-ucu-da-paralel-yapiya-cikti>
- Sabah. (2014b, 04 07). Saldırdılar, çökertemediler. Retrieved from <https://www.sabah.com.tr/Gundem/2014/04/07/saldirilar-yukselisimizi-durduramayacak>
- Sabah. (2015, 03 16). Redhack davasında karar çıktı. Retrieved from <https://www.sabah.com.tr/gundem/2015/03/16/redhack-davasinda-karar-cikti>
- Sabah. (2016, 12 25). RedHack'in algı ekibine operasyon. Retrieved from <https://www.sabah.com.tr/gundem/2016/12/25/redhackin-algi-ekibineoperasyon>
- Sabah. (2017, 01 20). 17 Aralık fezlekesini 2 ay önce yüklemiş. Retrieved from <https://www.sabah.com.tr/gundem/2017/01/20/17-aralik-fezlekesini-2-ay-once-yuklemis>
- Sabah. (2017, 01 03). Başkentte "RedHack" operasyonu. Retrieved from <https://www.sabah.com.tr/gundem/2017/01/03/baskentte-redhack-operasyonu>

References

- Sabah. (2018, 11 08). MİT TIR'ları ihanet şebekesi CHP-FETÖ-RedHack. Retrieved from <https://www.sabah.com.tr/gundem/2018/11/08/mit-tirlari-ihanet-sebekesi-chp-feto-redhack>
- Sasmaz, N. (2013, 06 12). (CNN Türk, Interviewer) Retrieved from <https://www.youtube.com/watch?v=sXVYT9j-Q8I>
- Satayev, A. (Director). (2016). *Hacker* [Motion Picture].
- Sendika. (2013, 05 30). Redhack'ten Gezi Parkı direnişine destek için Beyoğlu polisine hack. Retrieved from <http://sendika63.org/2013/05/redhackten-gezi-parkina-direnisine-destek-icin-beyoglu-polisine-hack-110941/>
- Sendika. (2013a, 10 15). RedHack, bayram mesajını hackleyerek yayımladı. Retrieved from <http://sendika63.org/2013/10/redhack-bayram-mesajini-hackleyerek-yayimladi-145222/>
- Sendika. (2013b, 11 22). RedHack operasyonunda 14 gözaltı. Retrieved from <http://sendika63.org/2013/11/anonymous-ve-redhack-operasyonu-14-gozalti-151024/#more>
- Sendika. (2014, 05 11). RedHack, Danıştay resmi sitesini hacklediğini açıkladı. Retrieved from <http://sendika63.org/2014/05/redhack-danistayin-sitesini-hackledi-189254/>
- Sendika. (2016, 09 30). “RedHack Damat Berat’ı hackledi” haberimize bildirimsiz, gerekçesiz sansür. Retrieved from <http://sendika63.org/2016/09/redhack-damat-berati-hackledi-haberimize-bildirimsiz-gerekcesiz-sansur-378887/>
- Sivas no. 5 Military Prosecutor's Office. (2013). Indictment [iddianame].
- Siyasi Haber. (2014, 10 29). Redhack bu defa Validebağ için hackledi. Retrieved from <http://siyasihaber4.org/redhack-bu-defa-validebag-icin-hackledi>
- Siyasi Haber. (2014a, 11 14). Redhack, Yırca ve Validebağ için halkın borcunu sildi. Retrieved from <http://siyasihaber4.org/redhack-yirca-ve-validebag-icin-halkin-borcunu-sildi>
- Siyasi Haber. (2015, 03 16). Redhack beraat etti. Retrieved from <http://siyasihaber4.org/redhack-beraat-etti>
- Siyasi Haber. (2016, 10 01). Redhack'ten yeni mailler: Kürt petrolünü usulsüzce taşıyan şirkette söz sahibi Albayrak'mış. Retrieved from <http://siyasihaber4.org/redhackten-yeni-mailler-kurt-petrolunu-usulsuzce-tasiyan-sirkette-soz-sahibi-albayrakmis>
- Siyasi Haber. (2016a, 10 04). RedHack RTÜK'ün internet sitesini hackledi. Retrieved from <http://siyasihaber4.org/redhack-rtukun-internet-sitesini-hackledi>
- Softley, I. (Director). (1995). *Hackers* [Motion Picture].

References

- SoL. (2011, 07 04). RedHack 2 Temmuz için hackledi. Retrieved from <http://haber.sol.org.tr/bilim-teknoloji/redhack-2-temmuz-icin-hackledi-haberi-44196>
- SoL. (2012, 05 03). Redhack bu kez 'sütçüleri' hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-bu-kez-sutculeri-hackledi-haberi-54391>
- SoL. (2012, 07 06). RedHack 'Terör örgütü' ilan edildi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-teror-orgutu-ilan-edildi-haberi-56680>
- SoL. (2012a, 05 03). RedHack, Zaman gazetesi, Melih Gökçek, Sağlık Bakanlığı, TTNET ve TÜBİTAK'ı hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-zaman-gazetesi-melih-gokcek-saglik-bakanligi-ttnet-ve-tubitaki-hackledi>
- SoL. (2012b, 07 13). RedHack MEB'in sitesini hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-mebin-sitesini-hackledi-haberi-57023>
- SoL. (2012c, 10 27). RedHack açlık grevine destek için hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-aclik-grevine-destek-icin-hackledi-haberi-61501>
- SoL. (2013, 02 27). Redhack Melih Gökçek'le ilgili belgeleri yayınladı. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-melih-gokcekle-ilgili-belgeleri-yayinladi-haberi-68883>
- SoL. (2013a, 04 18). YÖK'ün skandal soruları RedHack belgelerinde! Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/yokun-skandal-sorulari-redhack-belgelerinde-haberi-71625>
- SoL. (2013b, 06 01). Redhack'den Gezi Parkı yanıtı: İşte milletvekillerinin numaraları. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhackden-gezi-parki-yaniti-iste-milletvekillerinin-numaralari-haberi-73891>
- SoL. (2013c, 10 23). Redhack'ten bomba Egemen Bağış belgeleri. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhackten-bomba-egemen-bagis-belgeleri-haberi-81431>
- SoL. (2013d, 11 11). Redhack'ten yeni belgeler: 'Hani Utku suçluydu?'. Retrieved from <http://haber.sol.org.tr/node/82447>
- SoL. (2013e, 01 17). Redhack N.Ç. için Yargıtay'ı hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-nc-icin-yargitayi-hackledi-haberi-66360>

References

- SoL. (2013f, 04 08). Redhack Emek Sineması eylemini destekledi, dondurmacı MADO'yu hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-emek-sineması-eylemini-destekledi-dondurmaci-madoyu-hackledi-haberi-71073>
- SoL. (2013g, 05 07). RedHack Medical Park'ı hackledi. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-medical-parki-hackledi-haberi-72617>
- SoL. (2013h, 11 29). 'RedHack üyeliği' iddiasıyla gözaltına alınan Taylan Kulaçoğlu cezaevinde! Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhack-uyeligi-iddiasıyla-gozaltına-alınan-taylan-kulacoglu-cezaevinde-haberi-834>
- SoL. (2013i, 01 10). Bakan Yıldırım'dan Redhack açıklaması: Yolsuzluğa değil, hack'e önlem alacağız. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/bakan-yildirimdan-redhack-aciklamasi-yolsuzluga-degil-hacke-onlem-alacagiz-haberi>
- SoL. (2013j, 09 09). İşte Redhack'in ele geçirdiği o fatura! Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/iste-redhackin-ele-gecirdigi-o-fatura-haberi-79345>
- SoL. (2013k, 05 22). Redhack belgesini haber yapamayanlar: Sabah, Zaman ve Star... Retrieved from <http://haber.sol.org.tr/medya/redhack-belgesini-haber-yapamayanlar-sabah-zaman-ve-star-haberi-73436>
- SoL. (2014, 01 11). RedHack'ten TCDD'de yolsuzluk belgeleri. Retrieved from <http://haber.sol.org.tr/devlet-ve-siyaset/redhackten-tcddde-yolsuzluk-belgeleri-haberi-85779>
- SoL. (2014a, 12 05). Redhack Berkin Elvan için hackledi. Retrieved from <http://haber.sol.org.tr/turkiye/redhack-berkin-elvan-icin-hackledi-102413>
- SoL. (2016, 10 06). Taylan Kulaçoğlu ve Redhack gözaltıları serbest. Retrieved from <http://haber.sol.org.tr/toplum/taylan-kulacoglu-ve-redhack-gozaltıları-serbest-171444>
- SoL. (2016a, 09 30). Redhack'in paylaştığı Berat Albayrak mailleriyle ilgili soL'un yaptığı haberlere sansür! Retrieved from <http://haber.sol.org.tr/toplum/redhackin-paylastigi-berat-albayrak-mailleriyle-ilgili-solun-yaptigi-haberlere-sansur-170746>
- Sözcü. (2012, 09 17). Hatay için hacklediler. Retrieved from <https://www.sozcu.com.tr/2012/gundem/redhack-hatay-icin-hackledi-45904/>
- Sözcü. (2012a, 10 07). Redhack, İçişleri Bakanlığı'nı hackledi. Retrieved from <https://www.sozcu.com.tr/2012/gunun-icinden/redhack-icisleri-bakanligini-hackledi-70998>
- Sözcü. (2012b, 11 09). Redhack ODTU'yü hackledi. Retrieved from <https://www.sozcu.com.tr/2012/gunun-icinden/redhack-odtuyu-hackledi-109194/>

References

- Sözcü. (2013, 06 12). RedHack'ten art arda saldırılar. Retrieved from <https://www.sozcu.com.tr/2013/gunun-icinden/redhackten-art-arda-saldirilar-313630/>
- Sözcü. (2013a, 08 15). RedHack ASKİ'yi hackledi! Retrieved from <https://www.sozcu.com.tr/2013/gunun-icinden/redhack-askiyi-hackledi-354787>
- Sözcü. (2013b, 08 23). RedHack Ali İsmail Korkmaz için hackledi. Retrieved from <https://www.sozcu.com.tr/2013/gunun-icinden/redhack-ali-ismail-korkmaz-icin-hackledi-359920/>
- Sözcü. (2013c, 09 05). Redhack bu kez de Emniyet'i vurdu! Retrieved from <https://www.sozcu.com.tr/2013/gundem/redhack-emniyeti-hackledi-366766>
- Sözcü. (2013d, 11 25). Redhack AKP'yi hackledi! Retrieved from <https://www.sozcu.com.tr/2013/gundem/redhack-akpyi-hackledi-413236/>
- Sözcü. (2014, 05 14). Yas ilan edilmeyince! Retrieved from <https://www.sozcu.com.tr/2014/gundem/yas-ilan-edilmeyince-508806>
- Sputnik Türkiye. (2016, 02 04). Utku Kalı beraat etti. Retrieved from <https://tr.sputniknews.com/turkiye/201602041020641921-utku-kali-reyhanli-mit-tir-suriye/>
- Sputnik Türkiye. (2016a, 10 08). Türkiye'den Dropbox ve Google Drive'a erişim engeli. Retrieved from <https://tr.sputniknews.com/turkiye/201610081025200578-dropbox-google-drive-erisim-engeli/>
- Sputnik Türkiye. (2017, 04 21). RedHack operasyonunda bir kişi daha gözaltına alındı. Retrieved from <https://tr.sputniknews.com/turkiye/201704211028170698-redhack-operasyonunda-bir-kisi-daha-gozaltina-alindi/>
- Statista. (2019, 07 30). *Number of monthly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019 (in millions)*. Retrieved from Statista: <https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/>
- T24. (2012, 04 20). Redhack, İçişleri Bakanlığı internet sayfasını hackledi. Retrieved from <https://t24.com.tr/haber/redhack-icisleri-bakanligi-internet-sayfasini-hackledi,202075>
- T24. (2012a, 11 26). Redhack davasında tutuklu sanıklara tahliye kararı. Retrieved from <https://t24.com.tr/haber/redhack-saniklari-ilk-kez-hakim-karsisinde,218268>
- T24. (2013, 11 25). Times: Barış Atay'ın gözaltına alınması Gezi eylemlerine misilleme. Retrieved from <https://t24.com.tr/haber/times-baris-atayin-gozaltina-alinmasi-gezi-eylemlerine-misilleme,244731>
- T24. (2013a, 04 15). Redhack Çevre Bakanlığı'nın sitesini çökertti. Retrieved from <https://t24.com.tr/haber/redhack-cevre-bakanliginin-sitesini-cokertti,227790>

References

- T24. (2013b, 06 03). Anonymous bu kez Gezi Parkı direnişi için hackledi. Retrieved from <https://t24.com.tr/haber/anonymous-bu-kez-gezi-parki-direnisi-icin-hackledi,231178>
- T24. (2016, 09 29). RedHack'in Doğan Medya Grubu'na ait olduğunu iddia ettiği e-postalarla ilgili haberlere erişim engeli. Retrieved from <https://t24.com.tr/haber/redhackin-dogan-medya-grubuna-ait-oldugunu-iddia-ettigi-e-postalarla-ilgili-haberlere-erisim-engeli,362412>
- T24. (2017, 07 04). Savcılık, gazeteci Deniz Yücel'in dosyasını ayırdı. Retrieved from <https://t24.com.tr/haber/savcilik-gazeteci-deniz-yucelin-dosyasini-ayirdi,412560>
- Takvim. (2014, 04 23). Redhack paralel el ele. Retrieved from <https://www.takvim.com.tr/guncel/2014/04/23/redhack-paralel-el-ele>
- The Hacktivism Declaration*. (2001, 07 04). Retrieved 10 25, 2018, from The Cult of the Dead Cow: http://www.cultdeadcow.com/cDc_files/declaration.html
- The Wachowskis (Director). (1999). *The Matrix* [Motion Picture].
- Turkish Anti-Terror Law, Article no. 1. (1991).
- Turkish Anti-Terror Law, Article no. 2. (1991). Retrieved from http://www.opbw.org/nat_imp/leg_reg/turkey/anti-terror.pdf
- Turkish Anti-Terror Law, Article no. 3. (1991).
- Turkish Anti-Terror Law, Article no.7. (1991).
- Turkish Penal Code. (2004).
- Turkish Penal Code, Article no. 136. (2004).
- Turkish Penal Code, Article no. 220. (2004).
- Turkish Penal Code, Article no. 243. (2004).
- Turkish Penal Code, Article no. 244. (2004).
- Turkish Penal Code, Article no. 309. (2004).
- Turkish Penal Code, Article no. 314. (2004).
- Turkish Penal Code, Article no. 327. (2004).
- Turkish Penal Code, Article no. 329. (2004).
- Turkish Penal Code, Article no. 334. (2004).
- Türkiye Gazetesi. (2009, 07 28). Türk hackerlar BM'nin sitesini çökertti. Retrieved from Türkiye Gazetesi: <http://www.turkiyegazetesi.com.tr/Genel/a414721.aspx>

References

- Türkiye Gazetesi. (2013, 08 25). Redhack'den Koç Grubu'na saldırı. Retrieved from <https://www.turkiyegazetesi.com.tr/gundem/67391.aspx>
- Ulusal Kanal. (2013, 02 27). Retrieved from <https://www.ulusal.com.tr/gundem/tgbliler-mumtazer-turkoneyi-fena-yakaladigundem/milletvekillerine-rekor-zamyurt/akpli-ciftci-akpye-isyan-ettikultur-sanat/insanliki-kesti-cezayiri-dikecekgundem/ermeni-soykirimi-yalanini-yasar-kemale-sormayingundem/akpli-k>
- Vatan. (2013, 12 07). O polis görevden alındı..! Retrieved from <http://www.gazetevatan.com/o-polis-gorevden-alindi----590545-gundem/>
- Vatan. (2013a, 07 03). Diyanet'i hacklediler! Retrieved from <http://www.gazetevatan.com/diyanet-i-hacklediler--550662-gundem/>
- What is free software?* (2018, 10 15). Retrieved from GNU Operating System: <https://www.gnu.org/philosophy/free-sw.html#History>
- Whedon, J. (Director). (2012). *The Avengers* [Motion Picture].
- Who We Be*. (n.d.). Retrieved 10 25, 2018, from Cult of the Dead Cow: <https://w3.cultdeadcow.com/cms/about.html>
- Winkler, I. (Director). (1995). *the Net* [Motion Picture].
- Wiseman, L. (Director). (2007). *Live Free or Die Hard* [Motion Picture].
- Yeni Akit. (2014, 12 06). Komünist Hacker grubu MOBESE'yi hack'ledi! Retrieved from <https://www.yeniakit.com.tr/haber/komunist-hacker-grubu-mobeseyi-hackledi-39001.html>
- Yeni Akit. (2016, 10 03). Redhack grubu kimdir? Retrieved from <http://www.yeniakit.com.tr/foto-galeri/redhack-grubu-kimdir-9597>
- Yeni Akit. (2016, 12 25). Terör destekçisi RedHack'e operasyon! Retrieved from <https://www.yeniakit.com.tr/haber/teror-destekcisi-redhacke-operasyon-249624.html>
- Yeni Şafak. (2018, 11 12). MİT tırları ihanetinde düğüm Kılıçdaroğlu'nda çözülecek. Retrieved from <https://www.yenisafak.com/gundem/mit-tirlari-ihanetinde-dugum-kilicdaroglunda-cozulecek-3408266>
- Yeşil Gazete. (2012, 09 26). RedHack Sinop Valiliğinin sitesini hackledi. Retrieved from <https://yesilgazete.org/blog/2012/09/26/redhack-sinop-valiligi-sitesini-hackledi/>
- Yolculuk. (2016, 09 28). Sansüre karşı yeniden yayınlıyoruz: İşte #RedHack'in Berat'ın mailinden paylaştıkları. Retrieved from <https://gazeteyolculuk.net/sansure-karsi-yeniden-yayinliyoruz-iste-redhackin-beratin-mailinden-paylastiklari>

References

- Yolculuk. (2016a, 09 23). RedHack, Sözcü gazetesini hackleyerek kendi haberini yaptı. Retrieved from <https://gazeteyolculuk.net/redhack-sozcu-gazetesini-hackleyerek-kendi-haberini-yapti>
- Yolculuk. (2017, 06 20). RedHack, zehirlenen askerler için Savunma Bakanlığı sitesini hackledi. Retrieved from <https://gazeteyolculuk.net/redhack-zehirlenen-askerler-icin-savunma-bakanligi-sitesini-hackledi>
- Yolculuk. (2017a, 02 16). Daha önce RedHack'ten gözaltına alınan Tunay Şentürk, savcılık itirazıyla tutuklandı. Retrieved from <https://gazeteyolculuk.net/daha-once-redhackten-gozaltina-alinan-tunay-senturk-savcilik-irazıyla-tutuklandı>
- Zone-h. (2012, 05 13). hizmet.aile.gov.tr hacked. Retrieved from <http://zone-h.org/mirror/id/17620266?hz=1>
- Zone-h. (2012a, 07 03). public.mfa.gov.tr hacked. Retrieved from <http://www.zone-h.org/mirror/id/17997355>
- Zone-h. (2013, 01 08). ebys.yok.gov.tr hacked. Retrieved from <http://www.zone-h.org/mirror/id/18906528>

Secondary Sources

- Abbate, J. (1999). *Inventing the Internet*. Cambridge: The MIT Press.
- Akin, A., & Zıraman, D. (2015). Power struggle in/around the Turkish online realm and three forms of opposition: Redhack, Alternative IS Association and personal resistances against YouTube ban. *Global Media Journal: Mediterranean Edition*, 10(1), 13-21.
- Akser, M. (2015). The Revolution will be Hacktivated: Turkish Marxist Hacker Groups. In B. Akdenizli (Ed.), *Digital Transformations in Turkey: Current Perspectives in Communication Studies* (pp. 275-286). Lanham: Lexington Books.
- Albanese, J. (2015). *Organized Crime in Our Times*. London: Routledge.
- Albertazzi, D., & McDonnell, D. (2008). Introduction: The Sceptre and the Spectre. In D. Albertazzi, & D. McDonnell (Eds.), *Twenty-First Century Populism. The Spectre of Western European Democracy* (pp. 1-11). Basingstoke: Palgrave MacMillan.
- Alpaslan, M. (1983). *Kriminoloji ve hukuk açısından tedhişçilik*. Istanbul: Teknik Yayınları.
- Altheide, D. (2007). The mass media and terrorism. *Discourse & Communication*, 1(3), 287-308.

References

- Anderson, R. (2008). *Security Engineering. A Guide to Building Dependable Distributed Systems*. Indianapolis: Wiley Publishing.
- Aouragh, M. (2012). Tweeting like a Pigeon: The Internet in the Arab Revolutions. *CyberOrient*, 6(2).
- Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks, Freedom and the Future of the Internet*. New York: Or Books.
- Auty, C. (2004). Political hacktivism: Tool of the underdog or scourge of cyberspace? *Aslib Proceedings: New Information Perspectives*, 56(4), 212-221.
doi:<http://dx.doi.org/10.1108/00012530410549240>
- Barak, G. (Ed.). (1991). *Crimes by the Capitalist State. An Introduction to State Criminality*. New York: State University of New York Press.
- Barlow, J. (1996, 02 08). *A Declaration of the Independence of Cyberspace*. Retrieved from Electronic Frontier Foundation: <https://www.eff.org/cyberspace-independence>
- Baser, B., Akgönül, S., & Öztürk, A. (2017). “Academics for Peace” in Turkey: a case of criminalising dissent and critical thought via counterterrorism policy. *Critical Studies on Terrorism*, 10(2), 274-296.
- Bayraktar, K. (1982). *Politik Suç [Political Crime]*. Istanbul: İÜHF.
- Bayraktar, K. (2015). Siyasal Suç ve Terör Eylemleri. In H. İnancı (Ed.), *Türkiye'de Hukuku Yeniden Düşünmek* (pp. 141-150). Istanbul: İletişim.
- Becker, H. (1966). *Outsiders, Studies in the Sociology of Deviance*. New York: The Free Press.
- Benjamin, W. (1986). Critique of Violence. In W. Benjamin, *Reflections, Essays, Aphorisms, Autobiographical Writings* (E. Jephcott, Trans., pp. 277-300). New York: Schocken Books.
- Bennett, C. (2008). *The Privacy Advocates, Resisting the Spread of Surveillance*. Cambridge: The MIT Press.
- Berger, B. ((1974) 1986). Foreword. In E. Goffman, *Frame Analysis, An Essay on the Organization of Experience* (pp. xi-xviii). Boston: Northeastern University Press.
- Bowman-Grieve, L. (2015). Cyberterrorism and Moral Panics. In L. Jarvis, S. Macdonald, & T. Chen (Eds.), *Terrorism Online, Politics, Law and Technology* (pp. 86-106). New York: Routledge.
- Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.
- Boyras, M., Krishnan, A., & Catona, D. (2015). Who Is Retweeted in Times of Political Protest? An Analysis of Characteristics of Top Tweeters and Top Retweeted Users

References

- During the 2011 Egyptian Revolution. *Atlantic Journal of Communication*, 23(2), 99-119.
- Bruns, A., & Moe, H. (2014). Structural layers of communication on Twitter. In K. Weller, A. Bruns, J. Burgess, M. Mahrt, & C. Puschmann (Eds.), *Twitter and Society* (pp. 15-28). New York: Peter Lang Publishing.
- Bulut, E., & Yörük, E. (2017). Digital Populism: Trolls and Political Polarization of Twitter in Turkey. *International Journal of Communication*, 11, 4093-4117.
- Burrell, J. (2009). The Field Site as a Network: A Strategy for Locating Ethnographic Research. *Field Methods*, 21(2), 181-199.
- Carragee, K., & Roefs, W. (2004). The Neglect of Power in Recent Framing Research. *Journal of Communication*, 54(2), 214-233.
- Castells, M. ((1996) 2010). *The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I*. Oxford: Wiley & Blackwell.
- Castells, M. (2001). Epilogue: Informationalism and the Network Society. In P. Himanen, *The Hacker Ethic and the Spirit of the Information Age* (pp. 155-178). New York: Handom House Trade Publishers.
- Cavelty, M., & Jaeger, M. (2015). (In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous. *International Political Sociology*, 9, 176-194.
- Chambliss, W. (1989). State-Organized Crime - The American Society of Criminology, 1988 Presidential Address. *Criminology*, 27(2), 183-208.
- Cinar, M. (2017). "Gelişirken": Türkiye örneğinden hareketle iktisadi kalkınma söylemleri ve demokrasi ilişkisini yeniden düşünmek. *ODTÜ Gelişme Dergisi*, 44, 47-67.
- Cohen, S. ((1972) 2011). *Folk Devils and Moral Panics. The creation of the Mods and Rockers* (3rd Edition ed.). London: Routledge.
- Coleman, G. (2013). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.
- Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: the Many Faces of Anonymous*. London: Verso.
- Comaroff, J., & Comaroff, J. (2016). *The Truth about Crime: Sovereignty, Knowledge, Social Order*. Chicago: The University of Chicago Press.
- Conley, J., & O'Barr, W. (1997). Crime and Custom in Corporate Society: A Cultural Perspective on Corporate Misconduct. *Law and Contemporary Problems*, 60, 5-22.
- Connell, R. (1995). *Masculinities*. Berkeley: University of California Press.

References

- Cox, J. (2016, 01 25). *Chaos Communication Congress: A Very German Hacking Conference*. Retrieved from Motherboard:
https://motherboard.vice.com/en_us/article/xygxn4/chaos-communication-congress-a-very-german-hacking-conference-5886b73a9848b145c38b3f06
- Dahong, M. (2005). *The Passionate Time of Chinese Hackers*. Retrieved 10 23, 2018, from Chinascope: <http://chinascope.org/archives/6520>
- D'Angelo, P. (2002). News framing as a multiparadigmatic research program: A response to Entman. *Journal of Communication*, 52(4), 870-888.
- D'Angelo, P., & Kuypers, J. (2010). *Doing News Framing Analysis. Empirical and Theoretical Perspectives*. London: Routledge.
- Das, V. (2004). The Signature of the State, The Paradox of Illegibility. In V. Das, & D. Poole (Eds.), *Anthropology in the Margins of the State* (pp. 225-252). Oxford: Oxford University Press.
- Das, V., & Poole, D. (2004). State and Its Margins, Comparative Ethnographies. In V. Das, & D. Poole (Eds.), *Anthropology in the Margins of the State* (pp. 3-33). Oxford: Oxford University Press.
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. the OpenNet Initiative (ONI). Cambridge: The MIT Press.
- Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla, & D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288). California: Rand. Retrieved from
https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf
- Denning, D. E. (2011). Chapter 9: Cyber conflict as an emergent social phenomenon. In T. Holt, & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 170-186). New York: Information Science Reference.
- Deseriis, M. (2017). Hacktivism: On the Use of Botnets in Cyberattacks. *Theory, Culture & Society*, 34(4), 131-152.
- Doğu, B. (2013). Ana Akım Medya Gündeminin Yeniden Kurgulanması: Türkiye'deki Alternatif Haber Siteleri üzerine bir İnceleme. *Unpublished doctoral dissertation*. Ege Üniversitesi.
- Doğu, B. (2017). Environment as Politics: Framing the Cerattepe Protest in Twitter. *Environmental Communication*, 1-16.

References

- Dominguez, R. (1999, 11 25). Electronic Disturbance. (C. Fusco, Interviewer) Retrieved 10 27, 2018, from http://subsol.c3.hu/subsol_2/contributors2/domingueztext2.html
- Downey, J., Titley, G., & Toynbee, J. (2014). Ideology critique: the challenge for media studies. *Media, Culture & Society*, 36(6), 878-887.
- Durkheim, E. ((1893) 1960). *The Division of Labor in Society*. (G. Simpson, Trans.) Illinois: The Free Press of Glencoe.
- Dyer-Witheford, N.-D. (2015). *Cyber-Proletariat: Global Labour in the Digital Context*. London: Pluto Press.
- Eagleton, T. (1991). *Ideology. An Introduction*. London: Verso.
- Ellison, N., & Boyd, D. (2013). Sociality Through Social Network Sites. In W. Dutton (Ed.), *The Oxford Handbook of Internet Studies* (pp. 151-172). Oxford: Oxford University Press.
- Entman, R. (1991). Framing US Coverage of International News: Contrasts in Narratives of the KAL and Iran Air Incidents. *Journal of Communication*, 41(4), 6-27.
- Entman, R. (1993). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*, 43(4), 51-58.
- Ercan, F., & Oğuz, Ş. (2014). From Gezi Resistance to Soma Massacre: Capital Accumulation and Class Struggle in Turkey. *Socialist Register*, 51, 114-135.
- Eriş, U. (2009). *Türkiye'de Kırıcı (Hacker) Kültürü [Hacker Culture in Turkey]*. Eskişehir: PhD diss., Anadolu University Social Sciences Institute.
- Ferrell, J. (1995). Urban Graffiti: Crime, Control, and Resistance. *Youth & Society*, 27(1), 73-92.
- Ferrell, J., Hayward, K., & Young, J. (2015). *Cultural Criminology, An Invitation*. London: Sage.
- Forsythe, D. (1999). Ethics and Politics of Studying Up in Technoscience. *Anthropology of Work Review*, XX(1), 6-11.
- Fuchs, C. (2013). The Anonymous movement in the context of liberalism and socialism. *Interface: a journal for and about social movements*, 5(2), 345-376.
- Gaffney, D., & Puschmann, C. (2014). Data Collection on Twitter. In K. Weller, A. Bruns, J. Burgess, M. Mahrt, & C. Puschmann (Eds.), *Twitter and Society* (pp. 55-68). New York: Peter Lang Publishing.
- Garland, D. (1991). Sociological Perspectives on Punishment. *Crime and Justice*, 14, 115-165.

References

- Gitlin, T. (1980). *The whole world is watching. Mass media in the making & unmaking of the new left*. Berkeley: University of California Press.
- Goffman, E. ((1974) 1986). *Frame Analysis, An Essay on the Organization of Experience*. Boston: Northeastern University Press.
- Goffman, E. (1963). *Stigma: Notes on the Management of Spoiled Identity*. New York: Simon & Schuster.
- Goode, E., & Ben-Yehuda, N. ((1994) 2009). *Moral Panics, The Social Construction of Deviance*. Cambridge: Blackwell.
- Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication*, 13, 74-86.
- Gökdemir, O. (2013). *Sanal Alemin Klavyeli Asileri. Redhack [Keyboard Activists of Virtual Realm. Redhack]*. Istanbul: Destek Yayınları.
- Gramsci, A. ((1971) 1992). *Selections from the Prison Notebooks*. (Q. Hoare, & G. Smith, Dü) New York: International Publishers.
- Green, P., & Ward, T. (2000). State Crime, Human Rights, And the Limits of Criminology. *Social Justice*, 27(1), 101-115.
- Hacking, I. (1999). *The Social Construction of What?* Cambridge: Harvard University Press.
- Hall, S. ((1982) 2005). The rediscovery of ideology: Return of the repressed in media studies. In M. Gurevitch, T. Bennett, J. Curran, & J. Woollacott (Eds.), *Culture, Society, and the Media* (pp. 52-86). London: Routledge.
- Hall, S., & Jefferson, T. (Eds.). ((1976) 2003). *Resistance Through Rituals*. London: Routledge.
- Harvey, D. (2005). *A Brief History of Neoliberalism*. Oxford: Oxford University Press.
- Hauben, R. (1996, 06 05). *The Evolution of Usenet: The poor man's Arpanet*. Retrieved from <http://www.columbia.edu/~rh120/ch106.x02>
- Hayward, K., & Presdee, M. (Eds.). (2010). *Framing Crime: Cultural Criminology and the Image*. New York: Routledge.
- Heineman, D. (2007). The Digital Rhetorics of Hacktivism: Anti-institutional Politics in Cyberspace. *Unpublished doctoral dissertation*. The University of Iowa.
- Henderson, S. (2007). *The dark visitor: Inside the world of Chinese hackers*. Fort Leavenworth: Foreign Military Studies Office.
- Holt, T., Freilich, J., & Chermak, S. (2017). Exploring the Subculture of Ideologically Motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice*, 1-22.

References

- Hu, T.-H. (2015). *A Prehistory of the Cloud*. Cambridge: The MIT Press.
- Huschle, B. J. (2002). Cyber Disobedience: When is Hacktivism Civil Disobedience? *International Journal of Applied Philosophy*, 16(1), 69-83.
- Hülse, R., & Spencer, A. (2008). The Metaphor of Terror: Terrorism Studies and the Constructivist Turn. *Security Dialogue*, 39(6), 571-592.
- International Telecommunication Union. (2018). *Measuring the Information Society Report Volume 1*. Geneva.
- Jackson, R. (2005). *Writing the war on terrorism: Language, politics and counter-terrorism (New Approaches to Conflict Analysis)*. Manchester: Manchester University Press.
- Jackson, R. (2016). Introduction. In R. Jackson (Ed.), *Routledge Handbook of Critical Terrorism Studies* (pp. 1-13). London: Routledge.
- Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage. *Perspectives on Terrorism*, 9(1), 60-75.
- Jarvis, L., Macdonald, S., & Whiting, A. (2016). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*, 2(1), 64-87.
- Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.
- Jewkes, Y. (2004). *Media and Crime*. London: Sage Publications.
- Jordan, T. (2002). *Activism! Direct Action, Hacktivism and the Future of Society*. London: Reaktion Books.
- Jordan, T., & Taylor, P. A. (2004). *Hacktivism and Cyberwars: Rebels with a cause?* New York: Routledge.
- Klein, A. (2015). Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. *Communication Monographs*, 82(3), 379-401.
- Kramer, R., & Michalowski, R. (2005). War, aggression and state crime: A criminological analysis of the invasion and occupation of Iraq. *British Journal of Criminology*, 45, 446-469.
- Krapp, P. (2005). Terror and Play, or What Was Hacktivism? *Grey Room*, 21(8), 70-93.
- Kubitschko, S. (2015). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence: The International Journal of Research into New Media Technologies*, 21(3), 388-402.
- Laclau, E. (2005). *On Populist Reason*. London: Verso.

References

- Latour, B. (2002). *La Fabrique du Droit, une Ethnologie du Conseil d'Etat [The Making of Law: an Ethnography of the Conseil d'Etat]*. Paris: La Découverte.
- Levy, S. ((1984) 2010). *Hackers: Heroes of the Computer Revolution*. Sebastopol: O'Reilly.
- Lievrouw, L. (2011). *Alternative and Activist New Media*. Cambridge: Polity Press.
- Lindgren, S., & Lundström, R. (2011). Pirate culture and hacktivist mobilization: The cultural and social protocols of #WikiLeaks on Twitter. *new media & society*, 13(6), 999-1018.
- Linebaugh, P. (1993). Karl Marx, the Theft of Wood, and Working-Class Composition. In *Crime and Capitalism. Readings in Marxist Criminology* (pp. 100-121). Philadelphia: Temple University Press.
- Loftus, B. (2009). *Police Culture in a Changing World*. Oxford: Oxford University Press.
- Maireder, A., & Ausserhofer, J. (2014). Political Discourses on Twitter: Networking Topics, Objects, and People. In K. Weller, A. Bruns, J. Burgess, M. Mahrt, & C. Puschmann (Eds.), *Twitter and Society* (pp. 305-318). New York: Peter Lang Publishing.
- Malthaner, S. (2014). Field work in the Context of Violent Conflict and Authoritarian Regimes. In D. della Porta (Ed.), *Methodological Practices in Social Movement* (pp. 173-194). Oxford: Oxford University Press.
- Marx, K. ((1842) 1996). Debates on the Law on Thefts of Wood. *Rheinische Zeitung* (298).
- Marx, K. (1978). The German Ideology : Part I. In R. Tucker (Ed.), *The Marx-Engels Reader* (pp. 146-200). New York: W. W. Norton & Company.
- Marx, K. (1993). The Usefulness of Crime. In D. Greenberg (Ed.), *Crime and Capitalism: Readings in Marxist Criminology* (pp. 52-53). Philadelphia: Temple University Press.
- Matusitz, J. (2013). *Terrorism & Communication, A Critical Introduction*. London: Sage.
- May, C. (2010). *The global political economy of intellectual property rights, The new enclosures*. New York: Routledge.
- McCutcheon, M. (2007). Techno, Frankenstein and copyright. *Popular Music*, 26(2), 259-280.
- McLuhan, M. ((1964) 1994). *Understanding Media: The Extensions of Men*. Cambridge: MIT Press.
- Milan, S. (2013). *Social Movements and Their Technologies: Wiring Social Change*. New York: Palgrave Macmillan.

References

- Miles, M., Huberman, A., & Sald, J. (2014). *Qualitative Data Analysis. A Methods Sourcebook*. Thousand Oaks: Sage Publications.
- Nader, L. (1972). Up the Anthropologist – Perspectives Gained from Studying Up. In D. Hymes (Ed.), *Reinventing Anthropology* (pp. 284-311). New York: Pantheon Books.
- Nissenbaum, H. (2004). Hackers and the Contested Ontology of Cyberspace. *new media & society*, 6(2), 195-217.
- Noakes, J. (2000). Official Frames in Social Movement Theory: The FBI, HUAC, and the Communist Threat in Hollywood. *The Sociological Quarterly*, 41(4), 657-680.
- Noakes, J., & Wilkins, K. (2002). Shifting frames of the Palestinian movement in US. *Media, Culture & Society*, 24, 649-671.
- Norris, P., Kern, M., & Just, M. (2003). *Framing Terrorism*. London: Routledge.
- Oliver, P., & Johnston, H. (2000). What a Good Idea! Ideologies and Frames in Social Movement Research. *An International Journal*, 4(1), 37-54.
- Özbek, N. (2003). Alternatif tarih tahayyülleri: Siyaset, ideoloji ve Osmanlı-Türkiye tarihi. *Toplum ve Bilim*, 98, 234-254.
- Pacholok, S. (2012). Interviewing Elite Men: Feminist Reflections on Studying “Up” and Selling Out. In L. Aguiar, & C. Schneider (Eds.), *Researching Amongst Elites* (pp. 199-215). Farnham: Ashgate Publishing.
- Panitch, L., & Gindin, S. (2005). Superintending global capital. *New Left Review*, 35, 101-123.
- Polat, B., Tokgöz Bakıroğlu, C., & Demirhan Sayın, M. (2013). Hactivism in Turkey: The Case of Redhack. *Mediterranean Journal of Social Sciences*, 4(9), 628-636.
- Poulantzas, N. ((1968) 1978). *Political Power & Social Classes*. (T. O'Hagan, Trans.) London: Verso.
- Pratt, J. ((2002) 2013). Critical criminology and the punitive society: some new ‘visions of social’. In R. Hogg, & K. Carrington (Eds.), *Critical Criminology: Issues, Debates, Challenges* (pp. 168-184). London: Willan Publishing.
- Presdee, M. (2000). *Cultural Criminology and the Carnival of Crime*. London: Routledge.
- Quinney, R. (1977). *Class, State and Crime, On the Theory and Practice of Criminal Justice*. New York: David McKay Company, Inc.
- Rawls, J. ((1971) 1999). *A Theory of Justice*. Cambridge: Harvard University Press.

References

- Reese, S. (2010). Finding Frames in a Web of Culture: The Case of the War on Terror. In P. D'Angelo, & J. Kuypers (Eds.), *Doing News Framing Analysis. Empirical and Theoretical Perspectives* (pp. 17-42). London: Routledge.
- Ross, J. (Ed.). (2000). *Controlling State Crime*. New Brunswick: Transaction Publishers.
- Samuel, A. W. (2004, September). Hactivism and the Future of Political Participation. *Unpublished doctoral dissertation*. Cambridge: Harvard University.
- Sauter, M. (2014). *The Coming Swarm, DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. Bloomsbury Academic.
- Scheufele, D. (1999). Framing as a theory of media effects. *Journal of Communication*, 49(1), 103-122.
- Scheufele, D. (2000). Agenda-Setting, Priming, and Framing Revisited: Another Look at Cognitive Effects of Political Communication. *Mass Communication & Society*, 3(2-3), 297-316.
- Schiller, D. (1999). *Digital Capitalism. Networking the Global Market System*. Cambridge: The MIT Press.
- Schrock, A. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *new media & society*, 18(4), 581-599.
- Schwartz, M., & Milovanovic, D. (Dü). (1996). *Race, Gender, and Class in Criminology*. New York: Garland Publishing.
- Scott, J. (1998). *Seeing like a State*. New Haven: Yale University Press.
- Sehl, K. (2019, 02 20). *How the Twitter Algorithm Works in 2019 and How to Make it Work for You*. Retrieved from Hootsuite: <https://blog.hootsuite.com/twitter-algorithm/>
- Sell, S. (2003). *Private power, Public law: The globalization of intellectual property rights*. New York: Cambridge University Press.
- Shantz, J., & Tomblin, J. (2013). *Cyber Disobedience: Re://Presenting Online Anarchy*. Hants: Zero Books.
- Sim, J. (2004). The Victimised State and the Mystification of Social Harm. In P. Hillyard, C. Pantazis, S. Tombs, & D. Gordon (Eds.), *Beyond Criminology, Taking Harm Seriously* (pp. 113-132). London: Pluto Press.
- Snow, D., & Benford, R. (1988). Ideology, Frame Resonance, and Participant Mobilization. *International Social Movement Research*, 1, 197-217.
- Snow, D., & Benford, R. (1992). Master Frames and Cycles of Protest. In A. Morris, & C. McClurg Mueller (Eds.), *Frontiers in Social Movement Theory* (pp. 133-155). New Haven: Yale University Press.

References

- Sozeri, E. (2016, 09 30). RedHack Leaks Reveal the Rise of Turkey's Pro-government Twitter Trolls. Retrieved from <https://www.dailydot.com/layer8/redhack-turkey-albayrak-censorship/>
- Springhall, J. (1998). *Youth, Popular Culture and Moral Panics*. London: Palgrave.
- Steinmetz, K. (2016). *Hacked, A Radical Approach to Hacker Culture and Crime*. New York: New York University Press.
- Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks: Sage Publications.
- Sumner, C. (2004). The Social nature of crime and deviance. In C. Sumner (Ed.), *The Blackwell Companion to Criminology* (pp. 1-31). Oxford: Blackwell Publishing.
- Tanczer, L. (2016). Hactivism and the male-only stereotype. *new media & society*, 18(8), 1599-1615.
- Tanczer, L. (2017). The Terrorist – Hacker/Hactivist Distinction: An Investigation of Self-Identified Hackers and Hactivists. In M. Conway, L. Jarvis, O. Lehan, S. Macdonald, & L. Nouri (Eds.), *Terrorists' Use of the Internet* (pp. 77-92). Amsterdam: IOS Press.
- Tarrow, S. ((1994) 2011). *Power in Movement. Social Movements and Contentious Politics*. Cambridge: Cambridge University Press.
- Tatar, Ü., & Çelik, M. (2015). Hactivism as an emerging cyberthreat: Case study of a Turkish hactivist group. In L. Jarvis, S. MacDonald, & T. Chen (Eds.), *Terrorism Online. Politics, Law and Technology* (pp. 54-71). London: Routledge.
- Taylor, P. (2004). Hactivism – Resistance is Fertile? In C. Sumner (Ed.), *The Blackwell Companion to Criminology* (pp. 486-500). Oxford: Blackwell Publishing.
- Thatcher, S. (2006). The Hunt for the paper tiger: The Social construction of cyberterrorism. *Unpublished doctoral dissertation*. London: London School of Economics and Political Science.
- Thomas, D. (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.
- Thomas, D. (2005). Hacking the body: code, performance and corporeality. *new media & society*, 7(5), 647–662.
- Tierney, J. (2009). *Key Perspectives in Criminology*. McGraw-Hill Education.
- Tilly, C. (1985). War Making and State Making as Organized Crime. In P. Evans, D. Rueschemeyer, & T. Skocpol (Eds.), *Bringing the State Back In* (pp. 169-191). Cambridge: Cambridge University Press.
- Turk, A. (1972). *Legal Sanctioning and Social Control*. Rockville: National Institute of Mental Health Center for Studies of Crime and Delinquency.

References

- Türkiye'de Bilişim Hukuku*. (2016, 11 29). Retrieved from Bilgi Teknolojileri ve İletişim Kurumu: <http://internet.btk.gov.tr/turkiye-de-bilisim-hukuku-detay-70.html>
- Uçkan, Ö. (2013). Dijital Aktivizmin Sınır Boyunda Hacktivizm: Anonymous ve RedHack örnekleri... In A. Keleş, & Y. Sal (Eds.), *Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi* (pp. 53-79). Istanbul: Alternatif Bilişim Derneği.
- Üstel, F. ((2004) 2008). *"Makbul Vatandaş"ın Peşinde*. Istanbul: İletişim.
- Van Gorp, B. (2010). Strategies to Take Subjectivity Out of Framing Analysis. In P. D'Angelo, & J. Kuypers (Eds.), *Doing News Framing Analysis. Empirical and Theoretical Perspectives* (pp. 84-109). London: Routledge.
- Vegh, S. (2002). Hacktivists or cyberterrorists? The changing media discourse on hacking. 7(10).
- Vegh, S. (2005). The Media's Portrayal of Hacking, Hackers, and Hacktivism Before and After September 11. *First Monday*, 10(2).
- Vlavo, F. (2015). Framing Digital Activism: The Spectre of Cyberterrorism. *First Monday*, 20, 1-12.
- Wacquant, L. (2016). Bourdieu, Foucault, and the Penal State in the Neoliberal Era. In D. Zamora, & M. Behrent (Eds.), *Foucault and Neoliberalism* (pp. 114-133). Malden: Polity Press.
- Walgrave, S., & Manssens, J. (2000). The making of the white march: The mass media as a mobilizing alternative to movement organizations. *Mobilization*, 5(2), 217-239.
- Wall, D. (2008). Cybercrime and the culture of fear. *Information, Communication & Society*, 11(6), 861-884.
- Wall, D. (2012). The Devil Drives a Lada: The Social Construction of Hackers as Cybercriminals. In C. Gregoriou (Ed.), *Constructing Crime* (pp. 4-18). London: Palgrave Macmillan.
- Weber, M. ((1919) 1946). Politics as a Vocation. In H. Gerth, & C. Mills (Eds.), *From Max Weber: Essays in Sociology* (H. Gerth, & C. Mills, Trans., pp. 77-128). New York: Oxford University Press.
- Welch, M. (2006). *Scapegoats of September 11th : hate crimes & state crimes in the war on terror*. New Brunswick: Rutgers University Press.
- Weller, K., Bruns, A., Burgess, J., Mahrt, M., & Puschmann, C. (2014). Twitter and Society: An Introduction. In K. Weller, A. Bruns, J. Burgess, M. Mahrt, & C. Puschmann (Eds.), *Twitter and Society* (pp. xxix-xxxviii). New York: Peter Lang Publishing.
- Williams, R. (1977). *Marxism and Literature*. Oxford: Oxford University Press.

References

- Wray, S. (1998). Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics. *Switch: New Media Journal*, 4(2). Retrieved from <http://switch.sjsu.edu/web/v4n2/stefan/>
- Wykes, M., & Marcus, D. (2009). Cyber-terror. In Y. Jewkes, & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 214-229). Routledge.
- Yaman, A. (2014). *The Gezi Park protests: The impact on freedom of expression in Turkey*. London: English PEN.
- Yaman, U. (2013). Hack'ikatin Red'di. In A. Keleş, & Y. Sal (Eds.), *Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi* (pp. 48-52). Istanbul: Alternatif Bilişim Derneği.
- Yar, M. (2006). *Cybercrime and Society*. London: SAGE Publications.
- Yegen, C. (2014). Dijital Aktivizmin bir Türü olarak Hacktivizm ve "Redhack". *E-journal of Intermedia*, 1(1), 118-132.
- Yesil, B. (2016). *Media in New Turkey. The Origins of an Authoritarian Neoliberal State*. Urbana: University of Illinois Press.
- Yesil, B., Sözeri, E., & Khazraee, E. (2017). *Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance*. The Internet Policy Observatory (IPO). Retrieved from http://repository.upenn.edu/internetpolicyobservatory/22/?utm_source=repository.upenn.edu%2Finternetpolicyobservatory%2F22&utm_medium=PDF&utm_campaign=PDFCoverPages
- Yıldırım, B. (2014). *Sanki Devrim*. Istanbul: Nota bene.
- Yip, M., & Webber, C. (2011). Hacktivism: a Theoretical and Empirical Exploration of China's Cyber Warriors. *Websci'11*. Koblenz.
- Young, J. (1971). The Role of the Police as Amplifiers of Deviancy, Negotiators of Reality and Translators of Fantasy: Some Consequences of our Present System of Drug Control as Seen in Notting Hill. In S. Cohen (Ed.), *Images of Deviance* (pp. 27-61). Harmondsworth: Penguin.
- Yörük, E., & Yüksel, M. (2014). Class and politics in Turkey's Gezi protests. *New Left Review*, 89(1), 103-123.
- Zajác, R. (2013). WikiLeaks and the problem of anonymity: A network control perspective. *Media, Culture & Society*, 35(4), 489-505.
- Zuo, J., & Benford, R. (1995). Mobilization Processes and the 1989 Chinese Democracy Movement. *The Sociological Quarterly*, 36(1), 131-156.

APPENDIX:

APPLICABLE ARTICLES IN JUDICIAL PROCESSES RELATED TO REDHACK⁶⁷

TURKISH PENAL CODE (Act Nr. 3713, 2004)

CHAPTER II: Offences Against the Person

Part 9: Offences Against Privacy and Confidentiality

Illegally Obtaining or Giving Data

Article 136

(1) Any person who illegally obtains, disseminates or gives to another person someone's personal data shall be sentenced to a penalty of imprisonment for a term of two to four years.

CHAPTER III: Offences Against the Public

Part 5: Offences against Public Peace

Establishing Organisations for the Purpose of Committing Crimes

Article 220

⁶⁷ <https://www.legislationline.org/> is used for the translation of articles from Turkish Penal Code and from Law on Fight Against Terrorism in Turkey.

- (1) Any person who establishes or manages an organisation for the purposes of committing offences proscribed by law shall be sentenced to imprisonment for a term of two to six years provided the structure of the organisation, number of members and equipment and supplies are sufficient to commit the offences intended. However, a minimum number of three persons is required for the existence of an organisation.
- (2) Any person who becomes a member of an organisation established to commit offences shall be sentenced to a penalty of imprisonment for a term of one to three years.
- (3) If the organisation is armed, the penalty stated in aforementioned paragraphs will be increased from one fourth to one half.
- (4) If an offence is committed in the course of the organisation's activities, then an additional penalty shall be imposed for such offences.
- (5) Any leaders of such organisations shall also be sentenced as if they were the offenders in respect of any offence committed in the course of the organisation's activities.
- (6) (Amended on 2/7/2012 - By Article 85 of the Law no. 6352) Any person who commits an offence on behalf of an organisation, although he is not a member of that organisation, shall also be sentenced for the offence of being a member of that organisation. The sentence to be imposed for being a member of that organization may be decreased by half.
(Additional Sentence: 11/4/2013 - By Article 11 of the Law no. 6459) This provision shall only be applied in respect of armed organizations.
- (7) (Amended on 2/7/2012 - By Article 85 of the Law no. 6352) Any person who aids and abets an organisation knowingly and willingly, although he does not belong to the structure of that organisation, shall also be sentenced for the offence of being a member of that organisation. The sentence to be imposed for being a member of that organization may be decreased by one-third according to the assistance provided.
- (8) A person who makes propaganda for an organization in a manner which would legitimize or praise the terror organization's methods including force, violence or threats or in a manner which would incite use of these methods shall be sentenced to a penalty of

imprisonment for a term of one to three years. If the said crime is committed through the press or broadcasting the penalty to be given shall be increased by half.

Part 10: Offences Related to Data Processing Systems

Accessing a Data Processing System

Article 243

(1) Any person who unlawfully accesses, partially or fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.

(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.

(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.

Preventing the Functioning of a System and Deletion, Alteration or Corrupting of Data

Article 244

(1) Any person who prevents the functioning of a data processing system or renders such useless shall be subject to a penalty of imprisonment for a term of one to five years.

(2) Any person who deletes, alters, corrupts or bars access to data, or introduces data into a system or sends existing data to another place shall be subject to a penalty of imprisonment for a term of six months to three years.

(3) Where this offence is committed in relation to a data processing system of a public institution or establishment, bank or institution of credit, then the penalty to be imposed shall be increased by one half.

(4) Where a person obtains an unjust benefit for himself or another by committing the acts defined in the aforementioned paragraphs, and such acts do not constitute a separate

offence, he shall be subject to a penalty of imprisonment from two years to six years and a judicial fine of up to five thousand days.

CHAPTER IV: Offences against Nation and State and Final Provisions

Part 5: Offences against the Constitutional Order and its Functioning

Violation of the Constitution

Article 309

(1) Any person who attempts to abolish, replace or prevent the implementation of, through force and violence, the constitutional order of the republic of Turkey shall be sentenced to a penalty of aggravated life imprisonment.

(2) Where any other offences are committed during the commission of this offence, an additional penalty for such offences shall be imposed according to the relevant provisions.

(3) Legal entities shall be subject to security measures specific to them for the commission of offences defined in this article.

Armed Organisation

Article 314

(1) Any person who establishes or commands an armed organisation with the purpose of committing the offences listed in parts four and five of this chapter, shall be sentenced to a penalty of imprisonment for a term of ten to fifteen years.

(2) Any person who becomes a member of the organisation defined in paragraph one shall be sentenced to a penalty of imprisonment for a term of five to ten years.

(3) Other provisions relating to the forming of an organisation in order to commit offences shall also be applicable to this offence.

Part 7: Offences Against State Confidentiality and Espionage

Documents Relating to State Security**Article 326**

(1) Any person who, partially or completely, destroys or damages documents or certificates relating to the security, or domestic or foreign political interests of the State, or who falsifies, steals or, by deception, removes them or makes use of them, even temporarily, outside their assigned place, shall be sentenced to a penalty of imprisonment for a term of eight to twelve years.

(2) If the aforementioned acts are committed during wartime or jeopardise the State's preparations for war or its effectiveness in war or its military movements, the penalty of life imprisonment shall be imposed.

Securing Information relating to State Security**Article 327**

(1) Any person who secures information that, due to its nature, is to be kept confidential for reasons relating to the security, or domestic or foreign political interests of the State shall be sentenced to a penalty of imprisonment for a term of three to eight years.

(2) If the act has been committed in wartime or has jeopardised the State's preparations for war or effectiveness in war or military movements, a penalty of life imprisonment shall be imposed.

Disclosure of Information Relating to the Security and Political Interests of the State**Article 329**

(1) Any person who discloses information that, due to its nature, must be kept confidential for reasons relating to the security, or domestic or foreign political interests of the State shall be sentenced to a penalty of imprisonment for a term of five to ten years.

2) If the act has been committed during wartime or has jeopardised the State's preparations for war, effectiveness in war or its military movements, the offender shall be sentenced to a penalty of imprisonment for a term of ten to fifteen years.

(3) If the act has been the result of recklessness on the part of the offender, the offender shall be sentenced to a penalty of imprisonment for a term of six months to two years in circumstances described in paragraph one and for a term of three to eight years in any of the circumstances described in paragraph two.

Securing Prohibited Information

Article 334

(1) Any person who secures information that, due to its nature, must be kept confidential and the disclosure of such has been prohibited by a regulatory act of a competent authority in accordance with the law shall be sentenced to a penalty of imprisonment for a term of one to three years.

(2) Where this act jeopardizes the State's preparations for war, its effectiveness in war or its military movements, the offender shall be sentenced to a penalty of imprisonment for a term of five to ten years.

LAW ON FIGHT AGAINST TERRORISM OF TURKEY (Act Nr. 3713, 1991)

CHAPTER ONE: DEFINITION AND TERRORIST OFFENCES

Definition of terrorism

Article 1

Any criminal action conducted by one or more persons belonging to an organisation with the aim of changing the attributes of the Republic as specified in the Constitution, the political, legal, social, secular or economic system, damaging the indivisible unity of the State with its territory and nation, jeopardizing the existence of the Turkish State and the Republic, enfeebling, destroying or seizing the State authority, eliminating basic rights and

freedoms, damaging the internal and external security of the State, the public order or general health, is defined as terrorism.

Terrorist offender

Article 2

Any person, who, being a member of organisations formed to achieve the aims specified under Article 1, in concert with others or individually, commits a crime in furtherance of these aims, or who, even though does not commit the targeted crime, is a member of the organisations, is defined as a terrorist offender.

Persons who, not being a member of a terrorist organisation, commit a crime in the name of the organisation, are also considered as terrorist offenders and shall be punished as members of such organisations.

Terrorist offences

Article 3

Offences defined under articles 302, 307, 309, 311, 312, 313, 314, 315, 320, and paragraph 1 of art. 310 of the Turkish Penal Code dated 26 September 2004, Act Nr. 5237, are terrorist offences.

Offences committed with terrorist aims

Article 4

Offences specified below are considered as terrorist offences if they are committed within the framework of activities of a terrorist organisation:

a) Offences defined under articles 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318, 319 and paragraph 2 of article 310 of the Turkish Penal Code

b) Offences defined under the Law on Firearms, Knives and Other Instruments, dated 10 July 1953, Act Nr. 6136

c) Offences of intentional forest arson, as defined under paragraphs 4 and 5 of article 110 of the Law on Forests, dated 31 August 1956, Act Nr. 6831

ç) Offences punishable by imprisonment defined under the Law on Fight Against Contraband, dated 10 July 2003, Act Nr. 4926

d) When committed within regions, in which a state of emergency has been declared according to article 120 of the Constitution, offences relating to events that have lead to the declaration of the state of emergency

e) The offence defined under article 68 of the Law on the Protection of Cultural and Natural Assets, dated 21 July 1983, Act Nr. 2863

Terrorist organisations

Article 7

Those who establish, lead, or are a member of a terrorist organisation in order to commit crimes in furtherance of aims specified under article 1 through use of force and violence, by means of coercion, intimidation, suppression or threat, shall be punished according to the provisions of article 314 of the Turkish Penal Code. Persons who organise the activities of the organisation shall be punished as leaders of the organisation.

Any person making propaganda for a terrorist organisation shall be punished with imprisonment from one to five years. If this crime is committed through means of mass media, the penalty shall be aggravated by one half. In addition, editors-in-chief (...) who have not participated in the perpetration of the crime shall be punished with a judicial fine from one thousand to fifteen thousand days' rates. However, the upper limit of this sentence for editors-in-chief is five thousand days' rates. The following actions and behaviours shall also be punished according to the provisions of this paragraph:

a) Covering the face in part or in whole, with the intention of concealing identities, during public meetings and demonstrations that have been turned into a propaganda for a terrorist organisation

b) As to imply being a member or follower of a terrorist organisation, carrying insignia and signs belonging to the organization, shouting slogans or making announcements using audio equipment or wearing a uniform of the terrorist organization imprinted with its insignia

If the crimes indicated under paragraph 2 were committed within the buildings, locales, offices or their annexes belonging to associations, foundations, political parties, trade unions or professional organisations or their subsidiaries, within educational institutions, students' dormitories or their annexes, the penalty under this paragraph shall be doubled.

