Contextualizing Hacktivism: The Criminalization of Redhack

Bülay Doğan

Follow this and additional works at: https://repository.upenn.edu/cargc_papers

Part of the Communication Commons, and the Law Commons

This paper is posted at ScholarlyCommons. https://repository.upenn.edu/cargc_papers/10
For more information, please contact repository@pobox.upenn.edu.
Contextualizing Hacktivism: The Criminalization of Redhack

Description
Through an empirical examination of the criminalization of the Turkish hacktivist group Redhack in social, legal, and cultural discourses, CARGC Paper 10 – “Contextualizing Hacktivism: The Criminalization of Redhack” by Bülay Doğan – explores the critical conflation of hacktivism with cyber-terrorism that enables states to criminalize non-violent hacktivist groups.

Disciplines
Communication | Law

Creative Commons License
This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License.
Contextualizing Hacktivism: The Criminalization of Redhack
I am delighted to introduce Bülay Doğan’s CARGC Paper 10, “Contextualizing Hacktivism: The Criminalization of Redhack.” Bülay was a Fellow at the Center for Advanced Research in Global Communication in 2017-2018, a Fulbright Scholar, and a PhD candidate at the Department of Media and Visual Arts in Koç University in Istanbul, studying the interaction of social movements and ideology with science and technology, in addition to information technology and criminal law. She is also one of the founders and executive board members of Ozgen Berkol Doğan Science Fiction Library, a unique association specialized in science-fiction, fantasy, and horror literatures in Turkey.

CARGC Paper 10 is an original contribution to the literature on hacking, hacktivism, criminalization and the state. Through a meticulous empirical examination of the criminalization of the Turkish hacktivist group Redhack, Doğan explores the critical conflation of hacktivism with cyber-terrorism—by national security organizations and academic researchers alike—that enables states to criminalize non-violent hacktivist groups. The paper’s empirical sources include interviews with Turkish security agents, legal and regulatory texts, and its theoretical grounding is a combination of literatures on moral panic, hacking, social movements, critical criminology, and framing analysis. In examining how Redhack constitutes an anomaly, and in exploring how anomalies point to the necessity of grounded, context-sensitive research, Doğan contributes conceptual development beyond Turkey and beyond hacktivism. In doing so, this publication embodies CARGC’s mission to set regional expertise and theoretical advancement in a heuristic tension with each other.

CARGC Paper 10 is our first publication under our recently launched research theme, “Digital Sovereignties,” which will shape research groups, lectures and conferences at CARGC from 2018 to 2023. The recent return of populism, chauvinism and protectionism have reasserted a pugnacious nationalism vitally concerned with territorial control and cultural purity, as satellites, drones, cyberwarfare, and digital platforms further erode sovereignty. Questions we will explore under this theme include: How have social media altered our understandings of sovereignty? How are notions of political, cultural and sexual sovereignty shifting in the digital era? How have non-state actors affected and exploited these changes? Should we rethink our theories of geopolitics in light of algorithmic communication and digital disinformation? Do the combined geopolitics of infrastructure, data, artificial intelligence and cyberwarfare portend a new global order?

In addition, as we embark on our sixth year, we at CARGC are happy to announce that we have six outstanding postdoctoral fellows in residence in 2018-2019. They will be working with CARGC Doctoral, Undergraduate, and Faculty Fellows on individual and collaborative research projects. They will also lead the inaugural edition of South by Southeast: the CARGC Fellows Biennial Conference, which will be held in March 2019. You can read more about our established and new initiatives in CARGC@5, a detailed report about our first five years, released in July 2018.
As you read CARGC Paper 10, please check out our other CARGC Papers, CARGC Briefs, and special issues of journal articles co-published by CARGC Press. If you like what you read, please spread the word about us, and help us fulfill our mission in nurturing emerging scholars worldwide.

Marwan M. Kraidy  
Professor of Communication  
The Anthony Shadid Chair in Global Media, Politics & Culture  
Director, Center for Advanced Research in Global Communication (CARGC)  
@MKraidy
Contextualizing Hacktivism: The Criminalization of Redhack

INTRODUCTION

This CARGC Paper examines the criminalization of Redhack, a hacktivist group that was very active between 2012 and 2017 in Turkey. Although they were founded in 1997, their activity started to peak in 2012, which also happened to be the year of global uprisings like the “Arab Spring” and the Occupy movement. For Turkey, it was the year that mounting frustration against the Justice and Development Party government (known by its Turkish acronym, AKP) boiled over into the mass popular uprising of the Gezi protests.

The most difficult aspect of a scholarly analysis of Redhack is to decide which path to follow for a rigorous examination. In both popular imagery and academic literature, Redhack is a peculiar object of study for many reasons. Redhack are a group of hackers, objects of fear and fascination at the same time, but they are also activists, to which academic interest has turned in the aftermath of global tumults. Moreover, the activism of Redhack is not limited to the ideology widespread among new social movements but includes a class-based activism articulated, in the group’s own words, through a Marxist-Leninist ideology. This characteristic coincides with the renascent interest in Leninism in academia and in political discussions.¹ Another layer of fascination for Western audiences is that this group is in Turkey. Through this Orientalizing lens — according to which the only political alternative to capitalism in the Middle East is either moderate Islam, compatible with market economy and ‘human rights,’ like the Justice and Development Party (AKP) of Recep Tayyip Erdoğan between 2002 and 2007, or radical Islam, like the Islamic State of Syria and Iraq (ISIS) — Redhack appears as an anomaly. The presence of anticapitalist, anarchist, or socialist alternatives in Middle East, in Turkey, is an uncommon phenomenon in the perception of many US and Europe-based academics.

I structured my approach to the case study of Redhack by recognizing these particularities of representation. Is Redhack an anomaly, in the sense that they were transgressing the boundaries of normality demarcated by the presumptions mentioned above? Other questions followed, like what are the boundaries of normality? Who draws these boundaries? When are these boundaries activated and in which fields are they present? This led me to these further question, if Redhack is an anomaly, what might it tell us about the Turkish context in which it is found and

¹ The interest in Leninism is noticeable in the writings of different scholars in the wake of the global uprisings of 2010s. Alain Badiou, Etienne Balibar, Daniel Bensaïd, Alex Callinicos, Terry Eagleton, Fredric Jameson, Antonio Negri, and Slavoj Žižek are some of the popular leftist thinkers who have written on Leninism in the 2000s and whose speech and writings were collected in Lenin Reloaded: Toward a Politics of Truth (Budgen, Kouvelakis and Žižek 2007). Other than this tendency to revalorize Leninist principles, there is another conceptualization of Leninism as “the Leninist right” with an effort to understand the nature of the recent rise of the right in the US (Tuğal 2017) and in Europe (Applebaum 2017).
about the phenomenon called hacktivism? In this CARGC Paper, I respond to these questions through the case study in which I problematize the anomaly of Redhack by critically examining the legal boundaries governing the group.

Being an anomaly is closely related to transgressing boundaries, which is always a powerful act, since such a crossing affects the boundaries themselves. Transgressions always have the potential to blur the area demarcated by these boundaries. In the case of Redhack, among many boundaries that can be problematized, I decided to examine legal boundaries.

A rich theoretical literature has examined how legal boundaries of normality can be problematized through the concept of exception. From Schmitt (2005) to Agamben (2005) and to Neocleous (2006), discussions have focused on deviations from norms, humans in the state of exception, perpetuity versus provisionality of exception, and whether exception is a fact that is intrinsic to capitalism or not. Appreciating these theoretical discussions, I tend towards a more sociological direction to examine the transgression of legal boundaries in Turkey through the example of Redhack.

Legal boundaries first seem like the easiest act of transgression for the social scientist to trace because of the presence of clear, written, demarcations of these boundaries. In general, it is the specific mission of the judicial body of nation-states to determine whether legal transgressions occur in order to decide who the criminal is. Yet, since the pioneering work of Howard Becker (1963), scholars from the fields of the sociology of deviance as well as critical criminology have problematized the processes of legal transgression. As this body of work demonstrates, legal transgression may actually be the most difficult act to trace. Even though it seems like it is exclusively dependent on judicial power, in fact, many social actors with power label others as criminals and are thus involved in demarcating the processes of legal transgression. Building on this scholarly work, I also adopt a social constructionist perspective of crime and understand crime not as a definite fact but as a process of criminalization. Thus, I pursue my research questions via an examination of how hacktivists in Turkey, based on the prominent example of Redhack, are criminalized in social, legal, and cultural discourses. That is, CARGC Paper 10 examines the seeming anomaly of Redhack in order to explore the criminalization of hacktivism in Turkey since 2012.

The larger dissertation project on which this paper draws is a multi-sited study that acknowledges how criminalization discourse for hacktivists is framed by different bodies of agents. I look at three specific sites for the examination of this discourse in Turkey for the time period between 2012 and 2017. In an ideal level, these sites are those who label (the state agents), those who are labelled (Redhack) and those who perceive and discuss this labelling (the public discourse visible in the mass media). However, as I mentioned above, at the material level, these categories are not strictly separate sites because they have serious effects on each other to construct, reconstruct, and deconstruct the criminalization discourse and the labelling processes. Within the limits of CARGC Paper 10, the focus of my case study is the state discourse, the discourse that first labels Redhack a legal anomaly.
I will proceed as follows: First, starting with attempts to define hacktivism as a neologism, (1a) I examine the divide between hacker and hacktivist. Next, (1b) I explore how hacking is represented in popular culture and how its relationship to moral panics constitute another main component of this crucial context. Then, (1c) I analyze representations of hacktivists within the wave of global protests of the 2010s. Secondly, I (2a) situate the case study of Redhack by referring to two bodies of work – critical criminology and framing theory. These overlapping spheres of literature allow me to view criminalization discourse in Turkey between 2012 and 2017. With a focus on state discourse, which fits the first category of the larger project, I (2b) analyze the criminalization framing of Redhack in judicial documents, in news about Redhack and in interviews that I conducted with experts on Redhack from and outside of the Turkish state. Third, in the section dedicated to my case study, I (3) exhibit discussions based on three findings: the centrality of the Turkish state, the general discourse of terrorism in Turkey, and the prominence of the hacktivist craftsman. Last, in the conclusion, I (4) return once again to my initial questions about the anomaly of the case study after the examination of the discussions based upon the research question of how Redhack is criminalized in Turkey to develop a new understanding of the literature of hacktivism as well as to contribute to Turkish studies.

**ENTER HACKTIVISM**

Hacktivism is a portmanteau of hacking and activism, which was coined in the US by the hacker group Cult of the Dead Cow in the 1990s (Shantz and Tomblin 2013). Many recently coined terms – digital activism, cyberactivism, e-activism, hacktivism, slacktivism, and clicktivism – are used frequently in media studies to describe emerging genres of political engagement. The proliferation of neologisms around the notion of activism is undoubtedly related to recent social phenomena. When Guobin Yang (2016) explored the cultural, social, and political implications of activism, he claimed that online activism should be thought of in the larger sociopolitical framework of activism, which for thirty years carried connotations of “moderate civic action” until the ambiguous yet significant impact of the worldwide uprisings and anti-austerity movements in the 2010s. The Indignados movement in Spain, Arab uprisings, Occupy movement in the US, and Gezi protests in Turkey can be cited as some of the examples.

From this perspective, neologisms about online activism correspond to new practices as “a promise for many retransformation toward a more radical grassroots politics” together with an opposite “pull toward depoliticization” through which radical elements are erased from the online activism discourse, especially in the Western context (Yang 2016, 6-7). However, an inquiry into the implications of neologisms should also include academic fields, which contribute to the popularization of these neologisms. Is there a reason other than recent social phenomena that a neologism like “hacktivism” becomes widespread in media activism studies? My answer is that this inclination corresponds to an effort of self-vindication. From this problematic perspective, ‘old’ terms of ‘old’ media and of ‘old’ social movements are considered incapable of capturing the novelties of the computer, internet, and social media ages, and now maybe the
application age. This technological determinism reflects the presentism related to the internet and a delusion of the internet as something always excitingly new, even though a quarter of a century has passed since its public commercial use at the beginning of the 1990s.

Putting aside the deficiency of the field of media activism, neologisms are bound to remain artificial unless they are supported by concrete experiences of media users. Hacktivism is a fortunate neologism because it is robustly supported by the actors themselves. Different experiences of collective action during the 1990s and the 2000s made hacktivism visible around the world. The Chaos Computer Club (CCC) is one of the first examples of hacktivism. This group did not just shut down websites but also attempted to disturb telecommunication infrastructures in protesting against censorship and protests against nuclear testing in the late 1980s (Anderson 2008, 5). Electronic Disturbance Theatre (EDT), which supported the Zapatista movement using internet technologies in 1998, and the Electrohippies, which participated in the protests in 1999 against the World Trade Organization in Seattle, are some of the later hacktivism examples (Jordan and Taylor 2004, 71-79).

In these first outstanding instances of hacktivism, hacking was used explicitly for political purposes, following the influential definition of hacktivism of Tim Jordan and Paul Taylor (2004, 9). This definition is also in line with the definition of hacking as “the imaginative re-appropriation of technology’s potential within countercultural and oppositional communities” (Jordan and Taylor 2004, 5), an inclusive definition when we consider hacking as not just equal to cracking, which means “illicit, illegal or unwanted computer intrusion.”

However, cracking became the dominant image of hackers in popular imagination by the mid-1990s and the representation of hackers in the cultural products of this period, originating mostly from the US, would prove central in the perception of hackers and hacktivists in following periods. To understand this perception, I now turn to the popular culture of the 1990s in Turkey and in the US, as the latter deeply influenced the Turkish context.

The 1990s were the peak of the wave of fear and fascination induced by the figure of the hacker in a global popular imaginary. In this trend, born in the early 1980s and continuing to be influential in the 2010s, the hacker is a criminal, an anti-hero, and usually a dangerous male, with whom the audience easily sympathizes. The dangerous image of the hacker does not always come from their malicious intentions. Based on the earliest example of a hacker movie, WarGames (Badham 1983), Kevin Steinmetz (2016) argues that hackers are represented as intrinsically dangerous in the sense that it is their knowledge and their skills that make them dangerous (180) and while destruction can arise from “hacker’s moral alignment” (182), the risk of destruction is already there, in the figure himself.

When Ulrich Beck wrote his influential Risk Society (1992), he claimed that there was a strong relationship between “the gain in power from techno-economic ‘progress’” and the production of risks (13). Jordan and Taylor conceptualize this argument within the framework of the antagonism between “society’s increasing dependence upon complexly networked
communication technologies” and “its inability to maintain and control such technologies” (Jordan and Taylor 2004, 21). The ghostly figure of the hacker perfectly occupies this intersection of technology with the perception of risk. As “the craftsman of informatics” (Sennett 2008, 24-27), hackers are represented as if they are “omnipotent technological wizards” (Steinmetz 2016, 181). If we put these abstract portrayals of the 1990s in a historical context, hackers are constructed as the unpredictable specialists of vulnerable technologies upon which emerging neoliberal globalism heavily depends. This vulnerability became much more visible during the financial crisis of 2007-2008, provoking a concretization of fears against hackers under the label of cyberterrorism.

Parallel to the disappearance of the older meanings of hacking, including social hacking, which means the manipulation of people to gain access to real and virtual places, the image of hackers became much more restricted to virtual space. In a very short time, the representation of the virtuality via the green codes trailing vertically down the computer screen in The Matrix (The Wachowski Brothers 1999) would become the dominant paradigm of hacker imagery. It would be used repeatedly by other movies about hackers.

As most of the cultural productions about hackers come from the US, understanding the elements of this imagery within this context is important. However, it is also important to understand that the implications of such elements are not universal. When we look at Turkey for example, the hooded figure does not connote criminal activity (as it does in the US and UK contexts). In Turkey, this figure is heavily used by the news media to represent hackers during the 2010s (see Medyatava 2013; Sputnik Turkiye 2015; Ulusal Kanal 2015; Sendika 2015; Cumhuriyet 2016; CNN TURK 2016; NTV 2016; Odatv 2017; aHBR 2017; SOL 2017; Yeni Akit 2017; Türkiye Gazetesi 2018). The roots of this representation can be traced back to hacker movies. Movies about hackers have been accessible and quite influential for hacker imagery in the
Turkish media since the 1990s. By the late 1990s, the release dates of movies like The Matrix can be found in movie databases (IMDB 1999). However, the first broadcast date of earlier movies that were not released in theaters but shown on TV are more difficult to find out. This methodological problem is added to the perception of the 1990s concept, as an important feature of the Turkish TV culture. Whether it is an academic work (Fidaner 2013) or a digital post in a giant blog (umut 2003), personal stories about the influence of these hacker movies from the 1990s are visible. In his doctoral research about the hacker culture in Turkey at the beginning of the 2000s, Ufuk Eriş (2009) claims that even hackers in Turkey have knowledge about the worldwide hacker culture, limited to the hacker movies and few books translated to Turkish, based on interviews that he conducted with hackers from Turkey (177). By the 2010s, when the hooded figure became widespread in hacker movies (such as Who am I? (bo Odar 2014), Mr. Robot (Esmail, Golin and Hamilton 2015-2018), and Hacker (Satayev 2016)), these movies were released or were accessible immediately in Turkey, either through official release or unofficial online streaming. Through these movies, the centrality of the hooded figure was added to the hacker imagery.

With the rising influence of these movies, the perception of the hooded figure settled into to the public imagination not as a general representation of the criminal but as the specific representation of the hacker in Turkey. In other words, the hooded figure is directly linked to cybercrime in such contexts without any history of hood as the symbol of crime. Even a simple Google search with the word ‘hackerlar [hackers in Turkish]’ is enough to provide a sense of the imagery of hackers in Turkey. Many examples from the Turkish news media that I cited above are quite explicit about the usage of the hooded figure only for news related to computer crimes, regardless of the ideological position of the outlet. The repetitive frame of hackers as hooded figures shows that ideological divides do not always imply a divide in the framing. Whether it is a conservative leftist, or mainstream news outlet, all hacker news stories are represented with hooded figures. This nuance between ideology and framing is actually a well-developed discussion within the field of social movement studies. Departing from how both anti-abortion and pro-abortion activists framed the abortion discussion as a secular space in the 1970s, Pamela E. Oliver and Hank Johnston (2000) claim that “a simple extrapolation of the underlying ideologies” (39) cannot be a source of an extrapolation of framing. This perspective is to acknowledge the importance of both ideologies and framings without reducing one to the other, as the only way to develop the analytical tools “for talking about this fascinating instance of the same ideologies diametrically opposed” (39).

The only exception to this repetitive framing of hacker images in the Turkish news media was the now defunct IMC TV, a leftist and pro-Kurdish TV channel and news outlet. Hooded figures were not used in their news framings about hackers. This is mostly because IMC TV’s broadcasting policy was inclined towards a very specific selection of news, mostly national and explicitly political. All of the stories which they framed as cybercrime were specifically about hacktivist groups in Turkey. In these stories, they used specific imagery produced by or related to
these groups, rather than more general hacker images like hooded figures.² In other examples cited above, the hooded image is typically used for cybercrime or hacktivism issues, with the exception of new stories about specific hacktivist groups, where the images of those groups are used. It is hard to tell if IMC TV would have used the hooded figure had they broadcasted cybercrime news. However, their choice of not covering these stories is also an ideological choice. For that reason, it is fair to claim that in this particular example, the framing selection and the ideological orientation overlap.

Setting aside the framing tactics of newspapers and other outlets, a deeper analysis of the hooded figure itself reveals other issues. The hood is a great tool for anonymization. In hacker movies and TV series, the inside of the hood is sometimes visible (Mr. Robot), sometimes invisible (Hacker), and there are other times when there is a mask inside the hood (Who am I?), for added emphasis on anonymity. Anonymity provided by the hood creates an ambiguity about the identity of the hacker, the dangerous criminal. This ambiguity is solidified with the fact that tracing a cybercriminal is much more difficult than an ordinary criminal for law enforcement agents. The fear of cybercrime crystallizes in the uncertainty and the high perception of risk: anyone could be a hacker, anyone could harm you, and they would not be caught. Slowly, hackers begin to go beyond this image of the “talented nerd” who has innocent but profitable pursuits towards to be seen as an “irreducible systemic threat of digital media” in the discourse of the news media (Krapp 2005, 71).

² This argument is relatively weak because the official website of the news outlet IMC was removed after the closure of IMC TV by a police raid right after their news about the leak scandal organized by the hacker group Redhack in October 2016. I was limited to an image search in their social media accounts (Twitter and Facebook) and to other sources like YouTube for records from their broadcasting.

Figure 2: Theatrical release poster of the movie Who Am I (bo Odar 2014).
The fear of hackers relates to the well-known notion of “folk devils” in critical criminology literature. Stanley Cohen, who coined the term, describes folk devils as “actors who embody the problem and agencies who are ‘ultimately’ responsible” (Cohen 2002, xxii). Critical criminology scholars examine the different meanings that the term “folk devil” carries for various groups, as well as the process of creating a folk devil itself. This latter points to a notion closely related to the former one – moral panics, or “a condition, episode, person or group of persons to become defined as a threat to societal values and interests” (Cohen 2002, 1). According to Goode and Ben-Yehuda (2009): “To actors caught in the coils of the moral panic, folk devils are the personification of evil” (27). In this relation, moral panics create the demonized contemporary images of drug dealers, child molesters, juvenile delinquents, and terrorists, as well as the more historic images of witches and communists.

Hackers have also navigated their share of moral panics. David Wall (2012) argues that hackers are constructed as cybercriminals through a security discourse that takes its roots from social science fiction (7). Moreover, while the construction of cybercriminals lies mostly in cultural rather than scientific roots (4), there is an “unquestioning assuredness” in public opinion, fueled by policy makers, law enforcement officers, and mass media, about “the seriousness of what hackers have done” (6). At the empirical level, studies of news media coverage show how “regardless of the reality of the cyberterrorism threat,” news media constructs cyberterrorism as a security risk (Jarvis, Macdonald and Whiting 2015). From the perspective of philosophy and politics of technology, Nissenbaum argues that there are two reasons for “demonizing hackers” (another way to describe the transformation of hackers into folk devils): 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 (Nissenbaum 2004, 199-200). Through the lens of critical criminology, Bowman-Grieve (2015) also emphasizes how mobilizing fear can be an instrument to promote social control, especially thinking about terrorism and cyberterrorism (103), two issues that will be of much more relevance in my later discussion on the criminalization of hacktivists.

Compared to the popular yet dangerous villains of film and news media, the image of the anonymized cybercriminal is the culmination of a much more politically loaded process of signification. Images are always central in moral panics and most commonly, moral panics function through “suasive images” that make meanings easy to grasp and that arouse emotions (Goode and Ben-Yehuda 1994) 2009, 27). The hooded image of hackers carries the vulnerability of global systems dependent on digital networks, increases fear of ambiguous cybercrime, and blurs the boundaries of who is and who is not the good citizen. Hackers as folk devils are much more complicated than previous folk devils because of the ambiguity of this representation. Yet, it would be unfair to say that this construction results just from the efforts of agencies of social control in the society. Hacktivists also embrace this anonymized popular image in their own way.
The performance of hackers and hacktivists differ from each other in the way they act and in the way they claim their deeds. Even though both identities are well invested in recognition, hackers mostly seek internal recognition from the hacker community, while hacktivists work for recognition by a wider audience. Most hackers use pseudonyms to achieve anonymized recognition. As hacktivists are political actors acting collectively, individual pseudonyms are insufficient to meet their need for recognition. Therefore, they seek a personally anonymized yet collectively distinguishable recognition. Then another tool comes onto the scene – masks.

The Guy Fawkes mask is one the most popular masks of the 2010s thanks to its shared usage by protestors all over the world. However, before the wave of Occupy movements and the Arab uprisings, it was the hacktivist group Anonymous who first collectivized the mask by borrowing it from internet forums to use in simultaneous street/offline protests against the Scientology Church in February 2008, as a follow-up to previous online protests (Deseriis 2015, 184). Originally, the Guy Fawkes mask referred to the seventeenth-century English Catholic revolutionary Guy Fawkes who tried to explode the House of Lords. This event, called the Gunpowder Plot, was commemorated in Great Britain by burning effigies of unpopular figures for more than two centuries. The stylized Guy Fawkes mask was first designed for the comic book V for Vendetta (Moore and Lloyd 1988-1989) but its spike in usage as a symbol in protest coincides with the eponymous movie (McTeigue 2005), adapted from the comic. When Anonymous began to use the mask in their video messages, it became the overarching symbol of the group.

According to art historian Broeckmann (2017), the Guy Fawkes mask is an example of how the human face has an important role in images of anonymity (400). In his work on political iconography, Kohns (2013) supports this argument by claiming that “a mask performs a double gesture: By veiling one face, it makes visible another” (93). Related to my discussion of folk
devils, the Fawkes mask is a transformative appropriation of anonymity by the labelled ones. While the mass media intensifies the fear of cybercrime by images of anonymity like hooded figures, the Guy Fawkes mask used by Anonymous makes visible the face of Guy Fawkes, an anonymous face full of historical and political meanings. In this sense, it is not just anonymity but also being a folk devil that hacktivists reappropriate.

The Guy Fawkes mask found its way to Turkey during the popular protests of 2013. Soon it was sold on every corner of Taksim Square, the main outlet of the Gezi protests in Istanbul. It became widespread during the Gezi protests but even before that, the mask was seen used by protesters who were holding banners of Redhack at May Day 2013.

Figure 4: 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.

Figure 5: Detail from “Gezi Parkı Direnişinin Sivrilen Aktörleri: Yenilmezler [Shining Actors of Gezi Park Resistance: Invincibles]” (Başka Haber 2013).

During the Gezi protests, the imagery from the photograph of a woman, relatively advanced in age, wearing traditional clothes and a Guy Fawkes mask, took its place among the imagery of the Gezi protests under the name of V for Vildan Teyze [Vildan Aunty]. It is through Vildan Aunty that the symbolic mask of the hacktivist group became one of the symbols of the Gezi protests.

Called the “Invincibles,” referring to the Turkish translation of the Hollywood movie The Avengers (Whedon 2012), a dozen individuals and few organizations became part of the Gezi imagery. V for Vildan Aunty was not the only figure with a hidden face from the Gezi pantheon. A black-dressed male figure with a hidden face under a red scarf was among the first four symbols of the Gezi protests. It was Redhack, the Marxist-Leninist hacktivist group. This time, distinct from the political baggage of the Guy Fawkes mask, Redhack’s red scarf was carrying other meanings and other fears: the imagery of folk devil was loaded with the history of radical left.
As did Anonymous, Redhack embraced anonymity, this time provided by the red scarf. The imagery from the documentary produced by a left-wing film production center (RED! 2013) about the group would become the representative image of Redhack, as it would repeatedly be used by the group itself, as well as the news media. The imagery of hackers and hacktivists reveals peculiarities of different subcultures worldwide and the interconnections between them. As a topic largely discussed in global media studies, these links, influences, and disconnections are embedded in their related contexts. A superficial reading that would consider hacker and hacktivist imagery in Turkey as an imitation of Anglo-American practices would be deficient if it did not include an examination of the hooded figure and its representation of crime or these examples of different shapes of anonymity with changing meanings in this discussion. So far, even though my focus was on Turkey, I examined diverse cultural meanings of hacking and hacktivism through comparisons between different contexts by following the perspective of Marwan Kraidy to consider the global not as “a settled geographical category” but as being “comprehensive” and “as a fundamental dimension of our world” (Kraidy 2018, 342). Cultural meanings of hacktivism in Turkey cannot be thought of separately from their global dimension, yet they cannot be understood without examining the embeddedness of the hacktivist culture in the Turkish context. This duality will be one of the theoretical underground streams in the remainder of this CARGC Paper.

**RED HACKERS AND HOW TO STUDY THEM**

Redhack is a hacktivist organization with a radical leftist identity, which is easily perceptible in their discourse and in their imagery. As a self-identified Marxist-Leninist hacktivist group (Redhack 2013), they diverge clearly from other hacktivist groups in Turkey, most of whom are “patriotic hackers,” those who work for the sake of nationalist causes, as defined in hacktivism.
literature (Denning 2011). Their explicitly radical political stance differentiates Redhack from other worldwide known hacktivist groups who espouse implicit libertarian and/or anarchist ideologies. Redhack does not possess just a general affinity with leftist politics in Turkey: they explicitly claim to cherish revolutionary solidarity (Redhack, Kısa Tarihçe [Short History] 2012). Even though the political ideology of the group does not correspond to other hacktivist groups’ political stances, their repertoire of contention is very similar to other hacktivists. Website defacements, Distributed Denial of Service (DDoS) attacks and information leaks are the principal tools that most hacktivist groups use in the 2010s. Redhack has defaced hundreds of public websites (and few company websites) in protest of events, to support offline protests, or to commemorate the martyrs of the revolution, a notion borrowed from leftist culture.

The group became highly popular with their first known leak from the Ankara Police Directorate website in February 2012. After the leak, Redhack publicized information about the citizen informants who had sent emails to the police directorate (Radikal 2012). This breach of the state’s website was a milestone for their judiciary history, too. Even though it was not a very crucial leak – compared to later leaks – it did serious damage to the authority of the state, resulting in an investigation that led to the first hacktivism trial in Turkey (Ankara Chief Public Prosecutor’s Office 2012). In that trial, all suspects were acquitted of “being a member of a terrorist organization, committing a crime in the name of the organization,” due to the lack of evidence (Ankara Heavy Penal Court no. 7 2015).

---

3 Some influential scholars within hacktivism literature like Dorothy E. Denning (2011) do not categorize patriotic hackers inside the hacktivism category. I find this distinction between hacktivists and patriotic hackers also very problematic, as it depends on a very abstract definition of what activism is. For that reason, instead of dissociating these categories, I put patriotic hackers under the umbrella term of hacktivism.
In May 2013, Redhack hacked and leaked documents allegedly belonging to the Gendarmerie Intelligence Department about the 2013 Reyhanli explosion. In the car bombing at Reyhanli, a Turkish town near the Syrian border, more than fifty people died and hundreds more were injured. The government claimed that this incident was the responsibility of a leftist group. The documents leaked by Redhack showed that it was the deed of Al-Qaeda and, more importantly, that law enforcement agents had intelligence about it before the explosion happened (Milliyet 2013). As a result of the leak, one private soldier who was accused of leaking state secrets spent half a year in prison before being released in November 2013 (Hürriyet, 2013); in 2016 that he was finally acquitted (Sputnik Türkiye 2016).

The last sensational leak of Redhack occurred in September 2016. The AKP government had issued a state of emergency right after the failed military coup.⁴ Even though the AKP declared that these measures were taken to consolidate the democracy, the state of emergency was used by the government to apply a large-scale purge of dissidents. In September 2016, Redhack declared that they had hacked the email account of the Minister of Energy, Berat Albayrak, also the son-in-law of President Erdoğan. They said that they would publicize the content if the leftist dissidents who had been taken into custody were not released (Birgün 2016). Redhack also stated that they witnessed preferential treatment, corruption, being a banana republic⁵, and the flattery of mass media executives in 17.3 GB of emails sent between 2000 and 2016 (Yolculuk 2016). The tight control of the government over mainstream media and social media platforms was also explicit in the leaks, as well as information about the formation of government 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 (Independent 2016). The mainstream media completely ignored the leak because of government pressure, and by December 2016, the government had begun to detain dissident journalists who had reported on the leaked emails (Bianet 2016). In October and December 2017, after one year of detention, the journalists were released (Diken 2017). As of March 2018, this case was still in process and the accused journalists were still facing charges of “being a member of a terrorist organization, committing a crime in the name of the organization,” of “making the propaganda of a terrorist organization,” and of “being a member of a terrorist organization”⁶ (Diken 2018).

⁴ This coup was allegedly caused by the Gülen movement, which is an economic and social community, politically active as the former ally and now rival of the Justice and Development Party (AKP).

⁵ A little bit distanced and simplified usage from its original meaning, banana republic is a popular term referring to non-democratic political contexts and used to criticize the prevalence of corruption and anti-democratic practices in Turkey.

⁶ In the first legal case against Redhack, the suspects were accused of being members of Redhack. In this trial, the journalists were accused of being members of different alleged terrorist organizations with opposite political ideologies, as opposed to accusations of being members of Redhack.
These cases, together with several investigations conducted by prosecutors specializing in anti-terrorism between 2013 and 2016, show the keen interest of the Turkish state in the hacktivist group and its framing not just as a criminal organization but explicitly as a terrorist organization. Even though these judicial events are concrete reflections of a criminalization process, fertile ground for an academic examination, my study on Redhack’s criminalization would not be an easy journey, mostly because of the dominant approach in the literature on hacktivism, which tends to disembed hacktivism from its contextual roots.

The early literature on hacktivism argued for a clear definition of hacktivism with a serious effort to differentiate it from cyberterrorism. For that reason, any discussion of legal transgressions is limited by the abstract categories of “civil disobedience” and “terrorism.” Scholars define hacktivism as “electronic civil disobedience” (Wray 1998), “cyber disobedience” (Huschle 2002), or simply, “a form of civil disobedience” (Krapp 2005). Even though academic works acknowledge the ambiguity of boundaries separating hacktivism from cyberterrorism, in many influential works, the definitional ambiguity between the two remains. Frequently-cited scholar in the field of hacktivism, Dorothy Denning, defines hacktivism as “operations that use hacking techniques against a target's internet site with the intent of disrupting normal operations but not causing serious damage [emphasis added]” (2001, 241). In another work, hacktivist acts are considered as “de facto illegal but not malicious acts [emphasis added]” (Auty 2004).

The repetitive effort of academia to sterilize hacktivism from the germs of terrorism should be considered within its larger sociopolitical context. Scholars study hacktivism under the heavy pressure of the label of (cyber)terrorism, which is another and much more popular category of folk devil in our era. Cohen argues that refugees and asylum seekers constituted an important category of moral panic in Europe through the 1990s (Cohen 2002, xix), associated with “bringing terror and violence” (xx). After 9/11, terrorism became a much more emphasized moral panic. For Goode and Ben-Yehuda, terrorists are the perfect example of contemporary folk devils (Goode and Ben-Yehuda 2009, 27). Bowman-Grieve (2015) is one of the first scholars to study cyberterrorism through the lens of moral panics. She claims that cyberterrorists are “vilified as the potential harbingers of social disintegration in relation to the potential attacks they could instigate using the Internet and/or IT” (2015, 99).

This context reveals the urgency behind the academic effort to distinguish hacktivism from cyberterrorism. However, I believe that this academic effort also became a part of the construction of moral panics around the subject of cyberterrorism. Moral panics are not always dependent on “noisy” constructions with public or mass media exposure. Rather, “quiet” constructions are mostly conducted by professionals, experts, and bureaucrats (Cohen 2002, xxiii). Academics should be added to this list. Their abstract categorizations and their efforts at differentiation support the construction of moral panics for cyberterrorism.

In contrast to earlier approaches that explicitly differentiated hacktivism from cyberterrorism, recent works focus on different aspects of hacktivism. Yet, in most cases, despite an implicit recognition of the distinction of hacktivist groups from cyberterrorism, they nonetheless...
reproduce the discourse of moral panics. Anthropologist Gabriella Coleman’s (2014) last book on Anonymous provides such an example. In her introduction, she shares an interesting anecdote with her readers. Widely considered to be an expert on Anonymous, Coleman was invited to the Canadian Security Intelligence Service headquarters to give a briefing about the hacktivist group. During her lecture, she outlined how she conceived of the supposed affinity between Al-Qaeda operatives and Anonymous:

I just could not fathom Al-Qaeda operatives watching Anonymous videos, much less grasping the nature of their culture or politics, and especially not the lulz. I imagined that jihadists would be rather repelled by Anonymous’ secular, infidel, offensive practices. Laughing heartily together, we all agreed that those jihadist terrorists likely did not celebrate the lulz (Coleman 2014, 15, emphasis added).

Coleman’s narrative about the briefing exhibits the widespread tendency by hacktivist specialists to differentiate hacktivism from terrorism. Coleman’s significant contribution to this effort is her emphasis on the humor of Anonymous, which is represented by “the lulz.” In her experience in Canadian security headquarters, this aspect becomes fundamental to convince intelligence analysts that Anonymous is different from terrorists like Al-Qaeda jihadists because the hacktivist group has this humor that the terrorists could not understand. This time, the humor, the laugh, the lulz, and trolling become the divergent point between hacktivism and terrorism. From this perspective, folk devils and humor cannot be compatible. The tendency to consider humor as the concretization of democratic resistance is a fetish that ignores what humor really is: one of many instruments of expression.

When cultural criminology scholars developed the method of synthesizing “structural factors with an analysis of group dynamics, ideological influence, and individual incentives and personal motivations” (Ferrell, Hayward and Young 2015, 137), they took terrorism studies a critical step further. Yet, when Ferrell, Hayward, and Young (2015) defend their position that, at the micro level, the question of how terrorists feel is as important as the questions of how they act and how they think; these feelings are restricted to “existential” feelings like “desire for excitement, desire for ultimate feeling and desire for glory” (141), as if to differentiate terrorists from ordinary people. At the end, even the critical field of cultural criminology suffers from a two-dimensional representation of terrorists, whose feelings and thoughts cannot include humor, an ordinary feeling that is inaccessible to inhumans.

Putting aside this implicit contribution to the discourse of moral panics, the effort to distinguish hacktivism from cyberterrorism creates two fundamental problems. At the theoretical level, it creates an ungrounded categorization that should be accepted to the detriment of contextual differences about what is hacktivism and what is terrorism. So, it makes hacktivism, terrorism,

---

7 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, 31). Trolls and hackers are the main actors of this subculture.
and cyberterrorism disembedded and definite categories. This is academically problematic and politically dangerous because of how it collapses all other political struggles apart from civil disobedience into the category of terrorism. What will we do when we have examples like Redhack who celebrate the lulz, in their own way, but do not fit the category of civil disobedience? These paradigms cannot provide explanation for groups like Redhack, contributing to the sense that it is an anomaly, as I pointed to in the introduction.

A more recent trend in hacktivism studies tries to problematize this disembeddedness of boundaries and develops two important perspectives. The first, like the work of Sandor Vegh (2005), emphasizes the discourse of criminalization used against hacktivists. Mainstream US media’s portrayal of hacktivism before and after 9/11 is a significant example in which this shift from criminals to cyberterrorists is considered as the “elite’s crusade” to eradicate hacking for being “an activity that may potentially threaten the dominant order” (Vegh 2005, 1). Fidele Vlavo (2015) claims that the myth of cyberterrorism was constructed in response to the concept of cyberprotest, when hacktivist groups were already performing online protest and writing about it (8). She claims:

The terms cyberterrorism and cyberprotest have been formulated to counter one another and are part of a discursive claim for political and legal recognition. What is at stake here is, on the one side, an activist re-appropriation of digital technologies and, on the other side, governmental and corporate compulsion to fully control the networks (Vlavo 2015, 9).

I find these approaches very important for the problematization of ungrounded boundaries. However, they lack another important step, which is the problematization of the categories themselves – of cyberactivism and cyberterrorism, as well as activism and terrorism.

The second recent approach to deconstructing criminalization discourse consists of making visible the self-perception of hacktivists. From this perspective, Leonie Tanczer (2017) vocalizes hacktivists’ objections to seeing hacking and hacktivism portrayed as violent acts. From the field of critical criminology, Kevin Steinmetz’s work (2016) is an interesting hybrid of criminology’s traditional preoccupation with the “actor,” similar to the anthropological interest in the “native,” and of Marxist and radical criminological perspectives, which seek to demystify the ideology surrounding hackers. Steinmetz calls for a “sensitivity to broader historical, social, economic, and political forces” in studying hackers and his book presents a good example of “situating hacking within the conflicts and contradictions of late capitalism” (Steinmetz 2016, 221).

However, his earlier emphasis on the perception of hackers limits the work in the sense of a preoccupation with the “terrorist” actor. As the label of “terrorist” actor is the product of terrorism discourse, I follow the suggestion of Hülsse and Spencer (2008) to take not the actor but the discourse of criminalization as my starting point (575-576).

The intellectual pitfalls I have tried to avoid in this CARGC Paper also provide rescue lines that I use to develop my own approach to the study of the criminalization of Redhack. I rely on two principal perspectives from different fields. The first is the constructivist turn in the field of criminology and terrorism studies.
criminology and terrorism studies. The constructivist turn in criminology coincides with the rise of critical criminology. The term *folk devils* that I introduced at the beginning of the paper is one of the main notions that I take as a reference point during my case study. From the constructivist turn in terrorism studies, Hülsse and Spencer’s aforementioned work (2008) guides me away from the preoccupation with the actor and towards attention to the discourse of criminalization. A step already taken by critical criminology scholars, this is still a heterodox approach in terrorism studies mainly because terrorists are still the most widely accepted folk devils of our era.

The other rescue line is the revival of a focus on ideology within framing theory that I borrow from social movements studies (SMS). Many of the works on the criminalization discourse about hackers and hacktivists are based on framing analysis, some cited in this paper. Based upon the influential work of Goffman (1974), framing analysis is both a favored and criticized method in the study of social movements (Oliver and Johnston 2000), in political communication (Carragee and Roefs 2004), and in cultural criminology (Hayward and Presdee 2010). Framing analysis is a shift of “focus to linguistic analysis of conversational conventions that mark the application and changes in interpretative frames” (Oliver and Johnston 2000, 40). Oliver and Johnston claim that in its current form, framing analysis is used most commonly to understand individual cognitive structures (41). They argue that to understand the social and political content of framing processes, ideologies should be taken into consideration because “framing points to process, while ideology points to content” (45). In the field of political communication, a similar perspective is articulated by Carragee and Roefs (2004) with an emphasis on “how political and social contexts shape framing contests” (214), alongside an investigation of “how the distribution of power shapes the construction and interpretation of these frames” (215). Scholars working on framing analysis in the field of communication focus mainly on the construction and circulation of frames in news media (see Entman 1993; Scheufele 2000; and Liebler, Schwartz and Harper 2009), while SMS scholars look to the frames used by the actors of social movements (Benford 1993; Gamson, Meyer and Zald 1996; and Snow 2004).

Diverging from these traditions, Carragee and Roefs (2004) defend that framing research should have three pillars: the sponsoring of frames by political actors, their usage by journalists, and their interpretation by audiences (215). I adopt their multi-sited approach and adapt it to the context of the criminalization discourse about the hacktivist group Redhack in Turkey. However, I diverge from Carragee and Roefs in their consideration of these categories as separate entities. For me, different sites of a criminalization discourse constitute a whole in which the sponsoring, the circulation, and the interpretation of certain frames intermingle. For that reason, I expand the traditional use of framing analysis for my case study. In this perspective, I examine the construction of the criminalization of the hacktivist group Redhack in the (un)official discourse through the framing analysis.
THE CONSTRUCTION OF CRIMINALIZATION

In the remainder of this CARGC Paper, I focus on how the Turkish state constructs the criminalization of Redhack. While examining state discourse, I do not consider the Turkish state as a monolithic entity. On the contrary, I problematize how different parts of the Turkish state tend to act like an indivisible whole, especially in specific political issues, which has the effect of making invisible the conflicts between power elites. My aim in this section is to make visible official and unofficial state discourses. By unofficial, I mean the discourse of state agents whose voices are not heard explicitly, but who implement official discourse. They actively shape the criminalization discourse without being recognized as the official constructors of discourse.

There are judicial actors and law enforcement agents (LEAs). There are the sources from which I collected data to examine the criminalization process of the Turkish state: court documents from the Redhack case, information on the legal investigations about Redhack collected from news media, and interviews I conducted with the unofficial constructors of the criminalization discourse.

The first Redhack-related case was the result of the breach of the Ankara Police Directorate website in February 2012, as mentioned above. The investigation of this leak led to a trial in November 2012 (Ankara Chief Public Prosecutor’s Office 2012), resulting in the acquittal of all suspects in March 2015 (Ankara Heavy Penal Court no. 7 2015). The indictment and the reasoned decision of the court are the two main written documents on which I rely. Concerning the legal investigations of Redhack, there is a scarcity of sources because these investigations are conducted under confidentiality order, which prevents access to investigation materials. For that reason, my sources are limited to what little information is shared in the mass media. Concerning the interviews, I used a snowball technique to reach interviewees who were specialized or interested in cybercrime and/or terrorism, the two main camps of official accusation towards Redhack.

The framing that the Turkish state uses for the hacktivist group Redhack is quite different from other criminalized persons or groups in the contemporary sociopolitical context. It is almost a non-framing when compared to its typical, aggressive crime framing. However, it does not mean that the Turkish state has a positive image of the group. This was an important point to consider in the methodology of my data collection. As a perfect mirror image to the hacktivism literature, naming an organization “hacktivist” implies a negative image and a non-neutral position in the eyes of state agents. For that reason, the explicit word that I used in my interviews was “hackers” rather than “hacktivists,” even though the discussion was mostly about hackers with political motivations, so implicitly with the same category as hacktivists. Judicial documents, information about the legal investigations, and my interviews reveal a pattern in which the state appears in a very central and constant role while the hackers’ position is quite ambiguous and unstable.

8 Interviewees’ interest or specialization in cybercrime or terrorism does not necessarily coincide with active duty.
The Turkish state’s presence in Turkish political discourse is always highly visible. This presence is not limited to the state agents’ discourse and it is not even restricted by the discourse. Even during quite different forms of mediation like popular protests, oppressive reactions coming from the government, municipal policy-makers, law enforcement, and judicial bodies are easily interpreted as the reactions of the state from the perspective of outsiders and dissenters to state policies. Certainly, the state has a historical centrality in the Turkish political context according to many influential scholars, like sociologist Çağlar Keyder (1987). Recent works criticize this argument of powerful state tradition for creating an antagonism between state and society that covers class contradictions and exploitation (Dinler 2003, 50). Following this criticism, political scientist Şebnem Oğuz (2009) analyzes the contemporary centrality of the state in politics as a restructuring related to the neoliberal transformation in the 1980s, resulting in “neoliberal authoritarian statism” (17), rather than because of the powerful state tradition in Turkey.

In the case of hacktivism, this centrality of the state appears once again. During the first semi-structured interview that I conducted with LEAs, my question of whether there are good hackers and bad hackers, referring to the well-known distinction between “black” and “white” hackers was responded to with “the hacker of the state is the good hacker [emphasis added]” (LEAs 1 2017). I have already mentioned above how different bodies inside the Turkish state are perceived as an indivisible whole named “the state” by outsiders. In an interactive way, these bodies – especially the “punitive” ones like law enforcement agents – self-describe as “the state,” as if the Turkish state is a homogenous and constant whole, too. It is the state’s police, the state’s army, the state’s courts, the state’s prosecutors and so on. From this perspective, hackers can belong to the state, too. Here, I use belonging in the sense of serving the ideology of the Turkish state, which is consistently framed as a constant whole. As another interviewee stated, “Hackers should act like a shield and as a sword, to prevent another attack (LEAs 4 2017). Actually, this war frame is not that unfamiliar to us when we recall that almost every antivirus software brand that we use in our computers have shields as their symbols.

This ideal hacker described by law enforcement agents corresponds to the concrete category of patriotic hackers. In Turkey, patriotic hackers existed long before the popularity of groups like Anonymous or Redhack. Ayyildız Tim and Cyberwarrior Tim are some of the well-known examples, which have been visible in the hacktivism scene since the early 2000s. In this context, Redhack is the first widely known hacktivist group in Turkey who did not espouse a nationalist ideology. Even though all contemporary hacktivist groups share a similar “digital repertoire of contention” (Earl ve Kimport 2011), the difference between them become much more apparent related to their targets. In accordance with their nationalist ideology, patriotic hackers never targeted Turkish state’s websites, while these websites were the main target of Redhack. This point emerged during the interviews, too. Redhack is “not a good hacker organization because they attacked public institutions [emphasis added]” (LEAs 1 2017).

In the Turkish language, “people” [halk] and “public” [kamu] are not overlapping terms. “People” has a class-based connotation designating lower-classes and it is a whole, separated strictly from the state. On the other hand, public means that which is not private, used often to
define urban public places that are not enclosed. But “public” also designates the ownership of the state. In this sense, public is an ambiguous term, an intermediary between two distinctly separate categories: people and the state. When state agents accuse Redhack of attacking public institutions, this accusation implies “the state” but also “the people,” without indicating either. Such an ambiguity creates an interpretative political space where different notions of people, public, and state fluidly overlap. This overlap is emphasized much more when the label of terrorism is discussed.

As a part of a recent global trend, the label of terrorism became quite popular in political discourse in Turkey starting with the military coup of 1980. Politician and economist Sungur Savran (1987) characterizes the military coup of 1980 as the erasure of the political regime, which was built upon the struggle of the working class (153). This date is an important milestone for the development of neoliberal conservative policies in the Turkish context, as the coup succeeded in totally erasing the leftist political presence, both discursively and physically. The Turkish Anti-Terror Law of 1991 is the embodiment of this, accentuated by the civil war in the Kurdish regions of Turkey, alongside the last fragments of the armed radical leftist tradition struggling for a socialist revolution in different parts of the country including the Kurdish regions. The expansion of the terrorism label is part of this larger transformation of political crimes (against the state) to terrorism acts sponsored by the Turkish state. This discursive transformation was criticized by legal scholars (Bayraktar 2015). However, through the mainstream news media’s widespread circulation, public opinion largely accepted this transformation. For that reason, it would be a mistake to consider the contemporary stretching of the term terrorism by the AKP government and especially by President Erdoğan, as something new. However, he undeniably contributed perfect examples of this legacy.

Erdoğan’s definition of “unarmed terrorists” in March 2016 was a milestone that would determine the period ahead. Advancing a new frame of terrorism, he declared: “There is no difference between terrorists and those who gave order to [influenced] the terrorists by using

---

9 On September 12, 1980, the armed forces, led by the chief of staff, General Kenan Evren, took over political power in Turkey. A state of emergency was declared. They dissolved the parliament and deposed the cabinet. All political parties and some trade union confederations were suspended. The political party leaders were arrested and mass trials were organized against political organizations from leftwing and from extreme rightwing. Those responsible for the military coup justified their actions on the civil war and on the political violence in the late 1970s. However, the coup resulted in hundreds of dismissed, imprisoned, and tortured leftists. More details about the coup can be found in Zürcher’s work (2005, 278-288).

10 After the military coup, the Kurdish movement became much more independent from the larger leftist groups in Turkey, which were diminished by imprisonment, assassination, and exile. On the other hand, the remainder of these leftist groups in Turkey tried to continue their armed struggles but they did not have the power they had in the 1970s. Against both of them, the Turkish state developed a policy of zero tolerance, which resulted in a civil war and the massacre of leftist and Kurdish militants during the horrifying days of the 1990s. This is in this political atmosphere that the Anti-terror Law was promulgated in Turkey.
its position, its pen and its title. An academic, a journalist, the director of an NGO are also terrorists” (Diken 2016). This statement dates to a period in which political conjuncture was heavily dependent on the use of violence. While the Turkish state was using violence against civilians in Kurdish regions, suicide bombings had become a political tool used by ideologically diverse groups like ISIS and TAK, an armed, Kurdish ultra-nationalist organization. This also coincides with the dissemination of the Petition for Peace, a call for action to the Turkish state to stop the violence against the civilians signed by thousands of academicians.11

Although the judicial reaction was quite severe against Redhack, political actors and the mainstream news media were mostly silent about the discourse of terrorism applied to the group in this densely politicized media atmosphere. Before Erdoğan’s new frame of terrorism in March 2016, the only attempt to label Redhack’s hacktivism as terrorism came from judicial bodies. Nevertheless, this labelling was marked with explicit indecision.

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, Prosecutor Demands RedHack be Declared ‘Terrorist’ Organization 2012). When the trial opened after this investigation, material from Redhack’s website, which was shut down the same day Redhack published the leaked information, was exhibited as evidence of a terrorist organization (Ankara Chief Public Prosecutor’s Office 2012). The reason for this accusation was that on their website, Redhack framed its mission as “being in solidarity with other revolutionary organizations in Turkey, especially illegal ones” (Redhack 2012). In May 2013, during another investigation related to Redhack, this time, anti-terrorism prosecutors declared that Redhack was not a terrorist organization because it was not an armed organization (Hürriyet Daily News 2013). In November 2013, during the second investigation into Redhack, the prosecutor specializing in cybercrime once again requested the investigation be taken up by anti-terror prosecution (Sputnik Turkiye 2013).

This indecision is meaningful in the larger context of the transformation of political crimes into terrorism in the political discourse. During my interviews, law enforcement agents emphasized that Redhack’s is a terrorism case because “they intended for the state [emphasis added]” (LEAs 4 2017). ’Intent’ is a commonly used term in the legal documents. Yet, its common direct use with the formative ‘for’ is when it is used when referring to killing, as an ‘intent to kill’ for which the formative ‘for’ can be used as ‘intent for life.’ Intent does not have just the meaning of neutral intention but also the meaning of “to harm, to kill, a wish to damage, a bad intention” (Türk Dil 11 In January 2016, more than 2000 academicians signed the petition “We will not be a party to this crime!” to criticize the violence of the Turkish State in Sur, Silvan, Nusaybin, Cizre, Silopi, and many others. More information about the petition text alongside the intimidation, repression, defamation, and prosecution processes against the academicians who signed this text can be found at this website: https://barisinakademisyenler.net.
Kurumu [Turkish Language Association]). For people inside the judicial field, this usage is quite familiar but through the critical perspective of social sciences, this usage evokes an almost equalization of “killing somebody” with harming the state.

During one of the interviews that I conducted with law enforcements agents, I encountered a concrete illustration in line with this equation of killing somebody with harming the state. As we were discussing cyberterrorism, the agent explained to me, “you just add cyber to normal crimes, like cyberattack, cyberterrorism.” Then, he gave me two examples; an attack on public institutions as cyberterrorism and the attacks of “the terrorist organization DAES” because they attack human rights (LEAs 4 2017). Here the framing of cyberterrorism, as a mere appendix to the word terrorism entails the critical synchronization of these two acts.

This emphasis on the weight of crimes against the state is not limited to the use of one word or to the imagery of one law enforcement agent. The Turkish Anti-Terror Law of 1991 is a rich source in this respect:

Terrorism is any kind of act done by one or more persons belonging to an organization with the aim of changing the characteristics of the Republic (…) damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish State and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat (Turkish Anti-Terror Law 1991, emphasis added).

The label of terrorism is frequently used by political actors, in news media, and during public discussions, yet there is not an agreed-upon definition. During my interviews, a leftist lawyer clarified that with the current Turkish legislation based principally on the Anti-Terror Law of 1991, it was logical for prosecutors and judges to consider Redhack as a terrorist organization even though for him, it was an issue of cybercrime (Lawyer 1 2017). Meanwhile, another interviewee specializing in cybercrime declared that Redhack could not be a terrorist organization, relying on the most universally accepted definition of terrorism (Lawyer 3 2017).

The 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, 4, emphasis added).

This lawyer defended his position by saying that Redhack was not terrorizing the people. This approach is quite critical of applying the label of terrorist to the group Redhack. However, as discussed above, to keep Redhack separate from other alleged terrorist groups and problematize only the labelling of the hacktivist group is an implicit endorsement of the
normative discourse of terrorism as it functions in the contemporary Turkey. It shows that while the state positions itself as the ultimate victim of terrorist acts by blurring the notions of people, public, and the state, the opposition to this discourse can be small-scale and not inclusive of other groups labelled as terrorists.

The last discussion about the (un)official discourse of the state is related to the framing of Redhack as a group of incompetent hackers. “Everyone knows a good hacker but no one knows an excellent hacker” (LEAs 1 2017). This phrase returns us to the introductory discussion about the combination of fear and fascination mobilized by the figure of the hacker. In 2016, during another hacktivism trial in Turkey against a less known hacktivist organization called Cold Hackers, the prosecutor in charge prepared an indictment in which categories belonging to the hacker community like “lamer,” “hacker,” and “security administrator” are defined in a very detailed, disconnected, and subjective way. “Lamer” is a pseudo-category that hackers use as an insult to incompetent hackers. In the indictment, lamer is defined with a very long paragraph, which begins, “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). Very different from the state who punishes the terrorists, the voice heard in this indictment is like one insider of the hacker community who insults another insider.

Together with the explicit regard for good hackers in my interviews, I venture that even in the discourse of the state, hackers are considered to be dangerous yet fascinating figures, folk devils. When a hacker group’s political motivations become much more apparent than their hacking skills, the alleged absence of hacking skills can be instrumental to discredit the enemy. From this perspective, it is not just their being terrorists, but also their being bad hackers, that becomes an issue.

Claiming that Redhack is a bad hacker group and just a “terrorist organization” that the Turkish state is adept at containing ideologically, is a useful strategy. However, such a strategy denies the perception of the state about the potential danger of hackers and its possible vulnerability against hacktivist groups. The absence of “noisy” terrorism frames in news media coincides directly with this pretended negligence of Redhack. The silent framing of terrorism for Redhack creates a controllable political blank in which public discussions cannot find a place for themselves. The framing of the state makes Redhack just one of many terrorists of Turkey, nothing special, not a folk devil. In this sense, even though Redhack is the first hacktivist group framed as a terrorist organization, its framing is closely dependent upon the contextual needs of the Turkish state.
CONCLUSION: THE FUNCTION OF AN ANOMALY

Let us return to the introductory question of “if Redhack is an anomaly, what could it tell us?” Even though this CARGC Paper is part of my larger PhD dissertation, the construction of the criminalization discourse for Redhack, together with its labelling as a terrorist organization by the state, reveals that abstract categories of hacktivism and cyberterrorism cannot display the embeddedness of hacktivist organizations into their own contexts. An understanding of the sociopolitical context and a historicizing effort for this context are necessary to problematize the discourses around hacktivist organizations, without which hacktivism cannot be understood as a social phenomenon.

Focusing on Redhack was key to developing an approach that departs from the hacktivism literature because the present paradigm in the literature could not explain the criminalization of Redhack. That is one function of the anomaly of Redhack, in the sense of Thomas Kuhn’s classical work The Structure of Scientific Revolutions (1962):

> We always try to understand the different one, the anomaly, because it is the point where paradigms cannot provide explanation and that is because, it is the potential source for paradigm shifts / ones. Only when these attempts at articulation fail do scientists encounter the third type of phenomena, the recognized anomalies whose characteristic feature is their stubborn refusal to be assimilated to existing paradigms. This type alone gives rise to new theories (Kuhn 1962, 97).

Redhack opens the space for a paradigm shift with the possibility to create new theories – this is the main function of Redhack within the hacktivism literature. The underground stream of imagining global as a comprehensive question in communication studies is also related to this shift in the hacktivism literature. Grounding the analysis of Redhack in a legal-political-cultural context is closely in line with Geertz’s theoretically grounded and empirically based approach that Kraidy and Murphy (2008) advocate for global communication studies. The risks of abstraction of the current hacktivism literature can be eliminated through such a focus on “the peculiarities of the local in its broader structural and comparative context” (Kraidy and Murphy 2008, 341), while at the same time this focus can be the source of a paradigm shift for a new theorization.

Another function of Redhack is related to the context of Turkey. As an anomaly that resists assimilation to existing paradigms of terrorism, Redhack’s framing as (cyber)terrorism can become an important outlet to problematize the discourse on terrorism, which in Turkey has been a continuing, powerful state discourse since 1980. Small-scale opposition to this framing can be the source of a larger rethinking of the terrorism label. Such an approach provides a fresh critical perspective resulting in infertile soil for unbiased works, not just for the Turkish context but also for the global context in which terrorism frames become much more inclusive and oppressive.
ACKNOWLEDGEMENTS

I am deeply thankful to Marwan Kraidy, Marina Krikorian, Rayya El Zein and İbrahim Sarıkaya for their generous feedback on drafts of this paper. I would like to thank everyone in the CARGC team and especially Samira Rajabi for supporting me academically and emotionally. Thanks also go to my interviewees who gave their time and to the specialists who made accessible otherwise inaccessible sources. Without the unrestricted support of my parents and Pınar Uluer, I would not be able to accomplish this work. Last but not least, I am thankful to all friends, struggling for a better world, for motivating me to keep on working. All errors remain my own.
REFERENCES


Ankara Chief Public Prosecutor’s Office. 2012. “İddianame [Indictment].”

Ankara Heavy Penal Court No. 7. 2015. “Gerekçeli Karar [Reasoned Decision].”


Diyarbakır Heavy Penal Court No. 2. 2016. “Gerekçeli Karar [Reasoned Decision].”


Lawyer 1, interview with author, 2017.


LEAs 1, 2 & 3, interviews with author, 2017 (1).

LEA 4, interview with author, 2017 (2).


REDE 2013. Produced by Bağımsız Sinema Merkezi [Independent Cinema Center].


The Center for Advanced Research in Global Communication at the Annenberg School for Communication at the University of Pennsylvania is an institute for advanced study that produces and promotes advanced research on global communication and public life, bringing the very best scholarship to bear on enduring global questions and pressing contemporary issues. As an institute for advanced study, CARGC aims to produce world class, field-defining research, grounded in a vision of “inclusive globalization” that embraces the stunning diversity of global media, politics and culture. This vision is grounded in an unyielding commitment to academic excellence and global engagement. Our core value is the articulation of deep, expert knowledge of key world regions and their histories and languages, to theoretically sophisticated and methodologically rigorous research. We aim to stimulate critical conversations between “area” studies, interdisciplinary fields, and disciplines about entrenched and emerging structures, flows, struggles and outcomes in worldwide communication. We also explore changing dynamics of knowledge production and dissemination, including electronic publication, digital archives, and new ways of understanding and explaining the world, chiefly through CARGC Press. With a commitment to the development of early career scholars, CARGC hosts postdoctoral and visiting fellows who work in research groups, and organizes lectures, symposia and summer institutes.
CARGC Distinguished Lecture in Global Communication & Masterclass

September 20th
Lecture
“Almost Failing: Mexico’s Violence, Space, and Discourse”

Masterclass
“Coloniality and Communication”
with Hector Amaya, University of Virginia

CARGC Fellows Conference

March 28th
South by Southeast

CARGC Book Talks

October 1st
The Kingdom of God Has No Borders: A Global History of American Evangelicals
Melani McCalister, George Washington University

November 1st
Leaks, Hacks, and Scandals: Arab Culture in the Digital Age
Tarek El-Ariss, Dartmouth College

February 28th
Seeing the World: How US Universities Make Knowledge in a Global Era
Cynthia Miller-Idriss, American University

April 4th
Not Quite Not White: Losing and Finding Race in America
Sharmila Sen, Harvard University Press

CARGC Colloquia

September 6th
“Struggles for Visibility: Surveillance Representations and Self-Representations of Terrorists in the News Media”
Mette Mortensen, University of Copenhagen & CARGC Faculty Fellow

October 18th
“The Cultural Logics of Digital Governance: Russia’s Great Power Identity and Internet Sovereignty Narrative”
Stanislav Budnitsky, CARGC Postdoctoral Fellow

November 29th
“Digesting Precarity: Digital Motherhood, Food Safety, and Health Panic in Vietnam”
Giang Nguyen-Thu, CARGC Postdoctoral Fellow

December 3rd
“Making Sense of Millennial Childhood Trauma in Iraq through Nostalgic Cartoons and Social Media Posts in Arabic”
Zubaida Qaissi, CARGC Undergraduate Fellow

January 31st
Yakein Abdelmagid, CARGC Postdoctoral Fellow

February 14th
“Youth, Hashtags, and the Digital Circulation of Protests of Guinea”
Clovis Bergère, CARGC Postdoctoral Fellow

March 14th
“Innovation on Standby: Political Pitfalls, Economic Uncertainty, and Scientific Frustrations in Brazilian Computer Innovation”
Beatrice Choi, Northwestern University & Predoctoral Fellow, University of Pennsylvania