This is an accepted manuscript version for a book chapter published in *Terrorists' Use of the Internet*.

Please cite as:

Tanczer, L.M. (2017). The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists. In M. Conway, L. Jarvis, O. Lehane, S. Macdonald & L. Nouri (Eds.), Terrorists' Use of the Internet. (pp. 77-92). Amsterdam: IOS Press.

The final publication is available at IOS Press through http://dx.doi.org/10.3233/978-1-61499-765-8-77.

The copyright belongs to the author.

www.iospress.nl

Electronic copy available at: https://ssrn.com/abstract=2998202

The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists

Leonie Maria TANCZER[a,1]
[a]*University College London*

Abstract. The academic literature on terrorism is filled with references to online activities and the equation of hacking and hacktivism (i.e., politically motivated hacking) with cyberterrorism. This perspective ignores differences in capacities, scope, and motives in hackers/hacktivists. Besides, scholarly research is lacking examinations of those being perceived as alleged 'security threats'. The present paper therefore uses interviews with self-identified hackers and hacktivists (N = 35) to address this gap. It examines the distinction between hacking, hacktivism, and cyberterrorism and studies the discourses and practices of hackers and hacktivists. Building upon the theoretical concept of (in)securitisation and the method of thematic analysis, the findings provide insights into the perceived (a) external assessment of hackers and hacktivists by external actors and their (b) self-assessment that stands in contrast to the viewpoints expressed earlier. The results highlight interviewees' objection to the translation of hacking and hacktivism into violent acts of any nature, with participants articulating that the connection of these concept poses threats to civil liberties and political rights online. The paper has implications both for the academic as well as professional discourse. It seeks to foster a more reflected engagement with these concepts and is pointing to the need for concrete terminological delineations.

Keywords. Hacking, hacktivism, cyberterrorism, cybersecurity, online activism, critical terrorism studies

1. Introduction

The terrorism literature is filled with references to online activities, amplified through the gradient use of the internet and its substantial penetration of nearly all aspects of our life. With these developments in mind, also the fear of an alleged 'cyberterrorism' attack is gaining popularity. This is fuelled by the medial and academic discourse [1], while empirical observations of its factual existence and impact are practically absent. Particularly the interconnectedness of cyberterrorism with the concepts of hacking and less frequently hacktivism are thereby noteworthy. These perceptions range from hackers depicted as terrorists as well as terrorist hackers [2], notions of hackers-for-hire, or the understanding of hacktivists as being essentially cyberterrorists [3].

Specifically the latter equation of hacktivism and cyberterrorism is hereby of concern. It implies the labelling of politically motivated hacking as a form of online activism being akin to fundamental violent acts such as terrorism. This shifts the clichéd claim of 'one person's terrorist is another's freedom fighter' [4] onto the online sphere. While past examinations within the terrorist literature have engaged with this question [3,5,6], many of the existing publications fail to engage with the hacker and hacktivist community themselves. This creates a notional engagement with the issue, leaving a blind spot to the ethnographic dynamics and the voice of self-identified hackers and hacktivists.

The current paper therefore uses the existing literature on the topic as a starting point to re-emphasise the idea that hacking and hacktivism should not be mistaken for terrorism. This is done through interviews with those directly affected by this equation. Thus, the paper investigates the discourse and practices of self-identified hackers and hacktivists. The analysis firstly provides a conceptual grounding of the terms while reviewing the existing publications on the issue. It thereupon outlines the methods used in this study, which is followed by an in-depth analysis of the arguments provided by the interviewed participants. The paper ends with a discussion on the broader implications of the findings for both academics and security practitioners and hopes to stimulate a more critical, reflective engagement with the concept of hacking and hacktivism.

1.1. From Terror to Cyber to Hacktivism

Debates on terrorism have marked the academic literature for decades. The disputes range from definitional discrepancies to the methodological challenges of studying such an amorphous concept. Although scholars

[1]Corresponding Author.

Electronic copy available at: https://ssrn.com/abstract=2998202

such as Schmid and Jongman [7] try to provide elaborate examinations that seek to give an all-encompassing definition of this "method or technique of instrumental terror" (p. 55) [8], the idea of a distinct form of 'cyber'-terrorism adds to the complexity of what characterises terrorism from, for example, other forms of political violence. Just as Laqueur [9] claims that society is confronted with "different terrorisms" (p. 99), cyberterrorism seems in this regard only as one further form of a broader range of tactics.

Despite the existence of the term cyberterrorism for nearly twenty years [10,11] the concept itself is contested and contradictory [1]. Probably one of the most commonly cited sources on the issue relates back to Denning [12] and her testimony before the United States (US) Special Oversight Panel on Terrorism:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Notwithstanding the severity that Denning [12] expresses, publications frequently associate very benign activities such as website defacements with cyberterrorism. Weimann [13] echoed this, arguing that while concerns about the potential danger posed by cyberterrorism are according to him well founded, the fears that have been voiced in the media, political arenas or public forums seem not always reasonable. Incidents by individual hackers or hacktivist collectives such as Anonymous have repeatedly been conflated with the spectre of cyberterrorism. For example, leaked documents display that associated members of the hacktivist collective Anonymous were put on a FBI terrorism watch list prior to their arrest [14]. This, however, does not sufficiently represent their often innocuous intent. Some are aiming to reveal injustices or security flaws. While these acts might disrupt normal operations, cases are rare – if not inexistent – in which these incidents are then actually causing the kind of 'serious' damage Denning [12] is articulating.

Besides, these examples not only raise a concern regarding the way the concepts of computer misuse or terrorism are framed, but also in relation to the way hackers and hacktivists are perceived. Hackers or hacktivists are part of what Mott [15] called the "faceless detractors of security" (p. 34). This idea is deriving from the physical distance between the attacker and the target but also the inherent inability to actively see and frequently also identify the assailant. Hacking, as already highlighted in an earlier publication [16], relates to computer hacking [17], which can be considered as activities ranging from gaining unauthorized access to systems or data [18], to the production of free software [19], to manipulating technology for unorthodox means [20]. Hackers' representation has undergone a massive shift. Initially associated with a "geeky, apolitical (…) boyish" character (p. 1167) towards malicious thieves, or even the embodiment of terrorism [21].

Hacktivism on the other hand occupies an ambiguous position within the body of literature. The term has not been coined by Denning [22], as argued by some authors [13], but seems to date back far earlier to 1994. It derived from a member of the hacker collective 'Cult of the Dead Cow' [23] to describe hacking for political purposes. Hacktivism is a conflation of hacking and activism and currently commonly linked with publicly known collectives such as Anonymous, LulzSec, and to certain extend even the whistle-blower platform WikiLeaks [24-27]. While in many instances the term is associated with negative connotations, authors such as Deibert and Rohozinksi [28] or Kingsmith [24] perceive hacktivism rather positively. Hacktivists' ability to build tools which promote access to information and openness through the circumvention of surveillance and filtering are considered useful across various political movements e.g., Amnesty International, Reporters Without Borders [24]. The political element of hacktivism is in these instances considered more of assistance than an annoyance or even a threat.

In literature, both hacking and hacktivism have been entangled with cyberterrorism. This is particularly evident with regards to hacking (see for example: [29]), with Weimann [13] emphasising that the mass media, but also corporations frequently fail to distinguish between the two. The media would be exaggerating the threat by reasoning from false analogies. Weimann [13] thereby points out the quick association that is made between hacker and terrorist activities with both being incorrectly but potentially

also purposefully confused. Moreover, scholars such as Conway [30] or Dunn Cavelty [2] are critical about the idea of hackers' depiction as terrorists with Conway being scepticism towards the "sensationalism" (p. 73) to which academics contribute [31].

In addition to the conflation of hacking, cyberterrorism is also frequently mentioned in the same breath with hacktivism. For example, Neumann [32] talks about terrorists' use of the internet as a weapon and refers in the same sentence to the ability of the hacktivist collective Anonymous to conduct online disruption (p. 434). Similar arguments were brought forward in a survey of 118 researchers working on terrorism or cyberterrorism. Some respondents referred to the hacktivist collective Anonymous or the online activism of the Zapatista protests in the 1990s as examples of cyberterrorism [33]. Incidents like these are manifold within the terrorist literature [22,34-36], ignoring differences in capacities, scope, and motives [37].

Additionally, the activist component of hacktivism (and less frequently also the activist element of hacking) is commonly disregarded. The term activism comprises actions taken to promote change in opposition to prevailing powers [38]. Activism is, thus, about "political participation" (p. 132) [39] and involves an element of 'demand' [40]. It allows excluded and marginalized voices to be heard and has the purpose of influencing society at large [39]. 'Traditional' activist methods range from protest as the pure expression of objection to civil disobedience as the disobeying of the law for a perceived 'good' cause [41]. In the context of hacktivism, these activist methods are closely connected to direct action and ultimately conducted online. However, this societal, campaigning aspect of hacktivism is often overlooked and replaced by dynamics of (in)securitisation [42][2].

In spite of attempts to uncover these (in)securitisation dynamics by critical security studies scholars, the literature has so far not given enough voice to the actors affected by the (in)securitisation (see in comparison migration literature: [47,48]). It requires the shift from abstract engagements and purely textual analyses to ethnographic and observational methods that slowly seem to find a place in the academic terrorism scholarship. However, scholarly research output on cyberterrorism still lack a focus on understandings of individual perceptions, feelings and identity of those being perceived as alleged 'security threats'.

1.2. The Present Analysis

The present study fills this gap and is using a more bottom-up research approach. It expands the terrorism literature to focus on those affected by (in)securitisation dynamics i.e., hackers and hacktivists. It is furthermore keen on examining the distinction between hacking, hacktivism and terrorism more closely. Building on Critical Terrorism research's demand for "self-reflexivity" (p. 2) [49] towards the social construction of 'terrorism', this study tries to overcome the way meaning is given externally to actions and actors; rather, it studies how hackers and hacktivists view themselves and their fellow participants. It provides the first analysis of interviews with self-identified hackers and hacktivists within the terrorism literature and examines the consequences of (in)securitisation processes as perceived by these individuals/groups explored. This enables to investigate what (in)securitsation *does* to them and how hacktivists negotiate their identities, express difference and dissent, and communicate political positions in the online environment.

2. Method

The data derives from a PhD thesis that is based on a qualitative research design, using semi-structured and nonrecurring interviews with a self-selected sample of $N = 35$ self-identified hackers and hacktivists. Participants clustered themselves towards the term hackers (n = 17) and hacktivists (n = 14) or used both terms (n = 4) to describe themselves. The researcher enlisted participants through a variety of way, involving snowball sampling [50].

[2] The concept derives from International Political Sociology's (IPS) "sociology of (in)security" (p. 4) [43]. IPS scholars argue that security issues do not necessarily reflect the objective, material circumstances of the world [44]. Instead IPS emphasises the social and political construction of threat images termed as *(in)securitisation*[43]. It builds upon the work of Bourdieu leading to the understanding of (in)securitisation as a 'field effect', a result of the social space being a field of struggles, domination, and forces [45].It conceptualises the naming and framing of security/insecurity as a purposefully political act [46]. The competition within and between actors' (e.g., politicians, police, industry representatives, activists etc.) eventuates into a fight over the ability to define (in)securities.

The interviews were conducted in German and English between December 2014 and May 2015 either face-to-face or digitally using Voice over Internet Protocol services. Prior to the interview, participants received a *Participant Information Sheet* which briefed them about the purpose of the research as well as the adherence to their privacy and data protection rights. Participants were made aware of the limits to confidentiality and alerted about the potential risk of participating. This provided interviewees with the chance to reject participation but also to omit referring to possibly incriminating information.

Thematic analysis [51,52] underpinned the research and passages from the interviews will be used to exemplify the analysis. In the following section, interview extracts are used to support the investigation. German text fragments were translated into English by the researcher herself. Participants are referred to as *P* plus identifying number (e.g., P1). The symbol (…) is used to identify negligible sections of the interview, while "…" signifies short pauses.

3. Results

The current publication is keen on examining the distinction between hacktivism and terrorism more closely. In keeping with the method of thematic analysis, this article examines the viewpoints of self-identified hackers and hacktivists and studies their discourses and practices. It exhibits their assumed (a) external assessments by other actors such as, for example, politicians, the media or the cybersecurity industry and explores their (b) self-assessment that stands in contrast to the earlier expressed viewpoints by external actors. Each of these themes will be analysed in more detail in the upcoming sections.

Overall, the findings highlight that interviewees object the translation of hacking and hacktivism into violent acts of any nature. According to them, this equation ignores the complexity of these phenomena. They express caution of treating forms of activism, criminal activities, and terrorism interchangeably. The results indicate that in many ways hacktivism and hacking are facing analogical discussions and treatment as many terrorist-related debates and actions. Furthermore, interviewees see in the (in)securitisation of hacking and hacktivism and its equation to cyberterrorism severe threats to civil liberties and political rights. Participants stress the argument that the current political climate is very much focused on dealing with these existent but simultaneously also perceived and constructed security risks. They criticise the absence of a sufficient differentiation and express disappointment on the lack of expansion of security and rights online.

3.1. External Assessment

Interviewees have a very critical perception on the way external actors assess them and their actions. They often see a very purposeful attempt to criminalise and (in)securitise hacking and hacktivism that frequently is done through processes of othering and the equation with cyberterrorism. Seigfried-Spellar and Treadway [53] as well as other authors [3,54,55] have already emphasised that hackers are associated with negative connotations. They criticise the generalising level of clustering any form of computer misuse into a singular category. This leaves little room for a diverse understanding of the identity and activities conducted by hackers. Similar dynamics are evident with the term and concept of hacktivist. The connection of hacktivist collectives such as Anonymous with the "modern folk devil" (p. 85) hacker identity evokes a stereotypical portrayal. It leads hacktivists to become the "boogeym[e]n of the modern technical age" (p. 86) [56]. This notion of folk devils is also commonly applied to various other stigmatised groups such as illegal immigrants, drug users or single mothers [46,57], but has distinct implications for the here investigated community.

Participants argue that hacking and hacktivism are in this regard perceived as the criminological *other* akin to the portrayal of the "terrorist other" (p. 2) [49]. The other is a social fact that shapes ways to manufacture deviance and maintain social control and exclusion [58]. It creates a "cultural outsider" (p. 401) that is tied with feelings of anxiety and connected to calls for heightened control responses [58]. The present analysis shows that hackers and hacktivists are aware of these dynamics and outspoken about the potential effects of this process. They articulate that "the majority… of people have a very different picture of hackers" (P14) than what hackers and hacktivists would think of themselves. The sphere of politics, the industry as well as the media or the public would use a "categorisation that is lump-sided, broad and [where] a lot of people [would] fit into" (P3).

Interviewees express an equation of hacking and hacktivism with other actors and actions such as "terrorism" (P3, P14, P18, P25, P26, P29). Participants thereby criticise that the external assessment of their action predominantly focuses on the "illegal stuff [that] is a part of [hacking]" (P21) as well as hacktivism, even though "it's kind of a really small, small slice" (P21) of the actions the hacker and hacktivist community would perform. "[H]ackers are not just black hats" (P25), which is a common way of categorising them in accordance with the legality of their actions [59]. Participants refer to the duality and "ambivalence" (P28) of the concepts. Still, as a consequence of the (in)securitisation of hacking and hacktivism, this diversity of their community is no longer taken into account. In fact, their construction as "terrorists" (P14), "weirdos" (P3) or even "sociopaths" (P3) helps authorities, as Extract 1 highlights.

Extract 1

P3: And **governments try to find** all sorts of **ways to**, **to ah make them seem** like ah... either **sociopaths** or ah **weirdos** that don't, **don't fit into society**. So they acted out of, out of ah their **own impulses** or something like that. Ah it's really – it's **actually kind of necessary for them to do that**. Because **if they don't do that** and people would see it as a, as ahm... **an act of civil disobedience**, as an act of the... **imperative** to do something.

The participant argues that "governments try to find all sorts of ways" (P3) to make hackers and hacktivists not "fit into society" (P3). This process of constructing them as folk devils would be "necessary" (P3), as otherwise the public - emphasised through the usage of "people" (P3) - would realise that hackers and hacktivist are conducting acts of "civil disobedience" (P3). This reference displays their claim for legitimacy. It relates to participants' understanding of themselves doing "good for people" (P5). However, the (in)securitisation through the equation of their action with malicious acts ultimately extracts them from a sphere of acceptance. Instead they are mystified and their social causes for conducting their actions remain hidden behind their social construction as "weirdos" (P3) that allows for the ongoing equation with cybercrime or cyberterrorism to occur.

Extract 1 also touches upon another external assessment dynamic expressed by participants which is the instrumentalisation and misuse of their threat construction and biased portrayal. Subsequently, the (in)securitisation would function as a way for authorities and other institutions to favour their own interests. For instance, one participant argued that governments use hackers and hacktivists "to justify large terrorism-budgets" (P29). Authorities would "need boggy-men" (P29) in order to be "blaming them for some sort of terror plot" (P18). The ability to portray hackers and hacktivists as a security threat would be "an easy way to ahm make people fearful and make people trust the government" (P3). Besides, "intelligence agencies are always going to cry terrorist or national security or something" (P26), as it would have been done in the past with other social movements such as the "environmental" (P29) or the "animal rights movement" (P29). It would be due to such interests that hackers and hacktivists are framed just like "ecoterrorists" (P29).

This purposeful "attempt to put them [hacking and terrorism] near each other" (P29) or to "try to pull hacktivism" towards this "stupid word that they use 'cyber', 'cyberwarfare' or 'cyberwarrior' – all this nonsense" (P1) is according to some participants not only evident in the political sphere, but also in the IT industry and media. Both would foster the controversial depiction, as for example cybersecurity vendors would "love hacktivists, 'cause they gonna help [them] sell all kinds of crap" (P22). Their portrayal of hackers and hacktivists as a security threat is enhancing their "business model" (P33). Similarly, the media would profit from their (in)securitisation, as "they are writing a click-based story" (P2) to attract more readers and attention. It would be "propaganda" (P1), information would get "twisted" (P18) and "the media would measure everything by the same yardstick which is why hackers are now badly off" (P16).

In this regard, participants express a frustration about the othering, instrumentalisation as the purposeful attempt to tie hacking and hacktivism together with extreme associations such as cyberterrorism. Besides, hackers and hacktivist would have become the "wizards" (P21) and tricksters of our time. They have developed from curious whiz-kids as they have "grown up with computers" (P20) to smart and knowledgeable magicians. They are in a position of power the government and society would not comprehend. It is therefore that participants feel continuously more subjected to a (in)securitisation process.

They have to deal with the dichotomy of being geniuses and even to some extend "god[s]" (P22), while at the same time being equated with delinquents or terrorists. Participants highlight that everyone "assume[s] that you know how to do everything" (P22) whilst they also look at them "just as criminals" (P10). The public would see them either as "bad-ass vigilantes or these terrorists that are going to steal their credit cards [amused]. Ahm… so they either see us like these super-heroes or these super-villains" (P18). A participant expressed this quite trenchantly by saying: "[I] feel like a criminal and I have to be god at the same time" (P22). Their "magic" (P18; i.e., knowledge and skills) puts them in an out-of-sphere position. This would explain why the harsh legislative climate would be so keen on taming their skills, allowing to counterbalance power disparities.

Governments and security agencies would be concentrating on the incorrect actors when thinking of security threats. "[T]hey have mistaken the security vulnerability" (P24) by blaming hackers and hacktivists. One participant said to "be more concerned about Syria, Israel, USA hacking into my network" (P24) than hackers and hacktivists. Authorities would, thus, overestimate their capabilities. Hackers and hacktivists would be constructed as a threat that "does not exist in such a form" (P30). Hence, it would be essential to focus on actors such as nation states, rather than hackers and hacktivists. The latter would lack the required "skills and resources" (P24) to create the same "mess a high level attacker can bring" (P24). Examples of this are, among others, *Stuxnet*. It was a computer worm that disrupted Iranian nuclear enrichment in 2010. It was allegedly a joint US-Israeli attack and has been described as a new form of warfare that threatens even the strongest military power [60].

This practice of overestimation of hackers and hacktivists' capabilities is similar to the idea of 'new' terrorism [9] with its claim to be more dangerous than any of the terrorist activities seen before the 1990s. Further to this, organisational similarities are evident. New terrorism is considered as being organised in cell or horizontal network structures [61]. Traditional or hierarchical forms of organisation which facilitates executive decision making and central control and command are considered to not be in place. Such network dynamics are also evident in hacker and hacktivist groups. They are often flat and decentralized with decision making and action dispersed among multiple actors exhibiting a high degree of local autonomy [61]. This structural similarity may further explain the frequent equation of hacking and hacktivism with cyberterrorism.

In addition to this comparison and the articulated over-estimation that would be taking place, interviewees perceive that the (in)securitisation of hackers and hacktivists is increasing surveillance, censorship and the limitation of privacy. This is justified by constant references of their equation with "terrorism" (P25). It allows for the "erosion of the rule of law" (P25) and that "rights are getting circumcised" (P27).

Extract 2

P25: I do feel that **politics are <u>going crazy</u>,** this whole thing about **terrorism** is **<u>escalating</u>** and... going crazy. Before, **<u>before</u>** this last year ahm they – **cultural piracy** was the subject, the **red flag**. And **<u>now</u>** it has **become** terrorism. Not that terrorism does not exist, but that **terrorism <u>does not justify</u>** the ahm... **the <u>erosion of the rule of law</u>** as it is currently happening. It's a **<u>profound</u>** erosion.

For participants the "internet has been criminalised" (P26), which enabled to vindicate the leverage of fundamental rights. According to interviewees, even if states would "like to fight terrorism, that should not be a reason or should not be a justification for them [authorities] to diminish the privacy of all citizens" (P27). These acts are considered by participants as threatening and ultimately leading to less security and safety for everyone. One participant articulated that they "don't know what is going to happen in the next years. So, we [humanity] are screwed" (P23). The community would be "concerned about… the, the global surveillance operations" (P1), especially as they consider them as ways to ensure "control over a society" (P30).

This control is also evident in the treatment of hacking and hacktivism that would be disproportionate. Participants "think that first we need to [have] – the calculations by which these ah… acts of civil disobedience are categorised" (P3). Without proper categories and classifications, acts of hacking and hacktivism would always be misjudged, misrepresented and unfairly lumped together with cyberterrorism.

One participant also gave an explanation on how these actions could be assessed. Intentions and motives should be taken into account when dealing with acts of hacking and hacktivism. These assessments could also help to distinguish their acts from cyberterrorism or other forms of crime.

Extract 3

P15: I mean I'm guessing right like – say, say **you're on the plane that hit the Twin Towers** and you were a passenger and you were **able to like kill the hijacker**. You **wouldn't be prosecuted for murder**; that would be kind of ridiculous. Ahm that, that – I don't know what the **legal mechanism is in place** to protect you when, say you kill a terrorist that is about to kill a 1000 people. Ahm but **that, that should be a similar sort of thing for hacktivists**; if their **actions could be shown** to have a **significant beneficial impact on society**.

The participant articulates a disappointment about the fact that "laws aren't proportional" (P15). Currently hacking and hacktivism would be "criminalised" (P14) and prosecuted as if they "would be terrorists" (P14). Extract 3 claims to seek the judicial system to "take into account all parts of the situation" (P15), which according to participant is not taking place right now. This is ultimately leading to unfair judgements due to the predominant negative association with these terms, actors and actions.

3.2. Self-Assessment

Participants define hacking and hacktivism in opposition to these (in)securitised ideas and the negative external assessments. They perceive hacking as "innovating" (P10), as providing "shortcuts" (P18) or "outsmart[ing]" (P18) systems. For them being a hacker is having a certain kind of "mindset" (P1, P3, P6, P8, P9, P10, P21, P23, P26, P28, P34) or "attitude" (P28, P34). It implies using a "clever technical trick" (P21) and it is connected to the notion of "game, fun and pleasure" (P20) as well as "curiosity" (P16) and "entails sophistication and ahm using great skill to dismantle once thought unbreakable things" (P22). It involves utilising tools other than what they were "originally designed for" (P20) as well as "getting the most out of" (P34) technology. To a certain extend it is even a way of "finding truth" (P1).

Participants acknowledge that hacking is an "ambivalent term" (P28) and "just like so much broader" (P21) than "what our parents think hacking is, and what the media is telling them" (P20). It is such a "broad" (P3, P4, P5, P8, P10, P15, P18, P21, P26, P29, P35) concept that even "art can be understood as hacking" (P14). This is also applicable for hacktivism which "can be a lot of things" (P11). It is "a mixture of hacker culture and ah activism" (P3). It is hacking for a "politically minded purpose" (P10), "human rights" (P26) or even "religious" (P6) goals. It has to do with a "creative misuse" (P18) or "online rebellion" (P27) but "for like a general sense of social good, or social righteousness" (P18) or to "highlight grievances" (P27). All of this points to the difference from cyberterrorism that - as Denning's [12] definition highlights - requires more severe and malicious intentions.

Interviewees distinguish themselves from being lumped with vicious actors such as cybercriminals and terrorists. They would do "things which are legal" (P14), as there are "legal ways of being a hacktivist" (P10) as well as a hacker. Some participants heavily oppose hacks against the "media" (P21), "private individuals" (P12, P27) or "critical infrastructure" (P17, P24, P33, P34) such as supervisory control and data acquisition systems ("SCADA"; P1, P3). Hacking and hacktivism should not "hurt an individual" (P12) or "destroy servers" (P14). Instead actions may have a "virtual impact" (P11) which is why one participant understands hacktivism as an action causing solely "bit damage" (P11) rather than having a physical impact.

Extract 4

P11: I would simply define hacktivism as something **like "moving bits"** and **not physical things**. As long as you **only** move bits… then you can **only have a virtual impact**. And… ahm… a bit of damage or so, like **material damage**, I'd see this as **legitimate** to **achieve**

a political goal – it's like **bit damage** [laughing].

This idea of solely causing "bit damage" (P11) and that hackers and hacktivists are actually aiming to do good might be equivalent to ideas expressed by 'actual' terrorists. However, interviewees insist that they are helpful rather than harmful - which may be assessed in some form or another (see Extract 3). For example, one participant argues "I'm a hacktivist, because I target terrorist website" (P6). They do this to "to protect human lives" (P6). Interviewees acknowledge that "some governments see portions of hacking ahm and hacktivism as positive" (P6). Yet, despite their actual humanist intentions these actors would still mostly "see hacktivism as a security threat" (P6). Multiple participants, both self-identified hackers and hacktivists, also expressed that they have or had a background in the "free and open source software" (F/OSS) community (P7, P8, P11, P9, P14, P15, P21, P23, P29, P33, P35). This again refers to the legality of their actions and their alliance with the idea to collaboratively develop unlicensed software solutions.

This attempt to differentiate themselves and withstand the (in)securitisation is amplified through their continuous emphasis on the duality of hacking and hacktivist actions and actors. Participants stress that "there's criminals out there – cyber-criminals and, and spies and everything else that use the internet. Ahm... but there's legitimate people" (P6), which they consider themselves being part of. "[H]ackers aren't people that break into computers. – They're criminals" (P9). There would be "two different concepts" (P15), meaning the "legal and the illegal" (P6) respectively the "positive" (P17) and the "negative" (P17) side of hacking. The illegal, negative, and malicious forms are thereby frequently referred to as "cracking" (P7, P8, P16, P21, P24, P29, P33, P35). Yet, as a consequence of the (in)securitisation society is not talking about these two "different things" (P9), which is why participants articulate attempts to "keep the term somehow clean" (P17) in order to avoid the association with malicious actors.

One aspect where this positive notion of hacking and hacktivism becomes evident is in the way interviewees express that they are part of a far bigger security 'ecosystem'. Their concern to try "to fix [insecurity] with encryption" (P3) and to find "security loopholes" (P17) or other protection mechanisms is "show[ing] them [the industry] that there are problems existent" (P17). Their actions are considered to help improve security overall. Participants therefore resist their construction as a security threat by constructing themselves as *the* security in the current system. Interviewees show this by saying that they "want to improve" (P15), "fix things in different areas" (P35) and "increase our awareness (…) in order to make the population safe" (P24). In fact, not to hack would be a security risk in itself.

Extract 5

P7: You... if you have **something that is broken** and **somebody comes up and tells you that's broken** and you **put them into jail – that's a problem**. That is a security problem for the government – because **it's gonna leave it broken.**

This relates to an idea of resistance and being disobedient for a greater good. Thus, just like protesters might "knowingly violate certain laws of their community in what they reflectively conclude to be a larger interest" (p. 2) [62], hackers and hacktivists can breach systems in hope to do better. For interviewees it is better to know about vulnerabilities rather than leaving them unseen. It can be compared to the rationale of a protester who engages in a civil disobedient action and might rather go to jail and break a law but does so knowingly and deliberately in order conduct a political and/or moral act [63].

Participants emphasise that "if there wouldn't be any hackers anymore, ultimately everything would become a security vulnerability" (P12) because nobody would "point out where the security loopholes are" (P34). Laws against hacking are therefore pointless, as there is "no way you can regulate hacking" (PM34). The act of illegalisation of hacking would be comparable to the prohibition of "product testing" (P19) which does not compare to any discussions going on in relation to cyberterrorism.

Extract 6

P19: I mean **we can ban hacking**, but then we **also have to ban any form of product testing**. Then we have to prohibit that the **breaking load** is displayed at **lashing straps**, because they are **simply not allowed to test those**. – They are **not allowed to break those**, because

that would be a **risk** if you **know when they break**.

This notion of them actually enhancing security is therefore a way to counter the (in)securitisation. Besides, the equation between hacking and hacktivism with cyberterrorism lacks foundation, as interviewees often underline that "we need a legal system" (P8), which terrorist actions actually try to undermine.

Extract 7

P8: Most of the people here will **agree** – if you got a point. **If a judge signed a warrant** to go through my private data, **that's fine**. Because a judge is impartial and **we need a legal system**. It's **this universal sucking up of information** and **then not needing a judge** – because 'We don't need a judge! We can do this ourselves, we are geeks, we are geeks working in the NSA. – '**Cause we can;** we can mine data. **And we will**'. - And ahm I think most people – if you actually ask them – **agree to an actual legal environment**.

References like that highlight that participants would like to see more engagement of judicial bodies in the revision of surveillance techniques. They criticise that basic rights are essentially by-passed by state agencies. Appropriate legal measures would be ways to overcome this. It is therefore that many hackers and hacktivists make use of legal tools themselves. The notion that we "need a judge" (P8) is reflected in their active engagement with the judiciary. It ensures hackers and hacktivists with a mechanism to counteract (in)securitistaion processes and misconducts using legislative means. Specifically the engagements of the renowned German hacker collective Chaos Computer Club (CCC) with the German Federal Constitutional Court serves as a good example. In Germany a close relationship between hacker and hacktivist institutions and judiciary is sought. In the past the CCC has submitted action for a preliminary injunction (Chaos Computer Club, 1 July 2008), filed "constitutional complaints" (P28) or engaged in hearings and have written "reports" (P17, P28) for court cases (Chaos Computer Club, 6th July 2009).

As a consequence of such viewpoints and efforts, more "law informed hacker types" (P29) have developed. They are aware of the consequences of their actions and often familiar with ongoing legislation. This helps them to counteract the (in)securitisation as an active part with individual agency and the ability to engage in the political process. In addition to their cooperation with the judicial system, hackers and hacktivists resist the (in)securitisation through political engagement, support of digital rights organisation and various forms of activism. It highlights how in contrast to common perception hackers and hacktivist seek legal and legitimate ways to engage with and modify the current status quo. Participants say they lobby for causes such as "for a free and open internet" (P25) as "politicians in general are not security guys" (P6) and would need to input from hackers and hacktivists to write policies and legislation.

Participants therefore exercise "internet activism" (P21), "online activism" (P27, P28) or phrase their engagement as "advocacy" (P35). These commitments are not limited to participants who clustered and identified themselves as hacktivists. Instead, as the (in)securitisation of hacking rises e.g., through increase of legislation or heightened surveillance techniques, a lot of people would start to be active in some form or another within a political space or support digital rights organisations such as "Privacy International" (P2), "EDRi" (P27) or "Netzpolitik.org" (P27). These issues highlight how hackers and hacktivists have a political agenda that is within the scope of mainstream politics. This again stands in diametric opposition to the idea that hackers and hacktivists would be terrorists who refuse to engage in mainstream political processes.

Overall, the current theme indicates therefore that hackers and hacktivists counter the(in)securitisation that equates them with criminals or terrorist through their own perception of being ethical, ensuring security, and adjusting inequalities through their actions and activism. With that said, the (in)securitisation process that leads others to think of them as criminals or cyberterrorists helps simultaneously to make the hacking and hacktivist community understand itself as a supportive, legitimate and non-malicious collective. Their focus is on enhancing civil liberties and political rights, rather than the spreading of fear and anxiety should consequently be acknowledged.

4. Discussion

This research sought to explore the self-understanding of self-identified hackers and hacktivists in relation to their association with cyberterrorism. Based on the findings, a better comprehension of the hacker and hacktivist community could be achieved, helping future attempts to possibly distinguish more carefully between hacking and hacktivism and (cyber-)terrorism. The interviewees are expressing caution for treating forms of activism, criminal activities, and terrorism interchangeably, with the first part of the analysis investigating the perceived external assessments on hacking and hacktivism. The second part of the analysis explored the self-assessment of self-identified hackers and hacktivists with the findings standing in contrast to the earlier expressed viewpoints by external actors.

The first section of the results provides an overview of articulated perceived viewpoints of hackers and hacktivists by external actors. It outlines how interviewees feel purposefully misperceived by politicians, the cybersecurity industry or the media. The equation of hacking and hacktivism with cyberterrorism would be connected to the overestimation of their capabilities and the attempts to construct the hacker and hacktivist community as malicious. This hyped understanding would also lead to a disproportional treatment of hackers and hacktivists that is questioned by interviewees.

The second half of the result section challenges the earlier expressed social construction of 'cyberterrorism' and highlights how participants try to overcome the meaning given to hacking and specifically hacktivism by external actors. It shows how hacktivists view themselves and their fellow participants. The current findings exhibits that self-identified hackers and hacktivists are critical of their equation with other violent acts of any nature. For the interviewed participants this is ignoring the complexity of these phenomena, with participants articulating that the connection of the concept to terrorism poses severe threats to civil liberties and political rights.

In this regard it is important to recall the current definition of terrorism that is according to the interviewees surpassingly equalised with hacker or hacktivist acts. Jong and Schmid [7] are two of the most prominent proponents pressing the need to identify a cohesive classification for terrorism. They combined the most common elements of 109 major definitions to argue that terrorism is an anxiety-inspiring method of repeated violent action, which is employed by semi-clandestine individuals. Thus, terrorism in its most fundamental nature is about issues such as violence, political and social goals as well as fear and intimidation. It requires a target audience to transport the political message that has the intention to change a socio-political system and climate and is an act outside of the law.

Although the interviewed hackers and hacktivists might share some of these elements (i.e, political motive, will to change the system etc.), the activist root and the rejection of the physical use of violence and application of fear is ignored in such an equation. In fact, rather than hacking and hacktivism being equated with terrorism, they are increasingly considered to interrupt the online presence of established terrorist organisations [6]. This highlights again the activist element of these phenomena. Particularly in the aftermath of terror attacks such as 9/11 or the recent Paris attacks, hacktivist collectives such as The Dispatchers [6] or Anonymous [64] have acted as privately organised impairments to terrorists' online activities or supported the information and intelligence gathering by official law enforcement or policing bodies. Besides, they have uncovered misconduct of computer espionage companies such as Hacking Team, Gamma Group [65] or weaknesses in security precaution of computer security services such as HBGary [66]. Although such vigilant actions may well be disputed, it displays the diversity that 'politically motivated hacking' can encompass.

The criticism for the equation of hacking, hacktivism and cyberterrorism is also echoed by other scholars who argue in favour of their distinction [13,31]. For instance, Krapp [5] considers practices such as DDoS actions as virtual sit-ins rather than terrorism. Similarly, Weimann [13] claims that hacktivists do want to protest and disrupt; they do not want to kill or terrify. Despite Weimann's [13] articulation of cautiousness when it comes to their comparison, he is wary that the lines between the two might blur. Weimann [13] enunciates the possibility of them being hired for terrorist purposes. Conversely to this viewpoint, Conway [31] says that the possibility of terrorist organisations hiring hackers is rather limited. Such a move would pose operationally risks to any group, leading to the unlikelihood of such an exchange to occur. Due to the lack of empirical data on the accuracy of either of these two viewpoints, it is hard to draw conclusions and the complexity and multi-facet opinions that dominate the current literature.

Although the current work provides an insight into the perceptions and viewpoints of hackers and hacktivists, there are several limitations that require attention. One of the most profound confinements relates to the sampling and data collection procedure. Due to the qualitative approach of this study, the

researcher wants to emphasise that the present research is not representative for the general hacker or hacktivist community. On the one hand, it might be said that the current sample encompasses what Giacomello [67] referred to as "socially minded hackers" (p. 402) and hacktivists. This stands in contrast to the general idea of hackers being malicious. On the other hand, the research's limitation is further amplified, due to the fact that participants were exhorted to abstain from sharing incriminating details. They were made aware of the limits to confidentiality and alerted about the potential risk of participating. All of this may have skewed the response received and the answers provided.

One essential gap that seems to still remain after this examination is the establishment of a particular 'criteria catalogue' for hacking, hacktivism, and cyberterrorism. Although hacking and hacktivism will certainly remain or become akin contested concepts such as terrorism [68], at least the attempt needs to be made to find a common grounding on which one can talk about them. This is relevant not only for the attribution question of cyber-attacks by security practitioners [69], but also for the usage of these terms in the political, industrial as well as the public and academic context.

In closing, research such as the present study offer opportunities for a more substantial, reflected engagement with the concepts of hacking, hacktivism and cyberterrorism. Future investigations are exhorted to go beyond hysteria, but examine empirical facts that are often lacking in these discussions. Just as the meaning of terrorism throughout history has changed [4], certainly the understanding of hacktivism, hacking and cyberterrorism will turn out to be contested. Further research is therefore needed to highlight the diverse understandings and usages of these terms which should also give room to individuals and groups being prescribed and associated with certain labels. Without a thorough understanding of the political, activist, and terrorist element of all these concepts no concrete terminological delineation and most certainly no sufficient management of these actions may ever be found.

References

[1] L Jarvis, S Macdonald, A Whiting. Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage, Global Society. (2016) 1-19.

[2] M Dunn Cavelty. Cyber-terror - Looming threat or phantom menace? The framing of the US cyber-threat debate, Journal of Information Technology & Politics. 4 (2007) 19-36.

[3] M Conway. Hackers as terrorists? Why it doesn't compute, Computer Fraud & Security. 12 (2003) 10-13.

[4] M Bourne, Understanding Security, Palgrave Macmillan, New York, 2014.

[5] P Krapp. Terror and Play, or What was Hacktivism? Grey Room. 21 (2005) 70-93.

[6] M Conway, Terrorist use of the internet and the challenges of governing cyberspace, in: Dunn Cavelty M, Mauer V, Krishna-Hensel SF (Eds.), Power and security in the information age: Investigating the Role of the State in Cyberspace, Ashgate, Aldershot, 2007, pp. 95-127.

[7] AP Schmid, AJ Jongman, Political terrorism: A new guide to actors, authors, concepts, data bases, theories and literature, Transaction Books, New Brunswick, 2005.

[8] D George, Terrorists or Freedom Fighters, in: Warner M, Crisp R (Eds.), Terrorism, protest and power, Elgar, Aldershot, 1990, pp. 54-67.

[9] W Laqueur, The new terrorism: Fanaticism and the arms of mass destruction, Oxford University Press, New York, 1999.

[10] BC Collin. The future of cyberterrorism: The physical and virtual worlds converge, Crime and Justice International. 13 (1997) 15-18.

[11] S Gordon, R Ford. Cyberterrorism? Comput.Secur. 21 (2002) 636-647.

[12] DE Denning, Cyberterrorism.Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, (2000).

[13] G Weimann. Cyberterrorism: The sum of all fears? Studies in Conflict & Terrorism. 28 (2005) 129-149.

[14] E Pilkington, FBI put Anonymous 'hacktivist' Jeremy Hammond on terrorism watchlist, The Guardian. (2015).

[15] G Mott. Terror from behind the keyboard: conceptualising faceless detractors and guarantors of security in cyberspace, Critical Studies on Terrorism. 9 (2016) 33-53.

[16] LM Tanczer. Hacktivism and the Male-Only Stereotype: What Characterises the Discourse of Politically Motivated Hackers in Regard to Gender? Discourse & Society. (2014).

[17] BB Kelly. Investing in a centralized cybersecurity infrastructure: Why "hacktivism" can and should influence cybersecurity reform , Boston University Law Review. 92 (2012) 1663-1711.

[18] J Cresswell, Oxford dictionary of word origins, 2nd ed., Oxford University Press, Oxford, 2010.

[19] CM Kelty, Two bits: The cultural significance of free software, Duke University Press, Durham, 2008.

[20] S Turkle, The second self: computers and the human spirit, Granada, London, 1984.

[21] L Hansen, H Nissenbaum. Digital disaster, cyber security, and the Copenhagen School, Int.Stud.Q. 53 (2009) 1155-1175.

[22] DE Denning, Activism, Hacktivism, and Cyberterrorism: The internet as a tool for influencing foreign policy, in: Arquilla J, Ronfeldt D (Eds.), Networks and Netwars: The Future of Terror, Crime, and Militancy, Rand, Santa Monica, 2001, pp. 239-288.

[23] O Ruffin, Hacktivism, From Here to There, (2004).

[24] AT Kingsmith. Virtual Roadblocks: The Securitisation of the Information Superhighway, Bridges: Conversations in Global Politics and Public Policy. 2 (2013) 1-14.

[25] DR Canabarro, T Borne, Reflections on The Fog of (Cyber)War, 13-002 (2013).

[26] M Dunn Cavelty. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, Int.Stud.Rev. 15 (2013) 105-122.

[27] D Barnard-Wills. This is not a cyber war, its a...? Wikileaks, anonymous and the politics of Hegemony, International Journal of Cyber Warfare and Terrorism. 1 (2011) 13-23.

[28] RJ Deibert, R Rohozinski, Good for liberty, bad for security? Global civil society and the securitization of the Internet, in: Deibert RJ, Palfrey J, Rohozinski R, Zittrain J (Eds.), Access Denied: The Practice and Policy of Global Internet Filtering , MIT Press, Cambridge, 2008, pp. 123-149.

[29] JA Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Washington, 2002.

[30] M Conway. Against cyberterrorism, Commun ACM. 54 (2011) 26-28.

[31] M Conway, Cyberterrorism: Hype and reality, in: Armistead LE (Ed.), Information Warfare: Separating Hype from Reality, Potomac Books, Inc., Washington, 2007, pp. 73-93.

[32] PR Neumann. Options and strategies for countering online radicalization in the United States, Studies in Conflict & Terrorism. 36 (2013) 431-459.

[33] L Jarvis, S Macdonald, L Nouri. The cyberterrorism threat: Findings from a survey of researchers, Studies in Conflict & Terrorism. 37 (2014) 68-90.

[34] D Ronfeldt. Netwar Across the Spectrum of Conflict: An Introductory Comment, Studies in Conflict and Terrorism. 22 (1999) 189-192.

[35] EM Archer. Crossing the rubicon: Understanding cyber terrorism in the european context, The European Legacy. 19 (2014) 606-621.

[36] N Tereshchenko. US Foreign Policy Challenges of Non-State Actors' Cyber Terrorism against Critical Infrastructure, International Journal of Cyber Warfare and Terrorism (IJCWT). 2 (2012) 28-48.

[37] LM Tanczer, Emerging Security Governance in the Cyber Domain: Technology, Politics, and Rights in Practice, (forthcoming).

[38] J Hands, @ is for Activism :Dissent, Resistance and Rebellion in a Digital Culture, Pluto, London, 2011.

[39] C Neumayer, J Svensson. Activism and radical politics in the digital age: Towards a typology, Convergence: The International Journal of Research into New Media Technologies. 22 (2014) 131-146.

[40] E Laclau, On populist reason, Verso, London, 2005.

[41] T Jordan, PA Taylor, Hacktivism and cyberwars: rebels with a cause?, Routledge, New York, 2004.

[42] M Dunn Cavelty, MD Jaeger. (In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous, International Political Sociology. 9 (2015) 176-194.

[43] D Bigo, A Tsoukala, Understanding (In)Security, in: Bigo D, Tsoukala A (Eds.), Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11, Routledge, London, 2008, pp. 1-9.

[44] T Balzacq. Securitization Studies, Academic Foresights. 9 (2013) 1-7.

[45] D Skleparis. (In)securitization and illiberal practices on the fringe of the EU, European Security. 25 (2016) 92-111.

[46] D Bigo. Security and immigration: toward a critique of the governmentality of unease, Alternatives. 27 (2002) 63-92.

[47] RW Glover. The Theorist and the Practitioner: Linking the Securitization of Migration to Activist Counter-Narratives, Geopolitics, History, and International Relations. 1 (2011) 77-102.

[48] HL Johnson. The Other Side of the Fence: Reconceptualizing the ?Camp? and Migration Zones at the Borders of Spain, International Political Sociology. 7 (2013) 75-91.

[49] M Breen Smyth, J Gunning, R Jackson, G Kassimeris, P Robinson. Critical terrorism studies–an introduction, Critical Studies on Terrorism. 1 (2008) 1-4.

[50] P Biernacki, D Waldorf. Snowball sampling: Problems and techniques of chain referral sampling, Sociological methods & research. 10 (1981) 141-163.

[51] V Braun, V Clarke. Using thematic analysis in psychology, Qualitative research in psychology. 3 (2006) 77-101.

[52] G Guest, KM MacQueen, EE Namey, Applied thematic analysis, Sage Publications, Incorporated 2011.

[53] KC Seigfried-Spellar, KN Treadway. Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences, Deviant Behav. 35 (2014) 782-803.

[54] NB Sukhai, Hacking and cybercrime, (2004) 128-132.

[55] R Young, L Zhang, VR Prybutok. Hacking into the minds of hackers, Inf.Syst.Manage. 24 (2007) 281-287.

[56] M Sauter, The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet, Bloomsbury Publishing, New York, 2014.

[57] M Flinders, M Wood. From Folk Devils to Folk Heroes: Rethinking the Theory of Moral Panics, Deviant Behav. 36 (2015) 640-656.

[58] J Sheptycki. Criminology and the Transnational Condition: A Contribution to International Political Sociology, International Political Sociology. 1 (2007) 391-406.

[59] T Caldwell. Ethical hackers: putting on the white hat, Network Security. 2011 (2011) 10-13.

[60] JR Lindsay. Stuxnet and the limits of cyber warfare, Security Studies. 22 (2013) 365-404.

[61] M Eilstrup-Sangiovanni, C Jones. Assessing the dangers of illicit networks: Why al-Qaida may be less threatening than many think, Int.Secur. 33 (2008) 7-44.

[62] C Cohen, Civil disobedience: conscience, tactics and the law, Columbia University Press, New York; London, 1971.

[63] W Smith, Civil disobedience and deliberative democracy, Routledge, London, 2013.

[64] A Hern, Anonymous 'at war' with Isis, hacktivist group confirms, The Guardian. (2015).

[65] E Borràs, Phineas Fisher: “I’m wanted by much more powerful police forces than Catalonia’s and for much worse crimes”, Ara. (2016).

[66] P Bright, Anonymous speaks: the inside story of the HBGary hack, Ars Technica. (2011).

[67] G Giacomello. Bangs for the buck: A cost-benefit analysis of cyberterrorism, Studies in conflict & terrorism. 27 (2004) 387-408.

[68] WB Gallie, Essentially contested concepts, 56 (1955) 167-198.

[69] T Rid, B Buchanan. Attributing cyber attacks, Journal of Strategic Studies. 38 (2015) 4-37.