Personal and Ubiquitous Computing (2021) 25:843–852
https://doi.org/10.1007/s00779-021-01568-7

ORIGINAL ARTICLE

The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good

Aleksandra Pawlicka[1] · Michał Choraś[2,3] · Marek Pawlicki[1,2]

Received: 2 October 2020 / Accepted: 15 April 2021 / Published online: 10 May 2021

Abstract
The development of cyberspace has brought about innumerable advantages for the mankind. However, it also came with several serious drawbacks; as cyberspace evolves, so does cybercrime. Since the birth of cyberspace, individuals, groups and whole nations have been engaging in computer-related offences of various significance and impact, trying to exploit systems' vulnerabilities, disseminate malicious software and steal data or funds. The concept of a hacker has entered the collective consciousness and become an intrinsic element of popular culture. However, there are hackers, or rather, cyberspace actors, who challenge this common view. This paper presents three types of such people, namely hacktivists, members of cyber militias and Internet trolls. Although they all use the Internet to break the laws or rules, their internal motivations are not always utterly sinister; actually, some of them firmly believe that their actions are for the greater good. This paper is structured as follows: Firstly, the general profile of a hacker is presented. Then, the state of the art is outlined, concerning other papers dealing with the motivations behind cyber threat actors. Following that, the three aforementioned groups of cyberspace actors are contrasted with the profile of a 'typical' hacker. Then, the profiles of a typical representative for each of the group and their motivations are indicated, followed by the final conclusions.

1 Introduction

The development of cyberspace has brought about innumerable advantages for the mankind. However, it also came with several serious drawbacks; as cyberspace evolves, so does cybercrime. Since the birth of cyberspace, individuals, groups and whole nations have been engaging in computer-related offences of various significance and impact, trying to exploit systems' vulnerabilities, disseminate malicious software and steal data or funds. The concept of a hacker has entered the collective consciousness and become an intrinsic element of popular culture.

However, there are hackers, or rather, cyberspace actors, who challenge this common view. This paper presents three types of such people, namely hacktivists, members of cyber militias and Internet trolls. Although they all use the Internet to break the laws or rules, their internal motivations are not always utterly sinister; actually, some of them firmly believe that their actions are for the greater good. This paper is structured as follows: Firstly, the general profile of a hacker is presented. Then, the state of the art is outlined, concerning other papers dealing with the motivations behind cyber threat actors. Following that, the three aforementioned groups of cyberspace actors are contrasted with the profile of a 'typical' hacker. Then, the profiles of a typical representative for each of the group and their motivations are indicated, followed by the final conclusions.

The main contribution of this paper is concentrating on the hackers and actors who are 'the stray sheep' of cyberspace, i.e., the ones who are either misguided, ignorant or feel so strongly about something that they rationalise their actions, rather than 'typical' wrongdoers, who break the rules in full knowledge and with malicious intent.

✉ Michał Choraś
chorasm@utp.edu.pl

[1] ITTI Sp. z o.o., Rubież 46, 61-612 Poznań, Poland

[2] UTP: Uniwersytet Technologiczno-Przyrodniczy im Jana i Jedrzeja Sniadeckich w Bydgoszczy, Bydgoszcz, Poland

[3] FernUniversität in Hagen, Universitätsstraße 11, 58097 Hagen, Germany

2 Hackers

Based upon a review of the literature, there does not seem to be a universal scientific definition nor consensus on the term 'hacker' [1]. The today's mainstream usage of the word

mainly refers to online criminals, understood as highly skilled individuals who are capable of subverting computer security to 'crack in'. Commonly, they are portrayed as bright, intelligent, curious loners and brilliant geeks who lack social and communications skills, though. Although some of the stereotypes have been partially confirmed scientifically [2], constructing the profile of a 'typical' hacker is in fact not possible, due to the fact that they may come from every background, may be driven by several distinct causes, work in an organised group or be lone wolves [3]. The researchers who study the intentions behind illegal cyber activities also do not seem to have come to the same conclusions. The most general set of motivations was described by [4] who divided them into three groups: malicious intent or vandalism, greed and the quest for challenge [5, 6]. Nevertheless, not all the cyberspace actors whose actions fall under the umbrella of hacking fit the definition or the profile. The most distinct types of actors are hacktivists, internet trolls and the members of cyber militias.

The overview of the main distinctive features of the three groups is presented in Fig. 1:

2.1 State of the art

The scientists who have been dealing with the subject of the motivations that cyberspace actors are driven by have applied various ways of dividing and organising them. Li [5] reviews the motivations of illegal cyber activities in general, enlisting almost thirty reasons to break the law in cyberspace. However, the article does not organise them by the type of actor. Ablon [9] discusses the motivations of cyber threat actors as well as some ways they monetise the stolen data. In this paper, the four groups of cyber threat actors have been discussed, namely: cyberterrorists (theoretical), hacktivists, state-sponsored actors and cybercriminals. Thus, there is no distinction between the actors who break the law with malicious intent and those who may believe their actions can be justified.

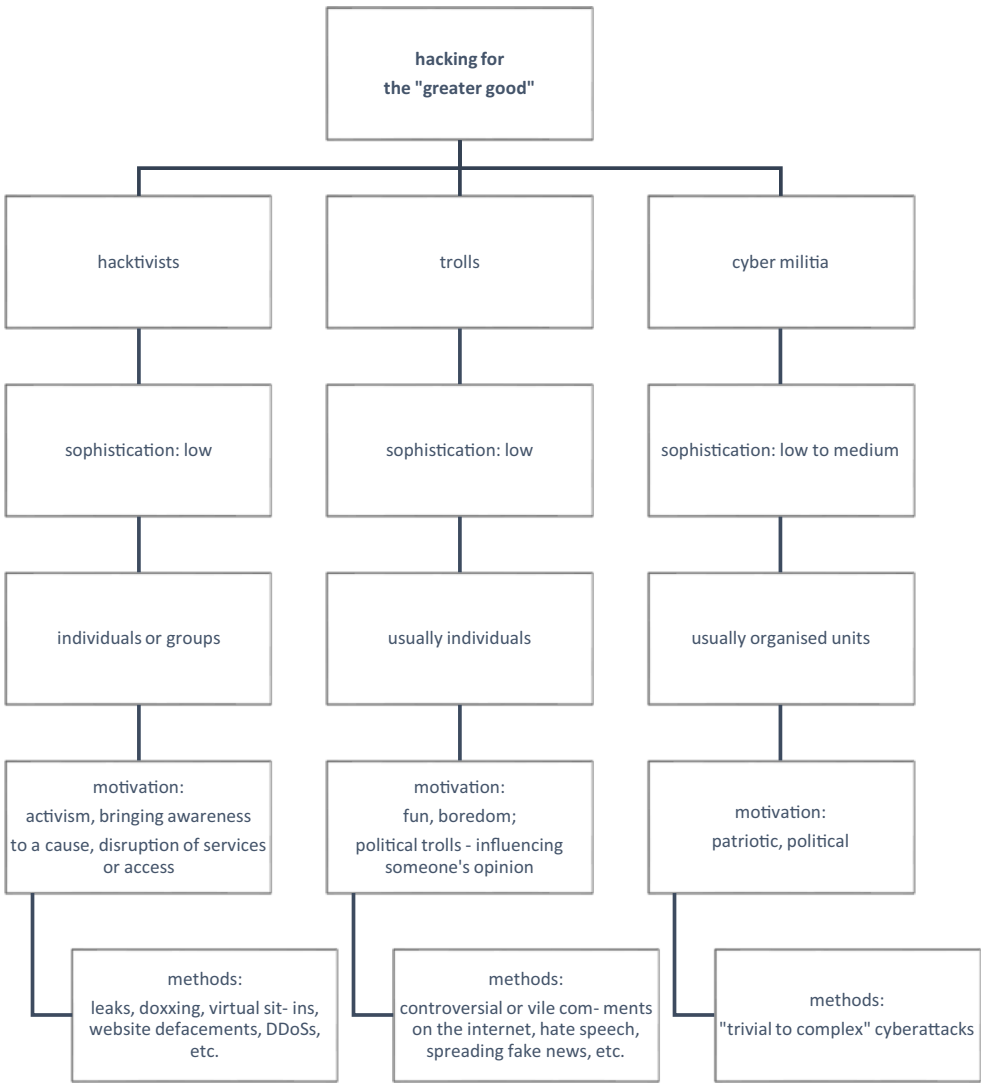

Fig. 1 The main features of hacktivists, trolls and cyber militia, based on [7, 8]

Sigholm [10] presents the various motivations of a large number of the non-state actors, excluding trolls. Ohlin et al. [11] discuss the motivations behind some of the actors; interestingly, hacktivists and 'patriotic hackers' are treated as two separate groups. This paper partially bases on a previous paper [8], which deals with raising the awareness of the less known cyberspace actors — nation states, hacktivists, cyberterrorists and trolls. Hereby, we discuss the hacktivists/trolls parts, which have been significantly extended and supplemented by adding the in-depth insights on the motivations of the actors. In addition to this, the motives behind the cyber militia members have been discussed. To the authors' best knowledge, the actors who believe they hack for the 'greater good' have not been collectively discussed yet.

3 Hacktivists

The term 'hacktivism' was coined by combining the terms 'hacking' and 'activism', in the early days of the World Wide Web [12] [13]. Back then, hackers mostly congregated on Usenet and message boards. As many of them were left-wing, anti-capitalist, anti-corporate idealists, their messing with people via the Internet soon switched to politically motivated hacks, inspired by diverse social and political issues [14]. This leads to a few groups rising to stardom, gaining international recognition and 'cyber-attacks are said to have entered a new phase' [15].

The methods they have employed are mostly basic, lack originality or sophistication [15]. Oftentimes, the tools and techniques involved are widely available and their deployment requires little to no technical skill [16]. The methods comprise:

- Denial-of-service attacks,
- Information theft, leaks and doxxing,
- Website defacements,
- Virtual sit-ins.

Additionally, hacktivists attempt other kinds of cyber sabotage, including Internet resource redirects and website parodies [11].

Research shows that hacktivists overwhelmingly favour attacking websites. It is so, as websites are often the most publicly facing aspect of a company or an organisation. Hacktivists are said to prefer DDoS (distributed denial of service) attacks which lead to site crashes. Thus, hacktivists deny access to a particular service or website. In addition, this kind of attack may also mean a huge hosting bills the website owner is presented with [10, 17].

When it comes to stealing data, hacktivists usually do it in order to expose sensitive files or records belonging to a target publicly over the Internet — a method typically deployed to expose targets with something to hide, such as large corporations or governments [14]. This kind of activities is also related to the so-called doxxing. The word 'dox', meaning documents or 'docs', refers to the action of revealing private, often highly personal information that allows identifying someone, on the Internet. The data may comprise a person's real name, date of birth, phone numbers, addresses and so on. Hacktivists doxx their opponents, such as public figures, celebrities or individual members of targeted organisations, in order to intimidate them or bring embarrassment upon them. They also are known for website defacements, i.e., tampering with the site's appearance or data integrity. This can range from daubing 'political graffiti' across Internet to corrupting systems, e.g., manipulating polls and skewing online votings [18]. Finally, hacktivists resort to virtual sit-ins, i.e., voicing their opinions by simultaneously accessing a website multiple times, creating disruption of the target website. It is geared toward slowing down, or even crashing a target website, thus preventing access to its regular users [19].

The transporting of activism to the digital space has transformed it. As protesters became anonymous and their causes borderless, civil disobedience turned into disruption. The difference is — now, just a few skilled individuals are enough (or even enjoy more significant power) to cause more disruption with a single click than masses of people occupying streets [20].

Some of the most well-known hacktivists and hacktivist groups include the following (Tables 1 and 2).

3.1 Profile

Constructing the profile of a typical hacktivist is not that simple. This mixed group of people may consist of individuals ranging from script kiddies to professional black hats, from bored teens to rogue non-state actors and from lone cyber-vigilantes to cyber-groups [10]. 'They may range from local units composed of no more than a dozen persons to large transnational organisms with several satellite sub-groups' [11]. What they do have in common is that they are almost always personally anonymous, yet they seek a collectively distinguishable recognition [13]. Also, most of them connect through a variety of non-mainstream social networking services, such as forums and message boards like '4chan', wikis like 'Encyclopaedia Dramatica' or specific IRC channels [10]. As hacktivists often work alone, their attacks are extremely difficult to predict or even respond to quickly and whether they are a network administrator, a mid-level IT person or even a college student, there is no way of knowing in advance who they are or when they will strike [17].

3.2 Motivation

Hacktivism merges traditional political activism with the Internet; disgruntled individuals or groups use hacking to bring about political or social change, and cyberspace

Table 1 Some well-known hacktivist groups

Name	Their target	Methods	Known for
Anonymous	At first: • 4chan message board's users • Internet personalities Later: • Political and ideological activism, e.g., attacks on the church of Scientology • Campaigns aimed at protecting Internet freedom (e.g., Stop Online Piracy (SOPA) and the Protect Intellectual Property Act (PIPA)) • Responding to military operations in the Gaza Pillar of Defence and the Russian manoeuvres in Crimea [11] • Targeting the online arms of the terrorist group ISIS, the 2016 presidential campaign of US President Donald Trump and Ku Klux Klan's (KKK) websites [14] [21]	• Pranks • Online abuse • Doxxing • DDOS attacks	• In fact, they are responsible for defining modern hacktivism • The Guy Fawkes mask they wore has become the symbol of hacktivism
Edward Snowden/Wikileaks	Leaked thousands of documents to the media, thus revealing the surveillance practices that he believed violated the right to privacy of the American citizens	Downloading and collecting the documents from the National Security Agency (NSA)	• Has yet to be tried for his actions, • Was granted temporary asylum in Russia [22, 23]
LulzSec	• Fox.com • PBS broadcaster • Gaming companies such as Nintendo and Bethesda Studios • Playstation network …and many more, 'to gain attention, embarrass website owners and ridicule security measures'	• Stealing and disseminating private data • Taking websites and systems down	• Their downfall began after some members attacked an FBI-affiliated website and brought themselves to the attention of federal authorities in the USA • Several members were arrested and charged [24–26]
Impact Team	Extramarital dating site Ashley Madison, which the group found immoral	• Stealing data of 32+ million users of the website • Demanding the site be taken down • Eventually — releasing the data publicly	• They argued they had to reveal the data as the website users were 'cheating dirtbags [who] deserve no such discretion' [14, 20]

Table 2 Some examples of other noteworthy hacktivist groups

Name	Ideology	Description
Redhack	• Radical leftist • (Self-identified) Marxist-Leninist	• An organisation from Turkey, one of the few there who are not 'patriotic hackers' [13]
Cyber Berkut	• Pro-Russian hacker group	• Known for repeatedly attacking NATO and Ukrainian websites [11]
The Red Hacker Alliance	• Chinese patriotic	• One of the most well-known hacker groups, has been particularly active since the late 1990s [13]
The Chaos Computer Club (CCC)	• Fighting against censorship and nuclear testing	• One of the earliest hacktivist groups • Its members not only shut down websites but also tried to disturb telecommunication infrastructures as a form of protest [13]
Worms Against Nuclear Killers	• Protested the launch of the Galileo probe into orbit	• Reportedly, due to the attack the project lost half a million dollars in lost time and resources [14]
Di5s3nSi0N	• Muslim hacking collective	• They have been targeting Amaq, the main online outlet and 'official' news agency of terror organisation ISIS/Daesh. They leaked the data of the Amaq's newsletter's subscribers and repeatedly took Amaq's website down [27]

becomes the medium that allows them to express their discontent [3, 21]. In addition to this, hacktivism can indirectly be utilised to reach hidden, underlying goals of political, military or commercial character; in some sense, hacktivists may be perceived as a cyberspace equivalent to the groups carrying out acts of civil disobedience, such as Greenpeace, and their actions, typically, have no lasting effect on their targets beyond reputation [11] [16]. Hacktivists (unlike typical cybercriminals) are usually not motivated with financial profit [17]. Rather, one may say they are motivated by a cause, 'burning rage inside them', no matter if they wish to embarrass celebrities, highlight human rights, wake up a corporation to its vulnerabilities or go after entities whose ideologies they do not find agreeable, who they feel do not align with their political views or practices [10, 28]. Hacktivists may also steal and disseminate sensitive, proprietary or, sometimes, classified data in the name of free speech [10]. It is worth noting that, unlike most other hackers, hacktivists do crave publicity; this is why they often enter public, popular social media platforms, like Facebook, Twitter or YouTube. Hence, they are eager to, e.g., share the data they have stolen [15].

4 Internet trolls

Another kind of Internet actors are the so-called Internet trolls. Although the idea of 'trolling' has been known for many years, there is a lack of academic consensus on the matter, owing to the fact it is a complex phenomenon [29, 30]. Generally speaking, the term 'trolling' has been used to describe all types of malicious or harassing activities in the Internet, both verbal and behavioural ones, with the latter mostly happening in the sphere of online gaming [30, 31]. However, beyond this basic agreement, almost every researcher has coined their own definition of trolling. For instance, Bishop [32] defines trolling as the 'act of posting a message (…) that is obviously exaggerating something on a particular topic', 'for the entertainment of oneself, others or both' [33]. Herring et al. [34] indicate that it 'entails luring others into often pointless and time-consuming discussions'. Another definition points it out that a troll 'posts a deliberately provocative message (…) with the intention of causing maximum disruption and argument' [35]. Cambria et al. [36] define trolling as 'emotional attacks on a person or a group through malicious and vulgar comments in order to provoke response'. Shachaf and Hara [37] call trolling 'repetitive, intentional and harmful actions that are undertaken in isolation and under hidden virtual identities (…) consisting of destructive participation in the community'. Hardaker [38] says trolling is 'the deliberate use of impoliteness/aggression, deception and/or manipulation (…) to create a context conductive to triggering or antagonising conflict'. Finally, Golf-Papez and Veer [39] define it as 'deliberate, deceptive and mischievous attempts that are engineered to elicit a reaction from the target(s), are performed for the benefit of the troll(s) and their followers and may have negative consequences for people and firms involved'. As one may notice, although the older definitions of trolling concentrated on stirring up discussions mostly for fun and amusement, the newer ones point it out that trolling aims to do emotional harm. The most recent ones emphasise the disruptive and deceptive nature of the acts of trolling. It may be thus stated that Internet trolling has become much more serious, harmful and potentially dangerous than it initially used to be. In fact, its potential as a tool of spreading deceptive and made-up content has already been utilised by many individuals and organisations. In the recent years, a new sub-group of trolls have caught the media's attention: the political trolls. They are usually 'user accounts whose sole purpose is to sow conflict and deception', their intent being 'to harm the political process and create distrust in the political system' [40]. Political trolls may be further divided into three groups: political bots masquerading as real users (spreading spam and harmful links), organised trolls (including hate and persecution campaigns) and the ones who spread 'fake news' [41]. Recently, the media have revealed several notorious cases of state-sponsored political trolling. For instance, before the 2016 US presidential elections, thousands of troll accounts injected false tweets or fake news in support or against certain candidates, aiming at creating discord and hate [42, 43]. The accounts were traced back to Russia and allegedly funded by the Russian government [40]. Russian trolls were also highly active in Australia, in the years 2015–2017. Their actions included, e.g., spreading tweets undermining support for Australian government in the light of its response to the downing of flight MH17 [44]. In August 2019, Polish Deputy Justice Minister Łukasz Piebiak resigned after it had been revealed he allegedly arranged and controlled a hate campaign and sought to discredit judges who were critical of the government's judicial reforms; it was done by planting media rumours about the judges' private lives. The incident sparked a massive outcry in the country [45, 46].

4.1 Profile

As with hacktivists, the profile of a 'typical' troll is difficult to establish; this is mainly due to the fact that the definitions of a troll vary to a great extent. Even so, there are some common traits to be found, which repeat across numerous study results and papers on the matter. For example, researchers consistently refer to the 'dark tetrad', i.e., specific psychological traits that many Internet trolls possess. The tetrad is constituted by narcissism, psychopathy, Machiavellianism and everyday sadism. Narcissism is the excessive sense of self-love and self-admiration, psychopathy means the absence of empathy, Machiavellianism is used to describe a detached, calculating, manipulative attitude, and everyday sadism means that a

person enjoys cruelty that is present in everyday culture; the cruelty may be part of violent films or video games, or refer to real-life events, like police brutality. Of the four traits, it is sadism which is believed to be the most closely associated with trolling behaviours on the Internet. Oher studies suggest that cyber trolls are often characterised by low self-esteem, conscientiousness and internal moral values. The results of the study aimed at revealing the demographic of trolls suggest that a typical troll is male and lacks affective empathy. In addition, the so-called online disinhibition effect may contribute to some people becoming trolls. The idea behind it is that some people, if they think they are anonymous, tend to dissociate from the harassment [47, 48].

4.2 Motivation

The motives of internet trolls also greatly vary and depend on the kind of troll. Papers suggest several possible motivations, such as everyday sadism, a need for attention, trying to boost one's low self-confidence, lack of empathy, a desire for amusement or simply the fact that trolls' victims differ from them. However, trolls in a way may also be fighting for their 'greater good', as one study suggested that trolls are motivated by the fact that their actions create a kind of online community. Engaging in hate speech and online harassment is a way of cementing or building the status in the group, gaining a sense of belonging. An alternative view suggests that part of the trolls are not atypical or antisocial; in fact, they are regular Internet users who simply engage in copycat behaviour, that is they mimic the trolling behaviours they are exposed to in social media. The motives for gaming trolls, besides the ones presented above, include responding to being trolled by other players, being bored or in a negative emotional state and wishing to win no matter what. In other words, they are motivated by personal enjoyment, taking their revenge on other trolls, or thrill-seeking [49, 50]. Finally, it is also worth mentioning that studies have shown Internet trolls tend to rationalise their behaviour, i.e., downplay the consequences of their actions, and thus minimise their blame and hurt others without guilt, so again — their motives may not be utterly mischievous, at least in their own eyes [47, 48]. Just the opposite — even if they might be perfectly aware of the fact that what they do is wrong, they feel their actions are justified, sometimes in a very twisted way.

5 Cyber militia

Cyber militias are defined as 'a group of volunteers who are willing and able to use cyber-attacks in order to achieve a political goal' [51]. The definition also encompasses the ways the members of a militia contact and gather: 'the members communicate primarily via Internet and, as a rule, hide their identity'. The anonymity is usually achieved by adopting hacker aliases. Cyber militias may be permanent or be formed ad hock. The definition emphasises the fact of the members being volunteers, as they participate in the cyber militia of their own free will. They are not contractually obliged to it. Usually, they do not receive any money for their actions (there are exceptions to this; sometimes the leaders of a cyber militia are paid salaries [52]). In addition to this, a member of a cyber militia decides upon their level of commitment. They may also leave it whenever they wish. This is the main difference between the members of cyber militias and the people who join a government-run cyber-attack unit. Ottis [51] also indicates that the word 'political' in the aforementioned definition 'refers to all aims that transcend the personal interest of the volunteer. This includes religious views, nationalistic views, opinions on world social order etc.' [51, 53]. According to the researcher, most cyber militias meet the following criteria:

- The communication within a militia is centralised; the communicating, planning and coordinating a cyber-attack campaign usually relies on on-line forums and instant messaging services.
- Usually, there is no direct state support or control of the militia. If there is direct state support, the unit should be considered an organic part of the state rather than the cyber militia.
- The members are loosely connected in real life; the leadership/core group may be personally acquainted, but the rest of the members usually do not know any other members, or know a few of them.

Forum posts allow identifying the roles certain members play in the militia. They can be divided into two categories: 'officer' roles — leaders, trainers, suppliers, etc., and 'soldiers' and 'camp followers'. The leaders motivate to act, coordinate actions and give the directions of attacks. The trainers give instructions of all kinds, including the ones concerning reconnaissance and attacks, as well as covering them. The suppliers are responsible for providing scanners, malware, attack kits, etc. 'Soldiers' are the ones who take active part in attacks. They usually remain quiet on the forum or are ordered to report the results of their actions. Lastly, the camp followers follow the forum threads out of curiosity but do not take part in any campaigns [51].

One of the most well-known cases of the employment of cyber militia is Estonia, where volunteer hackers were recruited to respond to cyber-attacks. Those civilian defence corps grew out of the aftermath of a 2007 attack, when banking, government, news and other websites were taken online and the authorities put the blame on Russian operatives. According to experts, the attacks have been one of the worst cases of state-sponsored warfare to date. Although the Estonian cyber militia hackers are mostly civilians, they have

been trained to handle this kind of assaults on hospitals, banks and military bases, as well as on, e.g., voting systems. Their commander says that the threat is taken as a given. His militia consists of all kinds of white-hat types, including amateur IT workers, economists, lawyers and so on. Some of their actions include running drills with troops, doctors and air traffic controllers, and gauging officials' responses to realistic attacks, for example, by sending out e-mails with sketchy links or dropping infected USB sticks. Allegedly, a CD labelled with a picture of Russian porn star in a bathing suit proved very effective bait for military officials. As a result, at present, the country's military computers turn off after having detected an unknown disc or USB drive. Officially, the militia is part of Estonia's national guard. Estonian's cyber militia has inspired many security officials elsewhere, including countries like France, Latvia and the USA [52].

China has also relied heavily on cyber militias. According to researchers, the collective membership of cyber militias in China has already amounted to over 10 million people. Most probably, the goal of the cyber units is to provide logistic support and rear area security for active duty units — similarly to militias in general. One of the most well-known faces of the Chinese cyber militias are the infamous, popular, nationalism-driven 'patriotic hackers' [54].

In the United States of America, one of the cyber militia, Missouri National Guard Team, has recently launched a non-profit organisation in order to share their network security monitoring system 'built by cyber warriors for cyber warriors' [55]. In Ohio, a bill has been introduced that is going to create a civilian cyber militia, the task of which would be to protect the state's critical government agencies and election systems. If the bill is passed, a new volunteer unit would be created under the authority of the Ohio adjutant general and operate at the same level as National Guard. The Ohio Cyber Reserve would recruit 'individuals who are interested in improving Ohio's cyber posture'.

In India, in 2011, Information Technology Minister Kapil Sibal called for a community of ethical hackers to help defend Indian networks. Reportedly, India has been considering using patriotic hackers for offensive operations, too [56].

There is a lot of controversy surrounding cyber militia. Although experts enlist the possible positive outcomes of employing the 'members of the cyber militia, recruited among a pool of civilians with the requisite forensic and IT skills', it is feared that the members of militias may use their skills and knowledge against other states with no authorisation, or even turn them back on home networks. Militias may also ignore orders, especially during a crisis. As Segal sums it up, 'patriotic geeks might be the answer to a lot of policy challenges. But in terms of cybersecurity, it may be best to either bring them completely into the fold, or keep them at arm's length' [56].

5.1 Profile

Ottis [7] has distinguished three models of cyber militia: the Forum, the Hierarchy and the Cell. The models refer to the operating principles of the militia, and the properties and relationships between the members of cyber militia.

The Forum consists of people who do not know one another in real life but are interested in a particular subject, meet online in a web forum, IRC channel, social network and interact there. The place is easily accessible over Internet, easy to find and provides visibility to the agenda of the group; it may be also used to recruit new members. The Forum mobilises in response to an event that is important to its members; it is more ad-hoc than permanent. It forms quickly; its attacks are hard to analyse and counter. However, as it comprises mostly of people inexperienced in cyber-attacks, it is highly reliant on the instructions and tools provided by the more experienced members of the Forum. Moreover, due to the nature of the utilised communication channels, it is relatively easy to infiltrate and de-anonymise.

Another model of a volunteer cyber force is a hacker cell. It encompasses several hackers who perform attacks on a regular basis; this may last over extended periods of time. The members are experienced in the use of cyber-attacks, some of them may be even involved in cybercrime. They are likely to know one another in real life; the cell is often built on mutual trust. The Cell, in response to a long-term problem, may exist for a long period of time but is able to mobilise very quickly and difficult to infiltrate.

Finally, the Hierarchy is the most organised model, suitable, e.g., for state-sponsored groups. The model resembles other military units, with sub-units specialised in some specific task or roles (like reconnaissance, infiltration, breaching and training). As the actions of a state-sponsored militias are attributable to the state (by definition), it is crucial that the militia is able to be controlled. However, it must be noted that not every cohesive group that adopts a command structure is sponsored by the state. State-sponsored militias may also require identified membership. The militias of this type may exist for a long time, even if no conflict occurs, and engage in training and recruitment in the 'peacetime'; if they are sponsored by the state, apart from money, they may expect infrastructure, cooperation with law enforcement or intelligence community.

5.2 Motivation

In order to engage in cyber militias' activities, a person must be driven by patriotism, or at least concerned about the matters of a particular nation. They may also be motivated by political reasons, e.g., strongly oppose a foreign country's governmental policies or disagree with them. Ottis [7] also suggests that some hackers engaged in cyber militia are confident in their

skills and proud of their achievements. Some of them, after performing an attack, may even leave their aliases or affiliations, in order to claim bragging rights and thus boost their ego [7].

6 Nation-state actors

It must be noted that when speaking about the cyberspace actors who believe they do good, one could also mention the nation-state actors. This kind of actors has been presented in detail in [8, 57–59]. However, this paper does not categorise nation-states as the 'stray sheep', as they are aware of what they are doing and their actions are deliberate, calculated and planned. With the nation-state actors, the ethical issue is of a different nature. Although their nation may grant them the right by law to carry out their undertaking, what they do might be strictly illegal in other countries, especially the ones they act against.

7 Discussion and conclusions

The presented kinds of cyberspace actors do differ from the image of a hacker-cybercriminal that has become mainstream owing to news items and pop culture in general. All of the actors rationalise their actions in various ways and are able to pinpoint their motives and reasons behind them, despite the fact the cyber-attacks they carry out are objectively illegal. Their actions might spark even more controversy, as substantial part of their activities are generally of lawless nature. Thus, they divide the public opinion. The actors themselves often claim their actions are for the greater good, e.g., in order to encourage better security or a more responsible custodianship of personal data, but does the fact that they wish to raise awareness about a particular matter and bring about some kind of social or political change make them 'good'? Some people actually applaud vigilante hackers who take the law into their own hands; is it enough to explain their actions, though? [14, 15]. Actually, how people categorise hacktivists, trolls and cyber militia members depends mostly on whether they sympathise with the same causes they do [20]. As Lohrman [60] describes this moral and ethical dilemma: 'There is an evolving definition of right and wrong regarding hacking. For example, I may think that Edward Snowden stealing NSA records was wrong. However, I may also agree that the information he disclosed was valuable to society to help protect online privacy. Although I do not believe that the ends justify the means, millions of Americans now believe that Snowden was a hero. Bottom line, they think his illegal actions were justified' [60]. However, what if the hackers' targets are not only faceless institutions, businesses and governments but also 'regular' individuals, and then, what was meant to be transparency turns into harassment [20]? With all the three discussed groups, there is the tension caused by the fact that what seems to be right to do, does not necessarily have to be legal or ethical. Ironically, sometimes perfectly legal actions are not ethical, or just the opposite — people may tolerate the law being broken if they believe the cause is worth it. However, the three groups vary in the intensity of these tensions, the balance between the ethics, morality and law, and the severity of the possible damage and harm their members are capable of doing.

7.1 Limitations and further work

This paper bases on a comprehensive review of recently published literature, including scientific articles, as well as various other sources. However, cyberspace is fickle and one might soon witness major shifts in the ecosystem, whether they be related to technical advancements or global political situation. The matter needs constant monitoring, following trends and drawing conclusions anew, in order for the divisions, names and drawn profiles to stay up-to-date and relevant. Thus, it has been planned for the research presented in this paper to be continued, and the changes in the ecosystem reported accordingly, if they do happen.

7.2 The implications for cybersecurity

The today's cyberspace is a complex and complicated ecosystem. Lumping the various cyber threat actors together might prove to be as unwise as underestimating the threat in general. Being aware of the various motives of the actors, the forces that drive them, the ways they form groups, etc., is also significant from the cybersecurity's point of view. Cybersecurity and cybercrime are forever and inherently connected; one cannot exist without the other [61]. For cybersecurity experts, being one step ahead of wrongdoers requires knowing as much as possible about them; for instance, being of the ways in which political trolls or hacktivists congregate could be enough to infiltrate them and get the information on the actions they are planning; being profoundly knowledgeable about the attack vectors they apply helps adopt the speediest or most comprehensive solutions. Lastly, not all the hackers are equally dangerous; some of them are rather more of a nuisance than a real threat. Encouraging increased awareness of the matter amongst cybersecurity experts may in turn help them produce the most appropriate response and eventually contribute to creating a safer, more friendly cyberspace.

7.3 Final conclusions

This paper has attempted to construct the profiles of 'typical' hackers who are not driven by malicious intents and present

the motivations behind the cyberattacks they perform. However, it is not possible to paint a simple, black and white image of the matter due to its remarkably diverse and complicated nature. Cyberspace is constantly developing. As a consequence, the future will surely bring even more difficult situations and ethical dilemmas related to hackers. It seems unavoidable, even if they break into systems with the best intentions.

Apart from the dilemmas of purely ethical nature, there is also the question of penalising certain behaviours in cyberspace. Even if people agree with the hackers' ideology or sentiment, and rationalise their actions, the law is the law and crime is to be punished. This issue does not only pose a considerable challenge for policymakers and law enforcement but also creates another ethical dilemma; there might not be a simple answer to. As it turns out, some hackers might be inflicting considerable harm to others, and yet, they will be warmly applauded for that. In cyberspace, the 'greater good' sometimes is a surprisingly relative concept.

Funding Open Access funding enabled and organized by Projekt DEAL. This work is funded under SIMARGL project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833042.

References

1. Pavlik K (2017) "Cybercrime, hacking, and legislation," *J. Cybersecurity Res.*, vol. 1, no. 1.
2. Chantler N (1995) "Risk: the profile of the computer hacker.," Curtin Business School, Australia.
3. Romagna M, van den Hout NJ (2017) Hacktivism and website defacement: motivations, capabilities and potential threats. In: *27th Virus Bulletin International Conference*
4. Maiwald E (2003) *Network Security A Beginner's Guide*.
5. Li X (May 2017) A review of motivations of illegal cyber activities. Kriminologija Soc Integr 25(1):110–126
6. Madarie R (2017) Hackers' motivations: testing Schwartz's theory of motivational types of values in a sample of hackers. Int J Cyber Criminol 11:1
7. Ottis R (2011) A systematic approach to offensive volunteer cyber militia (Vabatahtlikud küberründegrupid: süsteemiteoreetiline vaade). Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Informaatikainstituut
8. Pawlicka A, Choraś M, and Pawlicki M (2020) "Cyberspace threats," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–11.
9. Ablon L (2018) "The motivations of cyber threat actors and their use and monetization of stolen data: hearings before the Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, United States House, 115th Cong. 1".
10. Sigholm J (2013) Non-state actors in cyberspace operations. J Mil Stud 4(1):1–37
11. Ohlin D, Govern K, and Oxford CF (2015) "Nicolò Bussolati 'the rise of non-state actors in cyberwarfare'".
12. Jeff Shantz JT (2013) Cyber disobedience: re-presenting online anarchy. Zero Books, Hants
13. Dogan B (2019) "Contextualizing hacktivism: the criminalization of Redhack," *CARGC Pap.*, vol. 10.
14. Afifi-Sabet K, "What is hacktivism?" (2018). [Online]. Available: https://www.itpro.co.uk/hacking/30203/what-is-hacktivism. [Accessed: 20-Jul-2019].
15. Mansfield-Devine S (2011) Hacktivism: assessing the damage. Netw Secur 2011(8):5–13
16. C. C. for C. Security, "Cyber threat and cyber threat actors" (2018). [Online]. Available: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors. [Accessed: 20-Jul-2019].
17. "Proactive defense: understanding the 4 main threat actor types." [Online]. Available: https://www.recordedfuture.com/threat-actor-types/.
18. Pompon R (2017) Doxing, DoS, and defacement: today's mainstream hacktivism tools. *Application Threat Intelligence*
19. "Virtual sit-in," *Techopedia*. [Online]. Available: https://www.techopedia.com/definition/29626/virtual-sit-in. [Accessed: 20-Jul-2019].
20. Magal P (2019) "Who are the hacktivists?".
21. Gargano F (2019) "Three common threat actors and the one you might not know about".
22. Benton B (2015) "The misinformers: Edward Snowden, Aaron Swartz and the troubled relationship between hacktivists, mass media and American Government".
23. Sorell T (2015) Human rights and hacktivism: the cases of Wikileaks and Anonymous. J Hum Rights Pract 7(3):391–410
24. Arthur C (2013) "LulzSec: what they did, who they were and how they were caught", *The Guardian.*
25. Baraniuk C (2013) "Ten hacktivists who shook the web". [Online]. Available: https://www.dazeddigital.com/artsandculture/article/16368/1/ten-hacktivists-who-shook-the-web. [Accessed: 20-Jul-2019].
26. Stamm E (2015) "We are all anonymous: beyond hacktivist stereotypes," *Spectra*, vol. 4, no. 2.
27. McCallion J (2017) "Anti-Isis hacktivists compromise terrorists' website | IT PRO", *ITPro*.
28. Fowler K (2016) Data breach preparation and response.
29. McCoy J (2019) "7 Effective tactics to defeat Internet trolls," *Search Engine Journal*.
30. Cook C, Schaafsma J, Antheunis M (2018) Under the bridge: an in-depth examination of online trolling in the gaming context. New Media Soc 20(9):3323–3340
31. Jussinoja T (2018) Life-cycle of Internet trolls. University Of Jyväskylä
32. Bishop J (2012) "Tackling Internet abuse in Great Britain: towards a framework for classifying severities of 'flame trolling'".
33. Bishop J (2013) The effect of de-individuation of the Internet troller on criminal procedure implementation: an interview with a hater. *Int. J. Cyber Criminol*

34. Herring S, Job-Sluder K, Scheckler R, Barab S (2002) Searching for safety online: managing 'trolling' in a feminist forum. Inf Soc 18(5):371–384
35. Entity Alien, "Urban Dictionary: troll" (2002). [Online]. Available: http://www.urbandictionary.com/define.php?term=troll.
36. Cambria E, Chandra P, Sharma A, Hussain A (2010) "Do not feel the trolls".
37. Shachaf P, Hara N (2010) Beyond vandalism: Wikipedia trolls. J Inf Sci 36(3):357–370
38. Hardaker C (2013) Uh. . . . not to be nitpicky,,,,,but…the past tense of drag is dragged, not drug.': an overview of trolling strategies. J Lang Aggress Confl 1(1):58–86
39. Golf-Papez M, Veer E (2017) Don't feed the trolling: rethinking how online trolling is being defined and combated. J Mark Manag 33(15–16):1336–1354
40. Addawood A, Badawy A, Lerman K, and Ferrara E (2019) "Linguistic cues to deception: identifying political trolls on social media," in *Proceedings of the Thirteenth International AAAI Conference on Web and Social Media (ICWSM 2019)*.
41. Gorwa R (2017) "Computational propaganda in Poland: false amplifiers and the digital public sphere".
42. Pennycook G and Rand D G (2017) "Who falls for fake news? The roles of analytic thinking, motivated reasoning, political ideology, and bullshit receptivity", *SSRN Electron. J.*
43. Gerber TP, Zavisca J (2016) Does Russian propaganda work? *Wash Q* 39(2):79–98
44. Sear T and Jensen M (2018) "Russian trolls targeted Australian voters on Twitter via #auspol and #MH17".
45. Charlish A (2019) "Polish deputy minister resigns over judge trolling scandal". [Online]. Available: https://www.reuters.com/article/us-poland-politics-judiciary/polish-deputy-minister-resigns-over-judge-trolling-scandal-idUSKCN1VA1BJ. [Accessed: 24-Aug-2019].
46. Gf T (2019) "Onet.pl: deputy justice minister behind campaign to discredit judges". [Online]. Available: https://www.tvn24.pl/tvn24-news-in-english,157,m/polish-deputy-minister-orchestrated-trolling-against-judges-onet-pl,962578.html. [Accessed: 24-Aug-2019].
47. Buckels E (2019) "Probing the sadistic minds of internet trolls", *Character Context*.
48. Buckels EE, Trapnell PD, Andjelovic T, Paulhus DL (2019) Internet trolling and everyday sadism: parallel effects on pain perception and moral judgment. J Pers 87(2):328–340
49. Sanfilippo MR, Shengnan Y, and Fichman P (2017) "Managing online trolling: from deviant to social and political trolls," in *Proceedings of the 50th Hawaii International Conference on System Sciences*.
50. M. & S. Department for Digital, Culture, "Rapid evidence assessment: the prevalence and impact of online trolling" 2019.
51. Ottis R (2010) "Proactive defense tactics against on-line cyber militia," in *ECIW2010-Proceedings of the 9th European Conference on Information Warfare and Security*.
52. Drozdiak N (2019) "One of Russia's neighbors has security lessons for the rest of us", *Bloomberg Businessweek*.
53. Applegate S (2011) Cybermilitias and political hackers: use of irregular forces in cyberwarfare. IEEE Secur Priv Mag 9(5):16–22
54. Lyall N (2018) China's cyber militias. *The Diplomat*, Mar
55. Seffers GI (2019) "Cyber militia launches nonprofit to share technology", *SIGNAL AFCEA*.
56. Segal A (2012) "The rise of Asia's cyber militias," *The Atlantic*.
57. Ahmad A, Webb J, Desouza KC, Boorman J (2019) Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput Secur 86:402–418
58. Lemay A, Calvet J, Menet F, Fernandez JM (2018) Survey of publicly available reports on advanced persistent threat actors. Comput Secur 72:26–59
59. Desouza KC, Ahmad A, Naseer H, Sharma M (2020) Weaponizing information systems for political disruption: the actor, lever, effects, and response taxonomy (ALERT). Comput Secur 88:101606
60. Lohrman D (2015) "Hacking for cause: today's growing cyber security trend".
61. Pawlicka A, Choraś M, Kozik R, Pawlicki M (2021) First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. *Pers. Ubiquitous Comput*, Jan