BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES

ÚSTAV JAZYKŮ

HACKTIVISM: POLITICS, CRIME, OR FUN?

HACKTIVISMUS: NÁSTOJ POLITIKY, ZLOČINU, NEBO ZÁBAVY?

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR
AUTOR PRÁCE

Jindřich Raška

SUPERVISOR
VEDOUCÍ PRÁCE

Mgr. Miroslav Kotásek, Ph.D.

BRNO 2022

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Bachelor's Thesis

Bachelor's study field **English in Electrical Engineering and Informatics**

Department of Foreign Languages

Student: Jindřich Raška ***ID:*** 220922

Year of study: 3 ***Academic year:*** 2021/22

TITLE OF THESIS:

Hacktivism: Politics, Crime, or Fun?

INSTRUCTION:

The aim is to name the different forms hacktivism can take today.

RECOMMENDED LITERATURE:

Gabriella Coleman: Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. London: Verso 2014.

Martin Moore: Democracy Hacked. Oneworld Publication 2018.

Christina Dunbar-Hester: Hacking Diversity: The Politics of Inclusion in Open Technology Cultures. Princeton UP 2019.

Date of project specification: 10.2.2022 ***Deadline for submission:*** 31.5.2022

Supervisor: Mgr. Miroslav Kotásek, Ph.D.

doc. PhDr. Milena Krhutová, Ph.D.
Subject Council chairman

Abstract

The aim of the thesis is to analyze the phenomenon of hacktivism, its purpose, its impact on society, and the motivation of its participants. The term hacktivism comprises terms activism, in most cases political, and computer hacking, a criminal act aimed at exploiting a computer system. Hacktivists are mostly, like any other activists, organized in groups to effectively achieve their goals. This study focuses on the origin, motivation, and consequences of the hacktivist actions, especially on actions of an infamous group called Anonymous, including exemplary cases from history.

Keywords

Activism, Anonymous, cybercrime, cybersecurity, Internet freedom, hacktivism

Abstrakt

Cílem této bakalářské práce je zanalyzovat fenomén zvaný hacktivismus, jeho význam, dopady na společnost a motivaci jeho aktérů. Termín hacktivismus se skládá ze dvou následujících termínů; aktivismus, který bývá ve většině případů politicky motivovaný a hacking, jenž se jedná o kriminální činnost za účelem zneužití chyby nebo nedokonalosti výpočetního systému. Za účelem efektivního dosažení svého cíle, se aktéři hacktivismu, stejně jako jiní aktivisté, většinou organizují do skupin. Práce je též zaměřena na motivaci a následky konání těchto organizovaných skupin, zejména na skupinu s názvem Anonymous, s exemplárními příklady jejich akcí z minulosti.

Klíčová slova

Aktivismus, Anonymous, kyberkriminalita, kybernetická bezpečnost, svoboda internetu, hacktivismus

Bibliographic citation

Printed work citation:

RAŠKA, Jindřich. *Hacktivismus: nástoj politiky, zločinu, nebo zábavy?*. Brno, 2022. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/142535. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků. Vedoucí práce Miroslav Kotásek.

Electronic source citation:

RAŠKA, Jindřich. *Hacktivismus: nástoj politiky, zločinu, nebo zábavy?* [online]. Brno, 2022 [cit. 2022-05-11]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/142535. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků. Vedoucí práce Miroslav Kotásek.

Author's Declaration

Author:	*Jindřich Raška*
Author's ID:	*220922*
Paper type:	*Bachelor Thesis*
Academic year:	*2021/22*
Topic:	*Hacktivism: Politics, Crime or Fun?*

I declare that I have written this paper independently, under the guidance of the advisor and using exclusively the technical references and other sources of information cited in the project and listed in the comprehensive bibliography at the end of the project.

As the author, I furthermore declare that, with respect to the creation of this paper, I have not infringed any copyright or violated anyone's personal and/or ownership rights. In this context, I am fully aware of the consequences of breaking Regulation S 11 of the Copyright Act No. 121/2000 Coll. of the Czech Republic, as amended, and of any breach of rights related to intellectual property or introduced within amendments to relevant Acts such as the Intellectual Property Act or the Criminal Code, Act No. 40/2009 Coll., Section 2, Head VI, Part 4.

Brno, May 27, 2022 ----------

author's signature

Acknowledgement

I would like to thank my supervisor Mgr. Miroslav Kotásek, Ph.D. for his invaluable advice and support and family for their support and patience.

Contents

LIST OF FIGURES

1. INTRODUCTION

The world and society are constantly evolving. Modern technology, having a significant impact on this development, has become an important component of everyday life. With the continuous advancement of information technology, this development uplifted many aspects of our life and society, including activism. This thesis deals with hacktivism, which is activism that uses modern information technology to achieve its objectives. In contrast to any other form of hacking, the motivation of so-called hacktivists is not the personal or financial benefit of its participants. In general, hacktivists act in the name of greater good of a certain collective or society. However, it is possible to find a few exceptions everywhere else. A phenomenon that originally started as a form of entertainment on internet forums quickly evolved into a powerful tool that is capable to influence the opinion of the general public and enforce changes within the society.

In this thesis, I will analyze several various aspects of hacktivism, its background, motivation, consequences, used techniques, and methods, from its early development up to the present day. This thesis comprises of seven chapters, including this introduction. In Chapter Two, I have been concerned with the different types of hacktivist motivation and described the background behind their cause and their possible objectives. Chapter three contains the history of hacktivism and its development from the 1980s up to the current state in the Spring of 2022, with multiple exemplary cases from each period. At the end of this chapter, I have analyzed the recent development of hacktivism and its dynamics. The fourth chapter describes the different methods and techniques used by hacktivists for their activities, with a description of their purpose and functionalities. Chapter five contains the list of several notable hacktivist groups and whistleblowing collectives, that have had significant impacts on the development of hacktivism. In the sixth chapter, I have analyzed the implications and consequences of the hacktivists' actions, both positive and negative outcomes, and possible risks. The last chapter contains the conclusion, where I summarize this thesis and its findings.

The aim of my thesis was to analyze the current state of hacktivism, in particular, the nature of its activities and the goals pursued. To achieve this task, I had to analyze its history and development, to be able to compare it with its current status. As a primary source of information, I used professional books and articles, if available. To cover the recent events, it was necessary to use articles from mainstream media, thus parts of the thesis that contains this information may be disapproved in the future years, which is important to keep in mind. All the used relevant sources are listed in the literature section of the thesis. To avoid possible misinterpretation, I used various secondary sources not listed in the literature section for verification of the given information.

In an era of recurring cyberattacks, there is the need to separate the activities of hacktivists from hackers due to the different motivations and goals of each group. I hope

that my work will help to understand the thought processes that motivate hacktivists to act from multiple points of view.

2. MOTIVES OF HACKTIVISTS

The main factor that distinguishes hacktivists from other types of hackers is motivation. Generally, hacktivists do not seek financial or any other personal benefit except for the cases when they need resources to fund their activities, thus some hacktivists can even be sponsored by various organizations or individuals. Like any other activists, hacktivists believe that they are acting for the public good, or for the good of a certain collective. For some individuals hacktivism can also be a form of entertainment and those hacktivists can have pleasure by merging their amusement with what they consider a fight for the "greater good" or "for a better world". Hacktivism was in its beginnings strongly bounded to the hacker sub-culture, which was focused more on the entertainment gained by bypassing or abusing imperfections of devices or systems used in everyday life. For example, During the 1970s, Steve Wozniak and Steve Jobs, future founders of Apple Inc., designed a device that they called a "blue box". This "hacking device" was able to establish phone calls without paying any fee to the service operator. From the beginning, it was their form of entertainment. We can see some similarity to the hacktivist group called Anonymous, which originated as a meme, within the certain internet community and later became interested in various social and political issues that were relevant at the time. The main motivation of hacktivist participants may be for example political, social, or/and religious, depending on the focus of an acting individual or a hacktivist group and topic.

Socially motivated hacktivists mostly seek change within the society or try to highlight various social problems or topics, for example: war crimes, human rights and their violations, inequality within the society, or unethical behavior of certain institutions or individuals. Political motivation can be in many ways similar to the social, especially when we consider that any social issue can be politicized depending on the main discussed topic by the public. Religiously motivated hacktivists are concerned with the propagation of the beliefs of their church or sect. Since there are no well-known religiously focused hacktivist groups nor any significant events, it can be considered that the number of possible religious hacktivists is negligible. Furthermore, hacktivists can be even nationalistically motivated, which is typical for nations with high national pride or national sentiment. Furthermore, nationalistically motivated hacktivism can be observed in smaller nations that were or are under the rule of other, mostly stronger nations.

Many governments concluded that the modern trend of various social networks and rapid expansion of IT technologies and the internet across multiple fields may serve as a powerful tool. Similarly, to "real world" activists, even in cyberspace there exist hacktivists, whose activities are sponsored by national governments. In recent years, state-sponsored hacktivism has become a more common practice in the frequently discussed theory and practice of hybrid warfare. In the case of state-sponsored hacktivism, we are talking about hacktivists, who have similar goals as any other

hacktivists with the difference that their activities are partially or fully funded by state governments and thus sometimes it is unclear, whether these hacktivists should be called hacktivists or government paid hackers ("blackhat hackers").[1] In most cases, it is complicated to prove the association of a certain hacktivist group with its government.

An example could be the Syrian Electronic Army, which supports the government of President Bashar Al-Assad, a Chinese hacktivist group called Honker Union, or pro-Russian hacktivists called Killnet Group. State-sponsored hacktivism is a relatively young branch of hacktivism, which has not been analyzed in detail yet and much information about it stays unclear. Especially during the writing of this thesis, the Russo-Ukrainian war is ongoing, which is now the main topic on the internet and when there is regulated information flow. This additionally raises the question, of whether there are other known "traditional" hacktivist groups state-sponsored by any western government since their activities have risen with the start of the war when Anonymous has launched multiple caber-attacks on Russian institutions, companies, and influential individuals. Although there is yet no evidence to back up this instance, it might be possible due to fact that basically anybody can claim that they are members of Anonymous due to its decentralization.

3. EVOLUTION OF HACKTIVISM

Hacktivism went through approximately 40 years of development. To better understand the purpose of this form of activism and citizen participation in socio-political issues, it is important to go through its development and name most important events. The foundation of hacktivism was based on a hacking sub-culture, which started in the 1950s, with original purpose as a harmless amusement. Thus, hacktivism has been heavily influenced by constantly evolving hacking trends. This chapter is dedicated to brief history of hacktivism with notable events and examples of hacktivist actions. [2]

3.1 Origin in 1980s

The beginning of hacktivism can be traced back to the beginning of the 1980s. First hacker-activist were more focused on the values of the hacking subculture, rather than on sociopolitical motivations. These values were freedom of intellectual property and information, open-source software preference, unlimited access to computers and information. A perfect example from this period is a German hacker association named Chaos Computer Club, founded in 1981 in West Berlin and active even today.

3.2 Development in 1990s

The Malware called WANK (Worms against nuclear killer), unleashed by an unknown group of hacker-activists in 1989 is considered the first act of hacktivism. The malware attacked the network of DECnet computers running on VMS operating systems and spread into NASA and the US Department of Energy as a protest against the launch of a shuttle carrying radioactive plutonium. [3]

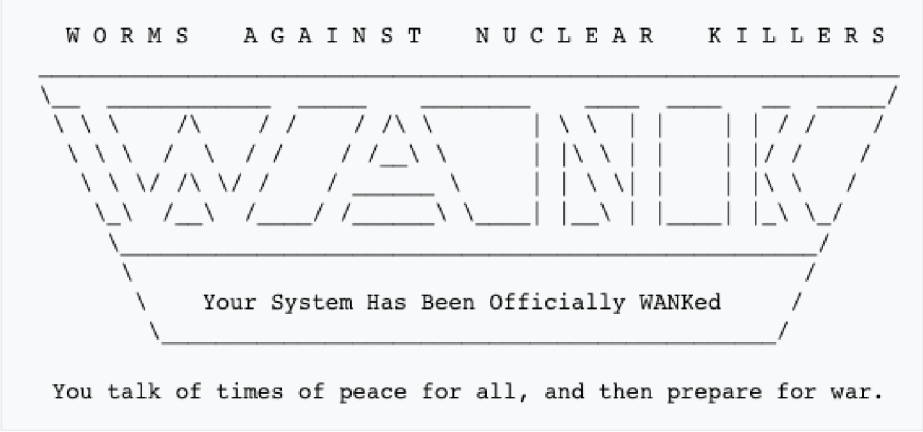


Figure 1: "Wank" message. (Source: https://www.realclearscience.com/blog/2019/01/12/when_nasa_got_wanked.html)

In November 1994, an activist group named Zippies, distributed malware by infected emails, that later launched a DDoS (Distributed denial of service) attack targeting British

Government websites. These websites were malfunctioning for more than a week. The attack has been launched as a protest against Prime Minister John Major and his Criminal Justice and Public Order Act. Section 63, 64 & 65 of the Act outlawed all music defined as: "music includes sounds wholly or predominantly characterized by the emission of a succession of repetitive beats". In addition, the act empowered police to stop rave with ten or more attendants and to turn away any person that was believed to willingly head towards to rave. [4]

In 1996, a member of Texas-based computer hacking group Cult of the Dead Cow nicknamed Omega, ironically coined the term “hacktivism” in his email correspondence with other members of the group. However, the term characterized the increasing political ethos of the group. Two years later, the group Milw0rn infiltrated the computer network of the Bhabha Atomic Research Centre (BARC) in Mumbai India, and put anti-nuclear weapons and pro-peace messages on the computers’ screens, similarly to already mentioned WANK malware.

Apart from above-mentioned acts and events, which were motivated socio-politically, there have been first foundations of patriotic hacktivism, focused on national ideas. In September 1998, the defacement of forty Indonesian websites, showing the message “Free East Timor” was motivated by nationalistic reasons. Similar series of attacks happened during the Kosovo conflict, where pro-Kosovo and Serbian nationalistic hacker-activists, were constantly defacing websites of each opposite side of the conflict. In 2001, over 140 hacktivist groups from China launched multiple DDoS attacks at more than 1,400 American websites as a response to the collision of a US drone with a Chinese fighter jet in the South China Sea. In the same year, a hacktivist group named Hacktivismo, created the manifesto “The Hacktivismo Declaration”, seeking to apply the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, to the internet (ICCPR).[5][6]

3.3 Golden age of hacktivism

With the dawn of the new millennium, hacktivism started to play a more significant role than in the 1990s and has evolved into a regular tactic mainly performed by individuals interested in various real-world matters. With the steady growth of the internet, access to information became easier and less reliant on traditional mass media. In addition, modern technologies became more accessible for unskilled users and opened more possibilities to engage in discussion of socio-political issues.

With the growing promotion of free speech rights, transparency, and access to information, new hacktivist techniques were rising. In this period, data leakage became more popular with server WikiLeaks, established in 2006. Nevertheless, it started to be clear that even a small group of individuals can greatly influence public opinion.

In 2007, Estonian officials removed a Soviet war memorial from its capital city. Consequently, various Estonian government websites were the target of a series of DDoS

attacks originating from Russian servers. A Pro-Kremlin group called Nashi claimed the responsibility for the attack, however, they denied that their action was led by the Russian government.

In 2008, hacktivist group Anonymous released a video on YouTube, with the announcement of Project Chanology, which started a series of hacktivist attacks against the Church of Scientology, due to its effort to suppress materials and publications criticizing the Church of Scientology and Scientology itself. In addition, Anonymous organized their first physical protest in various locations around the world. These protests became associated with the mask of Guy Fawkes used by protestors and supporters of Anonymous. Although the origin of Anonymous can be traced back to 2004, Project Chanology was their first significant hacktivist action. Later in 2010, Anonymous launched Operation Avenge Assange, against the decision of MasterCard, Visa, and PayPall to block all financial transactions to whistleblowing hacktivist organization WikiLeaks. Anonymous were supporting pro-democratic protests, during the Arab Spring, by attacking the websites of authoritarian governments in Northern Africa. This inspired other hacktivist groups, later involved in events that followed after the Arab Spring.

After the series of LulzSec members' arrests, between 2011 and 2013, Anonymous continued to grow. In 2014, the Philippine branch of Anonymous was responsible for a series of attacks against the Philippine government and Chinese websites. Furthermore, Anonymous has inspired various new hacktivist organizations in Myanmar, Indonesia and, the Middle East region. However, cyber-attacks of these groups were motivated by nationalistic and religious reasons rather than socio-political. [6]

3.4 Decline of hacktivism in 2015

Since 2015, the trend of hacktivism has been significantly declining. According to data from IBM X-Force Intelligence Index 2019, the number of hacktivist cyber-attacks has dropped by almost 95 percent between the years 2015 and 2018. Apart from, operation Icarus, which targeted national banks worldwide and defacement of Thai police websites, there was only a small number of less significant hacktivist attacks. However, it is important to note that these data cover only publicly disclosed cyber-attacks performed by hacktivists. Following figure 1 graphically visualizes the difference in the number of recorded cyber-attacks, accounted to hacktivist between the years 2015 and 2018.

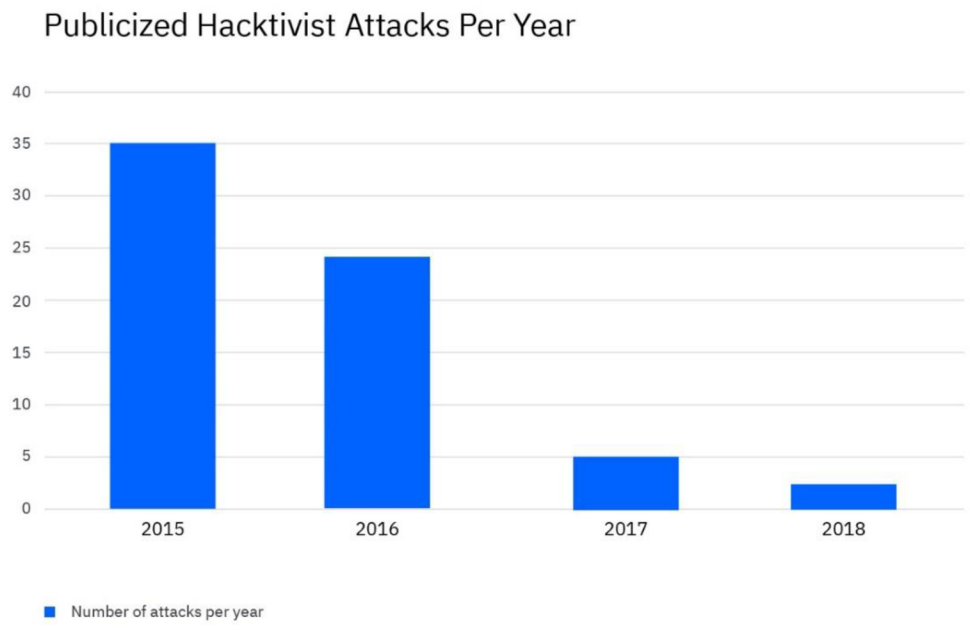


Figure 2: Number of publicized hacktivist attacks (Source: IBM X-Force Data, 2015-2018)

The total number of hacktivist attacks per year partially reflects in the number of cyber-attacks launched only by Anonymous, which can be seen in figure 2.

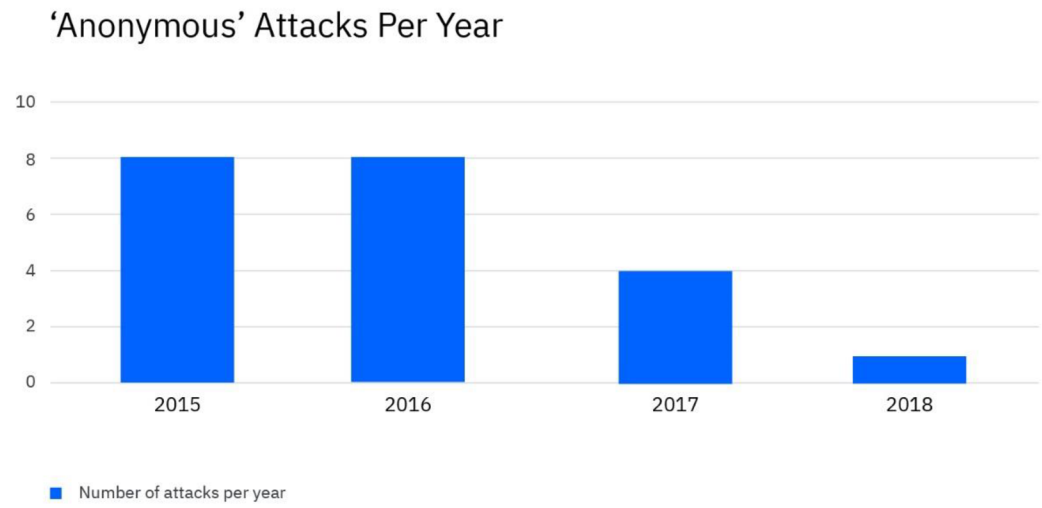


Figure 3: Number of publicized Anonymous hacktivist attacks per year (Source: IBM X Force Data, 2015–2018)

According to IBM X-Force researchers, there are several possible reasons which have caused this significant fall of hacktivist actions. Law enforcements across the world made significant progress with fighting cyber-crime. A large number of arrests and legal

warnings to hacktivist participants seems to be an effective countermeasure against possible hacktivist attacks, lowering the number of performed attacks. Furthermore, in 2018, there were three cases of hacktivists, who received a prison sentence for more than three years, with cases of hacktivists who switched sides and became ethic hackers or informants for the government. In addition, due to the lack of any form of leadership and decentralization with wide opinion plurality of Anonymous, the movement struggled to find a common ideological focus. This issue was reflected during the 2016 US presidential election when its members could not agree on whether they should attack the websites of the candidates.[7] Furthermore, general public and mainstream media became less interested in hacktivism, since their activities didn't achieve any greater goals.

3.5 Events prior 2022

With the constant decline of hacktivism and its "flagship" group Anonymous in the mid and late 2010s', there haven't been any significant or major hacktivist events. The situation started to shift slightly at the beginning of 2020, when the group Anonymous hacked web servers of the United Nations organization and created a pro-Taiwan page. This page contained the logo of Anonymous, the Taiwanese national flag, the emblem of the political party Kuomintang and the pro-Taiwan independence banner. It served as support for the recognition of Taiwan's independence from mainland China.

Later in June 2020, after the murder of George Floyd by a police officer in Minneapolis and during consequent protests around the world, hacktivist group DDoSecrets (Distributed Denial of Secrets) leaked 269 GB of internal US law enforcement data. This data leak became known as BlueLeaks and contained mostly police and FBI records, security bulletins, and other nonpublic documents from over 200 police departments and other law enforcement institutions, including personal data of their employees. These data were collected by fusion centers, which are responsible for information sharing between local, state, and federal agencies in the USA. Similarly, to other major hacktivist attacks, DDoSecrets announced their achievement on their Twitter account, however soon after the post was published, it has been deleted. In addition, DDoSecrets claimed that the data they leaked was obtained from another hacktivist group called Anonymous, which was at the time responsible for multiple DDoS attacks on websites of multiple U.S. Police Departments. In addition, several Police Department websites became the target of DDoS attacks and web defacements. [8]

In the the same year group Anonymous supported Nigerian movement named #EndSARS, calling for the dissolution of the Nigerian police unit called Special Anti-Robbery Squad (SARS), which have been frequently accused of various crimes against the citizens. Various government websites experienced frequent DDoS attacks during the period of the protests, which led to dissolution of the SARS unit. [9][10][11]

On the 3rd of September 2021, group Anonymous launched Operation Jane. This hacktivist operation targeted the controversial Texas Heartbeat Act that went into effect on the 1st of September. This act bans all abortions after the detection of cardiac activity (approximately after 6 weeks of pregnancy) under the 10,000 USD penalty. [12][13] On September 13, Anonymous defaced website of the Texas Republican Party with message "Texas: Taking voices from women to promote theocratic erosion of church/state barriers". [14] In addition, Anonymous run twitter account focused on fight against this act under ID @OperationJane. The wall of the twitter account is accessible on URL: https://twitter.com/OperationJane However, apart from continuous blogging on @OperationJane twitter wall, no other known moves were made by Anonymous against this act which is still active in April 2022.

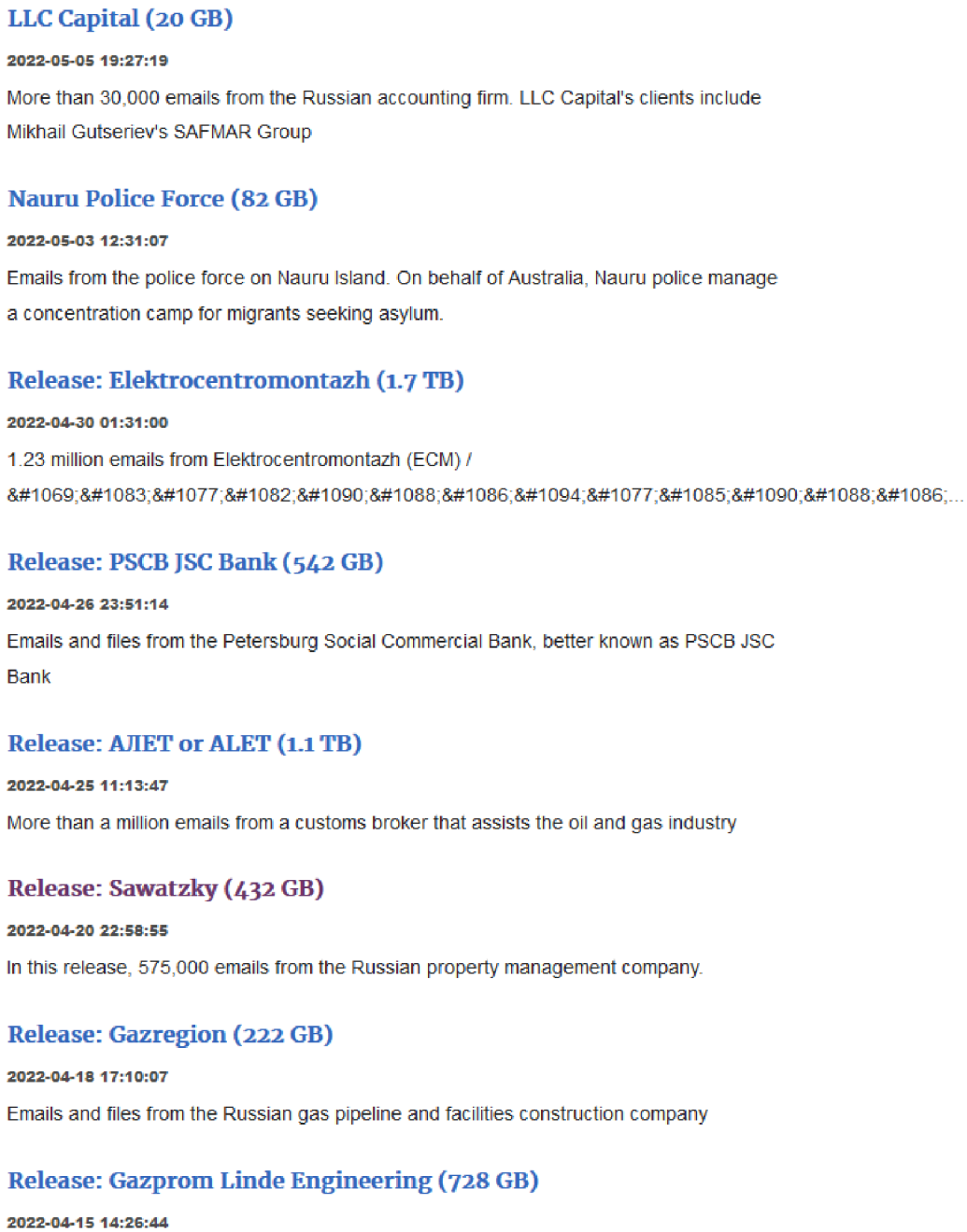
Later on September 13 2021, Anonymous obtained over 180 GB of data from webhosting company Epik Inc. Epik provides online hosting services, such as domain names or web hosting to various organizations on the right or far-right political spectrum, such as social networks Gab and Parler, far-right online imageboard 8chan, alternative social network founded by former US president Donald Trump or even website of Republican Party of Texas. Basically, it provides hosting to organizations and individuals who were denied by majority other hosting companies. The data included several databases containing records of Epik's customers. Hacktivist group DDoSecrets assisted Anonymous with the distribution of the leaked data.[15][16] In addition, on February 29, Anonymous published another 70 GB of data, which contained system files of Epik's servers. [17]

3.6 Current status in Spring 2022

During the writing of this thesis, Russian Federation launched invasion into Ukraine on February 24 2022. Following paragraphs of this sub-chapter is concerned with the currently known hacktivist activities in this conflict until the beginning of May 2022. It is important to highlight that information contained in the following paragraphs, may be in the future considered as outdated or misleading since the conflict is still ongoing and there are currently limited options to reliably verify the truthfulness of these information and whether is it a part of propaganda. Especially due to fact that most of the sources for this topic are mainstream media, hacktivist social media accounts and other non-professional articles. Furthermore, there is high possibility that additional information, may be revealed years after the end of the conflict. [18]

Day after the initialization of the invasion, various social accounts associated with Anonymous stated declaration of "cyber operations" against the Russian Federation. Since then, Anonymous claimed credit for DDoS attacks and web defacements of Russian institutions, namely official website of Kremlin or Russian Ministry of Defense. In addition to this, unknown hackers managed to hack Apple Maps to rename the Russian Ministry of Defense to "Ministry of Fascism of the Russian Federatiom". [19]

Furthermore, multiple state television channels in Russia have been hacked to post pictures and videos from the Ukrainian warzone, followed with Ukrainian content such as national and folk music. Another hacktivist group, DDoSecrets is also highly active and are participating in the cyberwar against Russia, by leaking series of files from various Russian institutions and companies. These leaks contain mostly emails and internal data up to hundreds of Gigabytes. Most notable yet is 1.7 TB leak of 1.23 million emails from Russian power organization Elektrocentromontazh.[20] Figure x, shows other notable examples of data leaks performed by collective DDoSecrets.



LLC Capital (20 GB)

2022-05-05 19:27:19

More than 30,000 emails from the Russian accounting firm. LLC Capital's clients include Mikhail Gutseriev's SAFMAR Group

Nauru Police Force (82 GB)

2022-05-03 12:31:07

Emails from the police force on Nauru Island. On behalf of Australia, Nauru police manage a concentration camp for migrants seeking asylum.

Release: Elektrocentromontazh (1.7 TB)

2022-04-30 01:31:00

1.23 million emails from Elektrocentromontazh (ECM) / Электроцентро...

Release: PSCB JSC Bank (542 GB)

2022-04-26 23:51:14

Emails and files from the Petersburg Social Commercial Bank, better known as PSCB JSC Bank

Release: AJIET or ALET (1.1 TB)

2022-04-25 11:13:47

More than a million emails from a customs broker that assists the oil and gas industry

Release: Sawatzky (432 GB)

2022-04-20 22:58:55

In this release, 575,000 emails from the Russian property management company.

Release: Gazregion (222 GB)

2022-04-18 17:10:07

Emails and files from the Russian gas pipeline and facilities construction company

Release: Gazprom Linde Engineering (728 GB)

2022-04-15 14:26:44

Figure 4: The list of leaks published before May 5, 2022 at 9AM (Source: https://ddosecrets.com/wiki/Distributed_Denial_of_Secrets)

From the early beginning of the war, there have been calls to general public to aid the Ukrainian side in this conflict.[21] Only two days after the initialization of the Russia's invasion, Ukraine's Vice prime minister and Minister for Digital Transformation Mykhailo Fedorov announced on his Twitter wall, creation of Ukrainian "IT Army", with calling for volunteers to join. This "cyber army" uses Telegram channel for communication and coordination. Russian invasion caused a vast citizen outrage across the world, especially in Europe. Apart from real world protest against the war, many citizens started to engage in the cyber-space. One of the examples is the review-bombing of Russian businesses on Google, where online activists are writing news and reports about the war to inform Russian citizens.[22] Furthermore, various easy-to-use software tools for DDoS attacks are widely distributed on the internet for volunteers that are eager to participate in this conflict, at least in the cyberspace. However, the use of these tools can be dangerous for the users, because in some cases it can contain malicious part of the code with unknown intension. Furthermore, Russian Government released in march list containing the IP addresses of these participants.[23][24] Additionally, not only Russian based companies and institutions have been target of hacktivists. On March 21, Anonymous posted via twitter account @YourAnonTV call on foreign based companies to end their activities in Russia. In addition, during the Russian offensive on Kiev, Belorussian railway, which have been used by Russian army for logistics, have been continuously hacked causing the delays in resupplying. It is presumed that unknown group of Belorussian "partisans" opposing the Belorussian government was responsible for these actions.[25]

Prior to the invasion, there were reports of pro-Russian hacker activities in the Europe. Especially Ukraine institutions have been the main target of several DDoS attacks and web defacements, prior the invasion.[26] However, these activities can hardly be considered as acts of hacktivism, with reference to the definition already mention in the introduction of this thesis. It is believed that Russian Government is responsible for these attacks, although these statements are rather difficult to be proved. These pro-Russian hackers mostly works silently, thus there are no publicly available specific information.

In terms of "true" pro-Russian hacktivism, there is currently collective known as Killnet Group. This hacktivists group is often presented by western media as ecample of state-sponsored or government sponsored hacktivism. KillNet Group have been responsible for attacks on institutions and infrastructure in Eastern EU countries such as Poland or Czech Republic, due to their support of Ukraine.

4. FORMS, TYPES AND METHODS OF HACKTIVISM

Hacktivism may come in many different forms with the use of various methods to achieve its objectives. Many of these methods can be considered in breach of law and their use might be in some way dangerous. Since some of these activities are considered illegal hacktivists need to work anonymously without leaving any detail that could be used to discover their identity. This chapter shows various possible methods used by hacktivists, in their fight for their thoughts and ideas.

4.1 Anonymous blogging

Blogging is one of the most successful methods. It comprises of sharing of the thoughts or ideas on the website, referred to as a blog. In the case of anonymous blogging, the authors use pseudonyms to remain in anonymity. In addition, anonymous bloggers use various techniques such as encrypted connection or posting their blogs from publicly accessible computers or networks. This is important for activists, who may be breaching the law of their country, especially in the case when a certain activist is a citizen of a country with an authoritarian government, partly or fully suppressing any kinds of free speech e.g. Public Republic of China or Russian Federation. Therefore, this type of hacktivism is widely favorited by whistleblowers and journalists.

4.2 DoS and DDoS attacks

DoS (Denial of Service) and DDoS (Distributed Denial of Service) are favorite types of cyber-attack used not only by hacktivists. Both of them are relatively simple and powerful techniques. [27]

4.2.1 DoS attack

The objective of this attack is to make its target, e.g. website, server, or network, incapable of providing its normal services for its users. This is achieved by flooding the target with a large number of requests, above its hardware or software capability. As the result, the target of the attack is not able to fulfill the requests of its legitimate users. However, this type of attack does not necessarily damage data either directly or permanently. In most cases DoS attacks target the bandwidth of the network or connectivity to the server, providing certain services e.g. website hosting.

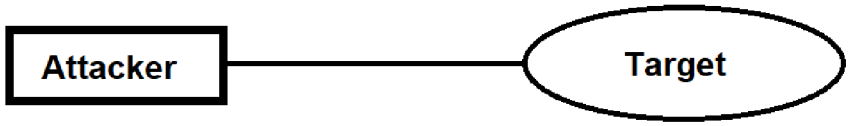


Figure 5: Visual scheme of DoS attack

Since this type of attack comes from one device or location, it is not difficult to track its origin and block its further access. Furthermore, various network devices can block DoS attacks automatically by their firewall or any other feature implemented by its manufacturer.

4.2.2 DDos attack

In comparison to DoS attacks, DDoS attacks use multiple computers to launch coordinated DoS attacks against single or multiple targets. Since it uses multiple machines, that can be located in various locations, it is more destructive than a basic DoS attack. It mainly consists of multiple "enslaved" computers, which were infected with malware, allowing the attacker to remotely use them to perform a DDoS attack. These "enslaved" computers are referred to as "bots" or "zombies", and most of the time are waiting for a command from their "master" or his "handlers" to attack a certain target. Handlers can be used as "middle man", between the attacker and bots. A group or network of bots is called a botnet. DDoS attacks act as an advanced version of DoS attack. It can be deployed much faster than a DoS attack and for the targeted device or network, it is more complicated to deal with multiple attackers, instead of one.

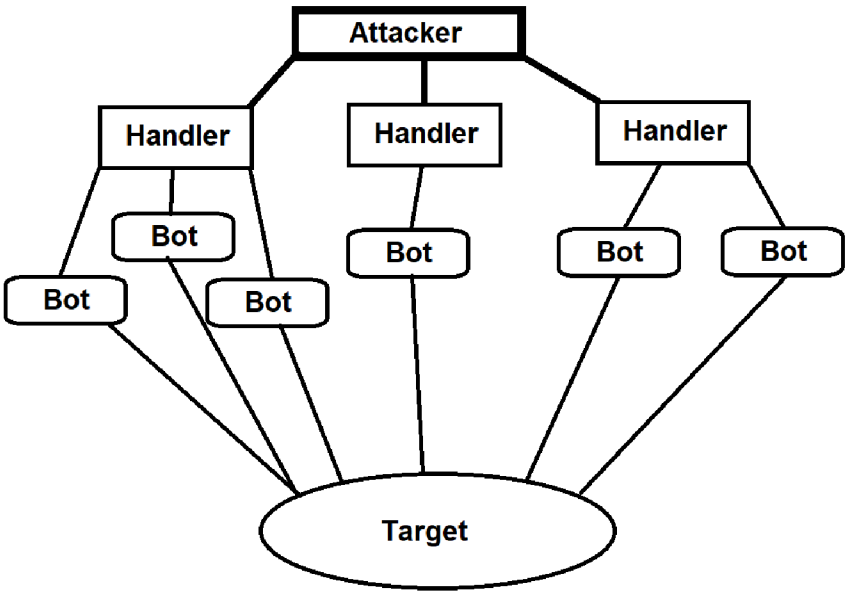


Figure 6: Visual scheme of DDoS attack

4.3 Doxing

The term 'doxing' comes from the phrase 'dropping documents' or 'dropping dox' on someone, which was a form of revenge in 1990s outlaw hacker culture that involved uncovering and revealing the identity of people who fostered anonymity (Honan 2014).

This type of hacktivism involves obtaining private or personal information of a certain person or organization and releasing it publicly onto the internet, intending to humiliate,

threaten, intimidate or punish its owner. Doxing can be split up into three following categories: Deanonymizing doxing, targeting doxing and delegitimizing doxing.

Deanonymizing doxing, reveals information that reveals or can be used to reveal the real identity of the individual, who has been anonymous or has been known under pseudonym, nickname or fake name. This mostly happens against the free will of the victim. Possible damage caused by this type of doxing depends on previous and current activities of targeted individual, for example when the doxed person is subject of criminal activity, law enforcements will start to be interested in this person, since they know their real life credentials. Furthermore, the doxed person can become vulnerable to other types of attacks. Typical targets of this attacks can be internet hoaxers, scammers or anonymous famous person, for example Satoshi Nakamoto, author of Crypto Currency BitCoin, whose real name is still unknown. It can be said that Deanonymizing doxing primary punishes certain individuals for their actions.

Targeting doxing reveals specific personal information, that can be used to discover the victim's physical location, e.g. home, working address or any other address associated with the targeted individual (alternatively email, or phone number). This removes the anonymity of the targeted person and thus, this person becomes more vulnerable to multiple options of harassment. It can start with irritating phone calls and end up even with physical harassment, which can create potentially dangerous situations. There has been case in February 2022, Czech anti-covid restriction activist movement called "Chcípl PES" published private addresses of 70 lower house representatives of Czech parliament, who voted for approval of new pandemic law and called on the public to organize demonstrations on these published addresses. This resulted in multiple cases of vandalism and in one case, one woman broke into the house of one of the politician with intention to demonstrate there. Similar incidents when somebody brakes into private property can be extremely dangerous for both the activists and the property residents since the activists may cause psychical or psychical harm to the residents, in case of high tension in the society, which could have been seen during the peak of covid pandemic. In addition, these activists can be mistaken for burglars or any other criminals, thus the residents may use force with intention to defend themselves, even with use of firearms if the resident or house owner poses one. [28][29]

Last category, Delegitimizing doxing releases certain private information to harm the credibility, reputation, or character of the targeted individual. In this case, the main objective is to humiliate the targeted person or collective resulting in public denial of the target by majority of the public. [30]

4.4 Geo-bombing

This technique uses an option to add a geo-tag on a YouTube video during its upload. Thanks to this tag, the location of the video can be found on Google Earth. This technique is used to tag the location of the videos, created by political prisoners or human rights

activists.[31] It is a simple method that does not require any sophisticated knowledge or skill, however there are no significantly known hacktivist events that used primary this technique. There are only few mentions of Geo-bombing use for activist purposes, from north African countries between the years 2007 and 2012.[32][33][34] Similar method, which could be described as “Review bombing” have been used in March of 2022, after the launch of Russian invasion in Ukraine, when people started writing Google reviews of Russian businesses, in which they tried to inform citizens of Russian Federation about ongoing conflict in Ukraine and to bypass the state censorship. However, it is questionable if this form of cyber activism against the Russian regime, brought any clear results, since there are more notable hacktivists actions and due to fact that the conflict is still ongoing during the writing of this thesis.

4.5 Information leak

It is a quite common tactic of hacktivism. A single individual or hacktivist group releases sensitive or classified information from a certain individual, company, or government institution, obtained from an insider source. Unlike doxing, this tactic does not take as its objective humiliation or any other similar harm to its target. Instead, the main objective is to inform the wide public about potentially controversial or in any other way negative actions of publicly active persons or institutions, such as politicians or government agencies. The most known example is server wikileaks.org launched in 2006.

4.6 Phishing

Apart from any other attacks mentioned in this chapter, phishing is not widely used by hacktivists. This type of attack is primarily designed to trick a human user to reveal their sensitive information, e.g. internet banking credentials, which can be later abused by an attacker. This is mostly done by creating a fake copy of a legitimate website e.g. internet banking or gmail.com, which requires some kind of login ID and password or any other sensitivity of the user. After entering the access credentials on the fake website, the attacker obtains them. This technique is more used by so-called “black-hat” hackers, who are concerned with personal benefit rather than ideological philosophy. However, hacktivists can use this technique to obtain resources to fund their operations. [35]

4.7 RECAP software

RECAP software was created as a free-of-charge alternative to the database PACER (Public Access to Court Electronic Records), allowing its users to access online copies of U.S. federal court documents, which would be under normal circumstances accessible only after paying a fee. The name RECAP derives from the back spelling of the word PACER. [36]

4.8 Website defacement

Web defacement is an attack in which hacktivists, get through the security of the website and replace its content with their own, mostly in form of a message to its users or providers or even with impropriate content. The objective of this attack is to express a certain opinion or harm the owners of the website in any other way. This type of attack requires more advanced knowledge website development.

4.9 Website mirroring

In some countries, certain websites might be censored. To bypass this censorship, the exact copy of the censored website is created, including all of its content with a slightly or completely different URL address. It makes government blocked websites, available to citizens, provides them better access to information, and promotes freedom of speech. This method does not damage or interrupt the original website.

4.10 Website redirection

Also called URL redirection or URL forwarding is a technique to redirect a user, who enters a certain website, to an alternative website containing support of hacktivist agenda, message, or malware. Thus, this method causes harm to the owner of the original website, since it cannot be accessed to its users. If the original websites run advertisements or provides paid services, it will lose its potential users or customers and hurts the income of the websites owner. Furthermore, in case of websites run by government or any other state or local authorities, citizens will not be able to access the information located at certain website and creates complication in order to access them. In addition, the destination website, to which is the user redirected to, can be potentially dangerous since it can contain script which can download malware to the visitors' computer without their acknowledgement. The purpose of this malware may be collecting data of its victim, creating a "bot" computer for future DDoS attack of its authors or have any other unknown purpose.

4.11 Social Media

Social media such as Facebook, Twitter or YouTube are widely used by hacktivists for communication with the public and mainstream media. Both hacktivist individuals and collectives use primary social media to announce their attacks against certain targets, claim responsibility for hacktivist event or to send message or warning to their potential target. This is typical behavior for hacktivist group Anonymous, whose name is carried by multiple twitter and Facebook accounts. However, due to fact that Anonymous is decentralized group without any form of structure or leadership, there are multiple social media accounts that carries their name and uses the Anonymous logo or mask of

Guy Fawkes as their profile picture, sometimes with slight differences.

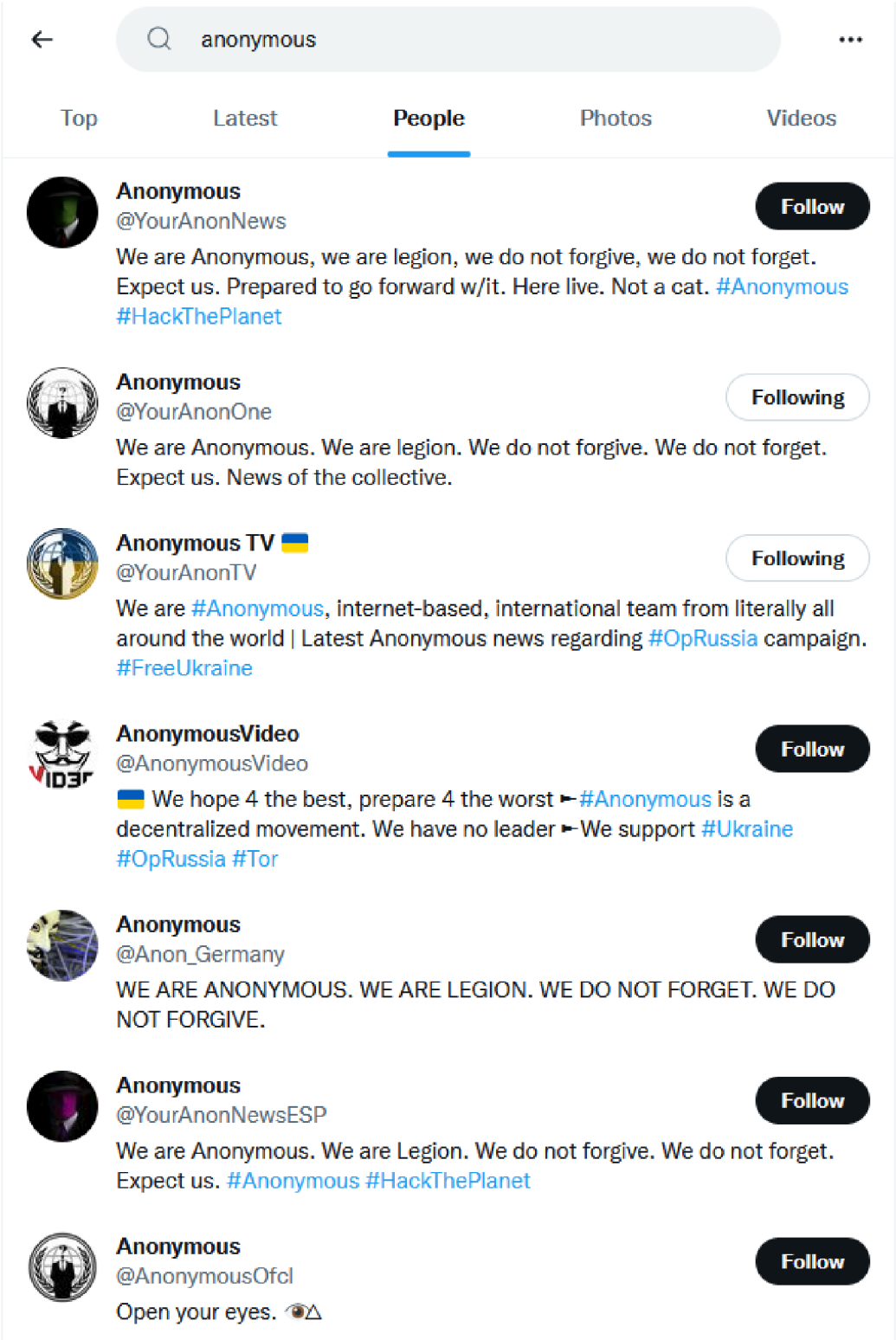


Figure 7: Twitter search results for "Anonymous" from March 6, 2022, at 12:18 AM

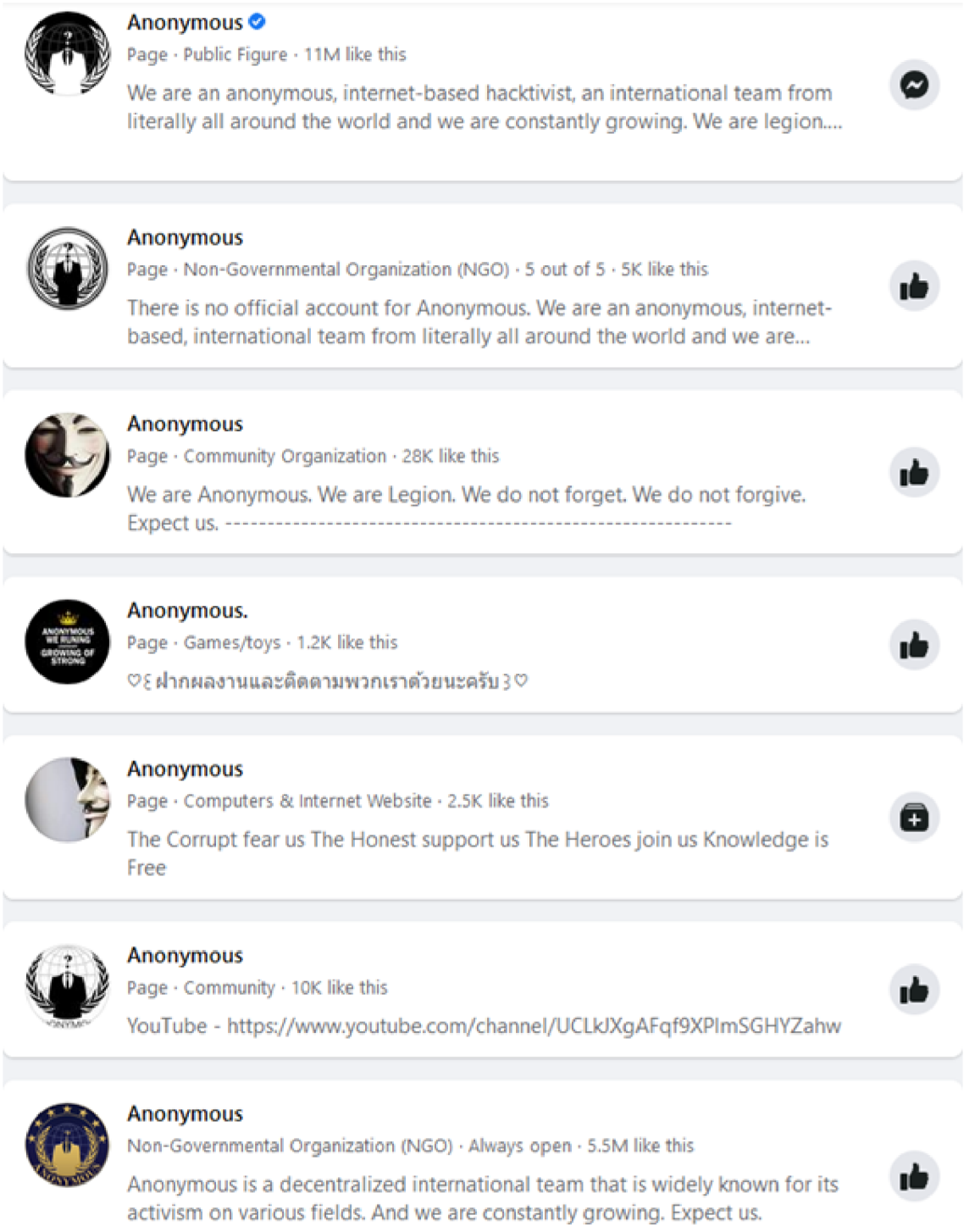


Figure 8: Facebook search results for "Anonymous" March 6, 2022, at 12:21 AM

The number of followers of these social media accounts varies from thousand to tens of millions. Additionally, hacktivists can use social media for information leak or doxing by publishing secret or private information on their public social media wall. However, hacktivists do not have to always use social media accounts that are directly associated with them. It is common practice that hacktivists hack into social media account of

other users with intention to use this account for their needs, often to acquire information which can be leaked or to publish their own posts propagating their thoughts. Thus, hacktivists target the social media accounts of well-known or popular companies, politicians or institutions with significant number of followers. Heavily social media accounts, such as Facebook or Twitter are primarily used for the hacktivists announcements, since there have been cases of deleted posts or even deleted accounts, additionally these big social networks can leak information about hacktivists to state authorities. For example in Vietnam, company Facebook even adopted the use of state censorship for Vietnamese users. Due to these facts, hacktivists often use other less regulated social networks, such as telegram for inner communication or to spread censored information or unverified information. [37][38]

4.12 Sharing files via BitTorrent

BitTorrent is popular IT communication protocol used for decentralized peer-to-peer (P2P) file sharing. Network which works on P2P model (also known as client-client model), have no specific centralized server which would share the data with the clients, thus the data can be received and sent directly between the clients. It is completely opposite technology to Client server model, where the data can be accessed via one or multiple servers. There is no data sharing between the clients. The biggest weakness of this model is its need of centralized server, which can be relatively easily shutdown by authorities or by other hacker attacks such as DDoS. In addition, it is more expensive and less reliable solution in comparison with P2P model. Following figures graphically describes the topology of P2P and Client-server model.

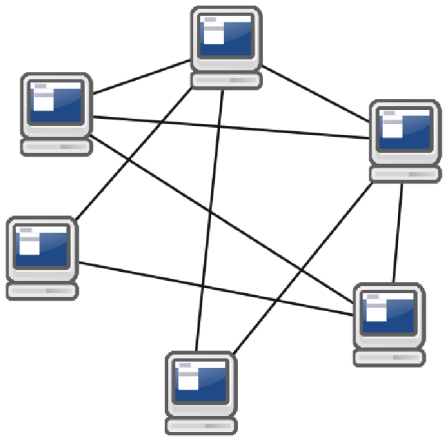


Figure 9: Visualization of P2P model (Source: https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/)

The figure x, shows that in P2P model, individual clients share the data directly between themselves. On the other hand, figure x visualizes the Client-server model in which the clients obtain data from only one source, which is being the server.

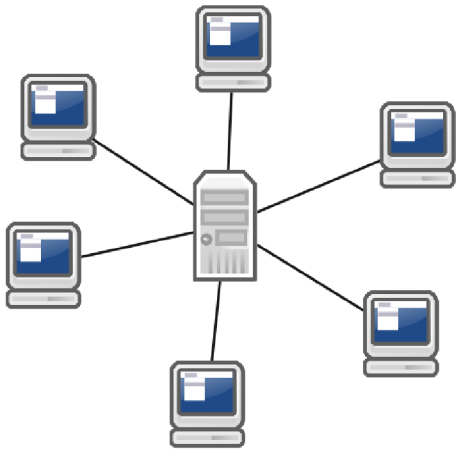


Figure 10: Visualization of Client-server model (Source: https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/)

To send or receive files containing the data, it is necessary to install BitTorrent client, which is program that can open files with appendix .torrent, that are allows user to receive and share the data.

Hacktivist group DDoSecrets uses BitTorrent technology to share leaked data. The torrent files are available on their websites, where user can easily download them. In contrast, organization WikiLeaks publishes leaked data on their servers which works on Client-server model.

4.13 Tor

In full name The Onion Router, is an open-source software which basically enables its user to maintain anonymous during their activities on the internet. In addition, this technology is used to access so-called dark web, where the websites are not indexed by search engines. To protect identity and privacy of its users, Tor consists of network of servers, which briefly works as a tunnel between the user and destination server, hosting for example website or any other internet service. To access Tor network, user needs to use a special web browser called Tor Browser, which is designed to protect anonymity of its user in contrast to other usual web browsers. This browser does not store any data, that could be used to identify the user, such as browsing history, cookies files or IP address. Tor network consist of more than six thousand volunteer servers. These servers work as relays or in other words, “middleman” between the user’s computer (Tor client) and destination server (e.g. website). Before the Tor client reaches the destination server, the traffic goes through three random Tor relays inside the Tor network. These three servers can be referred as Entry guard, Middle relay and Exit relay. In addition, whole traffic inside the Tor network uses three-layer encryption. This principle is often explained on

the onion, thus the onion itself have multiple layers, and to access next layer it is necessary to unpeel the previous layer. Following figure 10, graphically describes this method.[39]

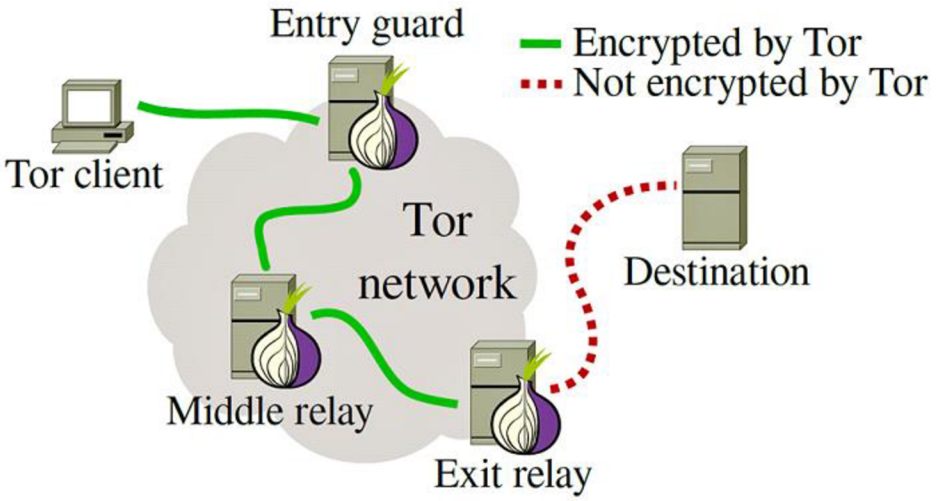


Figure 11: Graphical visualization of Tor network (Source: https://fossbytes.com/everything-tor-tor-tor-works/)

From the figure x above, it is clearly shown that the destination server, is able to recognize only the last point of the Tor network which is the Exit relay. Thus, the traffic which is flowing between Tor client and Exit relay, through Entry guard and Middle relay cannot be easily traced. Following figure 11, is similar to the previous figure x, however it additionally shows the encryption layers of the Tor system. Each key with different shade of blue signalizes, each different layer of encryption.[40] [41] [42]

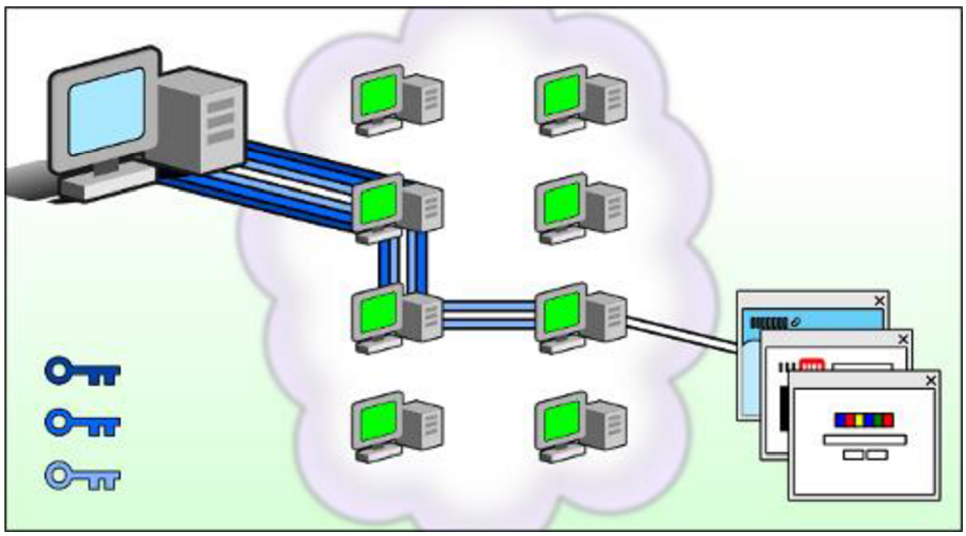


Figure 12: Additional graphical visualization of Tor network with its encryption (Source: https://tb-manual.torproject.org/about/)

Furthermore, the Tor browser is designed to protect its user against “fingerprinting” from the visited websites. Website fingerprinting (also referred to as device fingerprinting, browser fingerprinting or online fingerprinting) is tracking or surveillance technique, when websites uses specific scripts to collect information about its visitors. These scripts are often working in the background, without knowledge of websites visitors. These scripts can collect, seemingly irrelevant information about the users’ device, such as web browser and its plug-ins or add-ons, screen resolution, operating system of the device, MAC address, time zone of the device and many other. This information can be sometimes critical to reveal real identity of the hacktivist due to fact that these data can be provided by system administrators of the website to law enforcement authorities on their request.[43]

However, even this technique is not 100% secure way to browse internet websites without risk of tracking. Despite the fact that Tor network itself provides high level of security, it covers only the path between the user and website. That means, if there is malware on the user’s computer or any other program, which could share information of its user, the use of Tor can be completely pointless at this point. [44][45]

5. HACKTIVIST GROUPS

Like any other activists, hacktivists usually cooperate with each other and organize themselves in groups or organizations to more effectively achieve their common goals. The goals of each hacktivist group may vary the same as the motivation of the hacktivist group and its members or participants. Each hacktivist group tends to distinguish itself from each other, by its specific signs. This sign might be a visual logo, specific messages included in their attacks, or even a specific form of the attack itself. The goals and motivation of these organizations and their members vary with different origins, organization structure, socio-political background, or ideology. In this chapter, I have decided to make an overview of the publicly known hacktivist groups and organizations, whose actions had a significant impact on the development of hacktivism.

5.1 Chaos Computer Club

Chaos Computer Club is the largest hacker association in Europe, established in Germany in 1981, with the goal to promote education, freedom of information, and government transparency. Members of CCC organized many lawsuits and campaigns to support their beliefs. [46]

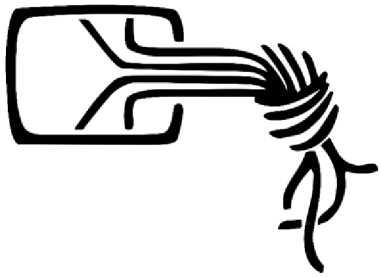


Figure 13: CCC logo (Source: https://en.wikipedia.org/wiki/File:Chaos_Computer_Club_(logo).svg)

5.2 Cult of the Dead Cow

Also known under the acronym cDc, was established in 1984, not as a hacktivist group but as a hacker organization, due to fact that the term “hacktivist” or “hacktivism”, was not known at the time. The term “hacktivism”, was coined by a member of cDc, nicknamed “Omega”, in email correspondence with the rest of the organization, for the first time in 1994. The primary focus of this organization is freedom of information and promotion of human rights, especially in the Public Republic of China and Hong Kong. In the late 90s, cDc created two of its offshoots, Ninja Strike Force, promoting cDc ideology and actions, and Hacktivismo, cDc independent group, which is known for the creation of the list of civil and political rights on the internet called “The Hacktivismo Declaration”.

Figure 14: cDc logo (Source: https://www.computerhope.com/jargon/c/cult-of-the-dead-cow.htm)

5.3 Anonymous

Probably the best-known hacktivist organization in the world, bounded with use of Guy Fox mask in their videos and on Anonymous organized public demonstrations. This movement originated on an online imageboard named 4chan.org, where users can anonymously post comments or visual content, dedicated to a wide variety of topics. This hacktivist group is unique in its structure and organization. Apart from other hacktivist groups, which are mostly formed by less than twenty members, Anonymous is an enormous, decentralized collective without any form of structured leadership. Thus every individual can consider themselves as a member.

Anonymous are well known for various doxing and DDoS attacks against government institutions, politicians, and international corporations. In 2010, this movement supported the whistleblowing organization WikiLeaks by launching various attacks against companies Amazon, MasterCard, VISA, and PayPal, at the moment when these companies decided to follow the encouragement of the US government to stop providing their services to WikiLeaks. Later in 2011 and 2012, Anonymous supported anti-government protests during the Arab Spring, which occurred in Northern African countries. Later in 2022, the group declared cyber war against Russian Federation and its president Vladimir Vladimirovich Putin, as reaction against Russian invasion of Ukraine which started on 24 February 2022.

Figure 15: Anonymous logo (Source: https://en.m.wikipedia.org/wiki/File:Anonymous_emblem.svg)

5.4 LulzSec

In full name Lulz Security, is a hacktivist group, founded by a few members of Anonymous. The first word in the group's name, "Lulz" is a neologism of the abbreviation "LOL" (Laughing out loud). LulzSec's highest priority is cybersecurity and privacy protection. Among their targets were multiple entertainment divisions of SONY Group, US Senate, Public Broadcasting Service, telecommunication company AT&T and many other high-profile corporations and public institutions. In comparison with movement Anonymous, the LulzSec organization is more centralized with a small number of members. [47]

Figure 16: LulzSec logo (Source: https://en.wikipedia.org/wiki/LulzSec#/media/File:Lulz_Security.svg)

5.5 WikiLeaks

Established in 2006 by Australian publisher and activist, Julian Assange. WikiLeaks is a well-known whistleblowing non-profit organization, primarily focused on transparency and publishing leaked information from various anonymous sources, covering a wide spectrum of social-politic topics. Main objective of this organization is to inform public about events that might be condemned or disapproved by public. To ensure anonymity of their sources, WikiLeaks designed a special website, where whistleblower can share their information, which is later released by WikiLeaks. To access this website, whistleblower need to use special web browser Tor Browser. Tor Browser, apart from other web browsers, hides user's IP address and does not store any data of its user which could be used to identify its user. Thus, WikiLeaks claims that none of the published data were not obtained by their own hacker attack.

During 2010, WikiLeaks published around 750,000 of US military and diplomatic documents. These files were obtained and passed to WikiLeaks by member of US Army, Private Bradley Manning (later known as Chelsea Manning) during his service in Iraq. These documents contained information about civilian causalities caused by US forces in Iraq. The leak of these documents caused big controversy at that time. Later, WikiLeaks published the remaining documents obtained from Manning, consisting nearly 250,000 documents. This controversy became known as "Cabblegate". Later in 2013, WikiLeaks

assisted Edward Snowden, who worked as IT consultant at National Security Agency (NSA) and was responsible for massive leak of information about NSA global surveillance program, known under codename PRISM. Furthermore, intervened in US presidential campaign in 2016, when it released documents and emails from Democratic National Committee (DNC). This leak revealed that DNC more favored Hillary Clinton over Bernie Sanders, as presidential candidate, which contradicted the official statement in which DNC stated its neutral position. This is one of the cases when hacktivism can influence democratic elections. WikiLeaks then gained vast disfavor from the Democratic Party and again was repeatedly accused of endangering of national security and of association with Russia. Other leaks in following years, revealed various cases of surveillance by US government run institutions. [48][49][50]

Figure 17: WikiLeaks logo (Source: https://logos-download.com/5899-wikileaks-logo-download.html)

5.6 DDoSecrets

Distributed Denial of Secrets (or in short DDoSecrets) is a whistleblowing non-profit organization, sometimes referred as alternative or successor to WikiLeaks. From its establishment in 2018, this hacktivist collective is constantly active in their activities focused on data gathering and consequent release on the websites www.ddosecrets.com and www.ddosecrets.substack.com by using torrent. According to the website of the collective, the data must meet two criteria, to be published on their server.

„Data we index must meet two criteria:

Is it in the public interest?

Can a prima facie case be made for the veracity of its contents?“ [51]

However, there are no further details on what other conditions members of the collective decide whether the data fulfills these conditions or not. The collective claimed to be cooperating with other hacktivist groups.

DDoSecrets are responsible for publishing data on shell companies, right to far-right groups, tax havens and companies operating within them, most known for event BlueLeaks, when the group released about 270 GB of internal data from various U.S. Law enforcement agencies. Furthermore, the collective is responsible for data leakage from alternative social networks parler.com and gab.com in January and February of 2021. Both social networks promote freedom of speech without any form of censorship,

however both of these social networks are often being associated with various far-right extremist groups.[52]

Figure 18: DDoSecrets logo (Source: https://ddosecrets.substack.com/)

5.7 Syrian Electronic Army

Syrian Electronic Army is first hacktivist collective, who emerged at the start of Syrian civil war as support for Syrian President Bashar al-Assad and his regime. It commenced various DDoS attacks against supposed enemies of the Syrian government. [53]

Figure 19: Syrian Electronic Army logo (Source: https://us.norton.com/internetsecurity-emerging-threats-hacktivism.html)

5.8 Killnet Group

Killnet Group is Russian hacker group supporting current Russian regime, responsible for cyber-attacks on various institutions, companies and infrastructure in the United States, Ukraine and other European countries, primary the members of European Union and NATO. Since it is relatively new collective, which have been established probably in January 2022, there are only few information about this collective with no sources that could be considered as reliable. It possibly acts as a countermeasure against group Anonymous who support Ukraine in currently ongoing war with Russian Federation.

Similarly, to other hacktivist groups, Killnet Group claims that their main goal is to protect other users from hacker attacks. [54]

6. CONSEQUENCES OF HACKTIVISM

The existence of hacktivism has had unquestionable impact on the modern world. Phenomenon that originated as an internet meme later became fairly powerful tool of modern activism and civil political engagement with resulting impacts and consequences, which can be considered both positive and negative.

Both hacktivism and hacking itself have had a vast influence on security both in the real world and in the cyberspace. Each successful hacktivist attack may show that the certain IT system has minor or major vulnerabilities, which have been exploited and can be exploited in the future. As a result, system administrators and technicians concerned with cyber security invent and implement according countermeasures. Furthermore, some hacktivists are even focused primary on the improvement of the cyber-security, namely the hacktivist group called LulzSec. Cyber-security is often disregarded, which can be extremely dangerous, since the information technologies can be nowadays found in nearly all aspects of everyday life. Various companies and institutions stores valuable data about its users, which can be misused and/or sold elsewhere. Basically it can be said that hacktivists concerned with the cyber-security and data privacy served as an inspiration for invention of ethical hacking.

In terms of national security, hacktivists managed to open discussions, whether is the mass surveillance of citizens or public officials necessary to ensure the national security on behalf of privacy of the individuals. In this case, it limited capabilities of governments to use such techniques without causing vast controversy and pointed out the importance of individual freedom and privacy. Consequently, national governments started to be concerned with adequate reforms of laws concerned with surveillance and data collection of the citizens.

However, some of the leaked information by hacktivists can have secondary negative effect. In case of classified documents, the leak can cause that these documents will easily end up in the hands of terrorists or foreign dictatorial governments. There are cases of Islamic fundamentalist groups, who were able to improve their encryption techniques, thanks to exposition of NSA surveillance methods, by Edward Snowden in 2013. As the result, the communication between members of these groups became harder to decode, thus they were able to plan their covert actions more effectively. This was case of jihadist group named GIMF, who developed special mobile encryption program called Tashfeer al-Jawwal. Other Islamic terrorist groups followed later, namely Islamic State of Iraq and Syria (ISIS) developed application called Asrar al-Ghurabaa and followed by Al-Qaeda, which had developed application called Amn al-Mujahid. However, when the growth of ISIS was rising, the group Anonymous launched operation called #OpISIS, with the goal fight the ISIS, in the cyberspace. Furthermore, after the capture and death of Al-Qaeda's leader, Osama bin Ladin, US officials obtained documents belonging, where Osama bin Ladin was calling for translation of the leaked US documents.

In addition, the “success” of the Arab Spring, in which hacktivists played a significant role, is also questionable. It is true that Arab Spring, assisted to bring down many authoritarian regimes in North Africa and Middle East, however at the cost of internal stability, which in some countries led to long-term civil wars. [55]

7. CONCLUSION

The aim of the thesis was to analyze the phenomenon of hacktivism, its historical and contemporary development, methods used, motivations of its actors, results, and impacts on society, and most importantly its current status. I was able to provided an overview of various currently known forms of hacktivism and showed the dynamics of this phenomenon. Actions and implications of this phenomenon have often been discussed by the both professional and general public. With the quick implementation of Information Technology, it is necessary to constantly educate mainly the general public about various forms of hacker activities and hacktivism is one of them.

The first chapter provided an introduction to the problematics of hacktivism and a brief background of its problematics. Chapter two explained the known possible motivations of hacktivist participants. Generally, the motivation of hacktivists can be compared to the motivation of basically any other type of citizen activism. Thus, depending on the topic, there is possible social, political, or religious motivation, which is basically fighting for better conditions for a certain social group or society itself. Social and political motivations are the most common among hacktivists. Furthermore, in recent years it has been possible to observe cases of possible state-sponsored hacktivism.

Following chapter three focuses on the evolution of hacktivism, with its origin in the 1980s up to the current state in Spring 2022. This chapter shows the dynamics of hacktivism, and how it reacts to particular situations, both on a local and international level, and supports it with notable exemplary cases. It was important to inform the reader about these events, thus the reader may be able to make a comparison with the most recent events. Generally, the main methods of hacktivists remained the same or similar, thus DDoS attacks, information leaks, and website defacements remain the most common hacktivist activities.

The fourth chapter provides a list of the various methods and types of cyber-attacks performed by hacktivists, with their description, purposes, and possible primary and secondary effects. Chapter five summarizes generally known information about well-known or notable hacktivist and whistleblowing groups.

In the last chapter, I discussed the consequences and impacts of hacktivism primary on society and overall security. Hacktivists indeed uncovered some unethical or disprovable actions of state governments and international corporations. Furthermore, the hacktivist attacks raised concerns about cyber-security, which is often disregarded even up today. On the other hand, in some cases, the positive effect of their actions can be questionable, like in the case of a sensitive data leak that can cause a risk to national security.

Hacktivists proved to react dynamically according to the current socio-political situation. This has been reflected in the writing of this thesis when Russian Federation invaded Ukraine, Russia has immediately become the target of cyber-attacks from

Anonymous, DDoSecrets, and other hacktivists. Thus, it is expected that hacktivists will be vastly active in comparison with the period between the years 2014-2021.

LITERATURE

[1] *Cyber War in Ukraine: Hacktivism or State-Sponsored Spying?*. (2022). Retrieved April 15, 2022, from https://spyscape.com/article/hacktivism-spyscapes-whos-who-of-hacker-activists

[2] McCormick, T. (2013, May). ANTHROPOLOGY OF AN IDEA HACKTIVISM. *Foreign Policy,* , 24-25. Retrieved from https://www.proquest.com/magazines/anthropology-idea-hacktivism/docview/1365771233/se-2?accountid=17115

[3] *Lagan, B.* (2010). *International man of mystery*. (2010). Retrieved November 12, 2021, from https://www.smh.com.au/technology/international-man-of-mystery-20100409-ryvf.html

[4] *Criminal Justice and Public Order Act 1994*. (1994). Legislation.gov.uk. Retrieved November 24, 2022, from https://www.legislation.gov.uk/ukpga/1994/33/contents/enacted

[5] Guntarik, O. G., & Grieve-Williams, V. (Eds.). (2020). *From Sit-Ins to #revolutions: Media and the Changing Nature of Protests*. Bloomsbury Publishing USA.

[6] McCormick, T. (2013, May). ANTHROPOLOGY OF AN IDEA HACKTIVISM. *Foreign Policy,* , 24-25. Retrieved from https://www.proquest.com/magazines/anthropology-idea-hacktivism/docview/1365771233/se-2?accountid=17115

[7] Singleton, C. (May 16, 2019). *The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015*. Securityintelligence.com. Retrieved November 6, 2021, from https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/

[8] *'BlueLeaks' Exposes Files from Hundreds of Police Departments*. Krebsonsecurity.com. Retrieved April 14, 2022, from https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

[9] Asadu, C. (2020, October 26) *'Anonymous' hacks NBC's Twitter account, supports #EndSARS campaign*. Www.thecable.ng. Retrieved April 17, 2022, from https://www.thecable.ng/anonymous-hacks-nbcs-twitter-account-supports-endsars-campaign

[10] BBC. (2020, October 23). *Nigeria protests: President Buhari says 69 killed in unrest*. BBC News. Retrieved April 18, 2022, from https://www.bbc.com/news/world-africa-54666368

[11] Opera News (2020). *Anonymous hacker denies giving the Nigerian government a 72 hours ultimatum in their latest update*. Ng.opera.news. Retrieved April 18, 2022, from https://ng.opera.news/ng/en/politics/8cb6f7855ba39db0d00e6214258a7dd7

[12] Goforth, C. (Sep 8, 2021). *'Anonymous' hackers have a message for Texas abortion 'snitch' sites: We're coming for you*. Retrieved April 17, 2022, from https://www.dailydot.com/debug/anonymous-hactivists-texas-abortion-ban-operation-jane/

[13] 86(R) HB 1500 - introduced version - Texas. (n.d.). Retrieved May 25, 2022, from https://capitol.texas.gov/tlodocs/86R/billtext/pdf/HB01500I.pdf

[14] Flahive, P. (September 11, 2021). *Texas GOP Website Hacked By Activists Protesting Abortion Law*. Texas Public Radio. Retrieved April 18, 2022, from https://www.tpr.org/technology-entrepreneurship/2021-09-11/texas-gop-website-hacked-by-activists-protesting-abortion-law

[15] Team CIM., (2021, September 16). *Anonymous exposed gigabytes of data from alt-right web host Epik*. Cyberintel Magazine. Retrieved April 20, 2022, from https://cyberintelmag.com/attacks-data-breaches/anonymous-exposed-gigabytes-of-data-from-alt-right-web-host-epik/

[16] Ax Sharma - Sep 20, 2021 12:32 pm U. T. C. (2021, September 20). *Epik data breach impacts 15 million users, including non-customers*. Ars Technica. Retrieved May 25, 2022, from https://arstechnica.com/information-technology/2021/09/epik-data-breach-impacts-15-million-users-including-non-customers/

[17] Sharwood, S. (2021, September 30). *'anonymous' reportedly leaks more stolen Epik Data.* The Register® - Biting the hand that feeds IT. Retrieved May 25, 2022, from https://www.theregister.com/2021/09/30/anonymous_second_epik_dump/

[18] Guardian News and Media. (2022, February 27). Anonymous: The hacker collective that has declared cyberwar on Russia. The Guardian. Retrieved April 28, 2022, from https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

[19] Republic World. (2022, March 4). *Russia-ukraine war: Apple Maps hacked, Russian mod marked as 'ministry of fascism'*. Republic World. Retrieved March 8, 2022, from https://www.republicworld.com/world-news/russia-ukraine-crisis/russia-ukraine-war-apple-maps-hacked-russian-mod-marked-as-ministry-of-fascism-articleshow.html

[20] Brandefense. (2022, April 28). *Russia-based energy organization Elektrocentromontazh targeted by anonymous*. BRANDEFENSE. Retrieved May 25, 2022, from https://brandefense.io/russia-based-energy-organization-elektrocentromontazh-targeted-by-anonymous/

[21] Hackers sound call to arms with digital weapon aimed at Russian websites. CyberNews. (2022, March 7). Retrieved May 25, 2022, from https://cybernews.com/news/hackers-sound-call-to-arms-with-digital-weapon-aimed-at-russian-websites/

[22] Mauran, C. (2022, March 2). *The fight to combat Russian misinformation via Google Restaurant Reviews*. Mashable. Retrieved May 25, 2022, from https://mashable.com/article/google-reviews-share-misinformation-russia-ukraine

[23] Paganini, P. (2022, March 4). These are the sources of ddos attacks against Russia, local NCCC warns. Security Affairs. Retrieved March 15, 2022, from https://securityaffairs.co/wordpress/128680/hacking/russia-shared-info-ddos-sources.html

[24] Gatlan, S. (2022, March 5). *Russia shares list of 17,000 IPS allegedly ddosing Russian orgs*. BleepingComputer. Retrieved March 18, 2022, from https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/

[25] News March 1. (2022, March 23). *Belarus hackers attack train systems to disrupt Russian troops*. Railway Technology. Retrieved March 12, 2022, from https://www.railway-technology.com/news/belarus-hackers-attack-train-systems/

[26] Bateman, T. (2022, May 10). *Russia attacked Europe's internet an hour before invasion, West says*. euronews. Retrieved May 13, 2022, from https://www.euronews.com/next/2022/05/10/west-says-russia-led-major-cyber-attack-on-satellite-broadband-network-just-before-ukraine

[27] *Douligeris C. and Mitrokotsa A. Computer networks: The International Journal of Computer and Telecommunications Networking*. Amsterdam: Elsevier. ISSN 1389-1286.

[28] *Demonstrace U Bytů poslanců - 17. únor - události: česká televize*. Úvodní stránka České televize. (2022, February 17). Retrieved April 26, 2022, from https://www.ceskatelevize.cz/porady/1097181328-udalosti/222411000100217/cast/894865/

[29] iROZHLAS. (2022, February 16). *Iniciativa CHCÍPL PES Zveřejnila adresy 70 poslanců. Vyzvala K Protestům před Jejich Domovy*. Retrieved March 30, 2022, from https://www.irozhlas.cz/zpravy-domov/pandemicky-zakon-chcipl-pes-adresy-poslancu-demonstrace-protest_2202161034_ako

[30] Douglas, D.M. Doxing: a conceptual analysis. *Ethics Inf Technol* **18,** 199–210 (2016). Retrieved November 15, 2021 from: https://doi.org/10.1007/s10676-016-9406-0

[31] *Geo-bombing: Youtube + google earth*. Global Voices Advox. (2019, April 15). Retrieved May 25, 2022, from https://advox.globalvoices.org/past-projects/advocacy-20-guide-tools-for-digital-advocacy/geo-bombing-youtube-google-earth/

[32] Geens, S. (2008, May 28). *Google earth bombing for a free Tunisia*. Ogle Earth. Retrieved May 25, 2022, from https://ogleearth.com/2008/05/google-earth-bombing-for-a-free-tunisia/

[33] Gharbia, S. B. (n.d.). *Geobombing - Rageuniversity.com*. Your YouTube videos on Google Earth. Retrieved May 26, 2022, from http://rageuniversity.com/blogsecure/files/geo-bombing-youtube%20and%20google%20earth.pdf

[34] *Geo-bombing · Global Voices Community blog*. Global Voices Community Blog. (n.d.). Retrieved November 10, 2021, from https://community.globalvoices.org/guide/technical-guides/geo-bombing/

[35] Devane Mar 16, O. (2017, October 17). *Hacktivists turn to phishing to fund their causes*. McAfee Blog. Retrieved May 20, 2022, from https://mcafee-uat.mcafee.com/blogs/mcafee-labs/hacktivists-turn-phishing-fund-causes/

[36] Johnson, B. (2009, November 11). *Recap: Cracking open us courtrooms*. The Guardian. Retrieved November 10, 2021, from https://www.theguardian.com/technology/2009/nov/11/recap-us-courtrooms
[37] Wade, P. (2021, October 25). *Facebook bowed to Vietnam Government's censorship demands: Report*. Rolling Stone. Retrieved March 15, 2022, from https://www.rollingstone.com/politics/politics-news/facebook-vietnam-censorship-1247323/
[38] Toulas, B. (2022, March 3). *Hacktivists, cybercriminals switch to telegram after Russian invasion*. BleepingComputer. Retrieved March 16, 2022, from https://www.bleepingcomputer.com/news/security/hacktivists-cybercriminals-switch-to-telegram-after-russian-invasion/
[39] The Tor Project, Inc. (n.d.). *About tor browser.* ABOUT TOR BROWSER | Tor Project | Tor Browser Manual. Retrieved April 10, 2022, from https://tb-manual.torproject.org/about/
[40] Tiwari, A. (2022, January 20). *Tor explained: What is tor? how does it work? is it illegal?* Fossbytes. Retrieved April 10, 2022, from https://fossbytes.com/everything-tor-tor-tor-works/
[41] The Tor Project, Inc. (n.d.). *About tor browser.* ABOUT TOR BROWSER | Tor Project | Tor Browser Manual. Retrieved April 10, 2022, from https://tb-manual.torproject.org/about/
[42] *The Tor Project: Privacy & Freedom Online*. Tor Project. (n.d.). Retrieved April 20, 2022, from https://www.torproject.org/about/history/
[43] Latto, N. (2021, November 25). What is browser fingerprinting and how can you prevent it? Retrieved April 11, 2022, from https://www.avast.com/c-what-is-browser-fingerprinting
[44] Crenshaw, A. (n.d.). *DEF CON® hacking conference*. Retrieved April 4, 2022, from https://defcon.org/images/defcon-22/dc-22-presentations/Crenshaw/DEFCON-22-Adrian-Crenshaw-Dropping-Docs-on-Darknets-How-People-Got-Caught-UPDATED.pdf
[45] Am I totally anonymous if I use tor? Support. (n.d.). Retrieved April 10, 2022, from https://support.torproject.org/faq/staying-anonymous/
[46] Anderson, K. (2006). Hacktivism and Politically Motivated Computer Crime. Retrieved November 15, 2022, from https://web.archive.org/web/20080227132540/http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf
[47] Gabriella Coleman: Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. London: Verso 2014. (2021)
[48] Heemsbergen, L. (2021). *Radical transparency and digital democracy: WikiLeaks and beyond*. Emerald Publishing.
[49] MARMURA, Stephen M. E. *The WikiLeaks Paradigm: Paradoxes and Revelations*. Imprint: Palgrave Pivot, 2018. ISBN 9783319971391.
[50] *Submit documents to WikiLeaks*. WikiLeaks. (n.d.). Retrieved March 30, 2022, from https://wikileaks.org/What-is-WikiLeaks.html
[51] *About* . About - Distributed Denial of Secrets. (n.d.). Retrieved May 4, 2022, from https://ddosecrets.com/wiki/About

[52] *'BlueLeaks' Exposes Files from Hundreds of Police Departments*. Krebsonsecurity.com. Retrieved April 14, 2022, from https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

[53] *The emergence of open and organized pro-government cyber attacks in the Middle East: The case of the Syrian Electronic Army*. The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army | OpenNet Initiative. (n.d.). Retrieved March 2, 2022, from https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army

[54] *Who are killnet and what are they known for?* AZLYRICS.COM.AZ | Lyrics Search Engine from A to Z. (2022, March 2). Retrieved April 28, 2022, from https://azlyrics.com.az/lyrics/who-are-killnet-and-what-are-they-known-for/

[55] Oduro-Marfo, Smith. (2015). IMPLICATIONS OF HACKTIVISM FOR INTERNATIONAL SECURITY. Retrieved from https://www.researchgate.net/publication/335330650_IMPLICATIONS_OF_HACKTIVISM_FOR_INTERNATIONAL_SECURITY

Rozšířený abstrakt

Tato bakalářská práce se zabývá fenoménem zvaný hacktivismus, jeho významem, motivací jeho aktérů, historickým vývojem, užívanými metodami a jeho vlivem na lidskou společnost a její bezpečnost. Cílem této práce je poskytnout přehled o tomto fenoménu, který jak v minulosti, tak i v současné době má nemalý vliv na široké spektrum aktuálně diskutovaných témat a jejich povědomí ve společnosti a to speciálně v době, kdy tento fenomén je opět na vzestupu díky vývoji současného geopolitického a společenského dění, zejména v Evropě a v Severní Americe. K dosažení tohoto cíle bylo využito různých zahraničních zdrojů a literárních děl. Jako hlavní zdroje informací sloužily články, analýzy a práce z řad odborných a akademických sfér. Tyto zdroje ale mnohdy nepokrývaly dostatečně všechny aspekty tohoto fenoménu, či se mnohdy informačně vzájemně překrývaly, což bylo na druhou stranu využito k vzájemnému ověřování čerpaných informací. V případě základních informací o daných hacktivistických organizacích byly využity informace uvedené přímo těmito kolektivy na jimi uvedených webových stránkách. Dále byly využity informace z webů organizací, které se zabývají kybernetickou bezpečností, zejména z webových stránek společnosti IBM a antivirových společností Norton, Avast a McAfee. K pokrytí nedávno provedených hacktivistických akcí bylo bohužel potřeba využít článků z různých internetových médií a z veřejných profilů sociálních sítí skupiny Anonymous z důvodu, že tyhle události zatím nebyly nikterak odborně zpracovány.

Pojem hacktivismus se skládá ze slov hacking a aktivismus. Za autora tohoto termínu je považován člen hacktivistické skupiny zvané Cult of the Dead Cow (v doslovném překladu „Kult mrtvé krávy“), vystupující pod pseudonymem „Omega“, který použil tento termín v rámci jeho emailové korespondence s ostatními členy této skupiny v roce 1996. Jedná se tedy o občanský aktivismus, který využívá hackerské praktiky k dosažení svých cílů.

Mezi tyto praktiky patří velmi oblíbené tzv. defacementy webových stránek, kde dochází k prolomení zabezpečení dané webové stránky a nahrazení jejího obsahu za obsah, který má za cíl propagovat danou hacktivistickou rétoriku či ideologii. Dalším velmi častým typem útoků jsou tzv. DDoS útoky, během kterých dochází k zahlcení serveru enormním množstvím požadavků odeslaných v jeden daný moment z vícera výpočetních zařízení. Následkem tohoto útoku je pak znepřístupnění služeb daného serveru jeho běžným uživatelům. Obojí výše zmíněné metody jsou jak nejrozšířenější tak zároveň i nejstarší hacktivisty prováděnými typy útoků, s tím že v případě DDoS útoku se též jedná i o relativně jednoduše proveditelnou techniku.

Často diskutovaným a kontroverzním aktem hacktivistů bývají úniky tajných anebo soukromých informací. Zde je typickým příkladem organizace WikiLeaks, která v minulosti stála za odtajněním nespočetného množství státních dokumentů z několika vládních institucí Spojených států amerických. V posledních letech se ale spíš mluvilo o hacktivistické skupině DDoSecrets, která stála za úniky dat z řad jednotlivých policejních

složek též ve státech USA. Mimo jiné, DDoSecrets se aktuálně angažuje ve válce na Ukrajině, ve které se zaměřuje na úniky dat z jednotlivých ruských institucí, státem vlastněných firem a dalších subjektů jakkoliv napojených na ruskou vládu.

Hacktivismus se dynamicky vyvíjel v návaznosti na rozvoj informačních technologií, zejména s rychlým rozmachem internetu. Díky tomu hacktivismus zažil na začátku milénia výraznější rozmach ve srovnání s 80. a 90. lety minulého století. Nemalý podíl na tom měly též sociální sítě, které během té doby nabývaly na popularitě. S přibývajícími počty jak haktivistických tak i hackerských útoků začaly vládní i soukromé organizace víc řešit problematiku kyber-útoků a kyber-bezpečnosti. Díky tomu přibývalo víc případů, kdy aktéři hacktivismu byli dopadeni policejními složkami a případně odsouzeni k výkonu trestu. To se začalo projevovat na počtu hacktivistických útoků, který od roku 2014 zažíval prudký pád.

V současnosti se často hovoří o tzv. návratu hacktivismu s návaznosti na současně probíhající ruskou invazi na Ukrajině, ve které jsou momentálně významně aktivní hacktivisti ze skupiny Anonymous a DDoSecrets. Od začátku války haktivisté ze skupiny Anonymous provedli několik DDoS útoků a mimo jiné byli schopni se nabourat do vysílání ruských státních televizních stanic. S ohledem na zatím nejasné vyhlídky na konec tohoto konfliktu lze očekávat, že počet takových útoků poroste za cílem nenadále vytvářet tlak na společnost, soukromé subjekty a státní činitele. Proto je vysoce pravděpodobné, že hlavním cílem budou subjekty, které spadají pod vládní aparát Ruské Federace nebo případně operují na území Ruské federace.