HACKTIVISM VS. CYBERTERRORISM

ELIF SU CALISIR

2021/2022

INTRODUCTION

With a ground-breaking development, variety of possibilities of opportunities, events, problems, solutions, and new dynamics crash into our lives. Internet technologies, which increasing number of people consider an integral part of life now, have become the new architect of present and the future by shaping dynamics of our interaction with the world. Ongoing technological revolution opens a window to everything that can be imagined about a new space or invention that involves complex characteristics of human. Gradual introduction of benefits and the side effects also brought long debates. In parallel with the increased accessibility to these technologies, crimes committed via information systems are also emerged and increasing with recursive interactions of communications technologies with their associated societal processes. Cybercrime is a type of crime that targets the security of an information system and/or its data and/or its user and is committed by using the information system. Despite the possibilities of harmful use, the internet is serving to businesses, officials, organizations and individuals with its role in communication, interaction, information sharing and more. In a study on the history of the Internet compiled with the contributions of many academics who are experts in their fields, internet was defined as "a global broadcasting function, a mechanism for disseminating information, and a medium for collaboration and interaction between individuals and computers regardless of geographic location".[1] When we expand the statement "regardless of geographic location", it can be discussed what effects the shortening or elimination of the distances will have. The fact that geographical proximity does not matter to have knowledge of each other has been a development that has the power to change the dynamics of politics, intercultural communication, and social movements. The power of instant communication and information, the effects of all kinds of online civic engagements have brought many perspectives and reactions to societies.

In addition to positive effects such as awareness of societal events brought about by the unity of the world, the strengthening of networks among people and the facilitation of interaction, the emergence of new problems has become inevitable. For this reason, understanding, analyzing, defining and separating these issues will be important in terms of creating a healthier social environment. The cyber world, which is a figurative space to define the world created within the scope of the internet[2], hosts these new problems, crimes, and actions as they are in the

[1] Leiner et al., A brief history of the internet. *ACM SIGCOMM Computer Communication Review*. 2009
[2] Institute of Directors. *A Handbook on Cyber Security*. India, 2021

physical world. The aim of this study is to focus on issues of definitions from the cyber world that are often confused with each other such as cyberterrorism and hacktivism by interpreting them based on different layers of the cyber world, and to reinforce the difference of these definitions by giving examples of the definitions put into practice. The focus will be on the concepts of cyberspace, cybercrime, cyberterrorism, online activism, hacktivism and and finally the differences will be discussed. The important point to be noted is that the structure of the actions should be the determining factor, and no matter how the group defines itself or how it is defined by others, it is the structure that will give the real identity of the action. Because although the group defines itself as an activist, if the actions become destructive and create an atmosphere of fear, terrorism is mentioned, and in the same way, some individuals or groups judged by states to be terrorists are just activists.

HOW REAL IS THE CYBERSPACE?

The right way to clarify the confusion of concepts would be to start with "cyberspace", which incorporates other concepts in this discussion. The hard-to-follow dynamism of the digital world leads to the diversity of definitions, and the literature adds new components to the definitions by constantly updating itself. In a 12-year-old study on the cyberspace definition[3], by adding human and time components to the definitions back in that time, cyberspace was defined as "time-dependent set of interconnected information systems and the human users that interact with these systems". One of the most important points emphasized in the study was human factor in cyberspace which highlights that cyberspace should not be defined as an abstract concept because it arises from the need, existence, and interaction of real people. Continuing on the path by accepting this aforementioned human fragment of cyberspace as a key point offers the opportunity to define other concepts related to the digital world better. On the other hand, when the subject is approached from a technical point of view, it can be concluded that the consists of components such as the "World Wide Web, intranets (private internets), extranets (internets with restricted memberships), and all other networks using different protocols (detailed operational specifications) from the internet[4]". From a broader perspective, it is possible to divide the cyberspace environment into three layers which are (1)

[3] Ottis, R., and P. Lorents. 'Cyberspace: Definition and Implications.'. In *5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April*

[4] Baldi, Stefano, Eduardo Gelbstein, and Jovan Kurbalija. *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace*. Msida, Malta: DiploFoundation, 2003.

physical layer, which includes geographic and physical network components, (2) social layer, that includes real persons (persona) and logical identities (cyber persona), and lastly (3) logical layer, which operates as a bridge between physical and social layers[5]. When the components of social layer cannot be adequately examined, people tend to misconceive the actions in the cyber world only based on the tools or methods used by actors. But in fact, although the cyber studies are under the title of "cyber", there is no sharp distinction between cyber world and real world since all the actions in the cyber world have a counterpart, value and meaning in the physical world. This fact might be even more valid for the cyber activities that are driven by political and social motives such as hacktivism or cyberterrorism than some others since they might lead to positive or negative social, economic, and political consequences that can be considerably effective or serious. Although the actions are initiated or take place in the digital world in some phases of these activities, the aim is to draw attention to a particular societal issue, damage particular institution, organization or government, support or harm a specific group which means the actions create change in the "real" world. So that, "cybersecurity is no longer the remit only of private or corporate practitioners but has become a complex site of interaction between a very wide range of people, organizations and technologies, especially in statist discourses".[6] In addition to this reality, most of the cyber-attacks have not yet been addressed by the international existing legal bodies or adequate studies have not been carried out.[7]

CYBERCRIME

Crime is a dynamic and social phenomenon which its dynamics varies within societal conditions. As the internet becomes extremely integrated into society, both social interactions and business or organizational networks started to take place online. This attachment to the Internet and the migration of society to computers has brought the concept of crime on the street to digital platforms by adding components of computers and networks. The types of crimes encountered in daily life are also frequently visible on the internet due to today's technological possibilities: illegal publications, credit card frauds, copyrighted software, etc. With the

[5] Lai, R. (2012). Analytic of China Cyberattack. The International Journal of Multimedia & Its Applications, 4(3), 37–56. https://doi.org/10.5121/ijma.2012.4304

[6] Stevens, Clare. 'Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet'. *Contemporary Security Policy* 41, no. 1 (2 January 2020): 129–52. https://doi.org/10.1080/13523260.2019.1675258.

[7] Madubuike-Ekwe, Joseph N. 'Cyberattack and the Use of Force in International Law'. Beijing Law Review 12, no. 02 (2021): 631–49. https://doi.org/10.4236/blr.2021.122034.

possibilities provided by information technologies and which cannot be said to be adequately controlled, crimes are enabled to be committed in a way that cannot be imagined in the very recent past. In his participation in Craig Mundie's podcast Darknet Diaries, a former adviser to Bill Gates mentions that there are simply three main categories of attacks: spray-and-pray attacks, targeted attacks, and APTs (Advanced Persistent Threats). [8] The first of these has been defined general way of scanning the internet and trying to find vulnerabilities that can be attacked. The second, targeted attacks, specifically target a group or individual. APTs are more sophisticated attacks with more motivation and resources.

One of the problems in tracing these offences is that people can hide themselves behind anonymity shield of cyberspace. In this regard, each country may have a different point of stand, and the existence of even individual differences have made this issue a controversial one. While for some, online anonymity is something that should be protected for many reasons such as "protection of right to seek, receive and impart information"[9], for others it should be regulated since it creates extreme challenges on the way to reach criminals. Even though anonymity is used by hobby hackers or hacktivist groups, majority of cybercrime cases are financially motivated.[10] From a gameplay point of view, where random people were targeted by hackers who wants to test and demonstrate their abilities, cyberattacks now have mainly become organized crime with deep financial gains. In any case, information technology tools such as "cloud computing" create "loss of location" for attackers and this leads to challenges against collecting the electronic evidence for prosecution[11]. Since perpetrators have lower probability of being detected with the limitations arise from territoriality, number of cases have been increasing and complicating the issue given the increased dependence to internet of things and software. To summarise the discussion in one statement: "although there is an increased need for the protection of anonymity in today's digital environment, there also an increased need for governments to protect people from cyber-harms"[12]. In topics such as this, there is no correct or wrong answers, yet.

---

[8] 'Operation Socialist – Darknet Diaries', n.d. https://darknetdiaries.com/transcript/48/.

[9] Land, Molly. 'Toward an International Law of the Internet'. *Harvard International Law Journal* 54, no. 2, 2013.

[10] Lusthaus, Jonathan. 'Cybercrime: The Industry of Anonymity'. University of Oxford, 2016

[11] Kleijssen, Jan, and Pierluigi Perri. 'Cybercrime, Evidence and Territoriality: Issues and Options'. In *Netherlands Yearbook of International Law 2016*, edited by Martin Kuijer and Wouter Werner, 47:147–73. The Hague: T.M.C. Asser Press, 2017. https://doi.org/10.1007/978-94-6265-207-1_7

[12] Land, 'Toward an International Law of the Internet'. 2013

Another challenge is that the fact that the scope of internet is across national boundaries makes enforcement of law difficult. Inapplicability of law internationally opens more space with low probability of being punished which leads encouragement for perpetrators. The concept and sanctions of crime, which is defined as an unlawful act that is considered a crime by the laws and is subject to criminal sanctions, can only be established or abolished by laws[13]. For this reason, if a behavior is not considered a crime by the law, it is not considered a crime even if it is an unlawful behavior. In other words, the criminal rule determines the crime in the legal sense. If there is no rule, there is no crime. If we define the concept of crime clearly in this field as well, we can then define positive and negative actions prohibited by law under the threat of punishment. E.g., hacking can be referred to accessing an information system unlawfully and without the consent of the owner, usually with this access many rights can be violated, and a door can be opened for other crimes to be committed. The motivation and position of the computer in the offence committed is helpful to define and trace the attacks. According to The U.S. Department of Justice[14], there are three different ways of involvement which are (1) computer as a target (e.g., software theft), (2) computer as a weapon (e.g., interference of service provided a server), (3) computer as a facilitator (e.g., mail fraud); but all activities that violates criminal law and involves computer is considered as computer crime. Even though most cybercrimes involve same tools and techniques, all cybercriminals cannot be put in one common box and motivation is the main indicator to divide different actors between each other.

WHAT IS CYBERTERRORISM

To define cyberterrorism, it will be useful to focus on the concept of terrorism and underline the different definitions and perceptions since it is a problematic issue itself by being one of the concepts that is widely used but does not have a universal accepted definition. Why is it so problematic? The main reason is the subjective nature of the concept. One defines as "the use or threat [of action] designed to influence the government or to intimidate the public or a section of the public, and the use or threat is made for the purposes of advancing a political, religious or ideological cause."[15] It can be mentioned the existence of few main elements, which are (1) violence or the threat of violence, (2) against government or public, (3) for certain specific

[13] Marchuk, Iryna. *The Fundamental Concept of Crime in International Criminal Law*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. https://doi.org/10.1007/978-3-642-28246-1.
[14] Chris, Kim, Newberger Barrie, and Brian Shack. 'Computer Crimes'. *American Criminal Law Review* 49, no. 2 (2012): 443–88.
[15] Terrorism Act, 2000

purposes. For instance, it is one of the controversial points and not entirely correct term to use that it must be against "public", regardless of who you are attacking, if the attack is made to a weak spot in an unexpected way, the other side does not stand a chance to defend. In this sense, the definition can be updated as "violence or the threat of violence against people that cannot defend themselves".

Other captious point that should be discussed is the limits of the purpose for which the terrorist actions are carried out, because "political, religious, racial or ideological cause" can include almost anything possible and the problem is that who is carrying out this action enables us to interpret that action as terrorism. This is not fully objective since the definitions only mention about non-state actors and the future existence of objective definitions seems difficult as long as the countries themselves are the ones making these decisions. Also, intention of terrorist act can be given with different definitions in different countries. For example, while intention of terrorist act is defined as "acts committed for political, religious, ethnic or ideological purposes suitable to create fear in the population or any section of the population and thus to influence a government or public body" in Germany, the same concept is defined in France as "seriously and intentionally disrupt law and order"[16]. Because of these differences, there has been a need for a common definition of terrorism in international law to fight terrorism and studies have been carried out on this. According to Zeidan[17], terrorism does not have a universally accepted definition, because countries have different political interests and are in different situations in different times. Definitions of terrorism, terrorist and terrorist organization often reflect the meaning given by the viewer. In other words, to describe it as a cliché, a terrorist according to one side can be a member of national liberation or a freedom fighter according to other side. The stretching or distortion of the definition due to political and economic interests has been a an obstacle on the way of the fight against terrorism. International organizations have organized conventions and seek solutions in order to meet on a common ground in this regard. For example, according to the United Nations[18] definition of terrorism:

[16] OECD. 'Definition of Terrorism by Country in OECD Countries', OECD International Platform on Terrorism Risk Insurance, n.d.

[17] Zeidan, Sami. "Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism". *Cornell International Law Journal*, July 2003, pg. 491-96.

[18]United Nations, *A/RES/49/60. Measures to eliminate international terrorism*, UN General Assembly https://web.archive.org/web/20190616073441/https://www.un.org/documents/ga/res/49/a49r060.htm.

> Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.

Apart from international organizations and institutions, there is a search for a common definition of terrorism in academic studies. Nevertheless, in a study on the definition of terrorism, the author gives examples from academics who wanted to meet on a common ground on terrorism and explained that this search was not very effective and argued that it is necessary to understand the relations and interactions of countries in order to see the reasons behind the terrorist label.[19] It is natural, but complex, that states and individuals have different definitions of terrorism according to their own values and interests in defining such critical and powerful concepts. Just as history is written by the winners, definitions can be dominated by the strong. Most states do not hesitate to define groups that oppose them as terrorists. Given the inadequate or unsuccessful effort of international institutions to find a common definition, in order to be against biased definitions of governments, it is important to have as impartial academic studies as possible.

The fact that terrorism and its consequences bear heavy costs for the societies in the whole world is clearly seen. Even though history of terrorism and terrorist acts go back much further, terrorist groups have entered more into international actions and interactions, especially through the opportunities provided by advanced technologies. These inherent risks of the network society, which can occur when terrorist organizations innovate in terrorism techniques. While these are the possible threats, if making a single common definition of terrorism is so challenging and has not been achieved yet, it is predictable that there may be definitional differences regarding cyberterrorism. For similar reasons, discussions on the subject of cyberterrorism continue both in the academic community and in other political and international institutions. According to Weimann[20]

> Psychological, political, and economic forces have combined to promote the fear of cyberterrorism. From a psychological perspective, two of the greatest fears of modern time are

[19] Petta, De Leon. "Why there is no real difference between a Terrorist Organization and an Organized Crime faction, just a matter of interaction towards the State". *Contemporary Voices: St Andrews Journal of International Relations*, c. 1, sy 1, May 2018, s. 26. *DOI.org*

[20] Weimann, Gabriel. *Cyberterrorism - How Real Is the Threat?* United States Institute of Peace, Dec. 2004.

> combined in the term "cyberterrorism." The fear of random, violent victimization blends well with the distrust and outright fear of computer technology.

At this point, one of the most likely questions that come to mind is: "if which conditions occur, the activity in the cyber world can be called cyberterrorism?" When there are so many definitions of terrorism, when a "cyber" label is added to it, the discussion becomes more difficult and involves many different activities, from "narrow" to "broad" definitions, can be examined under the heading of cyberterrorism.[21] If cyberterrorism is defined narrowly, it can be defined as the result of death of civilians by politically motivated attacks on information systems, if we expand the spectrum more, every activity in which terrorists use information systems for their activities can be called cyberterrorism.[22] Indeed, it is seen that the use of violence in the phenomenon of terrorism gains continuity in the social environment and provides effectiveness only if some facilitating factors help the aforementioned phenomenon. When we think about what these auxiliary elements can be, the convenience provided by modern technology comes to mind first, followed by the role of mass media and especially the "internet" draws attention. Another question that we can encounter in this discussion is whether cyber terrorism is a sub-branch of terrorism or a separate concept. In Jarvis & Macdonald's research[23] on defining the subject of cyber terrorism, most of the researchers who responded expressed cyberterrorism as a different type that has many common points with conventional terrorism. In order to avoid the confusion which is that all computer-related terrorist activities can be accepted as cyberterrorism, the situations where computer support is used in the processes as advertising, information gathering and recruitment for terrorist activities can be defined as "computer-assisted" terrorism.[24]

Cyberterrorism targets or uses cyberspace and has consequences outside of it. Cyber-attacks have potential that they can be capable of damaging national critical infrastructure, economy and national security. Threats include sabotage of information networks, theft of classified military and defense information, cyber-attacks that cause serious disruptions, and viruses that

---

[21] Brunst, Phillip W., 2010 "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet". *A War on Terror?* Springer, New York

[22] *Ibid.*

[23] Jarvis, Lee, and Stuart Macdonald, 2015 "What Is Cyberterrorism? Findings From a Survey of Researchers". *Terrorism and Political Violence*

[24] Giacomello, Giampiero, 2014 "Close to the Edge: Cyberterrorism Today". *Contributions to Conflict Management, Peace Economics and Development*, c. 22, Emerald Group Publishing

disable or completely destroy service which can cause financial loss, psychological and physical damage. Although attacking a country's critical system is not a new type of attack, the fact that countries' very crucial electrical infrastructures are very intertwined with software makes these networks an open target since the internet is not perfect in terms of security despite its resilient structure[25]. These examples can be expanded to the critical national systems of the army, traffic lights, natural gas networks, water systems, hospitals, airline management systems and many more. Although cyberterrorism carries out its attacks with the help of malicious software and computer technologies instead of the weapons used by conventional terrorism, it is similar to conventional terrorism in its motivation to cause physical and psychological harm to civilians for political, religious or ideological goals[26]. On the other hand, while academics, politicians, security experts and many others share concerns about the issue, the absence of recorded successful cyberterrorism activity leads some to believe that, although the threat has undeniable potential, it has been exaggerated.[27]

In defining cyberterrorism, some focus more on the activities, while others focus more on who the actors are. Denning stipulates that "an attack should result in violence against persons or property, or at least cause enough harm to generate fear"[28] to be qualified to be defined as cyberterrorism. This definition can be considered as actor-agnostic.[29] Such as Denning's definition, these definitions emphasize factors such as actions, motivation and destructiveness of the consequences rather than actors. In this actor-agnostic definition the actors involved in terrorist act can be state or non-state actors. With advances in digital infrastructures, the perpetrators of cyber-attacks are easier to trace and are not always non-state actors. On the contrary, state actors have the power and capability to be more destructive and higher change to be successful. Stuxnet[30] can be given as an example which was one of the first attacks that

---

[25] Geers, Kenneth. 'The Cyber Threat to National Critical Infrastructures: Beyond Theory'. *Information Security Journal: A Global Perspective* 18, no. 1 (6 February 2009): 1–7. https://doi.org/10.1080/19393550802676097.

[26] Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 'Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes'. *Journal of Cybersecurity*, 15 February 2017. https://doi.org/10.1093/cybsec/tyw018.

[27] Weimann, Gabriel. *Cyberterrorism - How Real Is the Threat?* Dec. 2004.

[28] Denning, Dorothy E. 'Statement of Dr. Denning', 2000. https://irp.fas.org/congress/2000_hr/00-05-23denning.htm.

[29] Jayakumar, Shashi. 'Handbook of Terrorism Prevention and Preparedness'. In *Cyber Attacks by Terrorists and Other Malevolent Actors: Prevention and Preparedness - With Three Case Studies on Estonia, Singapore, and the United States*, n.d.

[30] Baezner, Marie, and Patrice Robin. 'Hotspot Analysis: Stuxnet'. Center for Security Studies (CSS), ETH Zürich, October 2017. "Stuxnet was a malware first discovered in 2010 on an Iranian computer. It was designed to

attempted to cause physical damage and was that most people believe is being carried out by the U.S. and Israel governments.[31] Most non-state actors are unable to compete with the resources of large states. They, however, continue to effectively use social media and other web resources for fundraising, propaganda, and member recruitment. In the empirical study on the subject, it has been observed that ISIS and Al Qaeda organizations use platforms such as YouTube, Twitter and Facebook in their own ways to advertise their ideologies and reach new members.[32] Internet allows loosely cooperated terrorist groups to aggregate, forming larger networks. Since they are distributed, layered, and more redundant, and consequently more resistant to leadership changes and disruption, and even detection. In this way, the internet has amplified terrorist effectiveness many folds by enabling distribution of shared ideologies to a much wider population.

ACTIVISM IN CYBERSPACE

Activism can be defined as an action or set of actions taken consciously to bring about change in the political, economic or social structure. It has resonated in different ways in different times. Sometimes people went extreme and set government buildings on fire, and sometimes it was enough to write messages to the editor of the local newspaper to be heard by the authorities. As the internet revolutionized activism, many of such actions aiming to become visible, and create consciousness have been moved to digital platforms together with the expansion of the cyberspace as it is easier to announce the cause and intention with others. While some people engage in digital activism only through social media or certain websites, others go further to right political and societal wrongdoing that they oppose. In order to reveal the changing structure of social movements depending on the transformation of the form of society, Jan van Dijk[33] revealed that this modern society type, which he called "network society", an infrastructure formed in social and media networks which determines the individual and group organization style in society. Despite the high impact of digital platforms, while many people from different countries or groups may want change, fewer people actually can or are willing

specifically to sabotage centrifuges in the Iranian nuclear facility of Natanz. The discovery of Stuxnet raised awareness of cybersecurity issues for critical infrastructures around the World."

[31] Jayakumar, Shashi. 'Handbook of Terrorism Prevention and Preparedness'

[32] Choi, Kyung-shick, Claire Lee, and Robert Cadigan. 'Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS'. *International Journal of Cybersecurity Intelligence & Cybercrime* 1, no. 1 (1 August 2018): 21–39. https://vc.bridgew.edu/ijcic/vol1/iss1/4.

[33] Dijk, Jan van. *The Network Society: Social Aspects of New Media*. 2nd ed. Thousand Oaks, CA: Sage Publications, 2006.

to take action. One of the main reasons for this is that even when people believe that change is necessary, they may have as many reasons for not doing so as they have motivations to act. In the case of people who have to live in countries ruled by oppressive governments, there are people who are dissatisfied or are suffering from the consequences of restriction of freedoms and lack of fair governance of the country. While there are many things about their country that they have to fight against, paradoxically, they have less voice about injustices than citizens in countries that are relatively freer and justly governed. The restriction of freedom of expression is a great motivation for activism, even if it undermines these actions. For these reasons, the anonymity, mentioned above[34] as controversial, is what the cyber world offers to people which is a tool for those who are struggling to express themselves freely. Although there are situations where anonymity cannot be fully protected from time to time, it is used by activists to "check on governments"[35] and not easily detected by the authorities.

Activism in the cyberspace offers a new and broad environment to social movement organizations, to activists who participate in any collective movement or to the individuals who want to carry out their actions independently. These contemporary activist movements in the cyberspace divided into three different categories such as: (1) digital spectator activities (e.g., assertion, metavoicing, clicktivism); (2) digital transitional activities (e.g., e-funding, botivism, digital petitions, political consumerism); (3) digital gladiatorial activities (e.g., hacktivism, exposure and data activism).[36] Although these activities show similarities in motivation, they often spread over a wide spectrum in terms of methods and consequences.

To group the effects of digital activism; (1) cognitive effects which the aim is to influence an individual through logic and facts, (2) emotional effects which aims to have an impact on an individual's feelings, (3) financial effects which have an impact on revenues and costs, (4) operational effects which impact the functionality of the entity, (5) reputational effects which influences public view and awareness and (6) power effects which have impact on the level of control.[37] Differences in the categorization and definition of digital activist forms and effects also shape perception towards these acts. If it is mentioned about digital activism movements

[34] See pg. 4

[35] Megiddo, Tamar. 'Online Activism, Digital Domination, and the Rule of Trolls'. *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3459983

[36] George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), 100249.

[37] *Ibid.*

through social media; although it is easily criticized, it should be considered valuable in terms of the effect it creates. In addition to the views that define the means of communication as the means of reaching the ideal social order, there are also those who claim that the actions put forward in this context do not contribute to the real forms of social struggle that help individuals to satisfy themselves. Critics states that such movements hinder more determined "active" activities, and they can be perceived as less genuine or even lazy (e.g., slacktivism[38]). Nevertheless, even the power of online forums, petitions, likes, status updates, mass emails, retweets and shares should not be underestimated in terms of their effect on collective action. Increased transnationalization with the social media allows messages and reactions to spread and multiply more quickly by force of "more virtual, more fluid, more decentralized, more de-institutionalized and more global" nature of online activism.[39]

HACKTIVISM EXPLAINED

In the past, computer technology was used to give digital support to activism for communication purposes. With the media boom in the mid-90s, activists with computer programming knowledge began to discover new and different channels which they could react in different forms.[40] Thus, activism in the digital environment has begun to change. Hacktivism, being a part of the change, was defined as the combination of hacking and activism, which includes "illegal or legally ambiguous" hacking methods, and targets to disrupt an organizational or individual target without causing serious damage.[41] "Web sit-ins, virtual blockades, automated e-mail bombs, web hacks, computer break-ins, computer viruses and worms" can be given some of the examples of methods that are used.[42] Although there are many different definitions, we can define it as a form of activism integrated into the digital world through information and communication technologies. Emergence of this type of protest in digital world can have many

[38] 'Slacktivism', n.d. https://dictionary.cambridge.org/dictionary/english/slacktivism. "Activity that uses the internet to support political or social causes in a way that does not need much effort"

[39] Cammaerts, Bart. 'Social Media and Activism'. In *The International Encyclopedia of Digital Communication and Society*, edited by Robin Mansell and Peng Hwa Ang. The Wiley Blackwell - ICA International Encyclopedia of Communication. Chichester, West Sussex, UK: Wiley Blackwell/John Wiley and Sons, Ltd, 2015

[40] Busch, Otto von, and Karl Palmås. *Abstract Hacktivism: The Making of a Hacker Culture*. London: OpenMute, 2006.

[41] Alexandra Whitney. Samuel. 'Hacktivism and the Future of Political Participation'. Harvard University Cambridge, Massachusetts, 2004. https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

[42] Dorothy E. Denning (1999), Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Global Problem-Solving Information Technology and Tools https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

different causes such as human rights violations, inequalities, political oppression, environmental protection etc. Because of the high internet dependence almost anything can become a target for hacktivists. These include governments, large corporations, key leaders, local or national public institutions depending also on the level of ease to infiltrate or disrupt.

Hackers have created the cyberspace and the internet to be a free space for them. Cyberspace has a living nature, and only "netizens" can decide the way that nature will enter and the changes it will experience[43]. A foreign intervention or an attempt to establish power in cyberspace is seen as a situation contrary to the nature of cyberspace, which is unacceptable to hackers since they believe "non-violent intrusions to computer networks being morally permissible for increasing knowledge about Internet security technologies or for removing morally illegitimate barriers of information"[44]. Therefore, we see a lot of hacktivist actions, especially against countries that has internet censorship applications, on issues such as the free speech or free use of the internet.[45] The groups and individuals are "arrayed across a far wider political spectrum than the techno-libertarian agenda with which committed 'netizens', including the hacker fraternity"[46]. Hacktivists have problems and difficulties caused by the misunderstanding, misrepresentation that comes from negative image of the hacking culture. The power-oriented broadcasting structures of the media and the desire to make news by simplifying everything and without going to the core of the matter mislead those who do not have much relationship with the culture or people who emulate it. Besides, as we can see in the hacker portrayals in Chinese and US media, countries motivated by their own ideologies, domestic and foreign policy strategies, and therefore report different hacking activities in the media in a biased manner depending on the type and origin of the activity.[47] In other respects, for hacktivists their actions are necessary steps for change.

---

[43] Hauben, Michael. 'Chapter 1: The Net and Netizens: The Impact the Net Has on People's Lives'. In *Netizens: An Anthology*, 1995.

[44]Laitala, Nuutti. 'Hacktivism and Cyberterrorism: Human Rights Issues in State Responses', 2012. https://doi.org/20.500.11825/740.

[45] Samuel. 'Hacktivism and the Future of Political Participation' 2004

[46] Conway, 'Cyberterrorism: Hype and Reality', 2007.

[47] Pei, Jiamin, Dandi Li, and Le Cheng. 'Media Portrayal of Hackers in *China Daily* and *The New York Times* : A Corpus-Based Critical Discourse Analysis'. *Discourse & Communication* 16, no. 5 (October 2022): 598–618. https://doi.org/10.1177/17504813221099190.

When we consider activism as a form of protest, we are presented with five common methods used in this context: (1) Denial-of-Service attacks, (2) site defacements, (3) site redirects, (4) virtual sit-ins, (5) information theft.[48] The word 'hack' gives the impression that computer programming knowledge is important. Considering the abundance of simultaneous hacktivist operations, the large number of people involved and the human circulation, it does not seem likely that all individuals involved are hackers with advanced computer programming knowledge. One of the most used methods, DDoS (distributed denial of service) aims to block access to the targeted website with the mass involvement of the "voluntary or involuntary botnets".[49] It is a highly preferred and prevalent method, since it allows hacktivist organizations to create masses quickly.[50] One of the reasons why methods like DDoS remain popular even as technology evolves rapidly is to create an integrated version of the participation on the streets, which is the place of direct action in activism, in the digital world. In this way, it is possible to create electronic civil disobedience by creating virtual sessions.[51] Virtual sit-ins also aim to disrupt access to a targeted website by reloading the webpage, but unlike DDoS method, the reloading is attempted only by individuals.[52] Therefore, it is considered a more democratic form of hacktivism.[53] These two collective methods do not require extremely advanced computer programming knowledge which pave the way for to gain new members which enables collective action. The other three methods mentioned are carried out through unauthorized access to servers, and site defacement which are the most popular among three, in which the site is changed to give a specific message, site redirects are used to redirect to another site to give a message, and information theft is a special information obtained by unauthorized access.[54]

In 2000, a hacktivist group called Electrohippies carried out DDoS attacks on the World Bank and IMF websites for a cause which is represented as "a world where e-commerce is balanced

---

[48] Hampson, Noah C. N. 'Hacktivism: A New Breed of Protest in a Networked World'. *Boston College International & Comparative Law Review* 35 (2012): 511.

[49] *Ibid.*

[50] Adams, Joshua. 'Decriminalizing Hacktivism: Finding Space for Free Speech Protests on the Internet'. *SSRN Electronic Journal*, 2013. https://doi.org/10.2139/ssrn.2392945.

[51] Alexopoulou, Sofia, and Antonia Pavli. '"Beneath This Mask There Is More Than Flesh, Beneath This Mask There Is an Idea": Anonymous as the (Super)Heroes of the Internet?' *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique* 34, no. 1 (February 2021): 237–64. https://doi.org/10.1007/s11196-019-09615-6.

[52] Hampson, 'Hacktivism: A New Breed of Protest in a Networked World'. 2012

[53] Samuel. 'Hacktivism and the Future of Political Participation' 2004

[54] Hampson, 'Hacktivism: A New Breed of Protest in a Networked World'. 2012

by e-protest". The hacktivist group believed that their actions were not criminalized, and at the time there was no legal consensus on these actions, and although their identities were known, they were not punished.[55] As in this case, some believe that hacktivism should be separated from hacker groups that are financially motivated or destructive in nature while some associate it entirely with terrorism. Others summarize the situation as that "hacktivist actions are neither a dangerously criminal nor a totally justifiable political practice"[56]. Individuals (or groups) who perform these actions strive to get their message across to governments, global organizations, businesses, and society at large. These actions sometimes cause reputational losses as well as financial losses to the institutions that are the target of the action. While they define themselves as "heirs to those who employ the tactics of trespass and blockade in the realm of real-world protest"[57], there is no consensus on the subject. Some perceive "either negative, such as 'e-bandits', 'cyber lynch-mobs', 'cyber terrorists', and 'online avengers', or positive, such as 'freedom fighters', 'digital Robin Hoods', and 'white knights'"[58]. Although hacktivism is a concept that transcends borders, it may be seen as more acceptable or even necessary due to certain political, social and economic conditions in some countries. On the other hand, hacktivists, who are described as "stateless, elusive, sometimes lawless and almost always anonymous", may not be seen as necessary in the same way in countries that "protect privacy and that recognize generously interpreted freedom of expression"[59].

According to some sources, information identified as leaks is delivered through hacktivism or through the delivery of an 'insider', and this is categorized as the 'exposure' category of digital activism.[60] Although all systems have their own vulnerabilities, one of the weakest links is the 'human' element. For this reason, it seems that over time, we will be faced with bigger actions as a result of 'insider' information leaks from supporters/sympathizers who are employed in the system and have problems with power/authority and think they have been treated unfairly. Wikileaks, which describes itself as a "non-profit media organization[61]", is a well-known

---

[55] Baldi, Gelbstein, and Kurbalija. *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace*, 2003.

[56] Gareeva, A., Kira Krylova, and Olga Khovrina. 'Hacktivism: A New Form of Political Activism'. *School of Governance and Politics*, 2020.

[57] Conway, Maura. 'Cyberterrorism: Hype and Reality', 2007.

[58] Alexopoulou and Pavli. '"Beneath This Mask There Is More Than Flesh, Beneath This Mask There Is an idea": Anonymous as the (Super)Heroes of the Internet?'. 2021

[59] Sorell, Tom. 'Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous'. *Journal of Human Rights Practice* 7, no. 3 (November 2015): 391–410. https://doi.org/10.1093/jhuman/huv012.

[60] George and Leidner. From clicktivism to hacktivism: Understanding digital activism. 2019

[61] 'WikiLeaks - About', n.d. https://www.wikileaks.org/About.html.

example of this. Wikileaks and Anonymous, two of the most widely heard online activist groups, while they are examples from different spectrums of hacktivism for some sources, there are also actions in which these organizations cooperate.[62]

COMPARISON

In this section, the so-called 'thin' line between cyberterrorism and hacktivism will be examined in detail while points of intersection will also be mentioned. These two fields, which are similar in terms of propaganda, recruitment, fundraising, and the tools and techniques used, differ from each other, especially in terms of publicizing and announcing the aims of the actions to the public, due to the efforts of cyberterrorists to keep their objectives less clear to public.[63] For hacktivists who aim to raise public awareness and draw attention to an issue, it is very important that their organizational identity and aims are fully understood. If we try to explain cyberterrorism through hacktivism, it can be mentioned that there are three different categories of hacktivists, depending on how they approach their activities in cyberspace: whether they (1) merely use cyberspace, (2) misuse, or even (3) abuse (or offensively use) it, which possibly strays into the realm of cyber-terrorism.[64] The abusiveness can depend on the level of disruption that the groups desire and realize. As seen in definitions, expressions such as "without serious damage" are frequently used while identifying hacktivism.[65] In contrast, for cyberterrorism aiming harm is one of the main characteristics.[66]

If we summarize most mentioned types of the attacks within the scope and methods of politically motivated cyberattacks under several categories: (1) unauthorized access, which the main goal of is to gain access to a network to obtain information or to gain an advantage over the other party, (2) destruction which the main purpose is to destroy or damage computer systems, (3) Denial of Service which aims to lock down online computer systems, (4) defacing websites which aims to disrupt or deface websites to falsify the information on the website and make it suitable for the propaganda or awareness. From a methodological perspective, both hacktivists and cyberterrorists may use these similar tools that are aforementioned. If we take the example of accessing information through cyber-attack and system intrusion, different

[62] *Ibid.*
[63] Baldi, Gelbstein, and Kurbalija. *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace*, 2003.
[64] *Ibid.*
[65] See pg. 13
[66] See pg. 6

actors may differ in what is done with this information afterwards. The goal to use this information informs the next step. For a cyberterrorist, this may be to use the information to create politically or financially strategical leverage (e.g., blackmail or fund extortion)[67], while for a hacktivist it may be to inform the public by disseminating the information (e.g., leak). Although all of these actions are likely to be criminalized in terms of the illegality of the methodology, the actions may carry positive or negative deviance in terms of public or institutional perception.

While explaining the differences between hacktivism and cyberterrorism, it is necessary to consider both motivation and results of actions. Hacktivists are differentiated from cyberterrorists in that they are more concerned with the welfare of society or do not set out to harm. If their actions reach a level that destroys, seriously harms people, and creates an atmosphere of fear in society, these actions will shift to the field of cyberterrorism. The distinction can be explained as:

> "Cyberterrorism, which might include phenomena like hacking into air traffic control systems in order to crash airplanes, is still a hypothetical phenomenon. It is separated from hacktivism by its willingness to cross over into violence against actual human beings, or substantial damage to physical property."[68]

When they are compared in terms of their organizational structure, the structure of activist organizations can be described as (1) segmented, which represents informality and fluidity of the organization, (2) polycentric, which highlights the absence of one leader or center (3) integrated, which represents the ease to find ideological coherence and (4) networks, which are non-hierarchical, non-limited.[69] In contrast to this relatively loosely organized structure, it can be said that terrorist groups have a stricter hierarchy and centrality and show differences in terms of admission (e.g., entry or exit) to the organizations. Many methods such as sit-ins and DDoS, which require mass participation in order to be effective, are identified with hacktivism, not terrorism. So much so that hacktivist groups EDT and Electrohippies "view their operations as acts of civil disobedience, analogous to street protests and physical sit-ins, not as acts of

[67] Veerasamy, N. 'A High-Level Conceptual Framework of Cyber-Terrorism'. *Journal of Information Warfare* 8, no. 1 (2009): 43–55.
[68] Samuel. 'Hacktivism and the Future of Political Participation' 2004
[69] Gerlach, L. P. 'The Structure of Social Movement: Environmental Activism and Its Opponents', 2001.

violence or terrorism".[70] Therefore, cooperation is easier and stronger for hacktivists than for terrorists, both because of the nature of activism and because of the less hierarchical or more loosely organized schemes mentioned above.

Since the hacking culture originally rooted on the idea of "innovative use of technology to solve a problem"[71], it can be concluded that hacktivist groups are much more open to innovation than cyberterrorists. On the other hand, new methods may seem too risky for cyberterrorists because of their more result-oriented nature since an action without sufficient damage will not bring the desired sound, and therefore how sophisticated the attack is relatively less important.[72] For terrorists, the magnitude of the damage they inflict is more important than the sophistication of the method used since as it increases the attention they attract and the pressure or fear they create on society. It is not surprising that they continue to use old methods rather than risk failing. Terrorist acts, where it is most effective to make noise through subversion, cyber-terrorism methods do not seem to be the most optimal way from a cost and benefit perspective, as they are costly and do not cause enough damage[73]. While a conventional bomb is still more damaging than a cyberattack, the risk of cyberterrorism will continue to exist in our lives with our dependence on technology and the rise of internet of things devices, therefore, it may be possible that we may see the days where perpetrators can conduct online operations that enable "physically harming someone as easy as penetrating a Web site is today"[74].

As to how they are perceived, in a study, which examines the view of the member states of OSCE (Organization for Security and Co-operation in Europe), the world's largest regional security organization with the participation of 56 countries, on the concepts of hacktivism and cyberterrorism[75], such conclusion has been reached that:

> "Hacktivists and cyberterrorists share many tools and methods, but the main differences between these phenomena are intended use of violent methods and level of concern for the welfare of the other users. However, academia, governments and mass media often place hacktivism and cyberterrorism in the same category. OSCE states have responded to hacktivism

[70] Denning, 'Statement of Dr. Denning', 2000
[71] Hampson, 'Hacktivism: A New Breed of Protest in a Networked World'. 2012
[72] Denning, 'Statement of Dr. Denning', 2000
[73] Giacomello, Giampiero. 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism'. *Studies in Conflict & Terrorism* 27, no. 5 (September 2004): 387–408. https://doi.org/10.1080/10576100490483660.
[74] *Ibid.*
[75] Laitala, 'Hacktivism and Cyberterrorism: Human Rights Issues in State Responses', 2012

> and cyberterrorism with domestic legislation and institutions, international conventions, technical measures, and specialized institutions."

The definition of terrorism in line with the ideologies, policies and interests of countries gives rise to this debate. "Combination of ambiguity about what terrorism is and is not, combined with the power of such a pejorative label, created opportunities for the social construction of terrorism to serve very specific interests."[76] To discuss the issue with a few case studies, Operation Titstorm can be given an example, which was realized with Anonymous attack on Australian government websites and e-mail addresses as a result of Kevin Rudd government's decision to ban some pornographic content on arbitrary grounds. When the case is analyzed in terms of Australian anti-terrorism laws, the law should include "low harm" actions to exclude Operation Titstorm or a similar action from the political protest exemption and for it to be considered a terrorist act, since such actions only caused low economic damage, not injury or death of any person.[77] Although in this example such an inference is drawn from Australian anti-terrorism laws, in fact the statement "insufficient safeguards in the current legislation to maintain a distinction between acts of 'hacktivism' and 'cyber-terrorism'"[78] applies to other countries as well. Due to attacks with high media coverage such as DDoS and the fear of countries and organizations of cyber threats, hacktivism can easily be labeled as terrorism even if it does not meet any of the conditions.[79] Another example is the case of Turkish leftist hacktivist group Redhack, which was particularly active between 2012 and 2017, differs from other hacktivist groups in Turkey by its non-patriotic nature.[80] One of the most high-profile and legally troublesome actions of the group was the attack on official websites and sharing sensational information with public by hacking different websites and mail addresses belonging to the state. During the trial process, their cases started to be tried for terrorism, not cybercrime with judges changing their minds which can be explained by the fact that the judiciary and security bodies in Turkey consider any individual or organization that attacks or opposes the state as terrorist.[81] Redhack, which has been described as a "terrorist organization" by

---

[76] Shirley, Wesley D. 'When Activism Is Terrorism: Special Interest Politics and State Repression of The Animal Rights Movement'. University of Oregon, 2012.
[77] Hardy, Keiran. 'Operation Titstorm: Hacktivism or Cyberterrorism?' *UNSW Law Journal* 33, no. 2 (2010): 474.
[78] *Ibid.*
[79] Laitala, 'Hacktivism and Cyberterrorism: Human Rights Issues in State Responses', 2012
[80] Doğan, Bülay. 'Contextualizing Hacktivism: The Criminalization of Redhack'. *Center for Advanced Research in Global Communication (CARGC)*, 2019.
[81] *Ibid.*

mainstream media in Turkey, responded on their social media accounts with "Only in one month police put 65 people into coma, injured 10,000, left 12 eyeless and killed 5. They called us terrorists" comment by referring to information from the security forces they hacked.[82]

CONCLUSION

Developments change human behavior, changing human behaviors create new needs, new developments arise from emerging needs, and the loop continues. The facts that human beings can benefit from the information flow of the internet, can easily reach information around the world, and accordingly can be affected by everything that happens without being limited to their neighbors, has made them world citizens. The acceleration of globalization with these developments have changed the perspective of all individuals towards the world and to both international and local events. The world got smaller so much that political and societal issues from a particular region have become everyone's problem with the changes of regionalization concept. If we were not at a point where globalization is at its peak point, it would not have attracted the attention of anyone outside of the region where injustices suffered in one corner of the world, and perhaps no one would even know about others. In addition to the positive results and opportunities of sharing our values and problems with larger masses, such as distances being close and the voice of social issues being heard in the international community, there are also areas that can be exploited by users, organizations, and officials.

Actors behind the politically motivated hacking can be identified as nation states, terrorists, or other socio-political groups. However, in some cases the distinction between these actors has been blurred, which makes problematic to distinguish between them. Even if similar methods are used by both hacktivists and cyberterrorists, differences in factors such as motivation, level of damage intended to be inflicted, structure of the groups, ethical considerations are helpful in differentiating the actions and the actors. For hacktivists, it is preferable to draw attention to a problem with actions taken on digital platforms. Activities are generally not destructive in nature, e.g., instead of destroying a system, hackers aim to temporarily render it inaccessible or malfunctions. This is one of the main points where it differs from cyberterrorism. On the other hand, cyberterrorism acts aim to be damaging, subversive, destructive and corrosive to the

[82] Bianet - Bagimsiz Iletisim Agi. 'RedHack Identified as "Cyber Terrorist Organization"', n.d. https://www.bianet.org/english/other/148225-redhack-identified-as-cyber-terrorist-organization.

system. But it should not be forgotten that there is always the possibility of hacktivism turning into cyberterrorism depending on both the point of view and the degree of damage. Therefore, activist groups need to consider the consequences of their actions well and draw the line precisely.

The fact that the definition of terrorism varies according to different people and countries is an important problem encountered when trying to distinguish between different activities in the cyber world and the consequences of these actions. Terrorism is used as a tool for the fulfillment of political goals in the international political arena and conventional methods of terrorism are still heavily used to achieve these goals. Nevertheless, to combat the threat of cyberterrorism and to take precautions, states and international actors need to take initiatives so that this is not left to the arbitrary discretion of countries. Although theoretical discussions are useful in understanding the issue, it is likely that the states will continue to label actions according to their ideology, interests and policies. Therefore, activist groups will continue to be stigmatized as terrorists. In fact, since the differences between hacktivism and cyberterrorism have so far not been possible to differentiate on the international legal perspective, some argue that cyberterrorism is an exaggerated issue that states exploit in order to regulate internet and control activist easier. In this context, fair trials, detailed academic and legal studies, and the role of independent media have an important role to play in creating an impartial public perception, as such concepts of crime are socially constructed.

REFERENCES

Adams, Joshua. 'Decriminalizing Hacktivism: Finding Space for Free Speech Protests on the Internet'. *SSRN Electronic Journal*, 2013. https://doi.org/10.2139/ssrn.2392945.

Alexopoulou, Sofia, and Antonia Pavli. '"Beneath This Mask There Is More Than Flesh, Beneath This Mask There Is an Idea": Anonymous as the (Super)Heroes of the Internet?' *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique* 34, no. 1 (February 2021): 237–64. https://doi.org/10.1007/s11196-019-09615-6.

Baldi, Stefano, Eduardo Gelbstein, and Jovan Kurbalija. *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace*. Msida, Malta: DiploFoundation, 2003.

Bianet - Bagimsiz Iletisim Agi. 'RedHack Identified as "Cyber Terrorist Organization"', n.d. https://www.bianet.org/english/other/148225-redhack-identified-as-cyber-terrorist-organization.

Brunst, Phillip W. "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet". *A War on Terror?* Marianne Wade ve Almir Maljevic, Springer New York, 2010, ss. 51-78. *DOI.org (Crossref)*, https://doi.org/10.1007/978-0-387-89291-7_3.

Busch, Otto von, and Karl Palmås. *Abstract Hacktivism: The Making of a Hacker Culture*. London: OpenMute, 2006.

Cammaerts, Bart. 'Social Media and Activism'. In *The International Encyclopedia of Digital Communication and Society*, edited by Robin Mansell and Peng Hwa Ang. The Wiley Blackwell - ICA International Encyclopedia of Communication. Chichester, West Sussex, UK: Wiley Blackwell/John Wiley and Sons, Ltd, 2015.

Ching, Jacqueline. *Cyberterrorism*. 1st ed. Doomsday Scenarios: Separating Fact from Fiction. New York, NY: Rosen Central, 2010.

Denning, Dorothy E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", Global Problem-Solving Information Technology and Tools https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Denning, Dorothy E. 'Statement of Dr. Denning'. The Federation of American Scientists, n.d. https://irp.fas.org/congress/2000_hr/00-05-23denning.htm.

Denning, Dorothy E. "The Rise of Hacktivism". *Georgetown Journal of International Affairs*, September 2015, https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism.

Dijk, Jan van. *The Network Society: Social Aspects of New Media*. 2nd ed. Thousand Oaks, CA: Sage Publications, 2006.

Doğan, Bülay. 'Contextualizing Hacktivism: The Criminalization of Redhack'. *Center for Advanced Research in Global Communication (CARGC)*, 2019.

Europarat, ed. *Cyberterrorism - the Use of the Internet for Terrorist Purposes*. Strasbourg: Council of Europe Publishing, 2007.

Gareeva, A., Kira Krylova, and Olga Khovrina. 'Hacktivism: A New Form of Political Activism'. *School of Governance and Politics*, 2020.

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), 100249. https://doi.org/10.1016/j.infoandorg.2019.04.001

Gerlach, L. P. 'The Structure of Social Movement: Environmental Activism and Its Opponents ', 2001.

Giacomello, Giampiero. 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism'. *Studies in Conflict & Terrorism* 27, no. 5 (September 2004): 387–408. https://doi.org/10.1080/10576100490483660.

Giacomello, Giampiero. "Close to the Edge: Cyberterrorism Today". *Contributions to Conflict Management, Peace Economics and Development*, c. 22, Emerald Group Publishing, 2014, ss. 217-36. *DOI.org (Crossref)*, https://doi.org/10.1108/S1572-8323(2014)0000022015.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*. Published. https://doi.org/10.1093/cybsec/tyw018

Hampson, Noah C. N. 'Hacktivism: A New Breed of Protest in a Networked World'. *Boston College International & Comparative Law Review* 35 (2012): 511.

Hauben, Michael. 'Chapter 1: The Net and Netizens: The Impact the Net Has on People's Lives'. In *Netizens: An Anthology*, 1995.

Hardy, Keiran. 'Operation Titstorm: Hacktivism or Cyberterrorism?' *UNSW Law Journal* 33, no. 2 (2010): 474.

Jarvis, Lee, and Stuart Macdonald. "What Is Cyberterrorism? Findings From a Survey of Researchers". *Terrorism and Political Violence*, c. 27, August 2015, pg. 657-78. *DOI.org (Crossref)*, https://doi.org/10.1080/09546553.2013.847827.

Jordan, Tim, and Paul A. Taylor. *Hacktivism and Cyberwars: Rebels with a Cause?* 1. publ. London: Routledge, 2004.

Lai, R. (2012). Analytic of China Cyberattack. *The International Journal of Multimedia & Its Applications*, *4*(3), 37–56. https://doi.org/10.5121/ijma.2012.4304

Laitala, Nuutti. ‘Hacktivism and Cyberterrorism: Human Rights Issues in State Responses’, 2012. https://doi.org/20.500.11825/740.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22–31. https://doi.org/10.1145/1629607.1629613

Madubuike-Ekwe, Joseph N. ‘Cyberattack and the Use of Force in International Law’. *Beijing Law Review* 12, no. 02 (2021): 631–49. https://doi.org/10.4236/blr.2021.122034.

Manion, Mark, and Abby Goodrum. ‘Terrorism or Civil Disobedience: Toward a Hacktivist Ethic’. *ACM SIGCAS Computers and Society* 30, no. 2 (June 2000): 14–19. https://doi.org/10.1145/572230.572232.

Marchuk, Iryna. *The Fundamental Concept of Crime in International Criminal Law*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. https://doi.org/10.1007/978-3-642-28246-1.

Megiddo, Tamar. ‘Online Activism, Digital Domination, and the Rule of Trolls’. *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3459983.

NATO. “NATO’s Military Concept for Defence against Terrorism”. *NATO*, http://www.nato.int/cps/en/natohq/topics_69482.htm.

Negri, Claudia. *Organic bodies versus digital bodies: the differences between hacktivism and cyberterrorism*. 2018.

OECD. ‘Definition of Terrorism by Country in OECD Countries’, OECD International Platform on Terrorism Risk Insurance, n.d.

Ottis, R., and P. Lorents. ‘Cyberspace: Definition and Implications. ’. In *5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April*, n.d.

Petta, De Leon. “Why there is no real difference between a Terrorist Organization and an Organized Crime faction, just a matter of interaction towards the State”. *Contemporary Voices: St Andrews Journal of International Relations*, c. 1, sy 1, Mayıs 2018, s. 26. *DOI.org (Crossref)*, https://doi.org/10.15664/jtr.1472.

Samuel, Alexandra Whitney. ‘Hacktivism and the Future of Political Participation’. Harvard University Cambridge, Massachusetts, 2004. https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

Security Council Urges Greater Collective Effort to Prevent Terrorists from Acquiring Weapons, Unanimously Adopting Resolution 2370 (2017) | UN Press. https://press.un.org/en/2017/sc12938.doc.htm.

Sorell, Tom. 'Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous'. *Journal of Human Rights Practice* 7, no. 3 (November 2015): 391–410. https://doi.org/10.1093/jhuman/huv012.

'Terrorism Act 2000'. Accessed 2 July 2022 https://www.legislation.gov.uk/ukpga/2000/11/enacted.

United Nations, *A/RES/49/60. Measures to eliminate international terrorism*, United Nations General Assembly https://web.archive.org/web/20190616073441/https://www.un.org/documents/ga/res/49/a49r060.htm.

UNOCT (United Nations Office of Counter-Terrorism - UN Counter-Terrorism Centre), et al. *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counterterrorism*. 2018.

Veerasamy, N. 'A High-Level Conceptual Framework of Cyber-Terrorism'. *Journal of Information Warfare* 8, no. 1 (2009): 43–55.

Weimann, Gabriel. *Cyberterrorism - How Real Is the Threat?* United States Institute of Peace, Dec. 2004.

WikiLeaks - About', n.d. https://www.wikileaks.org/About.html.

Zeidan, Sami. "Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism". *Cornell International Law Journal*, July 2003, pg. 491-96.