2022

4(2), 171-196

Siber Tehdit Taksonomilere Siber Aktivizm Çerçevesinde Bir Değerlendirme

Deniz Gönç*[1]

Anahtar Sözcükler

Yeni medya
Dijital kamuoyu
DDoS saldırısı
Siber tehdit taksonomisi
Dijital aktivizm

Makale Hakkında

Gönderim Tarihi
2 Mayıs 2022
Kabul Tarihi
10 Ekim 2022
Yayın Tarihi
28 Aralık 2022
Makale Türü
Araştırma Makalesi

Öz

Çevrimiçi olarak sunulan milyarlarca yeni medya platformu insanlara kendilerini temsil etme ve benzer düşünen insanlarla tanışma olanak sağlar, böylelikle siber uzayda da insan temelli, canlı ve dinamik bir kamuoyu oluşur. Siber uzayda da demokrasiyi mümkün kılmak için, tüm toplumsal gruplar -tüm çatışmaları ile hür ve adil olarak temsil edilmelidir. Devletler ve egemen kullanıcıların siber alana da sirayet eden güç mücadeleleri demokratik bir siber kamuoyunun varlığını gölgelemektedir. Yeni medya ve siber aktivizm çerçevesinde ele alınan bu çalışmada, siber aktivizmin marjinal ve saldırgan bir türü olan hacktivizm motivasyonu siber alanda varlığını ve gücünü kanıtlama mücadelesi olarak ele alınmıştır. DDOS (Dağıtık Hizmet Reddi Saldırıları) saldırıları, siber uzayda iktidar ve kamu yönetimi mücadelesinin temsilcisi olan korsanlar tarafından en çok tercih edilen saldırı türlerinden biridir. Çalışmanın amacı, siber aktivizmi diğer siber suçlardan ayırt edecek kriterlerin belirlenmesine yardımcı olmaktır. Literatürde DDOS taksonomilerinde kullanılan kriterler sunulmuştur. Siber aktivizmi diğer siber suçlardan ayırt edebilmek için Türkiye'de kamuoyunu etkileyen siber saldırılar incelenmiştir ve hackerların mesajlarını içeren bir tablo ile bulgular sunulmuştur. Sonuçta hacktivism motivasyonları görünür kılınarak, belirleyici ölçütlerin DDOS taksonomilerine dahil edilmesi önerilmiştir.

An Evaluation of Cyber Threat Taxonomies in the Framework of Cyber Activism

Keywords

New media
Digital public sphere
DDOS attacks
Cyber threat taxonomies
Digital Activism

Article Info

Received
May 2, 2022
Accepted
October 10, 2022
Published
December 28, 2022
Article Type
Research Paper

Abstract

Billions of new media platforms available online allow people to represent themselves and meet like-minded people, creating a human-based, vibrant and dynamic public opinion in cyberspace. o enable democracy in cyberspace, to, all social groups - with all their conflicts - must be free egalitarian representing. The power struggles of states and sovereign users, which also spread to the cyber space, overshadow the existence of a democratic cyber public opinion. In this study, which is handled within the framework of new media and cyber activism, hacktivism motivation, which is a marginal and aggressive type of cyber activism, is discussed as a struggle to prove its existence and power in the cyber field. DDOS (Distributed Denial of Service) attacks are one of the most preferred attack types by hackers, who are the representatives of the struggle for power and public administration in cyberspace. The study aims to help determine the criteria to distinguish cyber activism from other cybercrimes. The criteria used in DDOS taxonomies are presented in the literature. To distinguish cyber activism from other cybercrimes, cyber attacks affecting the public in Turkey were examined and a table containing the messages of hackers and findings was presented. As the result, it has been proposed to include the determining criteria in DDOS taxonomies by making hacktivism motivations visible.

***Atıf*:** Gönç, D. (2022). Siber tehdit taksonomilere siber aktivizm çerçevesinde bir değerlendirme, *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(2), 171-196. https://doi.org/10.53694/bited.1112219

***Cite*:** Gönç, D. (2022). An evaluation of cyber threat taxonomies in the framework of cyber activism, *Journal of Information and Communication Technologies*, *4*(2), 171-196. https://doi.org/10.53694/bited.1112219

*__Sorumlu Yazar/Corresponding Author__: Deniz Gönç
[1] Yeditepe University, Media Studies, Turkey denizgonc@gmail.com, https://orcid.org/0000-0002-8338-6476

Giriş

Communication technologies that paved the way for globalization have enabled the information society revolution. Today internet has reached a unique structure that includes other networks and digital media like Machine-to-machine (M2M) and Internet of Things (IoT) technologies that covered other networks and digital media and reached a network structure whose boundaries have been unknown (Crowley & Heyer, 2010). In this way, big liquid data is feeding at any moment and provides creative opportunities and solutions in the fields of health, finance, security, logistics, commerce, and even education (Faritha, Revathi, Suganya, & Gladiss, 2020; Sun, Yan, Lu, Bie, & Thomas, 2012). New ways of reaching, creating and analysing information have created a heterogeneous and interactive mass communication model based on its digital-based and multi-format structure. The internet, as the new multi-media, unlike television, which has trapped people on screens, opens its forums and puts the agora on the mobile phone, where virtual communities meet (Genel, 2015). The powerful feedback system of new media allows users to share and discuss their opinions on political issues. This "participant-friendly" model also allows users to increase their online sharing about the world agenda. The new media also creates an environment in which users can share their feedback and opinions. Wide-based widespread use of the internet has brought security problems. It gives a dominant and decisive position to institutions and individuals who are committed to providing this security. Considering the new media as cyberspace, including also the public sphere, to see the struggle for sovereignty is natural (Müller & Kramer, 2014). The conquest of nation-states in cyberspace is continuing. Cyberspace is not a hobby, but a public struggle for existence with an international diplomatic dimension.

In terms of cybersecurity as a defense of cyberspace, there should be ethical principles between the democratic use of the public sphere and motivations of informatics crimes, as well as technical criteria. In this study, a literature review was conducted in terms of the determining criteria of taxonomies used in cyber security studies. The criteria found seem to ignore the democratic necessity of cyber activist actions, namely the nuance between cyber activism and cybercrime. The news of DDoS (distributed denial of service attacks) actions in Turkey was examined and subjected to content analysis. The purpose of the analysis, which examines the messages of cyber attackers, is to make visible the unique characteristics of DDoS attacks in terms of their motivation. As a result of the analysis, new parameters that are not included in the cyber crimea and threat taxonomies are proposed.

New Media

New media is an asynchronous form of media that gives the audience enable, to interact with all online things, that are computational and rely on computers for redistribution. The nature of new media, including traditional media, is purely digital and fluid, growing exponentially geometrically. The production process requires computer and internet technologies from the beginning to the end. Manovich (2002) describes the new media's four characteristics as (i)Digitalism is the conversion of all data into numerical codes. (ii) Automation is the ability of digital software to perform some operations on its own; (iii) Modularity defines the working of parts independently; (iv)Transcoding is the convertibility of content into different formats.

The five basic features of new media are communication, cooperation, community, providing creative thinking and convergence (Friedman & Friedman, 2008). Social media according to four main areas: modernity of communication; productive audiences; dialogic and network structure; and its searchable and tagged nature (Averweg, 2018). Because of their low cost and asynchronous nature, internet forums provide partial communication to unlimited recipients, occupy a global area, accelerate communication and are hypertext (Demircan, 2006). Digital games have hypnotic, imaginary, skinned, interactive, simulated, and cybernetic media culture (Giddens & Kennedy, 2006). Wearable environments are defined by movement, transparency, nanotechnology, brain-machine interfaces, augmented memory, portable technology parameters and participatory culture (Pedersen, 2013). Since new media has an intertextual and modular structure, these conditions can be generalized to all media within the scope of new media. Despite the lack of equal access to resources, cyberspace often provides freedom of expression and access to information. It offers users the opportunity to share their feelings and thoughts, and organize and act jointly.

The new media discussions gave theoretical hope that the internet, which facilitates access to information, can erode the inequality gap that is deepening day by day in the economic and social fields. The integrative effect of the new media and the phenomena of widespread use of social media in environments of conflict and unrest creates a digital public opinion. Especially for using social networks suitable for social movements and the dissemination of activist practices in the presence of political conflicts (Castells, 2008; Zizek, 2013).

Against these positive features, new media distribute the unvoiced information that is manipulated and make internet content unreliable systematically and purposively (Davenport & Prusak, 2001, s. 27). Exactly the political economy of the new media should always be taken into account. Although access to information is not theoretically restricted, transfer and sharing are limited. Internet access can be provided limitedly to the poor, disabled, women, elderly, and children against economic, geographical, gender and age-based inequalities and in internet access.

Digital Public Sphere

The public space is a unifying space where valour and virtue are displayed, where people come together, listen to each other and take action. The public sphere, which is the basis of the political community, is the space in which the individual constructs himself. It is the place where public problems become visible and perceptible, citizens access political information as legislators, and politics become legitimate (Arendt et al., 1997; Habermas, 2002; Onat, 2013; Sennett, 2010). According to Habermas, the public sphere is the living space where people reason and form ideas around a common subject. According to Fresier (1990), the public sphere is the ensemble of informally mobilized non-governmental discursive ideas that stabilize the state. The existence of public islets and public spaces composed of people and groups with similar aims accelerates the expansion of the discursive space. According to Ackerman's liberal dialogue model, the public sphere and the state sphere are identical, and the place of the citizen is in the private sphere. Sennet states that today the public sphere has become formalized, and the focus of the citizen, which has gained a submissive character, shifts to private matters and he states that the public sphere has collapsed. Güven and Satır (2018) cite change.org as an example, as a public space where claims for different sensitivities are expressed from a wide variety of locations. The digital public sphere is a cyberspace of discourse and action that encompasses and unites the public sphere, private and political spheres, and even individuals and institutions.

For understanding the digital public sphere and its functioning, it is required to know about the fact that the friendly appearance of cyber ideology and the network organization behind the internet mask the economic superpowers (Başaran, 2000; Schafer, 2015). As in the real world, the existence of the exploitation and oppression of the limited group that divides the power requires us to see the new media as a field of activism and struggle (Gazeteciler Cemiyeti, 2019). While individuals live parallel existences in the real world in cyberspace, it provides a very rapid social formation and consumption of the virtual public. Cyberspace is polluting like the real world.

In the digital public sphere as in the real world, we should see the existence of the exploitation and oppression of the limited group that divides the power, and the new media as a field of activism and struggle (Sausa, Pinto& Silva, 2015). While individuals experience parallel existence with the real world in cyberspace, it provides very rapid social formation and consumption of the virtual public. Unfortunately, new media, which enables the public space to be produced and consumed more, will not fill the information gaps of the media (Golman & Loewenstein, 2015; Trappel, 2019). Limited and unequal access to the Internet ensures the reproduction of economic inequalities (Giddens, 2012, p.445). According to Noris (2001) due to the digital gap between developed and undeveloped countries, the internet causes the gap between the knowledge levels of its people to continue.

Digital Democracy and New Social Movements

Democracy is based on a problematic pillar and civic participation, also a historical concept that is subject to the contingencies of the social interaction that shape it and challenge it (Sousa, Pinto & Silva, 2013). The reality and existence of democracy is a matter of deep debate, but cyber-public opinion provides the basic conditions of cyber democracy (Yengin, 2017). Thus, the eight criteria of democracy defined by Dahl (2001, p. 40); Freedom of expression, implementation of election results, electoral justice, equal voting rights, right to be elected, freedom to use alternative news sources, freedom of association and participation are theoretically possible in this cyber world. In terms of its contribution to democracy with its web 3.0 semantic feature, new media created opportunities for access to alternative information sources, founding organizations, participation, and freedom of expression. The globalization of actions can eliminate the knowledge monopoly of experts (Beck, 1997; Maigret, 2014, p., 346). In terms of the permeability and limitlessness of public, private and political spaces, we can talk about the existence of democracy in the digital public sphere in a theoretical framework. The interactive structure of the internet enhances the culture of participation and provides the opportunity to create cyber-public opinion. Thanks to the simultaneity, source verification possibilities and data sharing features of new media technologies, people can establish political, cultural, religious or commercial organizations regardless of location (Castells, 2008; Enjolras, Bernard, & Johnsen, 2017). In this respect, new media can be considered a public space due to the effect of bringing social groups together and creating identity (Timisi, 2003).

The characteristics of new social movements seen in the public sphere are also manifested in the digital public sphere. The class and economy-oriented labour struggle has been replaced by new social movements, which focus on political and social conflicts. Social media, which is a new field of existence for freedom of expression and personality performances, has an integrative effect on all users thanks to its fast, unfiltered, inclusive and partially democratic operation.

The integrating effect of the new media in individual and social unrest and conflict creates a virtual public opinion, and sometimes even replaces the real public opinion under pressure. In the presence of political conflicts, especially the use of social networks can turn into social actions, thus enabling social movements and

disseminating activist practices (Castells, 2008; Zizek, 2013). For example, social media allows people to coordinate their actions in the form of mass mobilization or protest both online and in the real world. Arab Spring, Occupy Wall Street, Travel, etc. We have seen a wide variety of uses of new media platforms in social network-based social movements (Bayhan, 2014; Zizek, 2013). The cyber public sphere represents the real system of physical life where violence and bullying have become the reality of new media in the cyber world, as well as the the democratic opportunities offered by the new media for democracy and civil rights. (Langos, 2012; Ang & Goh, 2010).

Digital Activism

Social movements making progress towards their goals often rely on some form of activism to promote change. Social activism is part of the broader field of social movements that take action to create social change. Digital activism is digitally mediated social activism (Bennett & Segerberg, 2013; Selander & Jarvenpaa, 2016). Activism in the traditional sense requires donations of money and time, and the struggle is not easy to spread. On the other hand, digital resources provide a strong social impact. Success factors in digital activism are digital skills, internet access, digital technologies and large social networks. Electronic civil disobedience is the most militant form of political resistance in the digital humanities and has become popular in recent years (Losh, 2012 p. 166). The use of digital information and communication technology encourages people's participation in activist efforts. Examples of civil disobedience that can be shown on these issues can be further diversified, such as hacking, worms and viruses, virtual sit-ins, fake websites, e-mail shelling, and online signature campaigns. The interactive structure of the internet enhances the culture of participation and provides the opportunity to create cyber-public opinions. The main topics of cyberactivism -parallelly to new social movements can be classified as women's movement, anti-war and peace movement, the environmental movement, farmers' movement, nuclear energy, the movement against low-wage workers, labor movement, and AIDS movement (Kalafatoğlu, 2010). There are many popular digital activism practices on the internet, such as selected internet content consumption, data creation and publishing, original content design and sharing, open-source software development, support, and organization for non-governmental organizations.

George and Leidner (2018, 2019) listed digital activism actions as clicking, meta-voicing, assertion, political consumerism, digital petitions, botivism, e-financing, data activism, disclosure, and hacktivism. Then they analysed the functions, mechanisms, and effects of digital activism actions according to the digital activism hierarchy.

1. Digital Spectator Activities are related concepts with the spectator tier of social media. Clicktivism is being an advocate, individually and remotely. Metavoicing is sharing social media posts and duplicating and recreating. The assertion is creating original digital materials and participation in e-government e-participation.

2. Digital Transitional Activities are exemplified by political consumerism, digital petitions, botivism, and e-funding. Political consumerism is to support a business financially that agrees with their views while boycotting (buycotting) firms that promote dissenting views. Digital petitions mandate a guaranteed response if a minimum number of signatures is met. Botivism refers to the virtual activist who plays the automated digital action like trolls. E-financing is using technology to generate income for a cause in the process of providing funds for business activities, making purchases, or investing.

3. Digital Gladiatorial Activities are not to do the participants do seek to influence change; they to make the change. Data activism uses the activities in open government data, data rescue, civic data hacking and data philanthropy to gain greater individual power over data held by others. Exposure is sharing of knowledge without permission as a leak. According to Coleman (2011, p.138) Hacking is an aggressive attack type of cyber activism through computer codes that exposes information, destroy data, or disrupt operations of individuals by hackers who target governments, and organizations.

Coleman (2011) matches the mechanisms and functions of cyber activism actions as identification: affirming and legitimizing; construction: creating, donating, designing, protecting; aggression: destroying, disrupting, appropriating, attacking, coercing; deception: deceiving, concealing; visibilitation: commending, denouncing, exposing; amplification: reinforcing, repeating, communicating, educating. Hacktivism techniques are listed by O'Malley (2013) as distributed-denial-of-service (ddos) virtual sit-in, website defacement, site redirects, cyber sabotage and information theft. Hacktivism is a type of online activism and is not necessarily cybercrime (Sabillon, Cano, Cavaller, & Ruiz, 2016a).

Hacktivism

The story of hackers includes the history of the devotion of youth, computer programs, authority and genius scientists, hippies, yuppies, liberals, anarchists, and classical socialists in the 60s, 70s, 80s, and 90s (Walleij, 2003). According to the analysis of Eriş (2009) this is a story that turns into a subculture from a mixture of ideologies. Hacker culture based on sharing, helpful, forgiving, reactive, and solidarity generally (Keleş, 2013) Hacker ethic works well intentioned cyber-attack actions are carried out with principles such as ethics, challenge and a field of struggle independent of the state's power apparatus, justice, creating original content and facilitating access to information, or the representation of public power in the cyberspace in political actions against the state and/or power. Ethic hackers defined as white hat, facilitate access to information by developing free software by sharing their knowledge and expertise. Contrastly black hackers self-set unauthorized access to computer systems and disrupt internet transactions attacks.

Hacker ethics was based on to explorer cyber world before '80s. However, in the changing information world, the authoritarian attitude of the state and the fact that many acts of hackers are considered crimes due to commercialization have also led to the transformation of hacker ethics. Since the beginning of the 2000s, Anonymous Turkey, RedHacker, Türk Hack Team, Ayyıldız Tim, Beyaz Hacker, Akıncılar, Turkish Security, Cold Hackers, Mesopotomia Hackers, Pkk Hack Team, belonging to different political frameworks, have been carrying out cyber attacks. These groups generally carry out internationally linked actions (Bıçakçı, Ergun, Çelikpala, p., 41). Hacktivists are categorized into three categories based on their ethic positions as civilian hackers, patriotic hackers, in a different term cyber militia and cyber terrorists (Dahan, 2013; Denning, 2000; Johnson & Robinson, 2014; Sauter, 2013). Civilian hackers organizing loosely groups that perform actions such as creating and updating digital systems for the good of society and legally (Hunsinger & Schrock, 2016; Schrock, 2016). Patriotic hackers has nationalist motivations and the state and/or power informally support their activities generally (Dahan, 2013; Green, 2016). Cyber terrorist is who act hacking and spreading viruses and malware, destroying websites, and performing denial of service (DOS) or botnet attacks among other activities for malicious trespass (Goode, 2015).

The crime-oriented approach working for understanding hacking activities associates the hacker phenomenon with the crime. On the other hand, the emancipatory approach determine within the framework of hacker ethics distinguishes hacking from the crime phenomena. It provides a way to broaden and deepen our understanding of the use and policies of tools and to question the uncritical instrumentality that many digital humanities projects assert (Losh, 2012, p.163).

Cyber Threats and DDoS attacks

Cyber-attack is intentional actions taking by people or information systems anywhere in cyberspace in order to destroy the confidentiality, integrity, or accessibility of information and industrial control systems in cyberspace or data processed by these systems (Turkey National Security Cyber Strategy Report). Kang et al. (2009) are listed digital threats of present-days as authorization violation, logic or time bombs, browsing, bypassing controls, data modifications, denial of service, eavesdropping, illegitimate use information leakage, intercept/ alter, interference database query analysis, masquerade, physical intrusion, replay, repudiation, resource exhaustion, sabotage, scavenging, spying, service spoofing, sniffers, substitution, terrorism, theft, traffic analysis, trap door/ back door, Trojan Horse, tunnelling, unauthorized access, violations of permission, unauthorized access, piggybacking, virus and worm.

The most common types of cyber attacks are denial of service (DoS) and distributed denial of service (DDoS) attacks and Man in the Middle attacks (Menlick, 2018). The DDoS attack relies on setting up a “zombie network” to cause the victim to overload web resources, rendering online resources inoperable. The attack targets a server or process on the victim system, making it unable to process legitimate requests for service. Unlike DDoS attacks, the cybercrime we have seen so far consists of the traditional crimes being committed with cyber tools. Theft, blackmail, harassment, trespassing, child abuse, encroaching the copyrights, as well as committing crimes such as murder are physical activities that can be carried into the cyber world. However, DDoS attacks do not correspond to any legal or illegal activity in the physical world. For this reason, it is a new type of performance, and the act may be defined as a crime specific to cyberspace only. International laws are not clear about DDoS attacks not also Council of Europe Convention on Cybercrime or Budapest Convention does not have a universal structure and evaluation of cyber crimes depend on local laws (Nikolskaia & Minbaleev, 2000). DDoS attacks considered the most effective attacks are actions that stand out by criteria such as procedural creativity, difficulty, and damage and impact. DDoS attacks, which became widespread with Mafiaboy, became the hacktivist tool of Annonymous' and SOCa in the 2000's. Cyber warfare is the nation-states use cyberspace to achieve their goals by using conventional military force.

According to Kelsey (2008) armies use cyber weapons for disabling civilian infrastructure serving as power plants, telecommunications, and transport infrastructure. Cyber warfare is the nation-states use cyberspace to achieve their goals by using conventional military force. In the context of national defense, reciprocal attacks that are macro in nature and between two or more countries have the potential to turn into wars between a number of sovereign states in the virtual arena (Indrajit et al., 2021). Cyber warfare is practised between states, whereas cyber terrorism is practised by non-state actors. Digital militarism different from cyber war is the use of digital technologies for war purposes and motivation differs from nationalist militarism attacks, commercial competition, or all cyber activism. The attacks have physical effects in the real world, and they are cyber attacks even, so their domain is

the real world. The purpose of cyberterrorism is to coerce or intimidate a government or its people to pursue political or social ends through illegal attacks and threats of attack on computers, networks, and stored information. Cyber terrorism's tactics are politically intended hacking operations (such as leaking and spying), unlawful attacks of intimidation, and controlling attack that ruins computerized systems for critical infrastructures tools. Terrorism in the real -world usually achieves its primary goal of demoralizing civilians by destroying property and injuring or killing civilians this distinguishes terrorism from warfare, which is not supposed to target civilians (Brenner, 2010, s., 387).

Cyber diplomacy is an important tool in furthering a nation's foreign policy as it enables direct interaction and engagement with the foreign public as a strategy for managing change through digital tools and virtual collaboration (Bjola & Holmes, 2015 p.89). It is the use of the Internet and ICT (information and communication technologies) to help implement diplomatic objectives or refers to harnessing the internet and modern communication technology to connect with an external audience in order to create an enabling environment for a country's foreign policy. Riordan (2016) made refers to cyber diplomacy as the use of diplomatic tools, and the diplomatic mindset, to resolve issues arising in cyberspace. Cyber diplomacy has five characteristics: Transparency, centralization and decentralization, disintegration and merger, possible accuracy and virtualization (Abdulsaliq, 2017; Ekşi & Taş, 2020). Serious attacks on critical infrastructures can be acts of cyberterrorism depending on their effects but for diagnosing as cyberterrorism, an attack must result in violence against persons or property (Denning, 2000). Specifying whether an attack is a terrorist or a war attack is a matter of diplomacy and law. Civil hackers may work for states informally as cyber militias, or information soldiers (Gürdal, 2021). If these hackers aim to provide the interests of the opposing state, cyber spies are declared traitors (Walden, 2005). It is a political choice whether to disclose information about the attacks carried out at the state level or not through diplomatic channels (Riordan, 2016; Shorter, 2014).

Cyber threat taxonomies

Cybercrime and threat taxonomies provide crime prevention by analyzing its origin and development. Bosh (2010) divided cyber crimes according to aims. Computer-assisted offences are the former include fraud and intellectual property offences that pre-date the Internet and are merely enabled by the socio-structural features of the internet. On the other hand, computer-oriented offences, are computer-oriented or computer-assisted offences such as viruses that target the computer hardware and software.

In the literature, many criteria are used in the evaluation of cyber threats, attacks, and crimes. Cyber threat and DDoS taxonomies which are of special importance were examined the existence of taxonomies suitable for the concepts of digital democracy and cyber activism in this study. Criminal taxonomies often focus on the purposive and technical dimensions of cybercrime (Indrajit et al., 2021). The purpose of classification is to reduce complexity and unnecessary hierarchy by organizing subtypes into well-defined categories along broad criteria. The main requirement for this is to ensure mutual exclusivity, which is possible with a clear definition of process and classification characteristics. The basic principle is that the first, direct and immediate point of impact must be specified for each cyber threat (Chandra & Snowe, 2020).

The main criteria of taxonomies are various according to analyzing data. Cyber threat taxonomy uses criteria such as attacker, victim, relationship, purpose, tool, tactic, result, impact, target, attack, and power of influence. Donald and Bryson's (2014) cybercrime taxonomy's nine attributes are victim, attacker, objective, tool & tactic, impact,

result, relationship, target, and offence. Narwal, Mohapatra, and Usmani (2019) describe cyber threat taxonomy which categorizes the threat into eight aspects.

Meyers, Powers, and Faissol (2009) presented a classification of different types of cyber enemies and their corresponding methods, motivations, maliciousness and skill levels, within the scope, prevalence and economic impact of cybercrime. Each of the enemy types is listed by respective skill level in table 1 (maliciousness, motivation, and method (adopted from Meyers, Power, & Faissol, 2009).

Table 1. A Taxonomy of Cyber Adversaries

Adversary Class	**Motivation**	**Method**
Script kiddies, novices	boredom, thrill seeking	download and run already-written hacking scripts known as ‟toolkits‟
hacktivist, political activists	promotion of a political cause	engage in denial of service attacks or defacement of rival cause site
cyberpunks, crashers,	prestige, personal gain, thrill seeking	write own scripts, engage in malicious acts, brag about exploits
user malcontens insiders,	disgruntlement, personal gain, revenge	uses insider privileges to attack current or former employers
coders, writers	power, respect prestige,revenge	write scripts and automated tools used by newbies, serve as mentor
white hat hackers, old guard	intellectual gain, ethics, respect	non-malicious hacking to help others and test new programming
black hat hackers, professionals	personal gain, greed, revenge	sophisticated attacks by criminals/thieves; may be ”guns for hire‟ or involved in organized crime
cyber terrorists	enemy nations, ideology, politics	espionage state-sponsored, well-funded cyber attacks against enemy nations

The criteria here are the target, the attack class, the degree of access gain, the source of the attack, the severity of the threat, the effects on the security targets, the result, and the motivation of the threat.

Sabillon, Cavaller, Cano, and Serre Ruiz (2016) extended to include elite, script kiddies, cyber-terrorists, disgruntled employees, virus writers, hacktivists, lamer, crackers, ethical hackers, GPS hackers, industrial spy hackers, government agent hackers, military hacker and cyber warriors. Kjaerland (2005) stated that cyber effects are tested in four categories as disrupt, distort, destruct, and disclosure. Simmons et al. defined a tree which classifies the cyber effect according to five core categories like attack vector, operational impact, defense, informational impact, target, and expanded than Kjaerland's (2006) taxonomy. Regarding the classification of cyber impact, Derbyshire et al. (2018) stated impact is the main motivation of a cyber attack and is the result of the action. Intended effects are usually denial of service, physical damage, leaks, premature code execution (Derbyshire et al., 2018). Cyber threat prediction and prevention applications are widely used to ensure the security of information systems. AVOIDIT cyber attack taxonomy figure includes attack vector, operational impact, defense, impact and the target parameters in figure1 is from Simmons, Ellis, Shiva, Dasgupta and Wu (2014). AVOIDIT is different from other taxonomies in the literature, categorizing cyber threats into attack vector, operational impact, defense, informational impact, and target categories, by aiming to educate the defender on possible cyber attacks.

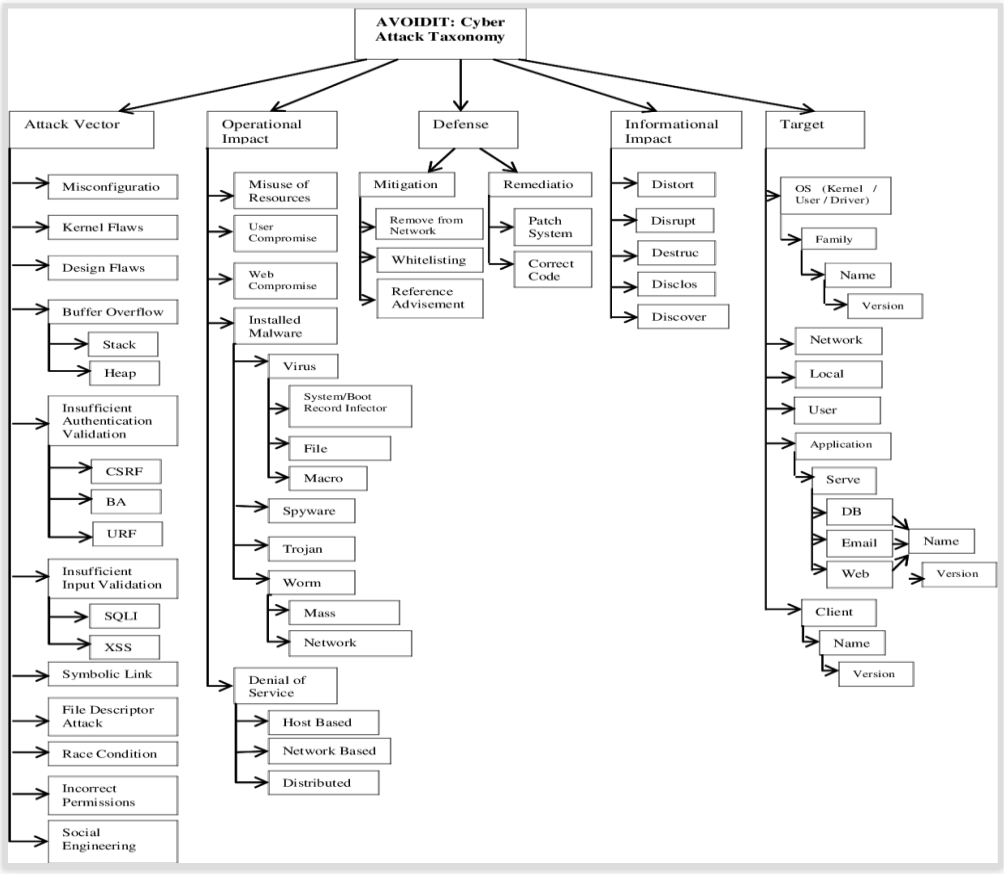

Figure 1. AVOIDIT

AVOIDIT could be extended to include new categories within each classification and it will provide a defender with the appropriate information to make an educated decision in defending against cyber attacks (Simmons, Ellis, Shiva, Dasgupta, & Wu, 2014).

CADAT is a process to make easier to the classification of cyber attacks with using of cause, action, defense, analysis, and target parameters (Banga, Gupta, & Bathla, 2019). Ebios risk management system determines the business and technical scope of the studied object the most appropriate source of risk/target pairs for the remainder of the study; identifies the stakeholders of the ecosystem of the studied object and creates operational scenarios that define technical attack methods that can be used by the risk source to assess threat levels and realize the identified strategic scenarios.

Lough (2001) developed IT (information technologies) security oriented a tree-like cyber-attack taxonomy for wired and wireless networks that used validation, exposure, randomness, deallocation, improper, and conditions parameters coded with VERDICT word. Cyberthreat and cybercrime taxonomies include the tool and the object dimensions (Urbas & Choo, 2008; Alkaabi et al, 2010) Cyber attacker's aims are linked to their motivation as challenge, status, revenge, politics, ideological, thrill, political or financial gain, and sexual impulses. (Choo, Smith, & McCusker, 2007; Howard & Longstaff, 1998; Moitra, 2004).

According to Chandra and Snowe (2020), the real question is "the actor who committed the crime". The taxonomy includes (i) accounting, which seeks to manage by measurement; (ii) technology, which provides efficiency through innovations; (iii) regulation, which seeks to provide transparency and accountability; (iv) enforcement,

which needs conceptual clarity; and, (v) public policy, which seeks capacity building and skill development in the society.

Cybercrime is divided into two pure technology crimes perpetrated by computers and networked systems, and advanced cybercrimes perpetrated by individuals, institutions, and governments at Chandra and Snowe's victim-centred taxonomy, which kept apart traditional- offline crimes from cybercrime. Pure technology crimes include computer systems, related technology and network system. Situations where a victim is a natural person, commercial institution, property, and governments suffering financial damage are considered as 'advanced cybercrime'. If the victim is the computer technology ecosystem, and networked systems, the cyber attack is considered in the category of pure technology cybercrime. The decisive point of reporting the denunciation of cyber crimes is the first direct and immediate effect of the event. Cyber advanced crime includes natural persons, property other than, and the governments. Situations where the victim is a natural person, commercial institution, property, and government suffering financial damage are considered 'advanced cybercrime'. If the victim is the computer technology ecosystem, and networked systems, the cyber attack is considered in the category of pure technology cybercrime. The decisive point of reporting the denunciation of cyber crimes is the first direct and immediate effect of the event.

Chandra and Snowe (2020) explained the classification of crimes against the government as: including acts that disrupt, hinder, assault or collapse its governing body or institutions, mechanisms or bureaucracy, and/or processes or systems, through which citizens and groups exercise their rights, meet their obligations, articulate their interests, and mediate their differences. Crime against Governments is a category of direct victims, including acts that target a nation, state or sovereign commonwealth. Crimes against governments affect their ability to effectively function and discharge their fiduciary, administrative, or statutory duties. If our taxonomies overlook and neglect to consider the structures of governments, the constraints of one type of government may fail to recognize the nature of the different forms of governments.

Moitra's (2004) modelling focused on victims. In the study, which also has a behavioral perspective, the motivations of cybercriminals to harm their victims were classified.

Magklaras and Furnell (2001) use semantics clues to classify the nature of IT insider threats. Online verbal behaviours may evaluate signs of aggression and domination score for an evaluated potential threat (EPT) (Schultz, 2002).

Meyers, Powers and Faissol (2009) presented a classification of different types of cyber enemies and their corresponding methods, motivations, maliciousness, and skill levels within the framework of the scope, prevalence and economic impact of cybercrime. Each of the adversary types has listed based on the corresponding skill level, maliciousness, motivation, and method.

DDoS taxonomies

While designing the Internet, the prime concern was to provide for functionality, not security. DDoS attacks mainly take advantage of the architecture of the internet, and this is what makes them powerful. As a result, many security issues have been raised, which are exploited by attackers. Cyber attackers have financial, political, and social motivations and they create diverse destructive tactics. DDoS attacks appear to be politically motivated (Yu,

2014). In these, the victim is thought to have wronged someone on the side of the attacker (Nazario, 2008; Simmons, Shiva, Bedi, & Dasgupta, 2014). Only a little subset of denial-of-service attacks is financially motivated.

Harry (2018) classified disruptive effects as data and physical attacks, internal and external denial of service, and message manipulation. Singh and Bhandari (2020) suggest a new-flow based DDoS Attack taxonomy which have four main category.

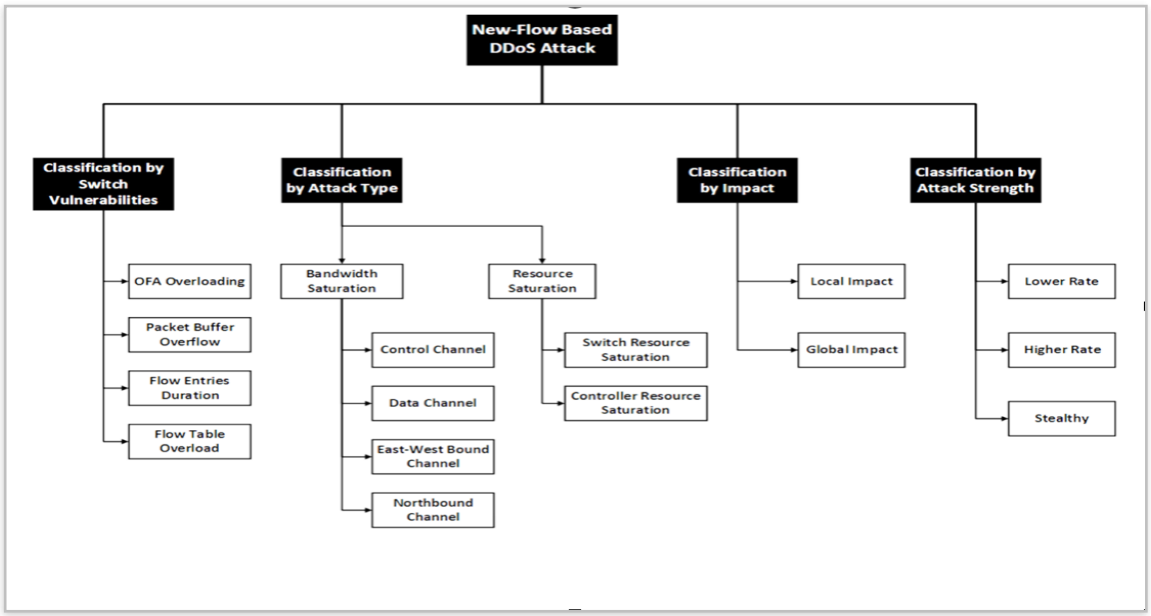

Figure 2. *New Flow based DDoS attack*

New flow-based DDoS attacks in figure 2, shows the taxonomy classified by switch vulnerabilities, attack type, impact and attack strength. DDoS defenses approaches are analyzing by Kaur et al. (2021) in literature at three popular categories. Fifty eight percent of the studies focused on Controller Resource Saturation, twenty eight percent bandwidth saturation of communication channel and thirteen percent are focused on flow table overloading and buffer saturation wiev (Kaur et al., 2021). Abhista et al. (2020) stated, to evaluate the reasons for selecting a victim, we make use of socio- cultural, economic and political (SPEC) dimensions. For the choice of target infrastructure, we utilize the dimensions of value, inertia, visibility and accessibility (VIVA).

Mirkovic and Reihner's (2004) taxonomy of distributed denial of services attack highlight features of attack strategies. The taxonomy of DDoS attacks has categorized into eight as:

1. Degree of Automation,
2. Exploited Weakness,
3. Source Address Validity,
4. Attack Rate Dynamics,
5. Possibility of Characterization,
6. Persistent Agent Set,
7. Victim Type,

8. Impact on Victim parameters.

Finally, in this study we categorized the taxonomies as effect and attack strength-focused, IT security focused taxonomy, user-oriented, and behaviorist taxonomies according to the literature basically.

Attack strength-focused taxonomies measures attacks as lower, higher and stealthy. Classification is by to attack strength and its measured as lower, higher and stealthy. (Banerjee et al., 1998; Guo & Yuan, 2012). Classification is by to attack strenght and its measured as lower, higher and stealthy. Effect and it security focused taxonomies are use these criterias too. Zhu et al. (2011) describe a taxonomy developed with an ICS focus, more specifically.

User oriented taxonomies use the parameters as cyber-bullying, awareness, phishing victims (Franz et al., 2021). Kjarland (2006), who also has a mixed evaluation perspective, analyzed Computer Emergency Response Team (CERT) related to computer crime profiling, highlighting cyber-criminals and victims. Method of Operation, Target, Source, and Impact analyzed. It can be understood from the scale of the target that the attack is for commercial, political or personal purposes.

IT security focused taxonomy presented by Specht and Lee (2004) divide into two DDoS attacks as bandwidth depletion and resource depletion attacks, which is IT security and also crime based oriented too. The work of Lee and Spetch (2000, p. 18) has raised important questions about DDoS taxonomies. As victims of attacks often fail to trace back to the attacker, there is the question of who is responsible for an attack in terms of contributory negligence. Can owners or agencies responsible for secondary victims be held responsible for participating in an attack? Are software and hardware vendors also responsible for cyber attacks? Do network providers have to keep victims away from DDoS packet traffic sent to the network?

Sabillon, Cavaller, Cano, and Serre Ruiz (2016b) presented to comprehensive a cyber crime taxonomy in twenty-seven titles as child pornography, cyberhate speech, cyber offenses against intellectual property, cyberbullying, cyberespionage, cyberextortion, cyberfraud, cybergrooming, cyberheist, cybering, cyberlaunderin, cyberstalking, cybertheft, cyberwarfare, data breach, disgruntled employees and former employees, identity theft, online gaming, online obscenity, phishing, racism and xenophobia-related cyber offences, religion-related cyber offences, revengeporn, spam and which we are focused in the study, the cyber terrorism, hacking and cyber vandalism. They define the distributed denial of service attacks (ddos) and social media account hijacking, website defacement, using malware to delete data, categorized as cyber vandalism different from cyber crime. They define hacktivism as a part of organized crime networks, operating with specific motives and a high degree of sophistication, which has been becoming illegal once it crosses the threshold of gaining unauthorized access to computer systems. Finally, they related the hacking with cyberterrorists who engage in terrorist activities that exploit computer vulnerabilities, and that will impact mostly civilians in metropolitan areas because of motivated by political ideology, religious beliefs, hacktivist proclivities or personal reasons.

Behaviourist studies, which focused on actors of cyber-attack or suspects and their decision mechanisms, are based on self-determination theory generally. The theory of self-determination distinguishes between autonomics and oppressive and controlled behaviours of cyber attackers. They are intrinsically motivated behaviour (Ryan & Deci, 2000). With regard to extrinsic regulators, research has shown that evident that compliant security behaviour greatly influences the protection of information assets on the social climate, software measures and facilitating conditions and these studies pointed out the importance of human motivation. Sherizen (1990) add the taking risk,

low self-control and opportunistic behaviour to factors that promote a maladaptive to compliant security behaviour. Posey et al. (2013) proposed a protection-motivated behaviour to protect information resources by insider. Venkatraman (2008) defined cyber deviant behaviour as violating organizational norms and endangering the organization, and proposed three measurable categories: members, institutionalization, and technical skill. Internalized norms such as embarrassment or shame, fear of informal sanctions from peers and internalization of legal norms may also be deterrents to crime. The aforementioned theory moderated by certainty of detection, severity of punishment and the celerity of detection is also known as the classical deterrence theory (Grasmick & Bursik, 1990).

Kumar and Carley (2016) revealed that new international events affect social media and sometimes the hacker community differently. It measured a general mood swing for countries through social media analytics and tracked cyber attack vulnerability. Kumar and Carley's (2016) taxonomy helped to find an answer this study's question. Cyber attack taxonomies may classify to focal points as IT and cyber security, attack impact, attack strength and behavior focused studies (Hansman & Hunt, 2005; Meyers, Powers, & Faissol, 2009; Kjarland, 2006).

As Abhistha et al. (2000) stated in the research compared and associated with DDoS attacks and eventful days (according to Google Alert) holistic perspective is imperative to accurately map threats and take appropriate protective measures against DDoS attacks.

Method

This is an interdisciplinary study carried out in the fields of mass communication and informatics, which is essential in terms of associating the movements toward cyberspace with the theories of mass communication and the use of public space. The aim of study is to evaluate the motivational dimension of cyber activism and to review the competency of cyber attack taxonomies to distinguish cyber activism from other cyber crimes. The research is based on seconder data and has a qualitative method and descriptional design. Research questions are: Is a democratic public space possible in cyberspace? And DDoS attacks are defined as hacktivism, cyber terrorism or the struggle to conquer cyberspace, depending on what conditions?

In the first part of the study, DDoS attacks in the cyber activism dimension was discussed in the context of new media and digital democracy. It has been investigated how to find the criterion that determines the distinction between activism and cybercrime. In the second part, basic concepts such as cyber threats, crime, war and cyber diplomacy are explained. A literature review is conducted to specify the focal points, criteria of current cyber threat taxonomies and purpose and motivations of DDoS attacks. The existence of taxonomies suitable for the concepts of digital democracy and activism and their contribution to the measurement of hacktivist activities and the evaluation of social protests have been questioned. Scope and criterion validity was ensured by examining the messages of hackers who carried out effective newsworthy DDoS attacks, which is a type of cyber activism in Turkey, in the context of moving the public agenda to the cyber space. (Coleman, 2011, p.138). Researchers who will examine the history of hacker messages and ddos attacks from the archives of scanned online news sites will see the impact of the social agenda on the risk of ddos attack and will understand a positive correlation between social conflict and attacks.

Sampling Research

Common cyberthreath and DDoS taxonomies in the literature were examined for determining their priority criterion. The secondary data was analysed, by non-experimental and descriptive design within the framework of cyber activism. DDoS attacks in the Turkish mainstream news media were subjected to content analysis in terms of new social movements. The three most clicked internet news sites from Alexa data were selected according to their belonging to different media organizations. The archives of Ensonhaber.com, Hurriyet.com.tr and Sözcü.com were scanned with the keywords "hacker", "cyber hacker", "crashed", "DDoS", and the perpetrators were analyzed by examining the history and perpetrators. In addition, the messages given by the hackers were examined to see if the DDoS attacks were related to the public agenda and to make the cyber activism dimension visible.

Findings

To evaluate the examples of cyber threath and DDoS taxonomies, the archives were scanned and the cyber attacks that had the most impact on Turkey's agenda were identified. The archive was scanned with the keywords "hacker, "cyber hacker", "crashed", "DDoS". The news includes the messages shared at the time of the attack and/or social media assuming and explanations. In this section, content analysis of the messages given in the hacking actions in the context of new social movements has been applied.

Table 2. Messages of cyber hactivists

Victim	***Date/Hacker***	***Messages of hackers***
www.bbm.gov.tr	2/5/2008 The Karan	Mr. Prime Minister, since you do not hear our voice, we will announce it like this.
*www.maliye.gov.tr	9/11/2011 ColdHacker	Get your dirty hands off the people of Kurdistan
www.osym.gov.tr	21/4/2011 V.O	**The system ıs fully off for now. frıends who want to use ıt can use the defıcıt and transfer ınformatıon. good luck:::))))
www.disisleri.gov.tr	3/7/2012 Red Hack	"It's not foreign affairs, it's war and slavery business.
ankara.pol.tr kirikkale.pol.tr POLNET	28/2/2012 RedHack	We have been working on the servers of Ankara-based POLNET and Ankara Police Department for about three weeks. The police will be stunned when they see how far we've come when the documents are released." We are protesting the green army Ankara Police of the community that killed Ethem Sarısülük by shooting him in the head!
www.diyanet.gov.tr	30/10/2012 RedHack	We will stop you playing the people like sheep by being a religious trader!"
www.thy.com.tr	26/8/2012 Anonymous	It's not the THY brand or planes that bring us to our loved ones, it's their workers.
www.tgc.org.tr	14/9/2012 Turkish Ajan Hacker	"You will apologize to Anadolu Agency.
www.yok.gov.tr	8/1/2013 Redhack	We said let's hack the institution that is the head of the snake.
www.yargitay.gov.tr	16/1/2013 Redhack	N.C. We will throw a firewood on your fire for every drop of tears that we do not know, maybe hundreds of our sisters."
İzmir İl Özel İdare	27/3/2013 RedHack	We open to the public all the electricity, gas, adsl, etc. invoice transactions of the Istanbul Administration ;)' Freedom for Palestine
www.basbakanlik.gov.tr	5/6/2013 Anonymous & SEA	Fear changed sides: Turkish people are not afraid, oppressors are afraid

www.rtuk.gov.tr	12/6/2013 Anonymous	you punished the media organizations that wrote the truth. Now Anonymous has punished you”
www.ulusalkanal.com	25/6/2013 RedHack	Pull like it's nation Panpa
www.chpankara.org	10/7/2013 Ayyıldız Team	Don't force us to do things we haven't done in years
www.tkib.gov.tr	15/10/2013 RedHack	Since #Berkin gave the orders, #Melis, #Ozan, #Serdar gave the orders; this run will be run without breath” The holiday of those who do not forget what happened in #Rojava, #Latakia, #Kirkuk
Kurtlar vadisi	17/11/2013 PKK Hack Team	Your site has been destroyed by PKK Hack Team
idrisnaimsahin.com.	21/5/2013 Cold Hackers	Martyrs of May are immortal.
Akp Ordu İl Başkanlığı	29/11/2013 RedHack	We will not leave Taylan alone either. Innocence is fearless.
www.tcmb.gov.tr	16/01/2014 RedHack	Has the Central Bank become uf?
www.taraf.com.tr	28/3/2014 Gözcü	"You Have Betrayed the Homeland and Nation! This Nation Will Not Forgive You!"
Türk İşbirliği ve Koordinasyon Ajansı	19/5/2014 RedHack	Email and user login disclosure
www.egm.gov.tr	5/9/2013 RedHack	Pull the plug, tidy up, tidy up,tidy up! :)
www.burhankuzu.com.tr	13/5/2013 RedHack	This is our wedding gift, it comes all the way from Hatay. We will not only enjoy your wedding, but also you.. The people of Hatay are not alone! We will not forget, we will not forgive!' also
www.emniyetyurdu.pol.tr www.polder	13/6/2013 RedHack	Our oppressed, self-sacrificing, long-suffering people have been playing a game for days... We are not slaves! They are not masters either! We are the People and the Peoples never bow You can't forget berkin elvan, you can't protect his murderer
HDP, PKK, Abdullah Öcalan etc.	25.7.2015 TürkhackTeam Anonymous	We love this country and we will not give anyone an inch of land no matter what the cost.
Nearly 400 thousand addresses with “.tr”	14/12/2015 Anonymous	If you do not stop supporting ISIS, we will continue to attack”**
www.rtuk.gov.tr	4/10/2016 RedHack	We condemn attacks agaınst the free press
www.Fgulen.com	14/8/2016 Akıncılar	Hail to the Tall Man. In memory of the Martyrs of July 15.*
700	2/11/2018 Turkz	Cumhuriyet Bayramı hediyesi
www.garantibbva.tr Turk Telekom	27/10/19 Cetinkaya	-
Sinovac	30/12/2020 Root Ayyıldız	"Greetings from the red flag, to the sky flag. May Allah grant us to perform the Friday prayer on the Great Wall of China.

The content analysis applied to DDoS attack news in Turkey provided us with the following outputs:

1. DDoS attacks can be carried out on a local and international scale, as well as organized or individually.

2. Different individuals and groups, positioned for or against the political power in the country, have made their reactions visible by attacking many different targets, local or global, especially on issues and times when freedom of expression is restricted. Due to the anonymous structure and organization of the contractors, especially for DDoS attacks, the issue is both collective action and a foreign policy issue.

3. It has been seen that the target selection is compatible with the desired message. In the attacks targeting the government and the current bureaucrats, the reputation of the state and the nation was taken into consideration,

and the material damage caused did not go beyond being a measure of the effect of the attack and did not become a matter of interest.

4. The DDoS attacks carried out are designed to take into account the messages published by the contractors and do not aim to provide a benefit or cause permanent harm and aimed to ensure that contractors' messages are taken into account.

5. Attacks are actions aimed at becoming a party to a power struggle in cyberspace. It has been observed that the target selection is compatible with the desired message. In the attacks targeting the government and the current bureaucrats, the reputation of the state and the nation was taken into consideration, and the material damage caused did not go beyond being a measure of the effect of the attack and did not become a matter of interest.

6. The motivation for DDoS attacks coincides with the culture of hackers. In other words, it has been seen that DDoS attacks, which have a high economic and social impact, have a reaction mission in the face of ethical and political issues. Following the cyber-piracy culture literature, DDoS attacks have the idea of showing will against unfair practices, disproportionate use of force, oppressive practices and anti-democratic rhetoric. The manifestation of the pirate culture, which wants to show that it will not obey the rules (including language rules) is defiance, sarcasm, humour and slang language.

7. High-impact DDoS-type hacktivist actions are in the range of follow-up activity periods between long sleep periods (overlap with Abhistha et al., 2000).

8.DDoS attacks and broad-based social conflict periods in the country show parallelism. The existence of cyber attacks, where the broadest impact is created, is an expression that the conflict has moved into cyberspace.

Discussion and Conclusion

Cyber crime and threats and DDoS taxonomies in the literature were examined, and priority criteria were determined in this study. The introduction part includes digital democracy and cyber activism in new media opportunities discussed. In the second chapter, in which the literature review of cybercrime taxonomies is presented, DDoS attack taxonomies are outlined. To contribute to the understanding of the hacktivist actions of the information on the public agenda, content analysis including the date, contractor, and messages of the DDoS attacks on the country's agenda applied. First research question, “democratic public space possible in cyberspace? answered by the new media and democracy frame. Cyber public opinion is the socialization and public sharing area of the new media. All new media help to ensure democracy theoretically by providing the function through access to resources, freedom of expression, and justice in equal voting rights, electoral justice, freedom to use alternative news sources, freedom of association and participation. As we seen in the findings of the study with like literature, the new media now offers more opportunities for users to access accurate information or synthesize data, although information pollution causes it to increase exponentially. The propaganda ability, in the hands of the sovereign powers, turns into an opportunity for users who upload and share the information they want to the internet. This makes it possible for all people who can make their voices heard and representatives of different views to make propaganda according to their own ideologies and provides a fairer environment. The second question, depending on what conditions are DDoS attacks defined as hacktivism, cyber terrorism, or the struggle to conquer cyberspace? It is answered in cyber activism, hacking and legal practices. Cybersecurity efforts that do

not follow the public agenda miss the motivation behind cyber activist actions. For this reason, prevalence, message forwarded, number of organic interactions, and official and public agenda should be taken into account in cyber attacks and DDoS classifications. In addition, big data, locators and wearable technology data, forums and social media analytics should be used to follow the agenda of the cyber public. The conquest of cyberspace is determined by the norms to which the explorer is subject, and also the consequences of translation, use, and management of digital spaces lack a universal legal framework. The actions such as cyber warfare, cyber diplomacy and cyber terrorism can be distinct by the guidance of political powers and the maker's motivation, as mentioned in the linked sections of the study. In addition, broad participation in collective actions during high political tension is a substantive criterion, too. DDoS attacks should be handled in the context of cyber public opinion and new social movements. Because they do not aim to conquest cyberspace, but a struggle for existence when cyber actions.

As a mobilization tool, new media is both a tool and a target of cyber activism, which enables participation in contemporary social movements and social/political protests. The power of social media has become more visible to Gezi and conflicts based on internet-based organizations such as Arab Spring and Occupy Wall Street. Howbeit, we should remember the messages that can unite viewers around certain values are also open to manipulation in the new media. There are risks of information pollution, manipulation of society, excessive support of certain groups, polarization, and conflict. The use of social media as a propaganda tool by terrorist and criminal organizations is another dimension of cyber activism (Zizek, 2013). In contrast, we should accept that social media is a quality and popular resource for setting the public agenda. The findings of the study showed parallelism between DDoS attacks and the public agenda of political pressures and anti-democratic practices. However, it cannot be said that DDoS attacks occur every time the public agenda is tense. Challenge-oriented DDoS attacks based on the struggle for existence in cyberspace are not a type of attack for financial gain. On the contrary, they represent cyber public opinion and generally even have the quality of political resistance. Therefore, hacktivism can be considered as a kind of cyber activism aimed at liberating the internet.

National cyber security is gaining importance day by day. New media-based actions need to be accurately questioned and evaluated in today's conditions. Contemporary cybersecurity studies should focus on threat intelligence aimed at preventing cyber attacks before they happen (Robertson et al., 2017). Unfortunately, popular DDoS attacks taxonomies do not measure the criteria to distinguish cyber activist actions from other cyber crimes and do not show cyber activism motivations. As a result, it is suggested to develop taxonomies of cybercrime that are sensitive to the digital activism motivation of actions that receive widespread support and are organized with broad participation and represent the public agenda. Cyber security efforts should not be seen as an obstacle to the democratic and fair use of cyberspace. Official governments should consider the need for democracy and the nature of protest actions against disinterested attacks on the population.

Cyber-activist actions other than hacktivism can be analysed by using social media analyses by extensive subsequent studies. In addition, it will provide valuable data for the cybersecurity field when the international background in the timing of effective DDoS attacks is questioned.

Geniş Özet

Giriş

İnsanlara kendisi olma performansını sergileyecek mecra olarak yeni medya platformları benzer görüşlere sahip insanlarla tanışma ve sosyalleşme imkânı sağlıyor. Böylece, yöndeşik yeni medya akışkan bir kamuoyu oluşturuyor. Fiziksel gerçeklik zaman ve mekân içine sıkışmış ve özgür olmayan bir dünyadır. Siber gerçeklikte doğan, demokratik katılımın sağlanabildiği sanal bir kamuoyunda çeşitli ifade yöntem ve tarzları bulunuyor. DDoS saldırıları, siber saldırıların en yaygın türlerindendir ve beyaz bilgisayar korsanlarınca sıklıkla tercih edilen bir saldırı türüdür.

Gerçek dünyanın siber yansımasını inşaa ederken hacking etkinlikleri naif bir konumda bulunur. Hackerlar, egemen güçlerin, gerçek dünyayı ve eşitsizlikler yeniden inşa ettiği baskıcı varlıklarının siber yansımayla karşı çoğunluğun temsilini sağlarlar. Siber kamuoyunun demokrasi bekçisi konumunda değilseler de bilgisayar korsanları siber uzayda, kamunun iktidar mücadelesinin temsilcisidir. Bu çalışmanın amacı, DDoS saldırılarını siber aktivizm bağlamında incelemektir ki bu çerçevede Türkiye'de yaşanan etkili DDoS saldırıları incelenmiş, amaç motivasyonları yeni toplumsal hareketler bağlamında değerlendirilmiştir.

Yeni medya, taşınabilirlik özelliği ile bilgiye erişimi kolaylaştırarak bilgi okuryazarlığı oranını artırmasına karşın eşitsiz ve sınırlı internet erişimi ekonomik eşitsizliğin yeniden üretilmesine yol açıyor (Giddens, 2012, s.445; Noris, 2001). Taşınabilir ve giyilebilir ortamlarıyla yeni medya, doğal olarak egemenlik mücadelesine dayalı bir siber alandır (Müller & Kramer, 2014). Dijital kamusal alan olarak yeni medya özel ve siyasi alanları hatta bireyleri ve kurumları kapsayan ve birleştiren bir söylem ve eylem siber alanıdır. Yeni medya bağlamında siber kamuoyu toplumsal hareketler ve siyasi çatışmaların mevcudiyetinde aktivist pratiklerin yaygınlaştırılması için uygundur (Castells, 2008; Zizek, 2013). Yeni toplumsal hareketlerin yapısına uygun olarak kadın hareketi, savaş karşıtı ve barış hareketi, çevre hareketi, çiftçi hareketi, nükleer enerji, düşük ücretli işçilere karşı hareket, işçi hareketi ve AIDS hareketi gibi temalarda toplumsal duyarlılık gösteren siberaktivizm eylemleri gerçekleştirilmektedir (Kalafatoğlu, 2010). Dijital aktivizm faaliyetleri tıklama, meta-seslendirme, iddia, politik tüketicilik, dijital dilekçeler, botivizm, e-finansman, veri aktivizmi, ifşa ve hacktivizm olarak sıralanabilir. George ve Leidner (2019) literatürdeki dijital aktivizm fonksiyonlarını fonksiyon ve mekanizma ilişkisini özdeşleşme, inşaat, saldırganlık, aldatma, görünürlük, amplifikasyon olarak sıralamıştır. Siber aktivizmi dijital izleyici etkinlikleri, dijital geçiş faaliyetleri ve dijital gladyatör etkinlikleri başlıkları altında sınıflandırmıştır. Hacktivizm hükümetleri, kamu ve özel kuruluşları ve bireyleri hedef alan ve bir olay veya politika tarafından veya bir grup diğerine göre ayrıcalıklı bir avantaj sağladığında tetiklenen ifşa, verileri yok etme veya kesintiye uğratma eylemleridir (Coleman, 2011). Dijital aktivizm olgusu özellikle sosyal medyanın takibi ve analizleriyle daha net anlaşılır kılacak ve siber suç ile ayrımının sağlanmasını kolaylaştıracaktır.

Siber korsanlarca en popüler eylemi DDoS saldırılarının mantığı, hizmet sitelerinin sunucuları engellemek için sisteme hizmet edemediği kadar sahte kullanıcı göndermek ve işleyişi kesintiye uğratmaktır. Bu eylemlerin amacı şahsi fayda sağlamak değil, düşünce özgürlüğü ve çok sesliliğe olanak sağlayarak siber kamuoyunda baskıcı uygulamalardan uzak tutmaktır.

Siber alanın dostane görünümü ve internetin arkasındaki ağ örgütlenmesi ekonomik süper güçleri maskelemektedir (Başaran, 2010). Gerçek dünyada olduğu gibi, iktidarı bölen sınırlı grubun sömürü ve baskısının varlığı, yeni

medyayı bir aktivizm ve mücadele alanı olarak görmemizi gerektiriyor. Bireyler siber uzayda gerçek dünyada paralel varoluşlar yaşarken, sanal kamunun çok hızlı bir toplumsal oluşumunu ve tüketimini sağlamaktadır. Siber uzay gerçek dünya gibi kirlenmektedir.

Yöntem

Bu, disiplinler arası bir nitel araştırma çalışmasıdır. Çalışmanın amacı, siber aktivizmi diğer siber suçlardan ayırt edecek kriterlerin belirlenmesine yardımcı olmaktır. Literatürün ilk bölümde DDoS saldırılarının arka planı siber aktivizm bağlamında ele alınmıştır. İkinci bölümde siber tehditler, suç, savaş ve siber diplomasi gibi temel kavramlar tanımlanmış ve son bölümünde siber tehdit taksonomilerinde kullanılan ölçütler sorgulanmıştır. Araştırma soruları “siber uzayda "demokratik bir kamusal alan" mümkün müdür?” ile " DDoS saldırıları hangi koşullara bağlı olarak hacktivizm, siber terörizm veya siber uzayı fethetme mücadelesi olarak tanımlanır?” Bulgular aşamasında Türkiye gündemini en çok etkileyen siber saldırılar, arşivler taranarak tespit edilmiştir. Alexa verilerine göre farklı medya kuruluşlarına ait en çok tıklanan üç internet haber sitesi seçildi. Ensonhaber.com, Hurriyet.com.tr ve Sözcü.com arşivleri taranmıştır. Arşiv "hacker, "cyber hacker", "crashed", "DDoS" anahtar kelimeleri ile taranmıştır. Siber saldırı haberleri; üstlenici, tarih ve mesajlar ölçütleri ile incelenmiştir. Hacking eylemlerinde verilen mesajlara , yeni toplumsal hareketler bağlamında, içerik analizi uygulanmıştır. Sonuç bölümünde ise elde edilen bulgular literatür ışığında değerlendirilerek DDoS saldırısı taksonomilerinde hukuk ve etiği koruma motivasyonlarla gerçekleştirilen siber aktivist eylemlerin ayırt edilebilmesi için bütünleşik bir yaklaşım önerilmiştir.

Sonuç

Yeni medyanın sağladığı imkanlar, paylaşım ve demokrasi kültürünü geliştirir. Siber uzayda insan temelli, siber aktivizm yoluyla canlı ve dinamik bir kamuoyu oluşmaktadır. Bu kamuoyu, yeni toplumsal hareketler çerçevesinde ele alındığında, siber aktivizmin agresif bir türü olan haktivizm genellikle kar amaçlı değil, meydan okuma, baskılara direnme ve siyasal duyarlılık kökenlidir. Geniş bir katılımın söz konusu olduğu haktivist eylemler gerçek bir yerel ve küresel kamuoyu gündemi ile paralellik gösteriyor ise demokratik egemenlik mücadelesi olarak tanımlanabilir. Siber uzayın demokratikliğini sağlamak için, tüm çatışmaları ile toplumsal gruplar da özgürce temsil edilebilmelidir. Mevcut güç mücadelelerini siber alana taşıyan devletler ve egemen kullanıcılar siber demokrasiyi kısıtlamaktadır. Yeni medya ve siber aktivizm çerçevesinde ele alınan bu çalışmada, siber aktivizmin marjinal ve saldırgan bir türü olan hacktivizm motivasyonu siber alanda varlığını ve gücünü kanıtlamak olarak kabul edilmektedir (Coleman, 2011).

Günümüzde en yaygın görülen siber saldırılar dağıtık hizmet engelleme (DDoS), Man in the Middle (MiM), oltalama, yetki ihlali, bombalar (Mantık veya Zaman), tarama, kontrolleri atlama, veri değişiklikleri, hizmet reddi, gizli dinleme, yasadışı kullanım bilgi sızıntısı, veri engelleme/değiştirme, girişim, veri tabanı sorgu analizi, maskeleme, fiziksel izinsiz giriş, reddetme, kaynak tüketme, sabotaj, süpürme, casusluk, hizmet sızdırma, sniffers, ikame, terör, hırsızlık, trafik analizi, tuzak kapı/arka kapı, Truva Atı, tünel açma, yetkisiz erişim, izin ihlalleri, yetkisiz erişim, bindirme, virüs ve solucanlar olarak örneklendirebiliriz.

Siber saldırı türleri; hırsızlık, dolandırıcılık, siber terörizm, sanal zorbalık, taciz, şantaj, veri sızdırma ve ifşa yoluyla şantaj gibi çeşitli suç motivasyonlarına göre gerçekleştirilir. Bilişim sistemleri aracılığıyla işlenen bu

suçlar fiziksel gerçeklikte cezalandırılmaktadır. Siber suçlar, gerçek suçların siber dünyadaki yansımasıdır. Korsan kültürü çevresinde, temel motivasyonları meydan okuma, gündeme paralel tepki gösterme ve adalet arayışı olan ve maddi çıkara dayanmayan en popüler siber saldırı türü ise DDoS'tur ve sadece çevrimiçi olarak gerçekleştirilen, fiziksel hayatta karşılığı olmayan bir eylemdir. Bu nedenle suç vasfını değerlendirme aşamasında daha fazla parametrenin analizi gereklidir. DDOS saldırıları siber uzayda iktidar ve kamu yönetimi mücadelesinin temsilcisi olan korsanlar tarafından en çok tercih edilen saldırı türlerinden biridir. Literatürde incelenen başlıca siber suç ve DDOS taksonomilerinde odak noktaları suçun amacı, suçlunun pozisyonu, hedefi, şiddeti, yarattığı hasar, kurban ve suçlunun kullandığı donanım, yazılım ve tekniklerdir. İncelenen ölçütler değişiklik gösterse de bu odak noktalarına göre seçilerek analiz edilmektedir. Saldırganın amaç motivasyonu ağırlıklı olarak maddi çıkar sağlama, suistimal ya da siber milislik yönelimlerini ölçen kriterlerdir. Bu taksonomilerin genel olarak toplumsal çatışma süreçlerini yansıtmadığı ve kamu gündeminden de kopuk olduğu görülmüştür. Siber aktivizmi diğer siber suçlardan ayırt edebilmek için Türkiye'de haber değeri görülen DDoS saldırıları tarihleri, üstleniciler ve onların mesajlarını içeren bir tablo ile bulgular sunulmuş ve literatür çerçevesinde yorumlanmıştır

Kamuoyu gündemini gözetmeyen siber güvenlik çalışmalarında, siber aktivist eylemlerin demokratik motivasyonunu gözden kaçırılması kaçınılmaz olacaktır. Siber demokrasinin sağlanması için siber uzayda var oluş mücadeleleri ve egemenlik mücadeleleri sınırlandırılmamalıdır. Siber uzay bir savaş alanından ziyade sonsuz bir varoluş pratiği ve iktidar mücadelesi olarak tanımlanmalıdır. Kamunun da yansımasını kapsayan siber uzayın savaş olanı olarak tanımlanması siber diplomasi ve siber güvenlik endişeleri demokrasiyi karanlıkta bırakmasına yol açmaktadır.

Sonuç olarak dijital aktivizm motivasyonuna duyarlı, kamu gündemini takip eden, yaygın destek alan ve geniş katılımla organize edilen eylemleri gözeten siber suç taksonomilerinin geliştirilmesi önerilmektedir. Siber saldırı taksonomilerinde siber aktivist motivasyonları görünür kılmak için yaygınlık, katılımcı sayısı, desteklenme yüzdesi, iletilen mesajların analizi, organik etkileşim sayısı, resmi gündem ve kamuoyunda gündemi gibi belirleyici ölçütlerin de DDOS taksonomilerine dahil edilmesi önerilmiştir. Mobil haberleşme uygulamaları, forumlar ve sosyal medyanın organik hareketiliği, lokasyon belirleyiciler ve giyilebilir cihazların verilerinin de gerçek dijital kamuoyu gündemini belirlemeye yardımcı olabileceği düşünülmektedir. Bu konuda gerçekleştirilecek daha geniş çaplı çalışmalarda sosyal medya analizlerinden yararlanılarak hacktivism dışındaki siber aktivist eylemler de analiz edilebilir. Siber suç taksonomilerinde güvenilir bir kamuoyu gündemi verisinin değerlendirilmesi siber güvenlik çalışmaların anlamlı bir katkı sağlaması beklenmektedir. Ek olarak etkili DDoS saldırılarının zamanlamasındaki uluslararası arka planının sorgulanması siber güvenlik alanı için değerli veriler sağlayacaktır.

Teşekkür ve Bilgilendirme

Bu araştırma makalesi özgündür ve bir tez ya da projenin bir parçası olarak üretilmemiştir. Bu araştırma makalesi için bir fon ya da kurum tarafından destek alınmamıştır. / This article is not submitted as a proceeding and is not a part of a project or dissertation. This article is not supported by a research institution or a fund.

Yayın Etiği Bildirimi

Bu araştırma makalesinin etik sorunu olmadığını beyan ederim. / I hereby declare that this research article does not have an unethical problem.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Bu makale tek bir araştırmacı tarafından hazırlanmıştır. / The article is prepared by one author. No contribution rate by another researcher.

Çıkar Çatışması / Conflict of Interest

Bu araştırma makalesinde bir çıkar çatışması bulunmamaktadır. / The study has no conflicts of interest.

Fon Bilgileri / Funding

Bu araştırma makalesi için bir fon ya da kurum tarafından destek alınmamıştır./ This article is not supported by a research institution or a fund.

Etik Kurul Onayı / The Ethical Commitee Approval

Bu araştırma makalesinin etik sorunu olmadığını beyan ederim. / I hereby declare that this research article does not have an unethical problem.

Kaynakça / References

Abhishta, A., Van Heeswijk, W., Junger, M., Nieuwenhuis, L. J., & Joosten, R. (2020). Why would we get attacked? An analysis of attacker's aims behind DDoS attacks. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 11*(2), 3-22.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2010, October). Dealing with the problem of cybercrime. in International Conference on Digital Forensics and Cyber Crime (pp. 1-18). Springer, Berlin, Heidelberg.

Arendt, H., Dworkin, R., Habermas J., Galtung M.L., Saner H., Rawls J., Thoreau H.D., (1997). *Sivil itaatsizlik*. İstanbul, Ayrıntı.

Averweg, U. R., & Leaning, M. (2018). The qualities and potential of social media. In *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 7106-7115). IGI Global.

Başaran, F. (2000). İletişim ve emperyalizm: Türkiye'de telekomünikasyonun ekonomi-politiği. Ütopya Yayınevi

Bayhan, V. (2014). Yeni toplumsal hareketler ve Gezi Parkı direnişi. *Birey ve Toplum Sosyal Bilimler Dergisi, 4*(1), 23-58.

Bjola, C., & Holmes, M. (2015). *Digital diplomacy* . Taylor & Francis.

Bıçakcı, S., Ergun, F. D., & Çelikpala, M. (2015). The Cyber security scene in Turkey. EDAM: The Centre for Economics and Foreign Policy Studies, Istanbul, Turkey. http://edam. org. tr/document/CyberNuclear/edam_cyber_security_ch2. pdf.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace.* Santa Barbara, California: Praeger.

Castells, M. (2008). Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi, çev. *Kılıç, İstanbul: İstanbul Bilgi Üniversitesi*.

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems, 38*, 100467.https://doi.org/10.1016/j.accinf.2020.100467

Choo, K. K. R., Smith, R. G., McCusker, R., & Choo, K. K. R. (2007). Future directions in technology-enabled crime: 2007-09. *Research and Public Policy series 78*, Canberra: Australian Institute of Criminology.

Crowley, D., & Heyer, P. (2015). *Communication in history: Technology, culture, society.* Routledge.

Dahl, R. A. (2001). *Political Equality in the Coming Century. In Challenges to Democracy* (pp. 3-17). Palgrave Macmillan, London.

Davenport, T., & Prusak, L. (2000) *Working Knowledge: How Organisations Manage What They Know.* New preface edition, Harvard Business School Press, Boston, MA.

Denning, D. E. (2000). *Barriers to Entry: Are They Lower for Cyber Warfare*? Calhoun, Dudley Knox Library. http://hdl.handle.net/10945/37162

Derbyshire, R. , Green, B., Prince, D.,İ, Mauthe, A. and Hutchison D., (2018). An Analysis of Cyber Security Attack Taxonomies," 2*018 IEEE European Symposium on Security and Privacy Workshops. (EuroS&PW), 2018*, pp. 153-161, doi: 10.1109/EuroSPW.2018.00028.

Faritha, B., J, Revathi, R., Suganya, M.,& Gladiss M. N. (2020). IoT based Cloud Integrated Smart Classroom for smart and a sustainable Campus. *Procedia Computer Science*, *172*, 77-81. https://doi.org/10.1016/ j.procs.2020.05.012

Flynn, I. (2021). *Deliberative democracy*. John Wiley & Sons.

Franz, A., Zimmermann, V., Albrecht, G., Hartwig, K., Reuter, C., Benlian, A., & Vogt, J. (2021). SoK: Still Plenty of Phish in the Sea—A Taxonomy of User-Oriented Phishing Interventions and Avenues for F u t u r e Research. In Seventeenth Symposium on Usable Privacy and Security ({SOUPS} 2021) (pp. 339-358).

Friedman, L. W., & Friedman, H. H. (2008). The new media technologies: Overview and research framework. Available at SSRN 1116771.

Gazeteciler Cemiyeti. (2019). İfade ve Basın Özgürlüğü Eylül 2019 Raporu.http://media4democracy.org/public/uploads/reports_4696242.pdf.

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

George, J. J., & Leidner, D. E. (2018). Digital activism: A hierarchy of political commitment. https://doi.org/10.24251/HICSS.2018.288

Golman, R., & Loewenstein, G. (2015). Curiosity, information gaps, and the utility of knowledge. Information Gaps, and the Utility of Knowledge (April 16, 2015), 96-135.

Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication, 13* (1), 74-86. https://doi.org/10.1080/15405702.2014.978000

Grasmick, H. G., & Bursik, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law & Society Review, 24*(3), 837–861. https://doi.org/10.2307/3053861

Gürdal, E. (2021). Dijital Diplomatlar: Dijital Diplomaside Yeni Nesil Diplomatlar. *Bitlis Eren Üniversitesi İktisadi ve İdari Bilimler Fakültesi Akademik İzdüşüm Dergisi, 6*(1), 114-127.

Hansman S. & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computer and Security*. https://doi.org/10.1016/j.cose.2004.06.011

Harry, C., & Gallagher, N. (2018). Classifying Cyber Events: A Proposed Taxonomy. *Journal of Information Warfare, 17*(3), 17–31. https://www.jstor.org/stable/26633163

Howard, J. D, & Longstaff, T. A. A (1998). Common language for computer security incidents. United States. https:// doi.org/10.2172/751004

Hunsinger, J. & Schrock, A. (2016). Democratization of hacking and construction. New Media and Society, 18 (4), 535-538.Indrajit, R. E., et al., "The Taxonomy of Cyber Threats to National Defense and Security," 2021 Sixth International Conference on Informatics and Computing (ICIC), 2021, pp. 1-8, doi: 10.1109/

Johnson, P. & Robinson, P. (2014), Civic Hackathon: Procurement or Civic Engagement? *Review of Policy Research*, *31*: 349-357. https://doi.org/10.1111/ropr.12074

Kang, D. J., Lee, J. J., Kim, S. J., & Park, J. H. (2009, October). Analysis on cyber threats to SCADA systems. In 2009 *Transmission & Distribution Conference & Exposition: Asia and Pacific* (pp. 1-4). IEEE.

Kaur, S., Kumar, K., Aggarwal, N., & Singh, G. (2021). A Comprehensive Survey of DDoS Defense Solutions in SDN: Taxonomy, Research Challenges, and Future Directions. *Computers & Security*, 102423.https://doi.org/ 10.1016/j.cose.2021.102423

Kjaerland, M. (2005). A Classification of Computer Security Incidents Based on Reported Attack Data. *Journal of Investigative Psychology and Offender Profiling*, *2*(2), 105–120. https://doi.org/10.1002/jip.31 .

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, *25*(7), 522-538.

Kumar, S., & Carley, K. M. (2016, September). Understanding DDoS cyber-attacks using social media analytics. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 231-236). IEEE.

Keleş, A.,R. & Sal, Y. (Edt.)(2013) *Hack kültürü ve hacktivizm.* Alternatif Bilişim

Kelsey, J. T. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review, 106*(7), 1427–1451. https://search.informit.org/doi/10.3316/ agispt.20191230022228

Lough, D. L. (2001). A taxonomy of computer attacks with applications to wireless networks (Doctoral dissertation, Virginia Polytechnic Institute and State University).

Nazario, J. (2008). DDoS attack evolution. *Network Security*, (7), 7-10.

Losh, E. (2012). Hacktivism and the humanities: Programming protest in the era of the digital university. Gold& Klein (Edt.), Debates in the digital humanities, 161-186. University of Minnesota.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62-73.

Manovich, L. (2002). *The language of new media*. MIT press.

Meyers, C. A, Powers, S. S., & Faissol, D M. (2009). *Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches*. United States. https://doi.org/10.2172/967712.

Mirkovic J. & Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms, *Computer Communication Review*, *34*, (2). https://doi.org/10.1145/997150.997156

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. *International Journal of Comparative and Applied Criminal Justice*, *28*(2), 105-123.

Müller, B.,& Kremer, J. F. (Eds.)(2014). Cyberspace and International Relations. Berlin: Springer. https://doi.org/10.1007/978-3-642-37481-4.

Nazario, J. (2008). DDoS attack evolution. Network Security, (7), 7-10.

Nikolskaia, K. & Minbaleev, A. (2020). Legal Regulation of Incidents Related to DDoS Attacks, 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), p. 53-55, doi: 10.1109/ITQMIS51053. 2020.9322874.

Norris, P. (2001). Digital divide: Civic engagement, information poverty, and the Internet worldwide. Cambridge university press.

O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review*, *16*, 137-160.

Onat, N. (2013). Kamusal Alan ve Sınırları: Hannah Arendt ve Jürgen Habermas'ın Yaklaşımları, İstanbul, Durakistanbul.

Pedersen, I. (2013). *Ready to wear: A rhetoric of wearable computers and reality-shifting media*. Parlor Press LLC.

Riordan, S. (2016). Cyber diplomacy vs. digital diplomacy: a terminological distinction. CPD Blog.

Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge: Cambridge University Press. doi:10.1017/9781316888513

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, *55*(1), 68. https://doi.org/10.1037/0003-066X.55.1.68

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016a). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4* (6).

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016b). Cybercriminals, cyberattacks and cybercrime," *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 2016, pp. 1-9, doi: 10.1109/ICCCF.2016.7740434.

Schäfer, M. S. (2015). Digital public sphere. *The international encyclopedia of political communication*, *1*(7).

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. New media & society, 18(4), 581-599.Selander, L., & Jarvenpaa, S. L. (2016). Digital Action Repertoires and Transforming a Social Movement Organization. *MIS Quarterly*, *40*(2), 331–352. https://www.jstor.org/stable/26628909

Schultz, P. W. (2002). Knowledge, information, and household recycling: Examining the knowledge-deficit model of behavior change. New tools for environmental protection: Education, information, and voluntary measures.

Sherizen, S. (1990). Criminological concepts and research findings relevant for improving computer crime control. *Computers & Security, 9(*3), 215-222.

Shorter, C. R. (2014). Digital Diplomacy in an Era of Rising Social Powers: How New Media Impacted the Practice of Public Diplomacy by Empowering Citizens and Terrorist Organizations (Doctoral dissertation, Webster University, London).

Singh, M. P., & Bhandari, A. (2020). New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. *Computer Communications, 154*, 509-527.https://doi.org/10.1016/j.comcom.2020.02.085

Simmons, C.B., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014, June). AVOIDIT: A cyber attack taxonomy. In 9th Annual Symposium on Information Assurance (ASIA'14) (pp. 2-12).

Sousa, H., Pinto, M. Silva, E.C. (2013). Digital public sphere: weaknesses and challenges.*Comunicação e Sociedade, 23*, pp. 9 – 12

Specht, S.M., & Lee, R.B. (2004). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. PDCS.

Timisi, N. (2003). *Yeni İletişim Teknolojileri ve Demokrasi*. Ankara: Dost Kitabevi Yayınları.

Urbas, G., & Choo, K. K. R. (2008). Resource materials on technology-enabled crime. Australian Institute of Criminology,Technical Bacground Paper no:28

Venkatraman, S. (2008). *The "Darth" side of technology use: Cyberdeviant workplace behaviors*. University of Arkansas.

Yengin, D., & Bayrak, T. (2017). Digital public in social media. *The Turkish Online Journal of Design, Art and Communication, 7* (2), 376-386.

Yu, S. (2014). *Distributed denial of service attack and defense.* Springer.

Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing (pp. 380-388).

Zizek, S. (2013). *Tehlikeli rüyalar görme yılı* (M. Öznur ve B. Özkul, Çev.). İstanbul: Encore Yayınları.