Abstract
The purpose of this article is to develop policy proposals for political parties in order to create a Cyber Politics Vision Document (SPVD) on the cyber domain, which encompasses every area of our lives and deepens its influence with new technologies such as blockchain technology, the Internet of Things (IoTs), mobile technology, cloud technology and big data. It is difficult for a political party to ignore cyberspace, which is becoming more and more important day by day, to receive the support of digital citizens in general, digital natives in particular, or the Z generation. Naturally, when developing cyber-related policies, a political party should prioritize positive security based on a rights-based understanding that targets a free and safe cyberspace. This study provides a design for the structure, scope and theoretical framework of a cyber-politics vision / strategy document within the framework of this approach.

Key words: Cyber Politics Vision Document, Political parties, Cybersecurity, Freedom, and Positive Security.

Introduction
Cyber technology has begun to influence, shape and transform every aspect of our lives in recent years. Information and Communication Technologies (ICT) has provided and continues...
to provide comfort and convenience to our lives in all areas from communication, commerce, transportation, entertainment, education to politics. The day does not pass so that ICT will not provide a new convenience to our lives. This process has both accelerated and is spreading rapidly at the global level along with cloud technology, big data, mobile technologies, blockchain technology and the Internet of Things (IoTs). However, in addition to all these comfort, convenience and advantages, cyber technologies have brought new risks and threats to our lives. Unauthorized access, identity theft, online human rights violations, electronic surveillance and intelligence, attacks on critical social infrastructures, and cybersecurity issues are among them.

The internet, which was established as a communication and information network with a transparent structure, faced the cybersecurity problem with the development of Morris Worm, which was accepted as the first harmful malware in 1988 (Jajoo, 2018: 1). Cyber security is broadly defined as the protecting the confidentiality, integrity and accessibility of computer systems, networks, hardware and software, and most importantly data / information (Nweke, 2017: 1-2).

Cyber security is a multi-layered structure consisting of individual security, society security, country security and global security. The weakest link in cybersecurity is the user, the individual (Akyeşilmen, 2018: 91). Cybersecurity, which has become an important component of both national and international policy, stability and security in recent years, has become a high polics issue in international relations (Choucri, 2012: 3).

There are two basic approaches to cybersecurity. One is negative security and the other one is positive security. Negative security is a pure security approach that tries to prevent risks and threats and eliminate cyber attacks, while positive security is not only about eliminating risks and threats, but also envisages to protects other human and moral values, especially personal freedoms along with security (Gjorv, 2012: 835-838).

Cyberspace, which deepens its place in our lives day by day, affects security, education, trade and communication as well as political processes and events in many ways. This technology,

6 The goals of cybersecurity are described in the literature with a formula commonly known as the CIA and 3A model. While the CIA model corresponds for confidentiality, integrity and availability the 3A model stands for authentication, authorization and accountability.
which directly affects social life, naturally deserves to be the subject of political suggestions and to be one of the main agendas of political parties. Today, there is a large audience with 21st century skills, dynamic, knowledgeable and with great voting potential, recognized as digital natives and defined as Generation Z. In order to attract these new generation voters, political parties should pay special attention in their plans and programs to the cyber world, which is an important component of the life of this generation.

Political parties are specific to democracy (Stokes, 1999: 245). In fact, it would not be wrong to say that they are an indispensable element for modern democracies. According to Biezen and Kartz, political “… parties have left such a strong mark on contemporary politics and democracy that parties are so indispensable for the organization of modern democratic institutions and the expression of democratic pluralism, which can best be described as “party democracy ”(2005: one). In this framework, naturally political parties play a very active role in modern democracies. In other words, “A basic claim of democratic theory is that democracy encourages governments to respond to the preferences of the people. Political parties organize politics in every modern democracy and some observers claim that parties are what push democracies to be sensitive ”(Stokes, 1999: 243). Political parties affect not only governments but also the public, they can change their perspective and transform society (Heijden: 187, 2002). The National Democratic Institute (NDI) claims that political parties are intermediary institutions that communicate the demands and needs of the people to governments and continue as follows:

*Citizens have the needs and interests that governments expect to address. In democratic societies, political parties collect these demands from different groups and express public policy options to respond to them. The elections offer voters the opportunity to choose from political parties that offer different proposals to address social needs. Political parties play an intermediary role through efforts to control and influence public policy, connect citizens to their representatives and act as the primary channel to hold the government responsible for its performance. Therefore, the development of party policy - the process of formulating and implementing political parties’ proposals for government actions - is at the heart of the healthy functioning of a representative democracy (NDI, 2013: 1).*

Political parties can find support from the society to the extent that they respond to the demands, interests and needs of the society, express them and reflect them on their policies.
and strategies. New developments, new conditions and new technologies bring with it new social demands, interests and needs. Today, cyber technology and its components have revealed different demands and needs in many different fields at different levels such as from individuals to societies, from countries to international organizations, from security to cooperation in domestic and foreign policy, from trade to education. Especially today, digital immigrants who born before 1995 (Taş, 2014), together with digital natives who have been growing with this technology since their births, with the age of 25 and below, are an important target group for innovative and visionary political movements. One of the methods of influencing and receiving support from this audience depends on the development of a cyber politics vision / strategy documents (CPVD) that targets a safe and free cyberspace and develops policies accordingly.

This article focuses on questions such as, what is a cyber politics vision document (CPVD) in general? Why is the CPVD important and necessary? What are the components of the CPVD and what is its structure? What should the scope of a CPVD be and what should it cover? In this context, this study will first discuss why a cyber politics vision document is needed, and then analyses the basic components of the cyber politics vision / strategy document (CPVD) of political parties. Later on, some social, political and legal suggestions that should be present in an CPVD will be discussed.

Why Do We Need A Cyber-Politics Vision Document?

Political parties should take the path of influencing this new generations, taking into account the cyber technology and its components that affect society in many dimensions. This is both a social necessity and a political investment. Failure or ignoring this fact will make it difficult to understand 21st century society and politics. According to my research for this short study, there is currently no political party in the field of cyber politics that sets a comprehensive policy / strategy in neither advanced nor in developing democracies. Since cyber technology is a dynamic process that develops and transforms very fast, it is difficult to determine precise / absolute and correct / valid principles and policies for every society and time. However, considering the current level of technology and its social impacts and the demands and needs of it, some social policy proposals that political parties should develop in this area are required as of today.
Cyber technology occupies a very important place in the daily life of all of us. Most of our business, entertainment, education and communication activities take place in cyberspace. According to the 2019 Digital report, 59% (4,616 billion people) of world population (internet live stats, 2020) use the internet today, while 67% (5.111 billion people) use mobile phones (Salim, 2019). People spend 6 hours and 42 minutes a day on the Internet. In other words, ignoring an area where 1/4 of our lives and more than 1/3 of our active lives (Salim, 2019) is spent, is not a rational behavior for any social and political movement, especially for a political party. Spending time on the internet differs from country to country. It is possible to claim an inverse equation between the development rate of countries and internet usage. Maybe it is more correct to say a correlation. For example, Philippine spends 10:02 on the internet, Brazil 9:29, Egypt 7:53, Turkey 7,17, Italy 6:04, Canada 5:51, England 5:16, 4:37 in Germany and Japan 3.45 (Salim, 2019). The details can be seen in the table below.

Table-2: Time the Countries Spend on the Internet in a Day


Given the effects of cyber technology on national and international policy and security, it is a fact that political parties need an exclusive cyber politics vision / strategy document. Today,
countries develop a set of documents related to national security that determine the basic national political and security parameters. Among them, the national political strategy documents come first. However, in recent years, the vast majority of the member states of the UN have developed a national strategy document containing all national political and strategic issues, as well as developing exclusive national cybersecurity strategy documents based on the importance of the issue. As shown in the map below, almost the entire world has the document in question, except for a few countries in Africa and Latin America (ITU, 2020). In this context, the statement of the UN International Telecommunication Union (ITU) regarding the necessity and scope of the said documents is as follows:

*In the digital age, modern societies are globally interconnected and increasingly dependent on ICTs and digital infrastructure. However, this interconnectivity also creates interdependencies, and vulnerabilities to emerging threats that need to be managed at the national, regional and international levels. Enhancing cybersecurity and protecting critical information infrastructures is essential to every nation's security and economic well-being – particularly in the global move towards the digital economy and information society. At the national level, cybersecurity is a shared responsibility which requires coordinated action for prevention, preparation, response, and incident recovery on the part of government authorities, the private sector and civil society. For this to operate smoothly and to ensure a safe, secure and resilient digital realm a comprehensive framework or strategy is necessary which has to be developed, implemented and executed in a multi-stakeholder approach. This framework is often referred to as National Cybersecurity Strategy (NCS) – and is a critical element for any country’s socio-economic security. ITU presents members with a reference guide to help countries create an effective national cybersecurity framework. (ITU, 2020).*

Map-1: Countries with National Cybersecurity Strategy Documents
Based on the fact that countries develop an exclusive cybersecurity strategy document, I believe that political parties also need to have an exclusive cyber politics vision / strategy document separate from their programs and election declarations, which will help them establish better dialogue and relationship with a large part of the society. This article was written for this purpose.

This work will be a guide for creating a cyber politics vision document for political parties. As mentioned above, these policies may vary depending on time, place and social needs, but this study aims to design a theoretical framework that covers basic parameters and principles as well as some policy recommendations.

Structure and Scope of the Cyber Politics Vision Document

The cyber politics vision document should adopt a rights-based approach in parallel with but not limited to the components of the International Telecommunication Union (ITU) stipulated in the national cybersecurity strategy documents. In this framework, cybersecurity forms the basis of cyber politics, but here security must be based on a positive security approach that aims to protect all human rights and other universal values, especially freedom together with security.

In this framework, a cyber-politics vision document (CPVD) should consist primarily of an introductory section, then after the vision and the principles, should include legal regulations, capacity building, digital infrastructure education, technical infrastructure and cooperation, as well as human rights and environmental protection. If sections / components of the CPVD are examined one by one, it will be more descriptive and understandable. As mentioned above, after a brief introduction, the vision of the document should be emphasized.

Vision: This section should be composed of a short vision sentence that aims to protect human rights and freedoms and security. For example, our vision is to ensure that “the most effective use of information and communication technologies” (Ministry of Transport, 2015: 9) to ensure the freedom and security and well-being of the individual and the society.
Principles: All individuals, society, private sector and public institutions should undertake their legal and moral responsibilities in order to gain the necessary approach, understanding and perception to users and society in order to create a free and safe cyberspace. Ethical behavior is a guarantee of a free and safe cyber world. In the cyber realm, the user should take care not to do what s/he doesn't like to do to him/herself. In the cyberspace, we must protect and respect not only our own rights, but also the rights of the others.

The basic components of a CPVD need to continue as follows.

Legal Arrangements: One of the basic components of the cyber politics vision / strategy document required for a free and secure cyber world is to make legal arrangements in line with universal legal principles. Legal measures and tools, which are an important component of cyber governance, should not be designed to control the cyberspace envisaged in authoritarian governments, but rather based on a more free and secure cyber world order. The importance of effective cyber / informatics legal arrangements at the national level is more critical since the international level of cyber legal regulations are negligible and the willingness at the international level to cooperate is weak.

Technical Measures: It is especially important to use new technological tools and updated programs for a free and safe cyber world. But more importantly, a vision and a goal must be set for the production and development of hardware and software used in all areas. Otherwise, it is difficult to create a truly free and secure digital space. If a society is aiming for a truly free and secure digital world, it must produce its own hardware and software. At least within this framework, policies and goals should be prioritized.

Capacity Building: Considering that the weakest link in cybersecurity is the user (individual), improving the knowledge and capacity of the individual is vital for cybersecurity and freedom. In order to avoid social engineering attacks, especially caused by user errors, things need to be done:

1. Insertion of cyber education at all stages of the curriculum; and
2. Digital citizenship education should be expanded to reach all segments of the society.
Digital citizenship education is an important tool for a free and safe cyberspace. Since cyber technology, which provides a series of convenience and comfort to our lives, is also very complex, difficult to understand and it also poses a number of new threats. For this reason, “In the cyber era, new skills, knowledge and theories are needed to use cyber tools correctly, useful and effective, and to protect them from threats” (Akyeşilmen, 2018: 143). The way to ensure freedom and security in the cyberspace is possible not only by developing technical knowledge and awareness, but also by a rights-based approach that envisages the moral use of cyber instruments. In this framework, Akyeşilmen's "Right-Based Approach: Ethics Phor Peace Model" (Akyeşilmen, 2018: 158) offers important suggestions. This approach is Equality, Time, Health, Information, Communication, Security, Participation, Human Right, Opportunity, Responsibility, Privacy, Empowerment, Accountability or Transparency, Creativity and Empathy (Akyeşilmen, 2018: 158-167)

Stakeholder Cooperation: Another important issue for a free and secure internet is the cooperation of all local and international stakeholders. Since the Internet is inherently a global network and a multi-stakeholder area, the way to ensure security and freedom in this area is possible with the cooperation of all stakeholders, including users (individuals), private companies, NGOs, governments and international organizations. This cooperation should be in every field, from law and technical fields to education and trade, security and transportation, communication and entertainment. Otherwise, it is quite difficult for any cybersecurity initiative that one or more actors of these will develop on their own.

The last component that forms the CPVD is about policy proposals related to human rights and environmental protection.

Human Rights and Protection of the Environment

One of the main components of a free and secure cyberspace is undoubtedly the protection and advocacy of human rights in cyberspace. The protection of new rights arising from digitalization, such the right to be forgotten and the right to access, should be the main

---

backbone of the political parties' cyber politics vision documents. In this context, some of the regulations to be done considering today's technology and needs are as follows:

- The right to be forgotten,
- The right to access the Internet,
- The right to be anonymous online,
- Implementing cyber surveillance and intelligence within the framework of human rights principles,
- Regulating personal data protection legal regulations in accordance with international law and human rights standards,
- Issuing legal arrangements for the protection of children, youth and mothers, especially women's rights,
- Supporting NGOs operating in the field of fact-checking (checking the accuracy of information) in cyberspace,
- Advocacy for e-participation or cyber democracy, e-democracy or digital direct democracy; and
- Effective use of cyber tools in environmental protection processes and creating an environmentally friendly cyberspace.

This list is not exhausted, it may vary depending on time and space and the needs of societies. Political parties, which can analyze the needs of the society and especially the Z-generation known as digital natives, can create more accurate and more realistic lists according to the needs of the societies they live in.

The paper will briefly discuss and analyze in this section the right to be forgotten from some of the concepts listed above, the right to access the internet, the right to be anonymous online, cyber surveillance and e-democracy.

Right to be forgotten: New domain, new situations emerged and rights violations may occur as access to the Internet and dissemination of information becomes easier. The right to be forgotten is accepted as one of these new situations and new rights. The right to be forgotten is the right to demand that some (unwanted) information about the person not to be indexed in search engines and deleted from websites. In other words, the person has a say in when, how and how much of the information about himself/herself can be published (Article 19, 2016: 1; European Commission, 2020).
The right to be forgotten is a phenomenon that affects many rights and freedoms with the spread of the Internet, especially the right to protect personal data and private life. One way to eradicate these rights violations is to put it under legal protection. This is only possible with the recognition of the right to be forgotten in national and international human rights instruments. This claim has been the subject of many court cases in democratic countries in recent years. Some countries such as France, Germany, Norway, England, Portugal, Spain, Canada, Israel, Japan and New Zealand have coded the right to be forgotten in domestic law (Acosta, et al. 2017: 1-59). In the cyberspace, partly, to protect personal data and to provide legal status to the right to be forgotten is one of the important tools to guarantee the rights and freedoms of the person. In this context, some measures have been taken at some national level in some regions, but it has not been possible to talk about an arrangement at the global level despite some weak attempts. In countries where the right to be forgotten is not yet included in the national legal texts, political parties should include it in their CPVD.

Right to Access to the Internet: The right to access the Internet has also been an important topic of discussion in the international human rights literature in recent years. As the Internet's role and power in social life increased, governments and companies tried to control it and manipulate it in line with their interest. They often even blocked access to the Internet. The internet, which has begun to shape every area of life and increases this effect day by day, affects not only access to information and sharing but also goods production, prosperity and development. In this respect, it affects the life of the individual and the society in every aspect. Therefore, access to the Internet has become vital for individuals and society.

In this age, it is almost impossible to be deprived of such an effective tool, to realize one's own life and to live a life with human dignity. For this reason, many lawyers, analysts and academics suggest that the internet is recognized as a human right, considering its role in our lives and relationship with other human rights (Berners-lee and Harpin, 2020; Amnesty International, 2020; Estes, 2011). In the report submitted by the Special Rapporteur of the UN Freedom of Opinion and Freedom of Expression to the General Assembly on 11 May 2011, Frank La Rue not only defines access to the Internet as a right, but also describes the obligation of member states to provide access to the Internet: “The rapporteur reminds all States of their right to freedom of expression and their obligations to promote or facilitate the means to exercise this right, including the Internet ”(UN, 2011: 18). For this reason, the report
of the UN special rapporteur is an important step in this direction, although it is not yet included in a human rights regulation at the global level. The political parties playing a leading role in this path will be playing an important role for both freedoms of expression and access to internet.

Right to Be Anonymous Online: Another important discussion about human rights in cyberspace is the right to be anonymous online. Online anonymity and encryption method are important tools for privacy and freedom of expression. Anonymity is a right that can be used for both good and bad purposes. It can be a tool for freedom of expression in the cyberspace or it can be a way to interfere with someone else's rights. But since freedom is the substance and prioritized in human rights, recognition of this right is essential. Limitation should be considered as an exception.

The right to be anonymous plays an important function in the context of freedom of expression. It provides a vital protection to individuals to express different thoughts and express themselves without fear, especially in repressive regimes. But governments are looking for ways to restrict or even ban anonymity and encryption for different reasons. In recent years, they have provided a consensus from international NGOs and academic circles that anonymity and encryption are part of the right to freedom of expression and privacy, and should be legally assured. In this context, Article19 emphasizes that states should regulate anonymity as a component of freedom of expression in their domestic law, recognize anonymous speech, anonymous reading and anonymous search, and abolish regulations on social media platforms and states (if any) regarding real-name registration (Artic19, 2015: 1-3; Kim, 2010: 52-55). The right to anonymity should be regulated as a right, unless used as a means to attack someone else's name and reputation, violation of personal rights, insult and hate speech/crime. This right is not absolute and should be limited to court orders, not administrative mechanisms in cases of violations.

Cyber Surveillance and Human Rights: It has been a phenomenon throughout the human history to gather intelligence by people, private actors and governments for different purposes and with different methods. Intelligence through cyber surveillance is special information about people obtained through the use of cyber technology. According to the Encyclopedic Dictionary of Public Administration (2020), “Cyber surveillance is a mechanism for the surveillance of individuals, objects or processes. It is based on new technologies and is run on
data networks such as the Internet. Its purpose is to speed up surveillance in accordance with the amount, speed or complexity of the data”. Cyber surveillance is an inevitable reality today and is carried out both by private actors and governments legally or illegally, in accordance with laws and sometimes in violation of human rights.

Digital citizens, especially digital natives known as Z generation, use the internet very actively. They use social media for different purposes such as socialization, entertainment, acquiring and sharing information, and status (Kibby & Fulton, 2015: 1). While it can be easily monitored on social media, sometimes it can be obtained through illegal methods in the form of intervention in the communication of persons or by banding legal ways. It is essential for cyber surveillance and intelligence to be structured within the framework of human rights principles in order to ensure that law operates more effectively and justice, as well as protecting personal data and guaranteeing human rights and freedoms. Otherwise, it is not possible to create a free and safe cyberspace. In this context, the Electronic Frontier Foundation (EFF) has identified 13 principles that are interrelated, interconnected and part of a whole, with the participation of different stakeholders of cyberspace. These principles envisage cyber surveillance / intelligence to be carried out within the framework of human rights and legal principles. These are legality, legitimate purpose, necessity, competence, proportionality, competent judicial authority, legal process, informing the user, transparency, democratic control, integrity of communication and systems, international cooperation and measures against unauthorized access (EFF, 2014). Cyber surveillance and intelligence must be carried out according to human rights principles and law requirements. Political parties can only get the support of digital citizens if they prioritize this important issue in their cyber politics vision documents.

E-Democracy or Direct Participation: It was realized in the practice of Greek City states, one of the first democracy practices known in history, with the participation of the people directly in decision-making processes. This practice is called direct democracy in the literature. Direct democracy includes “all the rules, institutions and processes that enable a proposed constitutional amendment, law, agreement or political decisions to be submitted to the direct approval of the people” (Bulmer, 2017: 3).

Democratic practices have been referred to in different forms and with different names for centuries. In essence, democracy or direct democracy associated with participation has
evolved into representative democracy due to constraints such as population growth and geography throughout history (Mattila, 2017: 30). Today, more than 500 definitions of democracy are mentioned in the literature. Gagnon and his colleagues even suggest the 507 theory of democracy (Gagnon, et al., 2014). Whether representative democracy is democratic today is widely discussed in the literature. Therefore, many theses have been developed on the crises of representative democracy today (Noé, 2018: 1-2).

In today’s digitalized world, defined as the age of information and communication, cyber technology offers humanity great opportunities to re-direct democracy. If a more free and secure internet is provided, the opportunity for all affected citizens to be involved in the direct decision-making processes will have arisen. E-democracy is in fact “an important factor in increasing the quality of democracy by increasing participation in political processes with an understanding of [government] sensitivity to the demands of citizens” (Afşar, 2019: 1101). The important thing here is that the supporters of representative democracy, according to some, are suspicious of democracy in this practice. At this point, Ateş claimed that the grounds that legitimate representative democracy do not exist anymore;

However, the possibilities offered by technology today greatly erode all the grounds that justify representative democracy. Today, millions of people can come together on social media networks, discuss many issues and reach a conclusion. The breadth of geography and the large population are no longer the challenges that legitimize representative democracy. People can gather in a virtual environment even if they are not physically. The necessity of choosing a representative imposed by numerical multitude or long distances has been greatly eroded today (Ateş, 2016: 172).

Whichever of the political parties supports such change and transformation, which envisages direct involvement of the people in democratic processes, having a say in their decisions and the division of democratic power to all, will attract the votes of the people, particularly of digital citizens or netizens.

Conclusion

As cyber technology evolves, more and more objects are connected to the Internet and more and more they are penetrating our lives. Today, cyberspace has become a natural part of our lives. In this period called the information and communication era, human beings have to shape and design every area of life according to this new environment. It is difficult for any social and political formation that cannot keep up with change to continue its existence. In
this context, it is vital to redesign political life in this framework and to transform it to respond new situations emerged and to meet new needs. Within the framework of the analysis above, it is possible to highlight some important outcomes below.

As emphasized before, it is observed that the world community and a large number of peoples on the basis of countries use the Internet both actively and intensely (on average 6 hours and 42 minutes a day). It is vitally important for political parties to give importance to a topic that is so much involved in social life, and to produce vision / strategy documents by developing policies in this regard.

Having a cyber-politics vision document will be of great advantage comparing to other political parties in order to get the support of the digital natives known as the Z generation and the generation Y known as the digital immigrants who use the internet.

Cyber politics vision documents should naturally be security and freedom - centered which is one of the basic needs of the individual and society. In this framework, a positive security approach that prioritizes freedom and cybersecurity need to be adopted.

The cyber politics vision documents should primarily include newly emerged human with the rise of digitization such as the right to be forgotten, the right to access the internet and the right to be online anonymous, and traditional rights such as the protection of personal data, the protection of the environment, the protection of women, youth and family, and it also should include new participatory issues such as e-democracy.

Finally, political parties, that want to continue their existence strongly, need public support and are the most important, active and dynamic actors of political life, need to transform and redesign themselves according to this new climate.

References


https://www.amnestyusa.org/is-internet-access-a-human-right/[Erişim tarihi: 10.07.2020].

Article19.(2015). Right to Online anonymity.

https://www.article19.org/data/files/The_right_to_be_forgetten_A5_EHH_HYPERLINKS.pdf [Erişim tarihi: 10.07.2020].


https://ecpr.eu/Filestore/PaperProposal/3402a19c-2e82-4b30-bf30-6a423927d5b0.pdf [Erişim Tarihi: 21.06.2020].


