Digital democracy in Peril. Safeguarding e-democracy by boosting cybersecurity

Claudiu Mihai CODREANU,
National University of Political Studies and Public Administration, Bucharest, Romania

cl.codreanu@gmail.com

Abstract

New technological developments and the digitalization of public life were not long ago thought to lay the foundation to a new step for liberal democracies all over the world, with the prospects of e-democracy and e-government. However, state-sponsored cyber operations held back progress in boosting e-democracy, and so did online disinformation campaigns, leading to a change in perception that digital technology will actually be detrimental to liberal democracies. Moreover, major illiberal and authoritarian state actors exploited cyberspace and engaged in using and exporting digital authoritarianism. The main objective of this paper is exploring the close relationship between e-democracy and cybersecurity, arguing that without sound cybersecurity policies and practices, digital democracy is in peril. Furthermore, I shall discuss the role of the state in cyberspace, focusing on the European Union, and argue for a set of cybersecurity policies that enhance the level of security while also safeguarding the values and gains of e-democracy, taking into account relevant literature on this topic and also EU's 2020 cybersecurity strategy. Current research and strategic documents suggest three main courses of action for enhancing e-democracy in a safe way in a cyberspace dominated by malicious activities: developing a sort of 'digital autonomy', securing critical infrastructure and maintaining a free and open Internet. The main contribution of this paper is facilitating the discussion on the relationship between e-democracy and cybersecurity, because as close as they are, as little they are linked together in relevant research. Furthermore, this paper should be relevant both for civil practitioners in the fields of public administration and cybersecurity and for academia, as it focuses on an issue that has become to be of utmost importance for liberal democracies. The final argument of the paper is that the whole digital democratic process should be considered critical infrastructure and shielded by proper cybersecurity measures.

***Keywords**: digital democracy, e-democracy, cybersecurity, cyberattacks, European Union.*

1. Introduction

In 2016, the US presidential elections were disrupted by a major campaign of information operations and cyberattacks attributed to the Russian Federation [27], one year later two cyberattacks showed the world how serious the cyber threat is: UK's hospitals had their activity disrupted by a global ransomware (the 'WannaCry' cyber campaign attributed to North Korea) [22] and Ukraine was the victim of the world's costliest cyberattack, 'NotPetya', which produced billions of dollars in damage worldwide, affecting transnational companies too [15]. One year before the cyber operations against US elections, Russian state-sponsored hackers already caused a serious disruption in Ukraine, launching a cyberattack against its electrical grid which caused a six-hour blackout for over two hundred thousand people [27]. This global context does not seem to be appropriate for moving parts of the democratic process online, and it also does not seem to be a proper environment for developing e-democracy on a widescale.

The Internet, or cyberspace more generally, is looking far worse than the cyber-utopian dreams and hopes of the 1990s and 2000s [3], and it looks like digital authoritarianism is actually becoming more popular and common than digital democracy [26]. Nonetheless, this does not mean that liberal democracies should abandon hopes regarding e-democracy, just that the process is actually way more difficult than the cyber-utopia dreams of the 1990s, and hence it should aim at boosting cybersecurity and also protect democracy at the same time – enhancing e-democracy should go hand in hand with consolidating cybersecurity. The answer to authoritarian and malicious attacks on democracies and democratic processes should not be authoritarianism, but actually more democracy.

In this paper, I shall discuss the relation between e-democracy and cybersecurity, beginning the study with the current state of e-democracy and e-government initiatives and with the cybersecurity context. The research will later focus on the European Union, because it is starting to become an important actor in cyberspace, and also because some of its member-states are already major actors in cyberspace. My argument is that e-democracy and cybersecurity should be enhanced and consolidated at the same time, because leaving digital affairs as they are enables tremendous opportunities for malicious cyber operations and so it lowers trust in e-democracy and in 'regular' democracy. In order to do this, I shall take into consideration relevant literature on e-democracy and cybersecurity, and also EU's 2020 cybersecurity strategy, which puts an emphasis on protecting democratic freedoms in cyberspace. Moreover, throughout this paper, I shall be using e-democracy, digital democracy and cyber democracy interchangeably, for convenience (even though it is not consensually accepted that the three names define the same exact concept in the same way). Moreover, I shall consider e-government as part of e-democracy and as a form of digital participation and digital relations between the public and governments.

2. E-democracy – the Internet to the rescue of democratic participation

2.1. Democracy and liberal democracy

According to Robert A. Dahl (1998), democracy, or the democratic process, is based on five key standards: effective participation (all members must have effective and equal opportunities for expressing themselves and making their opinions on public policies known by other members), inclusion of all adults, voting equality (all votes counted as equal, and every member must have the right to effectively vote), control of the agenda (all members must have the opportunity to choose and decide what should be on the public agenda) and enlightened understanding (all members must have effective and equal opportunities of obtaining information about public policies within reasonable limits) [6].

Thus, democracy guarantees its citizens essential rights, a broad range of personal freedom, self-determination, the opportunity to exercise the freedom of self-determination to a great extent, moral autonomy, providing human development and prosperity and political equality [6]. Moreover, it is assumed that liberal democracies are peace-seeking and do not engage in wars against each other, and also that democracy prevents tyranny and autocracy [6]. In addition to this, most of the countries with a high-level of democracy are represented by a particular form of democracy – liberal democracy, a type of democracy based on representation and an elected government (and hence on elections), where the constitution, the legislature, rule of law, political freedoms and individual rights (e.g., freedom of speech, of assembly, property or religion) are essential [16].

2.2. E-democracy, e-government, e-participation

The Internet has been seen as a mean to raise the level of democracy worldwide and deepen it, consolidating the relationship between citizens and between citizens and governments. The 1990s, at the beginning of the World Wide Web, are illustrative for this idea, with the technological and Internet counterculture promoting a utopian 'Internet revolution'. In the 2000s, hopes were that the Internet will facilitate public deliberation on a scale unthinkable before, closing the gap between and citizens and governments and reducing the gaps and divides within societies. Moreover, in the early 2010s the Internet became a space where social movements formed, grew, and coordinated online and offline actions (e.g., the Occupy or anti-austerity movements worldwide, the Arab Spring etc.), leading to renewed hope that the Internet will generate a radical transformation of democracies, for the better. [3]

According to David F. J. Campbell and Elias G. Carayannis (2018), cyber democracy "is connected to democracy by building and by forming IT-based infrastructures and public spaces" [4]. In addition to this, cyber-democracy, given the characteristics of cyberspace, is also understood as "transcending the boundaries of the nation state, as such adding to the building of transnational, in fact global public space", and hence public spaces in cyberspace have multiple levels (global, national and subnational) [4].

E-democracy, or digital/cyber democracy can be described mainly by the operation of democratic processes through digital means (or ICT), whether it refers to political communication through social media or government websites and platforms or to e-participation through government initiatives or informal platforms. E-democracy refers predominantly to the concepts of participatory democracy, direct democracy or deliberative democracy, as it focuses more on public discussions and deliberations and a more direct public involvement in the decision-making process, even though most progress was achieved only in the 'obtaining information' dimension of e-democracy. Moreover, e-democracy consists both of passive forms of participation, such as governments making documents and information accessible and transparent, and of active forms of participation, such as online voting processes (e.g., voting for local projects) or platforms for public consultation. However, the emergence of digital means has not led to a transformation of liberal democracies, where political participation is still fundamentally done through representation and parliamentarism, and hence the primarily form of participation of the people (or demos) is realised by voting during elections at different levels or during referendums. [20; 21]

However, despite previous hopes that the Internet will enhance democracy, the events of the last two decades have led to the believe that the Internet will actually increase support for populism, increase inequality and that online deliberation will be nothing than superficial. For instance, social media is, unfortunately, a double-edged sword for democracies, while it can provide a more inclusive involvement of citizens in public deliberations, it can also be a mean for malicious activities, such as disinformation campaigns. [21]

E-voting (online voting), e-petitions and various platforms, portals and forums for citizens to engage with their representatives or to discuss among themselves were tried along the years, but their success varied. Nevertheless, these initiatives did not lead to the expected massive renewal of public participation in political processes and not even to a dramatic reform of democracies. Two of the greatest hurdles for massive and effective online public participation are anonymity and distance, which embolden chaotic and uncivil discussions, and also efforts of maliciously influence public opinion. For the most part, e-democracy has only meant traditional democracy done in virtual interconnected spaces so far, without major and radical changes, furtherly maintaining the political status-quo. Moreover, even social movements fuelled by online participation, action and coordination were done outside institutionalised e-democracy platforms. [3]

Despite these rather grim conclusions, it does not mean that academia, democracy activists and governments should abandon hopes regarding digital democracy, just that these drawbacks need to be closely studied and addressed, in order to find a way forward. For the better or the worse, the Internet and all of its platforms will still be around in the foreseeable future, so we should strive to make the best of it and return to the hopes of the last decades that cyberspace will actually improve liberal democracies and that its ability to cross frontiers will promote and uphold democracy all over the world.

Nonetheless, digital technologies have expanded citizens’ opportunities to get more involved in political and civic life, such as expressing themselves freely on the Internet, associating, or by holding public authorities accountable. There are also many important positive outcomes of the widespread use of digital technologies, such as uncovering human rights abuses perpetrated in various countries and making them known worldwide. [25]

The Internet’s potential to become a tool of boosting democracies relies on its egalitarian nature and openness. Thus, liberal democracies should ensure that people have the ability to express themselves freely in cyberspace and also to continue sharing information regardless of borders and hold accountable leaders, in order to counter digital authoritarianism. Furthermore, upholding and boosting Internet freedom should be a fundamental element of democracy assistance programs. [14]

3. Cybersecurity and the role of governments

According to Thierry Balzacq and Myriam Dunn-Cavelty (2016), cybersecurity is “a type of security that enfolds in and through cyberspace, so that the making and practice of cybersecurity is at all times constrained and enabled by this environment” [2]. Cybersecurity is a collective endeavour in a society, being established by governments, international organisations, private companies, civil society and also by private users of digital devices and equipment [2]. Thus, cybersecurity can be understood as “a multifaceted set of practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access”, representing all practices and activities that actors take to secure cyberspace [2].

The central responsibility of the state is to secure its own networks, whether civil or military, against cyber threats and vulnerabilities and against cyber operations, and hence the state operates as a ‘guarantor and protector’ of central state institutions. Moreover, the state is also a ‘legislator and regulator’ regarding cyberspace and digital technologies, formulating and implementing policies in these areas. In addition to this, the state also acts as a ‘partner’ to public and private companies when it comes to protecting critical infrastructures, as producing and ensuring cybersecurity in the area of critical infrastructures is a joint effort that requires close cooperation with other actors. [9]

Regarding cyberspace and cybersecurity, the state can be seen as a ‘security guarantor’, ‘legislator and regulator’ or ‘security partner’ [9]. The role of the state is that of ‘owner” of networks’, ‘problem solver’, meaning that it must address and solve issues related to cybersecurity, and also of ‘originator of the problem’, as the state also creates security gaps in the networks of cyberspace [9].

In some cases, governments implement policies that indirectly reduce the level of cybersecurity globally, even for the same state-actor that enacts said policies, by maliciously and tacitly exploiting vulnerabilities detected in commonly used software or hardware, producing weaknesses inside systems or networks. For instance, governments are actively trying through actions and regulations to exploit and prevent the use of encryption, which can be a hurdle to ensuring cybersecurity and national security, but by doing this they also affect adversely the exercise of individual rights and human rights, as encryption is crucial to protecting personal data and online user security. However, the global network that comprises cyberspace should be secured for all users, no matter their citizenship or borders. Introducing weakness, 'backdoors' and exploiting vulnerabilities in networks and systems means that cyberspace would be made less secure in the quest of enhancing cybersecurity and ensure national security, but those vulnerabilities can be exploited by malicious state and non-state actors and so leaving them there creates opportunities for cyberattacks, which means that such actions eventually reduce the level of cybersecurity in the long-run. [7]

Intelligence services exploit and create security gaps in software in order to ensure and facilitate infiltration in various locations of the Internet infrastructure. These non-public access points, backdoors and implants can be activated whenever the government that placed them wants, as long as the victim does not detect them, and they serve multiple purposes, such as cyber espionage, surveillance or infiltration points for disruptive cyberattacks. Thus, in a quest for enhancing their own national security and cybersecurity, state actors become responsible for producing vulnerabilities and threats for the same national security they are trying to protect, as this access points can be exploited by other intelligence agencies or other actors against the same government that produced them or against other state-actors. [9]

In contrast to this, a human-centric approach to cybersecurity would place as primary objects of security human beings, regardless of citizenship and borders. State-actors would still be key to producing cybersecurity, but their main objectives would be aimed at protecting human rights, personal freedoms and wellbeing in cyberspace, promoting the integrity of cyberspace worldwide. [7]

4. The state of e-democracy and e-government in the European Union

The EU and its member-states are among global leaders in e-government progress, Internet freedom and cybersecurity levels. Among the first 30 countries ranked by the United Nations (UN) E-Government Development Index 2020, 15 of them are EU member-states. Moreover, only three EU countries rank lower than 50 – Croatia, Hungary and Romania [33]. Furthermore, the 2020 Global Cybersecurity Index, published by the International Telecommunications Union (ITU) measures and scores states' cybersecurity policies and measures. Half of the first 30 countries ranked by the ITU are EU member-states, with Estonia, Spain, Lithuania and France placed in the top 10 countries of the world regarding cybersecurity measures implemented [18]. Finally, the 2021 Freedom of the Net report published by the Freedom House shows that all of the EU member-states taken into consideration by the study have a free Internet [14]. However, the only EU countries mentioned in the report are Estonia, France, Germany, Hungary and Italy.

E-democracy can be considered as a possible answer to EU's democratic deficit but also to democratic limitations at national and local levels. Several EU member-states have initiated e-participation mechanisms on a national or local level (e-initiatives, e-petitions, e-consultations etc.), but most of these online deliberation platforms lacked where it mattered the most – they had a small impact on decision making. However, introducing such projects on an EU-level is particularly challenging, because regardless of general problems encountered by nation-states, the EU must also address the issues of transnationality, language diversity and large population. [19]

According to the European Commission, the EU is working on the development of cross-border digital public services, based on the idea that e-government can increase the levels of efficiency and transparency for governments, but also foster a greater participation of citizens in political life [10]. One issue regarding the pursuit of building or enhancing e-democracy in the European Union is the disputed existence of a 'EU demos' or a 'European constituency', as it is more challenging for a transnational body like the EU to refer to a public than for a traditional state-actor [17]. Moreover, L Hennen (2021) suggests in a study that online political communication is not expected to build a supranational public sphere [17].

In a study published in 2021 by the European Commission, the authors evaluated the overall e-government maturity scores of the EU and of its member states, ranging from 0% to 100%. EU's overall performance was determined to be only 68%, whilst the most well-evaluated member-states scored over 85% - Malta, Estonia, Denmark and Finland. The leading states have been described as having the most transparent, user-centric digital governments, which are also the most technologically enabled and open to users from other EU member-states. [34]

According to Eurostat, EU's statistical office, almost half of people in the European Union aged 16-74 have obtained information from public authorities' websites during 2020. Denmark, Finland and the Netherlands recorded the highest share of people that accessed information online from public authorities (over 80%), whilst Italy, Bulgaria and Romania rank lowest in the study, having less than 20% of their populations obtaining information online from public authorities (in Romania the share was only 10%). [13]

5. Securing both democracy and e-democracy through strengthening cybersecurity

5.1. Cyber threats against democratic processes and e-democracy

All things considered, when implementing tools and platforms of e-democracy and e-government, institutions must also pay attention to the security risks involved, pertaining both citizens and governments. The first issue is that of privacy, as online public services require and use citizens' data, and in many cases, this is not done in a transparent and well-regulated way. Moreover, e-government and e-democracy mechanisms, as everything digital, have vulnerabilities that can be exploited by malicious cyberattacks for various purposes, whether the attack is about obtaining private information of citizens, disrupting public services or generally undermining democratic processes such as elections. [32]

Elections worldwide, and especially in liberal democracies, have been prime targets of cyberattacks and information operations, and despite measures taken by governments, their infrastructure is still vulnerable to further malicious digital activities. One of the possibilities of cyberattacking democratic processes is targeting the electoral systems either by hacking into the voting process or into the databases with registered voters, although there are no major reports of such events. In the US, the Department of Homeland Security underlined that election systems and the voting process are part of state's critical infrastructure, and hence making it a top priority for cybersecurity endeavours. [23; 29]

Interference in free and fair elections is becoming an increasing threat against democratic countries as authoritarian states intensify the usage of cyberattacks targeting elections. There are several ways in which cyber operations can influence elections: undermining public confidence in state institutions or in the voting process, manipulating public opinion or influencing it to vote for or against particular parties through a mix of cyberattacks and information operations. In addition to this, malicious actors could also interfere in a more direct way with the voting process, such as hacking online components of voting or voter registration mechanisms or by changing the results, the latter being the most difficult to do, especially on a wider scale. Nevertheless, malicious cyber operations are not only serious threats to elections or democratic processes, as they can also materialise as threats to the physical security of individuals or states. For example, Russia has been using both cyber operations and disruptive cyberattacks alongside information operations in its hybrid war against Ukraine. [23; 25]

One of the most serious and well-known examples of foreign interference in elections by cyber means is the Russian interference during the 2016 US presidential elections. Russia used both cyberattacks and information operations in an effort to influence the elections. Russian state-hackers managed to launch a successful cyber operation against the Democratic National Committee and the campaign of the Democratic Party candidate Hillary Clinton, gaining access to private data, and then using the data and information obtained in disinformation campaigns organised on social media. [27; 35]

A couple of years earlier, Russian state-sponsored hackers managed to infiltrate Ukraine's central election commission during the 2014 presidential elections, the first after the Euromaidan. During the cyberattack, the hackers managed to implant a malware in the election commission's software that would have modified the results of the elections so that a small ultra-nationalist party (Right Sector) would be shown as winners, even though the party managed to get less than 1%. Moscow acted by the same playbook, doubling the cyber campaign by a disinformation campaign. More than this, even though the Ukrainian government had actually detected the malware one hour before announcing the results, Russian state media still reported the doctored results. However, this serious cyber operation was by far one of the less-damaging Russian cyberattacks that Ukraine has suffered. For example, in December 2015, a sophisticated and complex cyberattack targeted Ukraine's electrical grid, leading to a blackout for over 200.000 residents a day before Christmas. [27]

In addition to this, the Kremlin launched other cyber operations and disinformation campaigns in efforts to influence and undermine elections in liberal democracies, targeting the 2017 French presidential elections and then-candidate Emmanuel Macron's campaign and also the Catalan independence referendum in Spain [27].

Online voting is particularly vulnerable to cyberattacks, especially when compared to traditional paper-based voting. No matter how much it can be secured, it is likely that hackers, whether state-sponsored or not, will find a way to infiltrate and penetrate its digital infrastructure and networks. Elections and online voting systems are prominent targets of complex cyber operations given their importance, and hence taking into consideration that cybersecurity can never be completely perfect and bulletproof, moving large parts of the voting process online poses a great security risk for governments [24]. Thus, classic alternatives such as paper-based voting is less vulnerable than electronic/online voting [24]. Furthermore, Park et al. (2021) point out that introducing new digital technologies in the voting process would not make online voting more secure, their conclusion being that even blockchain-based voting systems (an idea that gained popularity both in academia and among governments) are still vulnerable to serious cyber threats [24].

5.2. Digital authoritarianism

Abuse of digital technologies and malicious usage of them varies from cyber espionage, disinformation campaigns, surveillance, cyberattacks to foreign actors interfering in other states' elections. Moreover, authoritarian states have started over the last decade to fragment the global Internet in order to have control of the information flow that occurs in their 'national' part of cyberspace, and even more concerning is that authoritarian states which expanded their authoritarian rule online (e.g., Russia, China, Iran or Saudi Arabia) have also started exporting their tools of digital authoritarianism to illiberal governments and other like-minded regimes. [26]

Both China and Russia underscored their sovereignty in cyberspace and prioritized the strategic engagement both in cyber operations and information operations, whether defensive or offensive. The two countries relate to cyberspace and the information space as being closely interconnected, and act in accordance to this. According to Freedom House, during 2020 global internet freedom declined once again, for the 11th consecutive year, online freedom of expression being the main target of governments worldwide. [14; 30]

5.3. EU's approach to cybersecurity and promoting democracy online

The EU started to focus on the issue of cybersecurity after the 2007 cyberattacks against Estonia and in 2013 the European Commission published the first Cybersecurity Strategy of the EU and the proposal of the NIS Directive. Since then, the European Network and Information Security Agency (ENISA), established in 2004, has been playing a key role in enhancing and safeguarding EU's cybersecurity. Moreover, since the early 2010s the European Union has promoted the idea of upholding a multi-stakeholder governance model of the cyberspace for a free and open Internet. [8]

According to EU's 2020 cybersecurity strategy, cybersecurity is referred to as an integral and essential part of Europeans' security. Moreover, the strategy highlights from the beginning that the EU's democracy, society and economy rely on secure and reliable digital tools and on connectivity and also that democratic processes depend more and more on increasingly interconnected network and information systems, which makes cybersecurity essential. In addition to this, threats on the democratic process emerging from the area of cybersecurity are mentioned in the strategy, such as disinformation campaigns and cyberattacks on democratic institutions, economic processes and infrastructure. [12]

EU's 2020 cybersecurity strategy sets forth three main instruments to address cybersecurity issues: promoting and consolidating resilience, technological sovereignty and leadership; building the necessary operational capacity to prevent, deter and respond to cyber threats; and advancing a global and open cyberspace both at an international and EU-level. The document stresses on the objective that cybersecurity must become an integral part of all digital investments, innovations and processes developed in the EU, especially in those related to technologies like quantum computing, encryption and Artificial Intelligence (AI). Furthermore, an essential element of the European Democracy Action Plan is strengthening the cybersecurity and the cyber resilience of democratic processes and institutions of the EU and its member states. [12]

For the EU, as stated in its cybersecurity strategy, international cooperation is a core component of the endeavour of maintaining and promoting a secure, stable, global and open cyberspace. Moreover, the European Union should work together with its international partners to advance a rather liberal and democratic political model of cyberspace, as its vision of cyberspace is based on human rights, fundamental freedoms, the rule of law and democratic values. Additionally, the EU aims to continue cyber capacity building in its neighbourhood, especially in the Western Balkans, assisting governments in addressing and overcoming malicious cyber operations that target and damage their societies and the security and integrity of their democratic systems. [12]

For example, the European Commission highlights that digital transition should, at the same time, uphold an open and democratic society, while also protect people from various cyber threats, such as ransomware or hacking [11].

In this context, Brussels started to act more against cyber threats, underlining through its actions that malicious state-sponsored cyberattacks against EU member-states will not be left without consequences. In 2020, the EU imposed its first-ever sanctions in relation to several major cyberattacks used by China and Russia, naming persons involved in the hackings and also publicly identifying several hackers as being officers of Russian intelligence agencies. In May 2021, the restrictive measures against cyberattacks have been prolonged for another year, the sanctions applying to four entities and eight individuals. [5]

Furthermore, a concept proposed and promoted by the EU and some of its member-states is 'digital sovereignty', a so-called 'Third Way' separating the EU from the US and China's approaches to the digital space – the libertarian 'Californian' view of the Internet in the United States (in which companies are allowed by governments to make decisions with important social and economic implications) and the robust digital authoritarianism implemented and promoted by China (in which the state has an almost-complete control of cyberspace and the digital technologies sector). 'Digital sovereignty', a concept mentioned several times by the leaders of France and Germany, especially by the French President Emanuel Macron, refers to the objectives that the European Union will develop a form of self-determination regarding cyberspace and digital technologies, in the way that the EU and its member-states should uphold control over data storage, data processing and over ITC infrastructures. [1; 14; 30; 31]

Digital sovereignty refers to the idea that governments should enhance their authority over the cyberspace, promoting the consolidation of the state's role (alongside with its economy and citizens) in the development and governance of digital technologies and infrastructures [26]. One of the main concerns of the EU and its member states in this regard is the possible interference of foreign states (such as China) in the upcoming widespread rollout of 5G networks. The issue is that the rollout could involve Chinese state-controlled companies (e.g., Huawei), which could lead to a less secure and more vulnerable critical infrastructure.

5.4. A way forward – boosting both cybersecurity and (e-)democracy

In the next years, democratic internet governance has the potential to play a key role both in protecting democracies from abuses of digital technologies, but also for boosting cybersecurity. Thus, liberal democracies should concentrate their efforts to protect democratic processes across the globe, enhancing the cybersecurity of democratic processes, especially of elections. Another key move would be to declare election systems/infrastructures as critical infrastructure, like the policy of the United States. Moreover, liberal democracies should strive to protect and also promote the protection of human rights in cyberspace internationally, while also advocating for an open and democratic internet governance (like the EU and some of its member-states are doing), taking into consideration that the traditional libertarian or 'Californian' way of promoting relations between governments and ITC companies is not likely to still be appropriate and efficient in the current global context, both online and offline. [25]

One possible response and countermeasure against the expansion of digital authoritarianism worldwide is the promotion of a free, open and democratic Internet and of a secure digital communication internationally. Similar to ideas and objectives mentioned in the EU's 2020 cybersecurity strategy, liberal democracies should promote and maintain Internet freedom and refrain from diminishing online privacy and liberties in the quest of counterbalancing digital authoritarianism or other abuses of digital technologies. One of the most important objectives should be strengthening policies regarding encryption, essential both to citizens of liberal democracies and especially to citizens of authoritarian countries. [36]

In order to address threats to major democratic processes which are increasingly relying on digital means, governments should act fast and prioritize their protection and their 'place' in national security policies. Democratic processes (especially elections which nowadays rely more on digital technologies) should be recognised and declared as critical infrastructure in order to ensure a more consolidated protection against cyber threats. Furthermore, the 2020 cybersecurity strategy of the European Union is a great example of how liberal democracies should develop policies regarding cybersecurity, as cybersecurity should not be enhanced whilst democracy, individual freedoms and human rights deteriorated, but on the contrary – cybersecurity should be strengthened alongside the promotion and consolidation of democratic processes, and this policy should also be promoted internationally.

Liberal democracies and their governments should focus more on protecting the democratic and egalitarian potential of the Internet, one of the qualities that could enable a widescale adoption of e-democracy. Focus should be put on protecting and enlarging current policies and initiatives regarding e-democracy and also consolidating public participation in political processes, while also promoting and protecting both on a national and international level individual freedoms and human rights online (e.g., online privacy or the right to encryption). In parallel, cybersecurity policies and practices should go hand in hand with protecting and deepening democracy. Nevertheless, in order to develop e-democracy, governments should also take into consideration and seriously address cyber threats. The more democratic processes move (even partially) in cyberspace, the more vulnerabilities are created, which also means there will be more opportunities for malicious cyber operations, and hence cybersecurity should be a core element of every policy, programme, initiative or activity of anything digital done by governments, whether it is about e-democracy, e-government platforms or political parties campaigning on social media during elections.

6. Conclusion

Despite all of the negative events that occurred in cyberspace or enabled by digital technologies, the project of e-democracy should not be abandoned. It is far from over and it is far too early to simply assume that digital authoritarianism 'conquered' cyberspace and there is no place left for cyber democracy. Liberal democracies should boost their efforts to promote democracy worldwide, both in the offline world and online, and to develop e-democracy in order to achieve greater and meaningful political participation. Regardless of how much e-democracy or e-government is developed, cyber operations will still target liberal democracies, whether they are cyberattacks on electrical grids, spreading ransomware on private users' computers or interfering with political processes.

Nonetheless, without sound cybersecurity policies, cyberspace, alongside digital technologies, social media etc., can actually weaken liberal democracies and enable authoritarian regimes and/or digital authoritarianism. Further developing e-democracy requires proper cybersecurity policies and practices, and also 'regular' democracy requires an enhanced level of cybersecurity in order to avoid threats from malicious actors. Moreover, as this topic is increasingly dynamic and complex, it also needs a tremendous amount of research in order to fully understand it, and for governments of liberal democracies to implement the most efficient policies. For instance, further research could be made on studying other cybersecurity strategies of important actors in cyberspace (such as the US) and also on the current worldwide state of e-democracy, especially in liberal democracies.

References

[1] Baezner, M., Robin, P. (2018), *Cyber Sovereignty*, Research Collection, ETH Zurich.

[2] Balzacq, T., Dunn Cavelty, M. (2016), *A theory of actor-network for cyber-security*, European Journal of International Security, vol. 1, no. 2, pp. 176-198.

[3] Bastick, Z. (2017), *Digital limits of government: The failure of e-democracy*, in A. A. Paulin, L. G. Anthopoulos, C. G. Reddick (eds), Beyond Bureaucracy: Towards sustainable governance informatisation, pp. 3-14, Springer, Cham.

[4] Council of the EU (2021), *Cyber-attacks: Council prolongs framework for sanctions for another year*, European Council – Council of the European Union, https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/ (Accessed 4 December 2021).

[5] Dahl, R. A. (1998), *On Democracy*, Yale University Press, New Haven & London.

[6] David F. J. C., Carayannis, E. G. (2018), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, Springer, Cham.

[7] Deibert, R. J. (2018), *Toward a human-centric approach to cybersecurity*, Ethics & International Affairs, vol. 32, no. 4, pp. 411-424.

[8] Dunn Cavelty, M. (2018). *Europe's cyber-power*. European Politics and Society, vol. 19 no. 3, pp. 304-320.

[9] Dunn Cavelty, M., Egloff F. J. (2019), "The politics of cybersecurity: Balancing different roles of the state", *St. Antony's International Review* vol. 15, no. 1, pp. 37-57.

[10] European Commission (2021), *eGovernment and digital pubic services*, Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/egovernment (Accessed 4 December 2021).

[11] European Commission (2021), *Shaping Europe's digital future*, A Europe fit for the digital age. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en (Accessed 4 December 2021).

[12] European Commission. (2020), *The EU's Cybersecurity Strategy for the Digital Decade*, Joint communication to the European Parliament and the Council. Brussels, 16.12.2020 JOIN (2020) 18 final, Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

[13] Eurostat (2021), *Even more citizens get government information online*, Eurostat, March 6, https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/edn-20210306-1 (Accessed 4 December 2021).

[14] Freedom House (2021), *Freedom on the Net 2021: The Global Drive to Control Big Tech*. Available at: https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

[15] Greenberg, A. (2018), *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, August 22, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Accessed 4 December 2021).

[16] Hague, R., Harrop, M. and Breslin, S. (2001), *Comparative politics and government: an introduction*, Palgrave Macmillan, New York.

[17] Hennen, L. (2021), *E-Democracy and the European Public Sphere*, in N. Kersting and K. Mossberger (eds.), European E-Democracy in Practice, pp. 47-92. Springer, Cham.

[18] International Telecommunications Union (2021), *Global Cybersecurity Index: 2020*, International Telecommunication Union, Available at: https://www.itu.int/pub/D-STR-GCI.01-2021.

[19] Korthagen, I., van Keulen, I., Hennen, L., Aichholzer, G., Rose, G., Lindner, R., Goos, K., Nielsen, R. O. (2018), *Prospects for e-democracy in Europe*, European Parliamentary Research Service, Brussels.

[20] Lidén, G. (2015), *Technology and democracy: validity in measurements of e-democracy*", *Democratization* vol. 22, no. 4, pp. 698-713.

[21] Lindner, R., Aichholzer, G. (2021), E-*Democracy: Conceptual Foundations and Recent Trends*, in N. Kersting and K. Mossberger (eds.), European E-Democracy in Practice, pp. 11-46. Springer, Cham.

[22] Newman, L. H. (2017), *Why Governments Won't Let Go of Secret Software Bugs*, Wired, May 16, https://www.wired.com/2017/05/governments-wont-let-go-secret-software-bugs/ (Accessed 4 December 2021).

[23] Nye, J. S. (2019), *Protecting Democracy in an Era of Cyber Information War*, Belfer Center Paper, Harvard Kennedy School – Belfer Center for Science and International Affairs.

[24] Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021), *Going from bad to worse: from internet voting to blockchain voting,* Journal of Cybersecurity, vol. 7, no. 1.

[25] Piccone, T. (2017), *Democracy and Cybersecurity*, Brookings, Policy Brief.

[26] Pohle, J., & Thiel, T. (2020), *Digital sovereignty*, Internet Policy Review, vol. 9, no. 4.

[27] Polyakova, A., Spencer, P. B. (2018), *The future of political warfare: Russia, the West, and the coming age of global digital competition*, The New Geopolitics: Europe, Foreign Policy at Brookings. Available at: https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/.

[28] Robertson, J., Mehrotra, K., Gallagher, R. (2021), *China's Microsoft Hack, Russia's SolarWinds Attack Threaten to Overwhelm U.S.*, Bloomberg, March 9, https://www.bloomberg.com/news/articles/2021-03-09/microsoft-solarwinds-breaches-spark-two-front-war-on-hackers (Accessed 4 December 2021)

[29] Rosenbach, E., & Mansted, K. (2018), *Can democracy survive in the information age?,* Belfer Centre for Science and International Affairs.

[30] Rosenberger, L. (2020), *Making Cyberspace Safe for Democracy*, Foreign Affairs, May/June 2020, https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy (Accessed 4 December 2020).

[31] Schneider, I. (2020), *Democratic Governance of Digital Platforms and Artificial Intelligence?. Exploring Governance Models of China, the US, the EU and Mexico*, JeDEM-eJournal of eDemocracy and Open Government, vol. 12, no. 1, pp. 1-24.

[32] Sgueo, G. (2020), *Digital democracy: Is the future of civic engagement online?*, European Parliamentary Research Service, Brussels.

[33] United Nations Department of Economic and Social Affairs (2021). *E-Government Development Index, 2020*, Data Center, https://publicadministration.un.org/egovkb/en-us/data-center (Accessed 4 December 2021).

[34] Van der Linden, N., Enzerink, S., Dogger, J., Regeczi, D., Geilleit, R., Cipponeri, S., Firth, E., Claps, M., Balla, A., Noci, G., Benedetti, M., Marchiop, G., Gaeta, M. (2021), *eGovernment Benchmark 2021 Insight Report,* Publications Office of the European Union, Luxembourg.

[35] Whyte, C. (2020). Cyb*er conflict or democracy "hacked"? How cyber operations enhance information warfare*, Journal of Cybersecurity, vol. 6, no. 1.

[36] Yayboke, E., & Brannen, S. (2020), *Promote and Build: A Strategic Approach to Digital Authoritarianism*, CSIS Briefs.