OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 13, Nº. 1 (May-October 2022)

JANUS.NET
e-journal of International Relations

PROTECTION OF DEMOCRATIC PROCESSES AND ELECTORAL ACTS FROM RUSSIAN DIGITAL ACTIVE MEASURES: 2016 AS A REFERENCE YEAR

RICARDO SILVESTRE
ricsilvestre@hotmail.com
PhD in Philosophy from the University of Connecticut, with a major in Human Physiology, and an MA in International Relations from the Lusófona University of Humanities and Technology in Lisbon, with a focus on the future of online political debate. International Officer of the think tank Social Liberal Movement (Portugal). Coordinator of political communication projects with the European Liberal Forum, the think tank of the Alliance of Liberals and Democrats for Europe party in the European Parliament. His main interests in the area of political research are: the future of democracy, digital solutions to societal problems, and the transition and energy independence of the European Union with its associated reduction of the security dilemma towards authoritarian and illiberal countries.

Abstract

Russia has been credibly accused of trying to weaken Western liberal democracies with use of digital means. Cybersecurity experts, intelligence agencies, investigative journalists, and government services, have detailed the Kremlin's actions in illegally accessing digital infrastructures, disseminating stolen contents online, and influencing political debate on digital platforms to create dissention and polarization. These initiatives are included in a wider strategy of altering the balance of power in the international order via what are known as 'active measures'. Two of the most consequential recent application of this kind of measures took place in 2016, in the United States Presidential Elections and in the Brexit Referendum. Reports made public with the assessments of errors committed by the United States and the United Kingdom governments show there was an insufficient protection of those two crucial public consultation processes. The mistakes made by these countries in protecting democracy from hostile agents with a high level of digital proficiency, should be a point of interest, and urgency, for the European Union. It is to be expected that this kind of influence operation will continue, and become more sophisticated, as they can target elections in Member States of the Union, but also for the European Parliament. The early detection, applying of countermeasures, and the sharing of information with the voters of this kind of attacks by foreign agencies is an important defense mechanism that needs to be strengthen and expanded.

Keywords

Democracy; intelligence agencies; digital platforms; Russian Federation; European Union

How to cite this article

Silvestre, Ricardo (2022). *Protection of democratic processes and electoral acts from Russian digital active measures: 2016 as a reference year*. In Janus.net, e-journal of international relations. Vol13, Nº. 1, May-October 2022. Consulted [online] on the date of the last visit, https://doi.org/10.26619/1647-7251.13.1.2

Article received on May 11, 2021 and accepted for publication on March 3, 2022

PROTECTION OF DEMOCRATIC PROCESSES AND ELECTORAL ACTS FROM RUSSIAN DIGITAL ACTIVE MEASURES: 2016 AS A REFERENCE YEAR[1]

RICARDO SILVESTRE

Introduction

The Kremlin has been trying to weaken western liberal democracies considered by the establishment, and by President Putin, as threats to the Russian Federation[2]. Cybersecurity experts, intelligence agencies, legislative bodies, and investigative journalists, have detailed some of Moscow's initiatives to meddle in democratic processes. Examples include Georgia, Estonia, Lithuania, Ukraine, Netherlands, France, Germany (Tennis, 2020). Russian's behavior, as seen through Robert Jervis' theory of the "four worlds", has an internal logic: the preference for offensive actions to tilt the balance of power in the international order (Jervis, 1978). Also, the decision of not assuming defensive postures could be seen as a response to political and social perceptions of threats coming from the borders to the west (Rato, 2018). Such concerns leads to a maximization of power, instead of cooperation (Baylis, Smith & Owens, 2019). In an anarchic international system, states seek their survival by weakening adversaries. One example is the creation of disrupting actions in those countries (Mearsheimer, 2001). One of these disruptions is the targeting of democratic systems, elections and organizations with digital tools. An analysis of cyber enabled incidents between 2014 and 2018 (Galante & Ee, 2018) show that these could be; exploitation of infrastructures via access to computer networks with collection or alteration of datum; manipulation of votes from voter registration, changing of vote counting or of casted votes in order to cause distrust of electoral results; dissemination of information obtained illegally with compromising materials for politicians or political parties; "false fronts" with counterfeit profiles of individuals and groups, mainly on social networks, with the intention of causing polarization; amplification of dissension with open or covert operations; production and spreading of false information and misinformation.

Two of the most consequential, and even striking, actions by Russia in interfering on democratic processes took place during 2016, in the United States Presidential Election and the United Kingdom European Union Membership Referendum. Getting back to the

[1] Article translated by Cláudia Tavares.
[2] To better understand the motivations of President Putin it is suggested the reading of "*The Man Without a Face. The unlikely rise of Vladimir Putin*", from Masha Gessen.

theories of Jervis and Mearsheimer, these actions can be seen as resulting from a calculation by the Kremlin of risks and benefits of said actions. The risks were further antagonizing the international community, with the possibility of sanctions and proportional responses. As for benefits, contributing to the breakdown of a neighboring economic and political bloc, and helping to defeat a candidate for President of the United States that was manifestly opposed to the regime in Moscow in favor of other clearly more friendly, if not eager to acquiesce to the Russian President intentions. The results were obviously positive for the Kremlin. The United Kingdom left the European Union, with internal divisions that could lead to the disaggregation of the Kingdom. In the United States, the Trump Administration alienated allies, tried to diminish the importance of the North Atlantic Treaty Organization (NATO), even threatening America's exit from the organization, privileged Russian interests in the Middle East, and placed the United States in economic and diplomatic "wars", that diminished the country's status in the international community. The European Union was also a target of these actions in some of its Member States, that lead to the implementation of measures to combat misinformation, false news, cyber-attacks, disruption and polarization operations. The Vice-President of the European Commission for the Digital Single Market said in 2019 that "[w]e must protect our free and fair elections. This is the cornerstone of our democracy. To secure our democratic processes from manipulation or malicious cyber activities by private interests or third countries" (ENISA, 2019).

Research goals and methods

The objectives of this paper is to produce a systematized body of knowledge, by describing how Russian digital active are being deployed in western liberal democracies with the intent of causing dissention, and disruption. Equally, solutions will be proposed on how better fight these threats. The methodology used is a qualitative research strategy, with the collection of information with the aim of developing a meaning associated with said activities and responses (Unikaitė-Jakuntavičienė & Rakutienė, 2013). This strategy allows for the creation of a constructivist narrative, which aims to develop a theory in a deductive way, starting with specific facts, empirical observation and advancing to a theoretical generalization of the facts related to the theory. Likewise, a qualitative scientific investigation will be applied, with the analysis of the behavior of the different agents involved in the construction of the theory, as well as values, beliefs and emotions. This will be done through observation, analysis of speeches, documents and opinions from governmental and civil society organizations and news articles. The research logic is thus inductive, with a starting point of cognition of reality, flexible concepts and analytical generalizations with the help of examples (Unikaitė-Jakuntavičienė & Rakutienė, 2013).

Literature review

The Russian Federation and "active measures"

The term active measures was developed in the Soviet Union, beginning in the 1950s, to characterize secret and subversive operations of political influence which are easily

refutable. They can range from creation of front organizations, support for pro-Russian political groups and the spread of disinformation (Galeotti, 2019). In 1982, the then leader of the State Security Committee (KGB), Yuri Andropov, made active measures one of the Kremlin's main forms of intervention during the Cold War (Andrew & Mitrokhin, 2006: 316). The use of these measures slowed down when the Soviet Union changed their approach to the international community, first led by Gorbachev, and then by Yeltsin, with attempts to have a closer relationship with the west. With the loss of influence of Russia and with the rise of Vladimir Putin to power, Moscow returned to hostilities towards countries, and blocks of countries, that promote liberal and democratic values. These values can then reach Russia and the countries at its frontiers. This was the case of the 2012 protests in Russia for free elections, which Putin explained as an American influence operation (Crowley & Ioffe, 2016), or in the case of the "color revolutions" on its borders (Stewart, 2009). Added to this concern, are the debilitating economic sanctions for primary sectors of the Russian economy, blockade to the sale of arms and related materials, freezing of economic assets and of the acquisition of equipment for the oil industry (Krausse, 2018). And then there is NATO, and in particular Article 5º of the organization charter, where an attack to one of the members is an attack on all (OTAN, 1949). This causes an attractive prospect for countries that Russia thinks as part of its sphere of influence. All these factors increase the perception by Putin of a siege around him (Rato, 2018).

With the decrease in the expectations of east-west understandings, Moscow returned to the array of actions already known, adding to recent ones carried out in the "near abroad" countries (Galeotti, 2019). Recently, in 2013, General Valery Gerasimov, Chief of Staff of the Russian Army, advocated the use of "indirect and asymmetric methods" to create political influence (Bartles, 2016: 33). This includes, changing the balance of power in adversarial countries (Bartles, 2016: 34), and support of political parties that defend a friendly relation with Moscow, as observed in Italy and Germany (Apuzzo & Satarino, 2019), and in France (Turchi, 2017). It is also attributed to Gerasimov the proposal that the tactics developed during the time of the Soviet Union should be updated and included in strategic military thinking, for a "new theory of modern warfare—one that looks more like hacking an enemy's society than attacking it head-on" (McKew, 2017). Strategic measures advocated by the General include combinations of technological, informational, diplomatic, and military actions (Galeotti, 2013). In September 2014, General Philip Breedlove, during a meeting of NATO, warned that Russia was engaged in "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare" (Vandiver, 2014).

Among the main Russian organizations, in terms of creating and applying active measures to intrude into the democratic processes of foreign countries, intelligence agencies stand out. The best-known examples are: the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, or GRU[3]; Federal Security Service of the Russian Federation, or FSB[4]; and the Foreign Intelligence Service of the Russian Federation, or SVR[5]. The Kremlin's administrative apparatus is characterized by being a

[3] *Glavnoje Razvedyvatel'noje Upravlenije*, in the original.
[4] *Federal'naya sluzhba bezopasnosti*, in the original.
[5] *Sluzhba Vneshney Razvedki*, in the original.

"non-institutionalized" system with a high level of coordination between agencies for the application of active measures (Galeotti, 2017). They then report directly to the Kremlin and/or President Putin (DNI, 2017). From there, three known forms of interference in elections are known: directed by the State with actions carried out by operatives in their capacity as representatives of the regime; encouraged by the State, where operatives are not directly responsible for initiating active measures, but whoever is responsible does so with the knowledge that it will be welcomed by leadership; and those aligned with the state, where individuals and/or organizations act for the promotion of the regime policies (Galante & Ee, 2018). As an extension of the intelligence agencies there are also private institutions, under the control of oligarchs in the orbit of Putin, that act to advance pro-Russian narratives, by creating polarization in the public opinion of targeted countries. That is the case of the Internet Research Agency (IRA), based in St. Petersburg, which will be presented in more detail ahead. These different "attack fronts" create a "connective tissue" of organizations that work towards the same goal (Watts, 2018), in the unconventional modern warfare model suggested by Gerasimov. These kinds of actions, its origins and applications, have been described extensively in reports made public by western intelligence agencies. Some of these examples will now be presented.

The United Kingdom European Union membership referendum

Before the 2014 referendum on the future of the relationship between the United Kingdom and the European Union (Brexit), another referendum happened on the possible independence of Scotland from the Kingdom. In that democratic process, Russian-based operatives were detected intruding in the public consultation (Carrell, 2017). Through Twitter, Facebook and YouTube, fake accounts spread allegations of interference in the referendum to bolster the maintenance of Scotland in the Union. Despite the absence of a direct link to Moscow, "pro-Kremlin accounts demonstrably boosted those allegations. The anger and disappointment felt by many yes voters [was] fanned by pro-Kremlin trolls, in a manner characteristic of Russian influence operations" (Carrell, 2017). The prospect of a desegregation of the United Kingdom matches to the aims of the Kremlin of destabilization of western bloc of countries, and a weakening of adversaries both in the military and political arena. The exit of Scotland of the Kingdom poses a challenge to the national security and economical prowess for all countries involved. A diminution of Great Britain's standing in the world leads to less advantageous trade deals, since Scotland accounts for one-third of the land mass and around 8% of consumers. Equally, a break-up of the Kingdom would lead to military questions. An exit of Scotland of the Union could "unilaterally disarm the UK of its nuclear deterrent", since those defences are "currently located at Faslane and Coulport but an independent SNP government would require their removal from Scotland" (Daisley, 2020). It should be added that Nicola Sturgeon, who assumed the position of Prime Minister after the referendum, denied that such influences had existed in the public consultation, and the Electoral Commission, which as the authority for holding elections and referenda, guaranteed that it had found no evidence of fraud. The same was assured, post-Brexit, by the Office of the Prime Minister Theresa May's, assuring there was no evidence to support the conclusion that

the referendum in the United Kingdom and the European Union relationship was targeted for interference by foreign governments (Syal, 2017).

However, evidence that Her Majesty's Government could have underestimated, or worse, minimized possible active measures during the Brexit referendum prompted the request for an assessment of the actions taken by institutions responsible for the protection of democracy in the Kingdom. After what was considered to be a excessive delay for the publication of the assessment, and accusations of attempts to minimize the importance of his contents by the Office of the Prime Minister Boris Johnson (Murphy, 2020), the Intelligence and Security Committee of Parliament published the report named "Russia" (ISCP, 2020). This Commission supervises the activity of intelligence agencies; the Security Services (MI5), the Secret Intelligence Service (MI6) and Government Communications Headquarters, or GCHQ. One of the justifications for the report production states that "[t]here has been credible open source commentary suggesting that Russia undertook influence campaigns in relation to the Scottish independence referendum in 2014" (ISCP, 2020: 13). Regarding the referendum in the relation between the United Kingdom and the European Union, "[t]he written evidence provided to us appeared to suggest that HMG [Her Majesty's Government] had not seen or sought evidence of successful interference in UK democratic processes or any activity that has had a material impact on an election, for example influencing results" (ISCP, 2020: 13). Going further, the Commission states that "[w]e have not been provided with any post-referendum assessment of Russian attempts at interference. This situation is in stark contrast to the US handling of allegations of Russian interference in the 2016 presidential election" (ISCP, 2020: 14). The Commission determined that Her Majesty's Government seriously underestimated the Russian threat and neglected countermeasures, therefore not protecting the referendum process (ISCP, 2020a).

In the report it is described that the Russian Federation tends to see foreign policy as a "zero-sum", where every action detrimental to the west is favorable to Moscow. This stems from an appreciation "fed by paranoia, believing that Western institutions such as NATO and the EU have a far more aggressive posture towards [Russia] it than they do in reality" (ISCP, 2020: 1). The decision center "is concentrated on Putin and a small group of trusted and secretive advisers (many of whom share Putin's background in the RIS [Russian intelligence services])" (ISCP, 2020: 29) causing those decisions to have an applicability and flexibility that western organizations cannot match. Mainly, and as assessed by the GCHQ, Russia has a high capacity in the digital area and is able to carry out cyber operations with a wide range of impacts in various sectors of society.

Since 2014, the Russian Federation has "carried out malicious cyber activity in order to assert itself aggressively in a number of spheres, including attempting to influence the democratic elections of other countries (…) GCHQ has also advised that Russian GRU actors have orchestrated phishing[6] attempts against Government departments" (ISCP, 2020: 5), something that was observed in the United Kingdom, Germany and the Netherlands (Silvestre, 2019). In fact, on the third of October 2018, the Minister of Foreign Affairs, at the time lead by Jeremy Hunt of the Conservative Party, publicly announced that the United Kingdom and its allies had identified a GRU campaign that are

[6] The act of *phishing* is the sending of fraudulent emails to induce users to share personal datum, such as passwords.

"reckless and indiscriminate: they try to undermine and interfere in elections in other countries" (NCSC, 2018).

Regarding proposals to fight the threats observed during the referendum, the Parliamentary Commission expressed that the "extreme care" by the intelligence agencies to get involved in democratic processes is "illogical". Interference in electoral acts by hostile countries should be seen as a priority regarding protection of the State and that this should be the responsibility of intelligence agencies (in particular, the MI5) (ISCP, 2020: 11). Another important recommendation in the report is that the Government should establish protocols with social media platforms to ensure that they detect active measures by hostile actors, with a clearly defined time for the removal of such contents. As legislative recommendations, the Digital, Culture, Media and Sport Select Committee asked the Government to assess whether current legislation to protect the electoral process from malign influence is sufficient and, that "[l]egislation should be in line with the latest technological developments" (DCMS, 2019: 71). They also propose that the Electoral Commission should have the power to "to intervene or stop someone acting illegally in a campaign if they live outside the UK" (DCMS, 2019).

The elections for the American Presidency

In February 2018 the then Special Counsel Robert Mueller delivered *de facto* evidence to a federal grand jury in the District of Columbia, which resulted in the indictment of thirteen Russian individuals and three Russian organizations for interfering in the 2016 American presidential election (USDJ, 2018). The indictment shows the scope, and the systematic nature of the attacks, which began in 2014. Particularly active was the company Internet Research Agency (IRA), with its *troll* farms[7]. By stealing American's identities, creating false accounts on social media platforms, and disseminating inflammatory content, both racial and social, IRA tried to cause disruption and political polarization. This company operations were not limited to remote actions from Saint Petersburg, but also in cooperation with members of the Trump campaign "on the ground" (USDJ, 2018: 4). Using fake profiles on Facebook and Twitter, IRA members organized rallies and meetings in the United States, via local campaign headquarters, and bought online advertisements to promote those rallies and meetings (USDJ, 2018: 21-28).

Like the Special Counsel Mueller, the US Senate Select Committee on Intelligence was also clear in its conclusions: Russian operatives, through the IRA, used digital social media platforms to conduct informational war campaigns, spreading disinformation and creating division in the United States (SSCI, 2019: 3). These campaigns were carried out under the direction of the Kremlin, and with the objective of reducing the chances of success of candidate Hillary Clinton in favor of candidate Trump (SSCI, 2019: 4), since the former was seen as more hostile to Russian interests (SSCI, 2019: 6). Although Moscow rejects the US Senate's conclusions, IRA owner Yevgeniy Prigozhin has direct links to President Putin, which points to a "Kremlin's direction, support and significant authorization in the operations and objectives of IRA" (SSCI, 2019: 5). Like the IRA, the

[7] A troll farm is group of internet users aiming interfere in the political discussion online with (mostly) nefarious purposes.

GRU was also accused of exploiting social media platforms to spread information obtained illegally. This was done by disseminating Clinton campaign e-mails, information that was obtained by the Units 26165 and 74455 inside GRU (USDJ, 2018a). In fact, Special Counsel Mueller charged Colonel Aleksandr Osadchuk, commander of Unit 74455, for assisting "in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU" (USDJ, 2018a: 5). In a joint statement by the Department of Homeland Security and the Director of National Intelligence (DHS, 2016) it was announced that the American intelligence community was confident that the Russian government had interfered in the elections through the misuse of emails obtained illegally from American political organizations. To this end, they used the help of external organizations, mainly WikiLeaks and Guccifer 2.0, the second being another front for Russian military intelligence services (Sanger & Schmitt, 2016). The American intelligence agencies that contributed to this investigation included the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Security Agency (NSA). Naturally, the degree of trust between the agencies in the results of the analytical processes was not uniform. However, most conclusions are presented with a "high degree of confidence" (DNI, 2017).

Regarding the use of social media platforms by Russian agents, Facebook confirmed to the Special Committee that activity attributable to the Fancy Bear group (Unit 26165 of GRU) was observed (Graff, 2018). Like the IRA, Fancy Bear also created fake profiles on the platform and through the organization DCLeaks to distribute information obtained illegally to journalists (Stretch, 2018). In the 2017 minority report from the US House of Representatives Permanent Select Committee on Intelligence (authored by Democratic Party members), with the results of an investigation into Facebook about disruption and polarization in the 2016 election, IRA actions included the purchase of 3,393 political ads, and creation of 470 Facebook pages that reached 126 million users (HSCI, 2017). On the other social media platform "giant" where there is a dynamic political debate, Twitter, between September first and November fifteen of 2016, more than 36,000 tweets about the presidential election were generated by *bots*[8] linked to Russian accounts. These tweets generated about 228 million interactions[9]. In addition, more than 130.000 tweets were from accounts directly linked to IRA (HSCI, 2017).

Active measures implemented by Russia are not a recent phenomenon. The KGB was responsible for authoring and disseminating false stories, as well as fraudulent letters, targeting Presidents John Kennedy and Ronald Reagan, and the activist Martin Luther King, Jr. (SSCI, 2019: 11). However, in the 2016 election, this type of action was refined by the use of social media platforms, with a special focus on suppression the vote, especially of the black community (SSCI, 2019: 39), promoting political narratives, namely, to entice the followers of Senator Bernie Sanders (Timberg & Harris, 2018); and targeting the coalition supporting the Secretary of State Clinton (Kim, 2018).

[8] A *bot* is an autonomous program that interacts with digital systems and users.
[9] Interactions include actions from users like retweets, replies, follows, inclusion of hashtags and tweet expansion.

Protecting democracy in the European Union from digital cyber-attacks

In the reports presented above, there is the concern on how to protect democratic processes and electoral acts from active measures by intelligence agencies from hostile countries. In the digital age, and in line with Thomas Jefferson edict that "eternal vigilance is the price of freedom" (TJM, 2020), it`s the European Union's job not to underestimate what happened in the United States and the United Kingdom. The Member States of the European Union, together with the European Parliament and the European Union Agency for Cibersecurity (ENISA), organized an exercise in 2019 to "test the EU's response and crisis plans for potential cybersecurity incidents affecting the EU elections" (ENISA, 2019). This exercise aimed to increase cooperation between national authorities in the areas of cybersecurity, data protection and cybercrime. In addition to working "on the ground", ENISA also produces practical documents to ensure security in electoral processes. For the European Commission, the objectives are to protect democratic systems in Member States but also to safeguard European values (European Commission, 2020). There is a set of instruments that exist already with similar objectives, including the Action Plan on disinformation[10], the European Democracy Action Plan[11], the European cooperation network on elections[12], the Compendium on Cyber Security of Election Technology[13], the EU Cybersecurity Act [14], the Revised Directive on Security of Network and Information Systems (NIS2)[15], as well as instruments to combat hybrid threats[16] and boost cybersecurity[17].

However, there is a visible absence in the protection systems in the European Union, be it through inaction, or due to a lack of communication to the citizens of the Union: what is the ability to collect information and analyze threats to democratic processes by hostile intelligence agencies? This applies both in elections whiten the Member States (if agreed upon them), and those for the European Parliament. Presently, there is the EU Intelligence and Situation Centre (INTCEN)[18] that has the mission of creating timely alerts for menaces, and assessing threats in the areas of security, defense and counterterrorism. This work is carried via the collection of information in collaboration with the agencies in the Member States, military authorities, and diplomats (Estevens, 2020). The inclusion of INTCEN in a wider and more integrated defense strategy is recommended, serving as an advanced system for signal detection, both from open source, digital means or through human resources. The assignment of this mission would be the responsibility of the European Commission: via a resolution with clear definitions about information handling and sharing between agencies in Member States; types of

10 https://ec.europa.eu/info/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en.
11 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250.
12 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.
13 https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf.
14 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
15 https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2.
16 https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123.
17 https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193.
18 https://eeas.europa.eu/sites/default/files/2021_-_01_-_02_-_eeas_2.0_orgchart.pdf.

rapid responses development and application; relationship with legislators both in the European Parliament and in the local governments; and with voters, when possible or advisable. Naturally, actions from intelligence agencies in detecting threats and applying countermeasures to defend electoral processes, sometimes, cannot be in the public domain. There is a need to find a balance between protection of sources and processes, and what threats can be shared with voters, so that they are informed and can make political decisions without malicious external influences.

Another growing demand, by organizations such as the European Commission, the US Senate Select Committee on Intelligence, and the Intelligence and Security Committee of the UK Parliament, is that social media platforms change their policies for a greater joint work with authorities, including intelligence agencies and legislative bodies. This joint work must include a timely and comprehensive sharing of information, mainly of malicious activities that exploit the digital architecture of the platforms, manipulation of algorithms, and dissemination of content for subversion of electoral processes. The Digital Services Act (DSA), proposed by the European Commission and accepted by the European Parliament does address some of these needs. In the DSA, internet providers of intermediary services need to produce transparency reports with information on interaction with authorities, description of illegal content, time taken for removal of content, actions taken and legal justifications (European Commission, 2020a). If bad actors or active measures are detected, intelligence agencies must be able to act in a precise and timely manner in collaboration with digital platforms for the application of appropriate measures. This process must be coordinated by overseeing governmental structures, and, if necessary, legislative bodies whenever there is a need for changes in laws to resolve structural problems. Likewise, there should be a joint work with political parties and/or candidates for governmental positions. Successful examples of such collaboration have taken place in France and the United Kingdom. In France, the Agence Nationale de la Sécurité des Systèmes d'Information, the agency responsible for protecting government infrastructures from cyber-attacks, organized cybersecurity information sessions for all political parties (although not everyone shown an interest in participating) (Daniels, 2017). In the United Kingdom, it was the turn of the Britain's National Cyber Security Centre, part of GCHQ, to offer help in strengthening the communication networks of political parties (Reuters, 2017).

Conclusions

A provocative question raised by Persily is "Can Democracy Survive the Internet?" (Persily, 2017). Some authors warn of the naivete of thinking that the internet is way to a utopia of debate, understanding and consensus, in a Madisonian perspective of governance[19]. At the same time, even more powerful digital tools, like personal data retrieving, big data, machine learning, algorithmic function, can open the space for companies, that are for hire, to generate political advertising targeted at the individual level, creating "digital bubbles", "echo chambers" that leads to political polarization and counterproductive political action.

[19] Some of these warnings can be found in books written by Timothy Garth Ash, Rebecca MacKinnon, Cass Sustein, Clay Shirky e Evgeny Morozov.

The US Senate Select Committee on Intelligence warns that active measures, having the Kremlin as an epicenter, and with an alleged direct connection to Vladimir Putin, "represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order" (SSCI, 2019: 11). It is worrying that countries with established democracies, sophisticated intelligence agencies, a free press and a vibrant civil society, such as the United Kingdom and the United States, did not realized, or ignored, the threats of the Russian Federation in disrupting the electoral processes of 2016. In the report of the Intelligence and Security Committee of Parliament, there is a disturbing warning that the United Kingdom government was in a "state of denial" about Russian influence, so as not to question the legitimacy of the executive associated with the outcome of Brexit (Ellehuus & Ruy, 2020). That was not exclusive of Whitehall. In the United States, President Trump spent part of his mandate denying, or minimizing, Russia's actions in the 2016 elections, even clashing with American intelligence agencies over whether Putin had authorized any of them. In fact, Trump would fire, in 2017, FBI Director James Comey because of, in the President's words, "Russia issue". This would result in the appointment of Special Attorney Robert Mueller and the impeachment process of the President (Balsamo, 2019). Still in the Parliament report, another important observation was lack of definition inside the United Kingdom government on what defense mechanisms to use against foreign active measures in democratic processes. This made the assuming of responsibilities to look like a "hot potato" (ISCP, 2020: 5).

Russian agents will continue to test these active measures in western countries. In 2018, on the eve of the midterm elections for the United States Senate and House of Representatives, another criminal complaint against the IRA, in the person of Elena Khusyaynova, was filed in the Eastern District of Virginia by a Federal Prosecutor, for conspiring to interfere with the American political and electoral process in the 2018 elections (USDC, 2018). In the same year, the CIA assessed that Vladimir Putin was "probably" responsible for another campaign to discredit Vice-President Joe Biden, then candidate for President (and eventual winner) (Rogin, 2020). Similar actions were seen in Europe, where in the period between 2017 and 2018, disinformation campaigns using state media and social media by Russian-sponsored outlets happened in Italy, Netherlands, Spain (the Catalan independence referendum), Czech Republic and Sweden (Tennis, 2020).

If the motivations for Presidente Putin and the Kremlin seem obvious in the light of the theories by Jervis and Mearsheimer, of trying to maximize an offensive posture by meddling with democratic processes and elections in the west, the "price" to be paid does not seem to be a deterrent. The Russia Federation is a (almost) a *de facto* pariah state regarding relations with the west (exacerbated by military interventions in the "near abroad"), hence, the threat of isolation is not operative. Similarly, sanctions due to election interference and cyberattacks continue to focus on individuals and organizations that are believed to relate to the center of power in Moscow (Turak & Macias, 2021). However the Russian government will keep denying any responsibility, while giving shelter to people and groups indicted, making them immune to persecution in the west. In this way it will be difficult to inflict serious blows to these structures that promote active measures.

The Vice-President of the European Parliament, Rainer Wieland, said in 2019 that "[c]yber-attacks are a recent but very real threat to the stability of the European Union and its Member States. A cyber-attack on elections could dramatically undermine the legitimacy of our institutions. The legitimacy of elections is based on the understanding that we can trust in their results. This very trust has come under pressure from cyber-attacks and other new types of election fraud in the Digital Age, and we must respond!" (ENISA, 2019). One of the most important needs, is to detect, as soon as possible, who is behind these attacks, how they started, how they are run, and the effects of these active measures in democratic processes, because of the influences in the way societies operate. Especially, adversarial intelligence agencies are known to be a "clear and present danger", as attested by open-source information. Agencies like GRU, FSB and SRV will continue to test the western systems and countermeasures. It is advised that a bloc of countries, with a centralized power at the European Parliament, like the European Union, should use all the instruments available in this line of defense, including exploring the potential of some of the already existing ones.

This work aimed to systematize some of the open-source information on digital active measures, their *modus operandi*, and to give some countermeasures to fight these threats. However, the battlefield is enlarging and becoming progressively dangerous. Sectorial responses, like the ones seen in the European Union, the United States, the United Kingdom, could be the entry points to a coordinated, multi-pronged, proportional strategy to strengthen western liberal democracies, and inspiring ones around the world, against these threats.

References

Andrew, C & Mitrokhin, V (2006). *The Mitrokhin Archive: The KGB in Europe and the West.* New York: Penguin Press History.

Apuzzo, M & Satariano, A (2019). Russia Is Targeting Europe's Elections. So Are Far-Right Copycats. [Consulted 15 de April 2021]. Available at: https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html.

Balsamo, M (2019). Trump depicted in Mueller report feared being called a fraud. [Consulted 15 de April 2021]. Available at: https://apnews.com/article/677b7b2f0c184e65921afe2314e468ac.

Bartles, C.K (2016). «Getting Gerasimov Right». *Military Review*. 96(1): 30-38.

Baylis, J, Smith, S, & Owens. P (2019). *The Globalization of World Politics. An Introduction to International Relations*. Eighth Edition. Oxford: Oxford University Press.

Carrell, S (2017). Russian cyber-activists 'tried to discredit Scottish independence vote'. [Consulted 15 de April 2021]. Available at: https://www.theguardian.com/politics/2017/dec/13/russian-cyber-activists-tried-to-discredit-scottish-independence-vote-says-analyst.

Crowley, M & Ioffe, J (2016). Why Putin hates Hillary. Behind the allegations of a Russian hack of the DNC is the Kremlin leader's fury at Clinton for challenging the fairness of

Russian elections. [Consulted 15 de April 2021]. Available at: https://www.politico.com/story/2016/07/clinton-putin-226153.

Daisley, S (2020). Why Putin wants Scottish independence. [Consulted 15 de April 2021]. Available at: https://www.spectator.co.uk/article/why-putin-wants-scottish-independence.

Daniels, L (2017). How Russia hacked the French election. [Consulted 15 de April 2021]. Available at: https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

DCMSC [Digital, Culture, Media and Sport Committee] (2018). Russian Influence in Political Campaigns. Disinformation and "fake news": Interim Report. [Consulted 15 de April 2021]. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm.

DHS [Department of Homeland Security] (2016). Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. [Consulted 15 de April 2021]. Available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

DNI [Director of National Intelligence] (2017). *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment, [Consulted 15 de April 2021]. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Ellehuus, R & Ruy, D (2020). Did Russia Influence Brexit? [Consulted 15 de April 2021]. Available at: https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit.

ENISA [European Union Agency for Cybersecurity] (2019). EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections. [Consulted 15 de April 2021]. Available at: https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-their-cybersecurity-preparedness-for-fair-and-free-2019-eu-elections.

Estevens, J (2020). «Building intelligence cooperation in the European Union». *Janus.net*, *e-journal of International Relations.* 11(2)

European Commission (2020). Tackling online disinformation. [Consulted 15 de April 2021]. Available at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation.

European Commission (2020a). Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. [Consulted 15 de April 2021]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en.

Galante, L & Ee, S (2018). *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*. Atlantic Council, [Consulted 15 de April 2021]. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf.

Galeotti, M (2013). The 'Gerasimov Doctrine' and Russian Non-Linear War. [Consulted 15 de April 2021]. Available at: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war.

Galeotti, M (2017). Controlling Chaos: How Russia Manages its Political War in Europe. ECFR Briefing. [Consulted 15 de April 2021]. Available at: https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

Galeotti, M (2019). Active Measures: Russia's Covert Geopolitical Operations. [Consulted 15 de April 2021]. Available at: https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

Gessen, M (2012). *The man without a face. The unlikely rise of Vladimir Putin*. New York: Riverhead Books.

Graff. G.M (2018). Indicting 12 Russian Hackers Could Be Mueller's Biggest Move Yet. [Consulted 15 de April 2021]. Available at: https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear.

HSCI [House Select Committee on Intelligence] (2017). Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements. [Consulted 15 de April 2021]. Available at: https://intelligence.house.gov/social-media-content.

ISCP [Intelligence and Security Committee of Parliament] (2020). *Russia*. Intelligence and Security Committee of Parliament, [Consulted 15 de April 2021]. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.

ISCP [Intelligence and Security Committee of Parliament] (2020a). *Press Notice. Intelligence and Security Committee of Parliament publish predecessor's Russia Report.* [Consulted 15 de April 2021]. Available at: https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDoxMmRkZmU2MjQ4ZWEzNDI0.

Jervis, R (1978). «Cooperation Under the Security Dilemma». *World Politics.* 30(2): 167-214.

Kim, Y.M (2018). *Uncover: Strategies and Tactics of Russian Interference in US Elections. Russian Groups Interfered in Elections with Sophisticated Digital Campaign Strategies*. University of Wisconsin, [Consulted 15 de April 2021]. Available at: https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_.v.5.0905181.pdf.

Krausse, C (2018). Exxon Mobil Scraps a Russian Deal, Stymied by Sanctions. [Consulted 15 de April 2021]. Available at: https://www.nytimes.com/2018/02/28/business/energy-environment/exxon-russia.html.

McKew, M.K (2017). The Gerasimov Doctrine its Russia's new chaos theory of political warfare. And it's probably being used on you. [Consulted 15 de April 2021]. Available at: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

Mearsheimer, J.J (2001). *The tragedy of great power politics*. New York: W.W. Norton & Company.

Murphy, S (2020). UK report on Russian interference: key points explained. [Consulted 15 de April 2021]. Available at: https://www.theguardian.com/world/2020/jul/21/just-what-does-the-uk-russia-report-say-key-points-explained.

NCSC [National Cyber Security Center] (2018). Reckless campaign of cyber attacks by Russian military intelligence service exposed. [Consulted 15 de April 2021]. Available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

OTAN [Organização do Tratado do Atlântico Norte] (1949). Tratado do Atlântico Norte. [Consulted 15 de April 2021]. Available at: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt

Persily, N (2017). «Can Democracy Survive the Internet? ». *Journal of Democracy*, 28: 63-76.

Rato, V (2018). «Romper o cerco: a Rússia de Putin e a Nova Guerra Fria». *Nação e Defesa*. 150: 116-148.

Reuters (2017). UK political parties warned of Russian hacking threat: report. [Consulted 15 de April 2021]. Available at: https://uk.reuters.com/article/us-britain-russia-cybercrime-idUKKBN16J0OE.

Rogin, J (2020). Secret CIA assessment: Putin 'probably directing' influence operation to denigrate Biden. [Consulted 15 de April 2021]. Available at: https://www.washingtonpost.com/opinions/2020/09/22/secret-cia-assessment-putin-probably-directing-influence-operation-denigrate-biden.

Sanger, D & Schmitt, E (2016). Spy Agency Consensus Grows that Russia Hacked D.N.C. [Consulted 15 de April 2021]. Available at: https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

SSCI [Senate Select Committee on Intelligence] (2019). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume2: Russia's use of Social Media with Additional Views*. 116th Congress, [Consulted 15 de April 2021]. Available at: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
.

Silvestre, R (2019). «A Rússia e os ciber ataques a instituições democráticas europeias». *ResPublica*. 19: 83-107.

Stewart, S (2009). «Democracy Promotion before and after the 'color revolutions'». *Democratization*. 16(4): 645-660.

Stretch, C (2018). *Written responses from Facebook's General Counsel to U.S. Senate Select Committee on Intelligence*. U.S. Senate, [Consulted 15 de April 2021]. Available at: https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.

Syal, R (2017). Brexit: foreign states may have interfered in vote, report says. [Consulted 15 de April 2021]. Available at: https://www.theguardian.com/politics/2017/apr/12/foreign-states-may-have-interfered-in-brexit-vote-report-says.

Tennis, M (2020). Russia Ramps up Global Elections Interference: Lessons for the United States. [Consulted 15 de April 2021]. Available at: https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states.

Timberg, C & Harris, S (2018). Russian operatives blasted 18.000 tweets ahead of huge news day during the 2016 presidential campaign. Did they know what was coming? [Consulted 15 de April 2021]. Available at: https://www.washingtonpost.com/ellipsis/russian-operatives-blasted-18000-tweets-ahead-of-a-huge-news-day-during-the-2016-presidential-campaign-did-they-know-what-was-coming/2018/07/20/6715a547-91db-43f0-b21a-a75ff3d9205a_story.html.

TJF [Thomas Jefferson Encyclopedia] (2020). Eternal vigilance is the price of liberty (Spurious Quotation). [Consulted 15 de April 2021]. Available at: https://www.monticello.org/site/research-and-collections/eternal-vigilance-price-liberty-spurious-quotation.

Turak, N & Macias, A (2021). Biden administration slaps new sanctions on Russia for cyberattacks, election interference. [Consulted 15 de April 2021]. Available at: https://www.mediapart.fr/journal/international/300317/marine-le-pen-signe-nouveau-pour-de-l-argent-russe.

Turchi, M (2017). Marine Le Pen Signe à Nouveau Pour de l'Argent Russe. [Consulted 15 de April 2021]. Available at: https://www.mediapart.fr/journal/international/300317/marine-le-pen-signe-nouveau-pour-de-l-argent-russe.

Unikaitė-Jakuntavičienė, I, & Rakutienė, S (2013). Writing a Bachelor's Thesis in the Field of Political Science. Didactical Guidelines. [Consulted 15 de April 2021]. Available at: https://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2013_metodine_priemone_Writing_a_Bachelors_Thesis.pdf

USDC [United States District Court] (2018). 1:18-MJ-464. [Consulted 15 de April 2021]. Available at: https://www.justice.gov/usao-edva/press-release/file/1102591/download.

USDJ [United States Department of Justice] (2018). Case 1:18-cr-00032-DLF. [Consulted 15 de April 2021]. Available at: https://www.justice.gov/file/1035477/download.

USDJ [United States Department of Justice] (2018a). Case 1:18-cr-00032-DLF. [Consulted 15 de April 2021]. Available at: https://www.justice.gov/file/1080281/download.

Vandiver, J (2014). SACEUR: Allies must prepare for Russia 'hybrid war'. [Consulted 15 de April 2021]. Available at: https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464.

Watts, C (2018). Russia's Active Measures Architecture: Task and Purpose. [Consulted 15 de April 2021]. Available at: https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose.