INTERNATIONAL CONFERENCE RCIC'18
Redefining Community in Intercultural Context
Bucharest, 17-19 May 2018

SOCIAL MEDIA TAKES A TOLL ON DEMOCRACY

Claudia LASCATEU GOGOAŞĂ

'Mihai Viteazul' National Intelligence Academy, Bucharest, Romania

Motto: "The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country."
Bernays (1928:10)

Abstract: *Typically, crisis spur when political systems reach a standstill, when all resources are finished and the last option that could get the government out of the struggle is military force. As history has shown, this is not the best way out. Crisis and conflicts are the motion power of permanent transformation of international interaction. They have all impacted mostly civilian population through numerous casualties and refugees that determined humanitarian efforts, thus crisis resolution and conflict mediation becoming one of most important concern in security. The post-Cold War world gave means and opportunity for states to try and assert their global influence through peaceful means, remotely control the ex-soviet countries through economic and energetic domination and influence western countries with a set of strategies that define hybrid warfare aimed at the core of its adversaries' source of political power, at population. This paper will analyse how social media is weaponised to achieve political gain over recent elections as a part of an effective toolset aimed at influencing public scrutiny. The purpose of this article is to establish if turning social media into a means of control over the population is a part of a greater operation to generate popular misperception and increase one actor's power, or it represents the new age exertion of soft power beyond privacy rights and international regulation.*

Keywords*: active measure; influence operation; private data; social media*

1. INTRODUCTION

Data brokers, advertising, social network providers and other digital business actors have ample information on individuals participating in today's digital society, and people are slowly losing track over their digital footprint. Targeted, profiled and assessed by actors[1] often beyond their control or knowledge, feeling somewhat helpless and in need of need being able to take control of their digital identity, people are starting to question the system designed to bear profit on personal data, even though *notice* and *consent* to terms and conditions are given (Buttarelli, 2016:5).

Considering the broad parts of our daily lives social media and the technology behind it interact and change, it comes naturally that issues like security, privacy, activism or terrorism are also influenced by networking in this manner. Nonetheless, it is changing the dynamics of soft power, turning interpretation into influence.

2. SOCIAL MEDIA GENERATES POPULAR MISPERCEPTION TO INCREASE ACTORS' POWER

Recently declassified the March 22, 2018 United States (U.S.) House of Representatives Permanent Select Committee on Intelligence Report on Russian Active Measures shows how beginning in 2015 Russia aimed influencing the U.S. presidential election basically by using covert tools and techniques mastered after the end of the World War II. The investigations started in January 2017 and were set to clarify the role played by Russian influence campaign in the cyberworld, and if it was purposely aimed at the U.S. and its allies to undermine confidence in democratic process.

[1]Actor: person or organization, including state and non-state entities, within the international system with the capability or desire to influence others in pursuit of its interests and objectives (NATO, 2011:1-3).

The report shows how Russian active measures unfolded over the past years and outlines methodically the processes involved providing recommendations for future prevention.

Soviet government has long used combined propaganda and intelligence activities, diplomacy and political assertiveness to achieve its goals (Bittman, 1985:43), and exercise its influence through third parties. The term *active measure* is actually the translation from Russian of *aktivnyye meropriatia* witch was used by KGB (*Komitet gosudarstvennoy bezopasnosti*, or Committee for State Security) for many of the influence activities used during the Cold War (Departement of State, 1987:viii). Others have defined *active measures* as soviet influence techniques to determine the way public perception and decisionmakers behave positively towards soviets and negatively towards their opponents, also called perception management.

KGB influence activities included forming and funding front organizations (*grey propaganda*[2]), clandestine broadcasting, media manipulation (*white propaganda*[3] and creating and distributing false stories), forgeries and disinformation (*black propaganda*[4]) and bribing agents of influence (Romerstein, 1989: 1-5). These techniques surpassed overt and secret operations to manipulate perception by turning to incitement, assassination or terror attacks.[5]

Pieces of news like "the US intelligence community was actively involved in the assassination of J.F.Kennedy in 1963 or the United States and Israel coordinated the attack on Mecca in 1979 or American scientists created AIDS as a bioweapon in 1983" (Patriot apud USIA, 1988:2-11)[6] are outspoken examples of Cold War Soviet propaganda and dissemination campaigns that remain on Russian public agenda (Schoen, Lamb, 2012:8-12), as Putin mentions in a recent interview in 2017 – he refers to Kennedy assassination while talking about the American intelligence community running false-flag operations to blame Russian secret services (Kelly, 2017:1). Other nations have developed diplomacy and disinformation programs based on active measures such as Iran and its proxy Hezbollah (Boghardt, 2006: 20-26), but also non-state actors like terrorist groups.

As Colonel Rolf Wagenbreth, long-time head of active measures operations for the East German Stasi, reportedly said,

> a powerful adversary can only be defeated through […] sophisticated, methodical, careful, and shrewd effort to exploit even the smallest 'cracks' between our enemies […] and within their elites (Rid, 2017:1).

While the technology has evolved, Russia's influence toolkit has transformed, like one Russian military intelligence textbook said, "Psychological warfare has existed as long as mankind itself" (Kovalev, Bodner, 2017: 1).

Nowadays the resources that Kremlin uses in malign influence operations are both state and non-state, including the intelligence community, media outlets, social media and internet trolls, private and public companies, organised crime, think tanks and foundations, and social and religious groups.[7] These endeavours have weaponised traditional and social network media, ideology and culture, crime and corruption and the energy market. The goal is to discredit politicians and democratic institutions like elections and independent media, to disrupt social cohesion and follow Kremlin's point of view, to influence politicians and infiltrate decision making bodies and to control vulnerable foreign governments (Galeotti, 2017:1).

[2] Grey propaganda is where the correct source of the information is never directly credited, and the sponsor's identity is concealed.

[3] White propaganda uses standard public relations techniques and one-sided presentation of an argument.

[4] Black propaganda is false information and material that purports to be from a source on one side of a conflict but is from the opposing side. It is typically used to vilify, embarrass, or misrepresent the enemy (Doob, 1950).

[5] Alleged Soviet support for terrorism and assassination have been controversial topics for ideological and diplomatic reasons. However, defectors such as Ladislav Bittman (1985) have detailed many of these Soviet activities in their memoirs and books.

[6] In 1983, the *Patriot*, a pro-Soviet Indian paper that published pieces provided by KGB agents, released a story claiming that the U.S. military created the AIDS virus and released it as a weapon. For a couple of years, the story appeared in minor publications that were mostly KGB controlled or sympathetic to the Soviets. After this incubation period, the slander was picked up in 1985 by the official Soviet cultural weekly newspaper, the *Literaturnaya Gazeta.* After that, the story began to spread rapidly. In 1987 alone, it appeared over 40 times in the Soviet-controlled press and was reprinted or rebroadcast in over 80 countries in 30 languages.

[7] The European Parliament passed a resolution recognizing the wide range of tools and instruments that Russia uses to disseminate disinformation and propaganda (see the *EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties*, 2016/2030).

Director of National Intelligence Dan Coats told the US Congress in 2018 that *hostile actors viewed elections as* "opportunities to undermine democracy" (White, 2018:1).

3. SOCIAL MEDIA THE NEW AGE EXERTION OF SOFT POWER BEYOND PRIVACY RIGHTS AND INTERNATIONAL REGULATION

Traditionalist intelligence experts tend to put the emphasis on the importance of communications for their impact on perceptions, believing that strategic deception – the open deceitful side of strategic communication – is of utmost importance, and that efforts should be aimed at understanding the adversary's intentions and to disseminate our own intentions in a manner that strengthens the political support of the nation's interests. Others are more concerned about capabilities, to rely and support national institutions, believing that maintaining public trust in the nations values will send a better message rather than diplomacy. While other experts would not choose between strategic communications and strategic capabilities but rely on comprehensive approach upon certain circumstances – like Ben Hiller, Cyber Security Officer at the OSCE Secretariat's Transnational Threats Department who stated the first meeting of the Organization of American States' (OAS)[8] working group on co-operation and confidence-building measures (CBMs) in cyberspace in Washington DC on 2 March 2018 "Many states now consider cyber capabilities a legitimate and necessary part of their strategic toolbox alongside diplomacy, economic influence and military might. …This requires decision makers to become involved and identify measures to prevent potential fallout from their use" (OSCE, 2018:1). The bottom line is that the importance of strategic communications and the need to counter disinformation is dependent to the threat assessment and international environment (Schoen, Lamb, 2012:117-118).

Private data has become the subject of intense debate whether the way technology has turned into a vast system based on limitless data gathering and analysis regardless of ethics or regulations afflicting on personal choices regarding various domains from consumer choices to influencing political views, thus endangering democratic institutions such as elections. Major actors at the centre of this system are the digital platforms feeding on digital advertising, gaining power as it revolves around users and their personal data much needed to segment, target and customise messages. Public treats lightly personal data and the system repays sensational by turning it into viral content without distinguishing weather the message advertised is commercial or political. Recent disclosures about how *fake news* – deliberate disinformation – works in this system have fuelled the suspicions that the integrity of democracies is under threat. Current solutions are focused on transparency, on exposing the source of information, rather than accountability of players who profit of the malign measures (EDPS, 3/2018:2).

Fundamental rights to privacy and to personal data protection should play a crucial part in each legislator's policy to keep up with such developments, and independent data protection authorities set it as a strategic priority. In 2005 the Montreux *Resolution on the Use of Personal Data for Political Communication* outlined the fact that data protection regulators identified an increase in processing of such data by non-commercial actors, referring specifically to the analysis of 'sensitive data related to real or supposed moral and political convictions or activities, or to voting activities' and 'invasive profiling of various persons who are currently classified - sometimes inaccurately or on the basis of a superficial contact - as sympathizers, supporters, adherents or party'. The outline of the 2005 Resolution urged the international community to issue and enforce data protection rules on data minimization, lawful processing, consent, transparency, data subjects rights, purpose limitation and data security (EDPS, 3/2018:5).

The European law on data protection and confidentiality of digital communication applies to data collection, profiling and microtargeting[9] so by using the toolset drawn by the EU General Data Protection Regulation (GDPR)[10] little harm would

[8] The OAS, after the Organization for Security and Co-operation in Europe (OSCE) and the Association of Southeast Asian Nations (ASEAN) Regional Forum, is the third regional organization addressing practical measures to enhance cyber stability between states.

[9] To differentiate from *commercial microtargeting*, the term 'political microtargeting' has been defined as the use of different means of communications (mail, phone, canvassing, direct mail, and social media advertising, etc.) to communicate and build a relationship with prospective voters (Bodo *et al.*, 2017). .

[10] The European Union General Data Protection Regulation (GDPR) is the most important change in data privacy in 20 years. After four years of preparation and debate the GDPR was finally approved by the EU

be produced when influence attempts on groups or individuals would appear. Political actors processing personal data fall within the scope of the GDPR while stating the exact cases when it is allowed.

The idea of the EU GDPR is to treat the data subject 'as an individual not simply as a consumer or user' and highlight the ethical issues that predictive profiling and algorithm-determined personalisation raise [11].

As stated by the European Court of Human Rights in the case of *Orlovskaya Iskra* v. *Russia*, "free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system. The two rights are inter-related and operate to reinforce each other: for example, freedom of expression is one of the "conditions" necessary to "ensure the free expression of the opinion of the people in the choice of the legislature". For this reason, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely. In the context of election debates, the unhindered exercise of freedom of speech by candidates has particular significance" (ECHR, 2017: para. 110).

The U.S. Department of State reports that Russian efforts to influence elections and referendums in Europe include "open and secret support for far right and left political parties, funding front groups and NGOs, and making small, low-profile investments in key economic sectors to build political influence over time" and that the techniques employed "focus on exploiting internal discord in an effort to break centrist consensus on the importance of core institutions" (U.S. Department of State, 2017). In the same keynote, a study by the German Marshall Fund's Alliance for Securing Democracy reveals that the Russian government has used cyberattacks, disinformation, and financial influence campaigns to meddle in the internal affairs of at least 27 European and North American countries since 2004.[12]

The New York Times reveals that fake news and social media trolls have been used by Kremlin against its own citizens and have increased in intensity after the 2011-2012 anti-Putin protests. Centered on social media domination and online platforms used by opponents to spread doubts of electoral process and to mobilize protesters, Kremlin developed and used software to monitor online public opinion and flooded social media with its own vision, paying bloggers to lobby for Kremlin (Chen, 2015: 1). In 2014, after winning undisputedly the elections Putin enforced a law that legitimizes the government to block sites hosting extremist content or that represented a public threat without court order, resulting in blocking 3 opponent news sites and Alexei Navalny's blog (The Guardian, 2014: 1).

Government has since been blocking IP addresses imposed by RKN (*Roskomnadzor* – Russian media and communications authority) the recent winner of a yearlong battle ended with the 13th of April court order to shut down *Telegram* (web encrypted messenger service), meaning immediate blocking of vast numbers of IPs causing interoperable internet services (from supermarket cashiers, purchase websites, ATM machines, to traffic apps) to meltdown (Lokshina, 2018: 1).

The disinformation measures used by Russians in the 2016 US presidential elections has by far been the most efficient of all times. Powered by botnets, social media trolls and by media outlets like Russia Today (RT) and Sputnik, Kremlin has succeeded in making the public sympathetic to Russian views (Treverton, Chen, 2017: 1).

In the Brexit Referendum campaign Russian press agencies have given extensive media coverage presenting one sided coverage of the debate, that of voting to leave European Union and the speeches of UKIP[13] representatives.

Parliament on 14 April 2016. Enforcement date: 25 May 2018 - at which time those organizations in non-compliance may face heavy fines. GDPR replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

[11] Profiles used to predict people's behavior risk stigmatization, reinforcing existing stereotypes, social and cultural segregation and exclusion, with such 'collective intelligence' subverting individual choice and equal opportunities. Such 'filter bubbles' or 'personal echo-chambers' could end up stifling the very creativity, innovation and freedoms of expression and association which have enabled digital technologies to flourish (EDSP, 4/2015:13).

[12]The countries included Belarus, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Italy, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Norway, Poland, Portugal, Spain, Sweden, Turkey, United Kingdom, Ukraine, and the United States (Dorell, 2017:1).

[13] The UK Independence Party is a hard Eurosceptic and right-wing populist political party in the United Kingdom.

At that time, Facebook and Twitter internal inquiries of the allegations that massive manipulation campaigns were enacted by Russians did little to acknowledge that more than 400 Russian controlled accounts were actively posting both in the American elections and the Brexit referendum as research conducted by the Edinburgh University shows[14]. Moreover, the conclusions of a common team or researchers from Berkeley University and Swansea University has identified 150.000 Twitter accounts directly tied to Russian government, that have spread messages about Brexit (Adam, Booth, 2017: 1).

During the French presidential campaign RT and Sputnik have covered ample materials depicting president Emmanuel Macron as the puppet of American political and economic interests, accused him of having a secret bank account in Bahamas to avoid paying tax and fuelled rumours of being in an extramarital homosexual relationship, all publicly denied (Bremmer, 2017: 1). In 2017 Facebook declared that 70.000 accounts were suspended during the French campaign for spamming or propaganda, that were proven to be controlled and used by the GRU (*Glavnoye Razvedyvatel'noye Upravleniye* - the main military foreign-intelligence service of the Russian Federation) in 2016 to attack the National Democratic Committee during the US electoral campaign (Reagan, 2017:1). In counterpart, the Russian sponsored media has channelled its efforts to depict an alternative image of how living in Germany is dangerous, depraved and undemocratic, presenting gratifying and biased news materials about AfD[15] (Shuster, 2017:1).

Kremlin's malign influence and hybrid warfare activities have inherently led to international sanctions, while many started when Russia illegally annexed Ukraine's Crimea and financed and backed separatist in Eastern Ukraine, they continued by both E.U. and U.S. sanctions as a response to cyberattacks, human rights violations or corruption. The aspects that make these influence campaigns effective also make them hard to counter, even so, establishments and media representatives in Europe have already begun to take actions to address and mitigate the threat of manipulation campaigns by raising public awareness, anti - fake news regulations, enforcing privacy laws and funding cybersecurity organizations, thus more is to achieve to make responsible parties assume actions.

[14] In 2016 a multi-disciplinary team in Edinburgh University has started to explore the role of social media in today's international affairs, and it began by analyzing big data from Twitter to track the UK's social media influence around the world. It contributes to a growing body of evidence that the future of soft power will include the capture and analysis of big data from digital media and the crafting of responses to what that data reveals.

[15] Alternative für Deutschland - a right-wing to far-right political party in Germany.

4. CONCLUSIONS

As part of the global community it has come to the point where we need to reflect, understand what recent events mean to us and our culture, find effective solutions and coordinate actions to counter any active measures directed by adversaries.

The possibility to use social network media as a means of strategic communications to assert power in conflicts or to achieve political goals has risen ethical issues that we only begin to address, by rewriting personal data policy, internet governance, diplomacy and by having a comprehensive approach to what technology brings in our lives to ensure that fundamental rights are not overlooked.

BIBLIOGRAPHY

1. Adam, K., Booth, W. (2017) Rising Alarm in Britain Over Russian Meddling in Brexit Vote. *The Washington Post*. November 17.
2. Bittman, L. (1985). *The KGB and Soviet Disinformation: An Insider's View*. Washington: Pergamon-Brassey's.
3. Bodó, B., Helberger, N., de Vreese, C. (2017) Political microtargeting: a Manchurian candidate or just a dark horse?. *Internet Policy Review*. 6(4).
4. Boghardt, T. (2006) Active Measures. The Russian Art of Disinformation. *International Spy Museum* [online]. URL: https://www.spymuseum.org/ education-programs/news-books-briefings/ background-briefings/active-measures/ [Accessed on April, 2018].
5. Bremmer, C. (2017) Websites Pump Out Fake News Minutes After Offshore Claims. *The Times.* May 5
6. Buttarelli, G. (2016). European Data Protection Supervisor (EDPS) Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data. *Opinion*. 9.

7. Chen, A. (2015) The Agency. *The New York Times*. June 2.
8. Department of State. (1987) *A Report on Active Measures and Propaganda, 1986 - 1987*, Washington: Department of State Publication.
9. Doob, L. (1950). Goebbels' Principles of Nazi Propaganda. *The Public Opinion Quarterly*. Vol. 14. No. 3. 419–442.
10. Dorell, O. (2017). Alleged Russian Political Meddling Documented in 27 Countries Since 2004. *USA Today*. September, 7.
11. Bernays, E. [1928] (2005). *Propaganda*. New York: IG Publishing.
12. European Court of Human Rights. (2017). *Orlovskaya Iskra v. Russia* [online]. URL: http://hudoc.echr.coe.int/eng?i=001-171525 [April 23, 2018].
13. European Data Protection Supervisor. (2015). Towards a new digital ethics. *Opinion*. 4.
14. European Data Protection Supervisor. (2018) Online manipulation and personal data. *Opinion.* 3.
15. European Parliament Resolution. (2016). *EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties, 2016/2030*(INI) [online] URL: http://www.europarl.europa.eu/ sides/getDoc.do?pubRef=- //EP//TEXT+REPORT+ A8-2016-0290+0+DOC+XML+V0//EN [April 28, 2018].
16. Galeotti, M. (2017). Controlling Chaos: How Russia Manages its Political War in Europe. *European Council on Foreign Relations* [online]. URL: http://www.ecfr.eu/publications/summary/ controlling_chaos_how_russia_manages_its_p olitical_war_in_europe [April 28, 2018].
17. House Permanent Select Committee on Intelligence. (March 22, 2018). *Report on Russian Active Measures*. Washington, DC: U.S. House of Representatives.
18. Kelly, M. (2017). Interview with Vladimir Putin, *NBC*. June 5.
19. Kovalev, A., Bodner, M. (2017). The Secrets of Russia's Propaganda War, Revealed. *The Moscow Times*. March 1.
20. Lokshina, T. (2018). Russia's Internet War and its Collateral Damage. *Human Rights Watch*. 24 April.
21. NATO. (2011). *Bi-Strategic Command Knowledge Development*, Pre-Doctrinal Handbook. Norfolk, Virginia: ACT.
22. OSCE (2018). *OSCE shares experiences with Organization of American States on how to enhance interstate co-operation, transparency, predictability and stability in cyberspace* [online]. URL: https://www.osce.org/secretariat/374389 [accessed April 22, 2018].
23. Reagan, T. (2017). Facebook helped blunt Russian meddling in French elections. *enGadget*. July 27.
24. Romerstein, H. (1989). *Soviet Active Measures and Propaganda: "New Thinking" & Influence Activities in the Gorbachev Era*. Toronto: National Intelligence Book Center, Mackenzie Institute for the Study of Terrorism, Revolution, and Propaganda.
25. Agence France Press. (2014). Russia Censors Media by Blocking Websites and Popular Blog. The Guardian. March 14.
26. Schoen, F., Lamb, J. C. (2012). Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference**.** *Strategic Perspectives*.
27. Shuster, S. (2017). *How Russian Voters Fueled the Rise of Germany's Far-Right*, Hanover: Time.
28. Statement of Thomas Rid, Professor, Department of War Studies, King's College London. (2017). *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, Hearing before the U.S. Senate Select Committee on Intelligence.
29. Treverton, G. F., Chen, A. R. (2017) Hybrid Threats: Russian Interference in the 2016 US Election. *SMA*. November 6,
30. U.S. Department of State. (November 7, 2017) *Report to Congress on Efforts by the Russian Federation to Undermine Elections in Europe and Eurasia, Pursuant to the Countering America's Adversaries through Sanctions Act of 2017*. Washington: U.S. Department of State Publishing House.
31. United States Information Agency (USIA). (1988). *Soviet Active Measures in the Era of Glasnost*, Report presented to the U.S. House of Representatives Committee on Appropriations. Washington: U.S. Department of State Publishing House.
32. White, J. B. (2018). *Top US commander in Europe says Washington lacks 'effective' coordination on Russian cyber-attacks.* San Francisco: The Independent.