From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment

Aurelian STOICA
National Institute for Research and Development in Informatics - ICI Bucharest
aurelian.stoica@ici.ro

Abstract: Social influence has attracted relevant attention from the social sciences researchers during the last century. Seen by many people as old as the history of the humankind, the social influence domain is strongly embedded with its various forms that it takes, studied extensively by different research schools: persuasion, propaganda, obedience, conformism, manipulation, disinformation. In the light of the exponential development of the new technologies in the digital era, we are faced now with an insufficiently self-regulated environment that is place for the social influence exchanges: the virtual space or the cyber space. State actors seeking to promote their objectives in a fully connected world will use this technology ecosystem to create, diffuse and extensively spread their key messages by empowering the governmental bodies with the flexibility and anonymity offered by the digital tools. Their main goal: to influence, distract, confuse and divide individuals, communities and even entire societies, to a point where they will not be able to distinguish facts and information from fabricated Potemkian reflections.

Keywords: Social influence, Cyber influence, Cyber diplomacy, Active measures, Disinformation, Computational propaganda.

INTRODUCTION

Different schools and theories assessed in the last century the way social influence works, with the aim to provide a better understanding of the concept and to set boundaries between its different categories. When individuals are faced with a social environment that is generating an attitude or belief change from their side, we can say the social influence process is in place. The individual's change may be divided into three different processes: compliance (agree formally due to the social effect), identification (when the change is determined by someone influent) and internalization (when the change is consistent with his values system) (Kelman H., 1958, p. 53). Changes are done either due to the informational social influence (when we act as others do because we consider they have more information that is going to solve the uncertainty of the current situation) or to the normative social influence, because we want to integrate in particular groups with unwritten rules (Deutsch, M. & Gerard, H.B., 1955, p. 629).

Due to having communication as a base layer, the social influence is integrating the components that empower every communication act and ensure its functionality: the source, the message, the receiver, the transmission channel and the context of the process. In this approach, the presence of others is capital and defines the social influence concept. Therefore, we will consider for the present study that the most comprehensive definition is the one provided by Robert A. Dahl in 1957, when he concluded that influence is when "A has power over B, to the extent that he can get B to do something that B would not otherwise do" (Dahl, R.

A., 1957, 203). Power, as the capacity or potential to change other's behavior, represents therefore the basis for the individual or group ability to influence. Furthermore, we approach the social influence as an "asymmetrical action between two social entities (individuals, groups) that interact with each other with the goal to change the attitudes and beliefs of one party, consciously or not" (Elinschi-Ciupercă, E., 2003, 185).

Other theories based on experimental studies argue that social influence is not conditioned by the presence, interdependency and identification of the group members, but even more emphasized when the group members benefit from anonymity. This is the case of the communication mediated by the computer, a context in which we can identify a powerful influence process based on the relation between the individual and the group as a whole. A reduced physical presence of the individual in the experimental group (by creating conditions for anonymity) has supported an enhanced group presence in each separate member (Postmes, T. et al, 2001, 1253). Other researches have further stressed that in the computer mediated communication, face-to-face socio-psychological dysfunctionalities can be avoided due to setting up an easier framework for public debate (Ho, S.S. & McLeod, D.M., 2008).

SOCIAL INFLUENCE CATEGORIES

Many studies have approached the various forms of social influence, defining them, establishing transmission laws and underlining differences between key categories. Nevertheless, a short description of these concepts is necessary for the purpose of this paper. In the case of persuasion, maybe one of the most clear descriptions is the one stating that it represents "the activity of influencing the attitudes and beliefs of individuals in order to produce changes in full synergy with the objectives of the initiating entity (individuals, groups, institutions or political, social, cultural or commercial organizations)" (Vlăsceanu M., 1993, 429). It is best known for the progress in the advertising and marketing industry, where key principles like those defined by Robert Cialdini (reciprocity, commitment/consistency, social proof, authority, liking and scarcity) have made history no matter the field of expertise.

With a different background, propaganda has its origins in the 1622 religious task to deliver the Catholic faith in non-Catholic countries (Congregatio de Propaganda Fide), but its maturity reached the highest peaks in the XXth century, when major combatant states used it as a tool to influence both the opponent's manpower and the civil minds of the adversaries. When the propaganda source is not known and its objectives and significance are disguised, we are dealing with "black propaganda". When the overt source is known by the public and the intentions are clear, we call it "white propaganda" (Ellul, J., 1973, 15). The mix between the two (in terms of source, intentions, objectives) is indicating us that we are facing a "grey" category.

In the last decades, all military conflicts involved heavily planned operations to persuade the enemies' morale and strategies to undermine their will, intoxicate their knowledge base and manipulate their decisions. The lights are on for new concepts like manipulation (determining someone to act accordingly to the desired objectives of the initiator), disinformation (false/fabricated information intentionally prepared to confuse), misinformation (inaccurate information that is spread, with no declared intention to generate disinformation), intoxication (specialized forgeries and fabricated content designed to mislead opponent's special services).

All those terms captured a bad reputation during wartime and especially during the Cold War period. Both the Western states and Russia tried to "rebrand" the concepts to become more agreeable; neither of them was to be associated with such sensitive topics. US and its allies structured a conglomerate of those activities applied during wartime with fields like "information operations" (IO), "information warfare" (IW), "psychological operations (PSYOPS)", "strategic communications" (STRATCOM), "computer network operations" (CNO) and "military deception" (MILDEC). For US strategists, information operations (IO) were defined as "actions taken in times of crisis or conflict to affect adversary information and information systems while defending one's own information and information systems" (Cordey, S., 2019, 9). It was probably the most important and the most comprehensive category among those mentioned above.

RUSSIA'S ACTIVE MEASURES

Meanwhile, starting with the 1950's, Russia provided a different notion to unify those concepts, namely "active measures" (*aktivnye meropriyatiya*), with two key differences compared to the West: there is no clear border between war and peace time when applying them and, moreover, own population can become a target for this propaganda arsenal. Other approaches tagged the influence activities portfolio with a specific term (*maskirovka*) that is considered more relevant for the understanding of its final purpose, covering activities such as "use of dummies, decoys, execution of demonstration maneuvers, camouflage, concealment, denial, deception and disinformation" (Daniel P. Bagge, 2019, 43). Other studies argue that "maskirovka" (which comprises all forms of deception) has not at all disappeared from the Russian operations strategies but is even evolved: "throughout the 20th century, Russian strategic theory has seen *maskirovka* as an essential tool of combat; recent operations in the Ukraine and Crimea have seen this elevated to a central position" (Scott, K., 2020, 59).

The active measures' main objective is to influence foreign targets, namely governments, key decision people, strategists, particular audiences, social groups, entire societies, by undermining confidence in democracy principles, country leaders and government decisions. This is done through a complex of disinformation measures, intoxications, manipulations, media distortions (or "fake-news" as known generically), fabricated stories, combined content (true and false assertions), front organizations (like proxy think-tanks), agents of influence, etc.

Every government is striving to promote its own foreign policy agenda and its key international objectives, but this is assumed to be an open and recognizable activity, which is done primarily through its state bodies and especially the diplomacy arm. Public diplomacy is the tool to influence foreign counterparts in order to better promote own ideas and negotiate partnership and cooperation with other state actors. What is fundamental in the diplomatic approach is the transparent, positive and declared influence towards recognizable objective. When applying the advantages offered by the new technologies in the virtual space encapsulated in the generic term "cyber", we obtain the "cyber-diplomacy", with the understanding of using new communication platform and tools to advance national interests and promote foreign policy goals and objectives in a digital environment.

The active measures link with the diplomacy in the point where they "may be conducted overtly through officially sponsored foreign propaganda channels, diplomatic relations, and cultural diplomacy" (Select Committee on Intelligence of the United States Senate, 2017, 4-5). Same Committee establishes five key objectives of Russia's active measures strategy, as follows:

1. *undermine citizen confidence in democratic governance*;
2. *foment and exacerbate divisive political fissures*;
3. *erode trust between citizens and elected officials and their institutions*;
4. *popularize Russian policy agendas within foreign populations*;
5. *create general distrust and confusion over information sources by blurring the lines between fact and fiction*.

Breaking foreign democracies main pillars is actually the central goal of Russia's Information Warfare Strategy; as Pomerantsev and Weiss wrote, „the effect is not to persuade (as in classic public diplomacy), or earn credibility, but to sow confusion via conspiracy theories and proliferate falsehoods" (Pomerantsev, P. and Weiss, M., 2014, 6).

INFLUENCE OPERATIONS

Influence operations (regardless of the cultural complex that they assume - information operations vs active measures) are categorized in two main classes. The first one is the *technical influence operations* (TIO), that targets the physical infrastructure like data centers, information systems and network nodes. The second one, *social influence operations*, is focusing exclusively on the content of the information aimed to change the behavior, attitudes and morale of the adversaries (Cordey, S., 2019, 10).

As recent studies define it, cyber-influence represents the terminology "to refer, to inform and influence operations that are run in the cyberspace, leverage this space's distributed vulnerabilities, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations" (Bonfanti, 2019, 54). Transitioning influence operations from traditional environments to the virtual space is done in many studies by adjusting the concept definitions to the new digital ecosystem: "cyber-propaganda", "cyber-persuasion", "cyber enhanced disinformation", "cyber enabled information operations", etc. (Cordey, S., 2019, 11).

When focusing on the influence operation targets, we consider comprehensive a structure of three main categories, and, interpreted in a similar key, the structure can be also applied for the cyber influence operations:

- General societal level (mass audiences): targeting entire society, through synchronization of key messages and narratives with general topics that are already being embedded in the society's population preferences;

- Sociodemographic targeting (groups): this category focuses on targeting more in-depth layers of specific communities and groups based on sociodemographic factors like age, income or education;

- Psychographic targeting (individuals): a very specialized category aiming to profile (like in the recent Cambridge Analytica case) and target individuals with a specific psychographic profile, regardless if they are citizens or high-level decision makers (Pamment et al., 2018, 25).

The advantages of using influence operations to push for central topics of the foreign agenda in the present context are attractive from several perspectives. With the advancements of technology (both in terms of hardware equipment and available software), the costs for using influence operations in what we call "hybrid" operations have become extremely low. The computing power is at an affordable level for any individual or group seeking to plan, deliver and disguise an efficient delivery of such an action toward a target that can be even state level administration.

There is also a benefit from the anonymity point of view, as those types of operations are difficult to be attributed clearly and when the perpetrators roots are found the effects are already damaging the target. Without a possibility to quickly attribute an influence operation or cyber-attack, the initiator is motivated to use these types of actions at large scale, avoiding retaliations and sanctions. The "hybrid war" era is just starting and human cyber capabilities become a key point in responding appropriately.

In addition, social media and communication platforms facilitate the exponential transmission of the message, within a "virus" spread model, so that the effects are multiplied, producing a high-level damage to the adversary when successful. As numerous case studies proved it, the mix between digital groups, governmental structures and partisan media is powerful enough to break audiences even in advanced democracies.

What once was a complex, yet classic, operation requiring planning and logistic resources for some specific activities is now hundreds of time cheaper. For example, operations prepared by Soviet intelligence services to compromise the public image of important adversaries of the regime were at that time complex to deliver. It meant preparing false documents, inserting them with the help of the abroad influence network in friendly newspapers, then making efforts to be published by more relevant media and finally convincing international level publications to put them on the first page.

This is now extremely easy, as many evidences demonstrate how US national media accepted and validated, with their name and prestige, fake stories designed and built in the Russian laboratories. There is a common understanding that old techniques are being applied nowadays to influence targets with the help of modern tools: "Russia has increased its active measures' audience by taking advantage of the technological developments such as social media and the Internet" (Perkins A., 2018, 12). Recent studies showed that we should be preoccupied about the effects that such malign operations have among online audiences because "fake accounts can measurably affect the subsequent conversations held by genuine users" (Gallacher, John D. and Heerdink, Marc W., 2019, 186).

CYBER INFLUENCE APPARATUS

The most important question that arises now for many researchers and experts is: how is this happening, which is the propaganda mechanism that allows Russia to influence public agenda and especially voting opinions in many democratic states nowadays? First, we need to understand the logistics and manpower allocated by Russia's leadership for the active measure strategy (with cyber-influence activities as distinct steps included). Dr. Roy Godson, Professor of Government at Georgetown University, stated – during the review of the Russian active measures campaign conducted against the 2016 U.S. elections in the Select Committee on Intelligence of the US Senate – that "Russia has 10,000-15,000 people in the world-wide apparatus for active measures, in addition to the trolls and other kinds of cyber capabilities" (Select Committee on Intelligence of the United States Senate, 2017, 4-5). Same sources estimate that thousands of trolls and botnets are used in the cyber influence operations to diffuse disinformation in the social media, that finally reached and influenced millions of Americans in the election process (idem, 3).

The main base for most of the false content being spread on the social networks is located in Saint Petersburg, where a Russian company called Internet Research Agency (by some sources rebranded "TEKA"), owned by the oligarch Yevgeny Prigozhin, with close ties to Kremlin, is being used by the government to push the objectives of the Russian agenda. 1000 people – known generically under the term of Internet trolls – are going to work everyday to accomplish target metrics in terms of number of comments, shares, likes on different social media platforms with fabricated content, conspirations, fake news and intoxications that touch significant social groups within the targeted countries.

Pushing content and engaging audiences are done through accounts which are typically "fake personas" with no social media profile history or personal details. They don't provide debate arguments and they have as primary mission to create confusion, seed uncertainty, provoke and generate social distress. Some other tools are used also in these campaigns like mimicked news outlets, websites and documents (reports, analyses, photos) with appearance of originality and informative neutrality.

Trolls disseminate in large social media groups and pages points of view, ideas with appearance of representing personal opinions, conspiracy theories, false claims, "news" issued by partisan sources and disinformation content. They comment extensively, repeating same details, they share in an organized manner fabricated content and endorse each other.

Trolls are not enough to get the desired social media organic reach. Automation is therefore used to exponentially forward the trolls content through bots (or "electronic sheep") and push it on different platforms. Bots are actually a software application that writes tasks over the Internet, creates simple and repetitive actions like reposting content on Twitter, Instagram and other platforms with a higher performance rate, that would be otherwise inefficient for humans to deliver. While the advantage is the speed in diffusing the false content, there is a big gap in terms of originality and genuine behavior on the Internet: bots will be much easier spotted by people due to the lack of authenticity and their response patterns. So, here are coming to the battle the cyborgs, which are "more advanced bots coordinating the activities of automated accounts and human controlled trolls" (Willemo J., 2019, 22).

This entire cyber influence agenda is using the extensive power of software automation to efficiently communicate topics to the audiences. For some aggressive actions, persuasion of the public or providing the general "truth" (as in the Soviet era, even if the "truth" was in fact a "lie") are no longer planned. The aim is to confuse and create a distorted reality so that the audience cannot distinct the shades while the clear opinions are lost in the echoes of the fake content creators. It is imperative for the cyber planners to send their messages in a quick manner and in large numbers, in order to get the best ratio in term of effects versus efforts. We now enter into the world of algorithms and automation used to spread disinformation in what Oxford Internet Institute experts named computational propaganda which "involves learning from and mimicking real people so as to manipulate public opinion across a diverse range of platforms and device networks" (Woolley, S.C. and Howard, P.N., 2017, 6).

Other tools used by the Russian cyber influence apparatus are the cyber groups with role in attacking western infrastructures in cyber espionage actions. Although one of the benefits of the hybrid war is that you can embrace anonymity, avoid links with government objectives, as some of them (like APT28 or "Fancy Bears", "Pawn Storm", etc.) were exposed by cybersecurity and software companies (FireEye, SecureWorks, Microsoft) as being actually FSB/SVR or GRU units. Main targets for APT28 attacks are considered "the Caucasus (especially the Georgian Government), Eastern European government and militaries, and specific security organizations" (Foxall, A., 2016, 11).

Another known cyber espionage group is APT29, or commonly known as "the Dukes", which is also a capability expert team linked to Russia's leadership being characterized as a "well-resourced, highly dedicated and organized cyberespionage group working with Russian Federation since 2008" (idem, 7).

A particularly interesting online group linked to the Internet Research Agency troll factory is AgitPolk, considered by cyber experts to be more likely a volunteer one type. On September 20, 2017, the group responded to an online video posted two days before by the American actor Morgan Freeman, in which he condemned Russian interferences in the 2016 US elections. AgitPolk therefore created a campaign on Twitter branded #StopMorganLie, but also on the Russian social media platform VKontakte. The tweet was subsequently shared in just 2 hours and empowered with authoritative prestige by Russian Government official accounts, mainly those of Russian Embassies and Russian General Consulates, as demonstrated by Digital Forensic Research Lab of the Atlantic Council (Nimmo B., 2018).

A previous 2017 campaign of AgitPolk to honor Russian diplomats was at that time empowered by the Russian Foreign Ministry itself. Next tool in the online plan is Russia Today, official media arm of the Kremlin, which produced an article and shared it on other platforms like Facebook, about how social media users were rejecting Freeman assertions. Several small impact websites have taken then the RT news and posted it later on.

CONCLUSIONS

The AgitPolk case study is helpful in understanding pragmatically how the traditional Soviet Active Measures Strategy shifted with the help of the 21st century technology to the point that is now transformed into a modern propaganda machine. There is a strong expertise in Russia's last century activities in terms of conceiving, transmitting and exploiting the results of carefully planned operations towards foreign and domestic adversaries. Various forms that once emerged from the general spectrum of social influence have been nowadays transformed and powered with the support of algorithms and automation and put at work to sustain unidirectional governmental points of view.

Humans and machines are bonded by authoritative regimes seeking not to convince, but to confuse and divide large audiences with ease and efficiency. As we have already seen in the last years, capital elections can be decisively influenced, national referendums could be subject to foreign interference, and significant public agenda topics are interchanged so that the audiences stay focused on marginal events while important activities are not correctly noticed and addressed.

To prevent and respond, we need to completely facilitate the engagement of citizens and valid supporters like education (from early stages), media, NGO's, factual check teams, think-tanks, cross-domain experts, volunteers and government institutions. Even more, legislative regulations, cooperation with other governments or international organizations, and partnerships with private technology suppliers are mandatory steps, as the digitalization, access to high-speed broadband Internet and free access social media platforms have increased both the usage of the digital services and the spread of misleading content.

REFERENCE LIST

Bagge, Daniel P. (2019). Unmasking Maskirovka. Russia's Cyber Influence Operations. New York. Defense Press

Bonfanti, Matteo E. (2019). An Intelligence Based Approach to Countering Social Media Influence Operations. Romanian Intelligence Studies Review, 19-20/2018 (pp. 47-66). https://issuu.com/animv/docs/rrsi_no._19_20

Cialdini, Robert B. [1984] (2004). Psihologia persuasiunii. Bucureşti. Editura Business Tech International Press

Cordey, Sean. (2019). Cyber Influence Operations: An Overview and Comparative Analysis. Cyber Defence Project (CDP). Center for Security Studies (CSS). ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf

Dahl, Robert A. (1957). The Concept of Power. Systems Research and Behavioral Science 2(3), 201–215

Deutsch, M. & Gerard, H. B. (1955). A study of normative and informational social influences upon individual judgment. Journal of Abnormal and Social Psychology. 51 (3): 629–636

Elinschi-Ciupercă, Ella. (2003). Influența Socială. In Chelcea, Septimiu & Iluţ, Petru (coord.). Enciclopedie de psihosociologie (185-186). Bucureşti. Editura Economică

Ellul, Jacques. [1965] (1973). Propaganda. The Formation of Men's Attitudes. New York. Vintage Books

Foxall, Andrew. (2016). Putin's Cyberwar: Russia's Statecraft in the Fifth Domain. Russia Studies Centre, The Henry Jackson Society, Policy Paper no 9

F-Secure Labs Threat Intelligence Whitepaper. (2015). The Dukes: 7 years of Russian cyberespionage. https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Gallacher, John D. and Heerdink, Marc W. (2019). Measuring the Effect of Russian Internet Research Agency Information Operations in Online Conersations. Defence Strategic Communication. Volume 6, Spring 2019, DOI 10.30966/2018.RIGA.6.5

Ho, Shirley S. and McLeod, Douglas M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. Communication Research. 35, 2, 190-207

Kelman, H. (1958). Compliance, identification, and internalization: Three processes of attitude change. Journal of Conflict Resolution. 2 (1), 51–60

Nimmo, Ben. (2018). Russia's Full Spectrum Propaganda. A case study in how Russia's propaganda machine works. https://medium.com/dfrlab/russias-full-spectrum-propaganda-9436a246e970

Pamment, James, Nothhaft, Howard, Agardh-Twetman, Henrik and Fjällhed, Alicia. (2018). Countering Information Influence Activities: The State of the Art. Department of Strategic Communication, Lund University

Department of Strategic Communication, Lund UniversityPerkins, Alexander. (2018). Soviet Active Measures Reborn for the 21st Century. What is to be done? Middletown. Progressive Management Publications

Pomerantsev, Peter and Weiss, Michael. (2014). The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. New York. The Institute of Modern Russia, Inc

https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

Postmes, Tom, Spears, Russell, Sakhel, Khaled & de Groot, Daphne. (2001). Social Influence in Computer-Mediated Communication: The Effects of Anonymity on Group Behavior. Personality and Social Psychology Bulletin. 27, 1243-1254

Samuel C. Woolley & Philip N. Howard. Computational Propaganda Worldwide: Executive Summary. Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 14 pp

Scott, K. (2020). "Nothing up my sleeve: information warfare and the magical mindset". In Benson, Vladlena and Mcalaney, John, "Cyber Influence and Cognitive Threats", Academic Press, Elsevier Inc

Select Committee on Intelligence of the United States Senate. (2017). Disinformation: A Primer in Russian Active Measures and Influence Campaigns Panel I. Washington. US Government Publishing Offices

Vlăsceanu, Mihaela. (1993). Persuasiunea. In Zamfir, Cătălin şi Vlăsceanu, Lazăr (coord.). Dicţionar de sociologie (pp. 429-430). Bucureşti: Editura Babel

Willemo, Jacob. (2019). Trends and Developments in the Malicious Use of Social Media. Riga. NATO Strategic Communications Center of Excellence. https://www.stratcomcoe.org/trends-and-developments-malicious-use-social-media

Aurelian STOICA

Is an International Technology Professional with extensive experience in managing complex projects in different markets (Europe, North America, Middle East and North Africa). He has more than 14 years experience in IT&C companies and organizations (Orange Romania, Huawei Technologies, S&T Romania, SIVECO Romania, Optaros by MRM//McCann, National Institute for Research and Development in Informatics), and 8 years in Academic Research and Consultancy projects.