analysis

ISTITUTO PER GLI STUDI DI POLITICA INTERNAZIONALE

Analysis No. 319, January 2018

"MIND HACKING": INFORMATION WARFARE IN THE CYBER AGE

Fabio Rugge*

The good old days of cold war *disinformatia* are gone. Social media are increasingly relevant in shaping the public opinion, but they are just "eco chambers". Foreign actors with malicious intent can easily exploit this intrinsic feature of social media manipulating online information in order to influence the public opinion. Moreover, cyberspace allows a large degree of anonymity, behind which it is easy to automate propaganda, and cyber attacks may be leveraged to exfiltrate and expose sensitive content or to gain information dominance during military operations, increasing the strategic relevance of the "information space". Operations in this domain are central in Russia's security strategic thinking, featuring predominantly in its "New Generation War" military doctrine. But the ongoing militarization of cyberspace risks having dangerous spillovers in the conventional domain.

What can we do in order to protect our open democracies while preserving a global, free and resilient Internet? The answer is multi-faceted, in as much as CEIW (cyber-enabled information warfare) is an emerging asymmetric threat that forces us to innovate our security approach in many ways.

*** Fabio Rugge** is Head of ISPI's Centre on Cybersecurity. He is a diplomat and an Adjunct Professor of Security Studies at the University of Florence, "Cesare Alfieri" School of Social Sciences.

The views expressed in this article belong entirely to the author and do not necessarily reflect any official policy or position of any agency of the Italian government.

The desire to influence the public debate in foreign countries is nothing new, as *disinformatia* and psychological operations (PsyOps) have long been a tool in the arsenal of States. What is changing is the level of directness, the scale of activity and the scope of effort of these operations, made possible by the increasing pervasiveness of the Internet and by its rising relevance in shaping the public opinion. Cyberspace is a powerful multiplier of the destabilizing effects of manipulated information because it allows high connectivity, low latency, low cost of entry, multiple distribution points without intermediaries, and a total disregard for physical distance or national borders. Most importantly, anonymity and the lack of certain attribution of an attack make cyberspace the "domain of ambiguity", as we have seen in the first Dossier published by ISPI's Centre on Cybersecurity. When we talk about influencing the online debate we are therefore discussing "perception management" in an environment that is already quintessentially non-linear ("the medium is the message"), as the expressions "eco chamber" and "information bubble" describing social media clearly show.

These intrinsic features of cyberspace are easily exploited by foreign actors with the malicious intent to plant and disseminate fake news and instruct paid trolls (each controlling multiple online profiles) to spread online manipulated content in order to deceive, distract, and disinform the public opinion, trashing the debate with diverging truths, which eventually disorient and corroborate a sense of doubt among the public, or shape the opinion of a specific target audience on a certain issue.

Hostile actors in cyberspace are also willing and capable of leveraging the panoply of tools allowed by computer network operations (CNOs) and "computational propaganda" to influence public opinion to a degree that old-fashioned PsyOps could only dream of. These cyber tools allow a much greater impact on the target audiences, for instance creating a virtually infinite number of automated scripts (bots) to populate social media and interact with real online unwitting users; using social engineering technics for targeting purposes; rerouting data-flows or launching distributed denial of service attacks (DDoS) in order to interdict information; attacking the hardware supply chain; infiltrating the opponent's networks to steal, modify, implant or expose privileged information. In the case of military operations, also the physical destruction or the hijacking of Information and Communication Technology (ICT) infrastructure is a powerful option to influence the public debate: one of the first objectives of Russia during the operations in Crimea, for instance, was the occupation of the Simferopol Internet Exchange Point (IXP) and the disruption of cable connections to the mainland, which indeed contributed to Moscow's total information dominance on the peninsula. The warning released just few weeks ago by the head of the British Armed Forces, Air Chief Marshal Sir Stuart Peach, about the risk that Russia could cut off the UK by severing undersea communications cables, is a recent remainder of the concerns about physical threat to ICT infrastructures.

Information warfare: a threat to international security

Russia's interest in influencing the democratic processes of the West is a very hot issue in the international security debate. The threat of Russia's information warfare is prominently indicated in the National Security Strategy of the United States, released last December, where it is stated (pages 35) that "Russia uses information operations as part of its offensive cyber efforts to influence public opinion across the globe". Proofs of Russia's meddling in the last US presidential elections' public debate raised serious concerns across the Atlantic. The President of France, Emmanuel Macron, announced this January that he will soon propose a law to tackle the issue of fake news, especially during electoral campaigns, for instance by requiring a more transparent profile of the authors of online content. Last October, Germany approved the law on the "Enforcement on Social Networks": it is one of toughest laws in the Western world, designed to ensure that social media platforms remove fake news and hate speech within set periods of receiving complaints, and foreseeing fines of up to 50 million Euros if they persistently fail to comply. Last November, at the traditional Lord Mayor's Banquet, Great Britain's Prime Minister, Theresa May, warned: "So I have a very simple message for Russia. We know what you are doing. And you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of Western nations to the alliances that bind us".

The issue is also relevant to Italy in the wake of the general elections due in a few months. Former Italian Prime Minister, Matteo Renzi, recently warned about the risk of "weird connections" between some of his political opponents and media outlets allegedly involved in influencing the public opinion with manipulated information; its Democratic Party launched last December a monthly bulletin to "name and shame" fake news. Connections between some Italian political parties and Russia were, instead, given for certain in the last December's issue of *Foreign Affairs* by former US Vice President, Joe Biden, and former US Deputy Secretary of Defence, Michael Carpenter, who overtly accused Russia of attempting to stir the discussion around the December 2016 Italian referendum on institutional reforms. The Italian intelligence community promptly denied that any such interference occurred in the past, but remains vigilant.

Russia's approach to the "information space"

Back in 1998 (while Operation "Moonlight Maze", one of the first and most devastating cyber campaign ever orchestrated by Russia's intelligence against US military targets, was well underway…) the Russian Federation presented to the UN General Assembly a proposal for a Resolution titled "Developments in the field of information and telecommunications in the context of international security". The Russians wanted to discuss both cyber security and the limitations to destabilizing online content (revealingly gathered together by Moscow under the label of "threats to the information space"). The West refused to have that discussion, on the ground,

essentially, of its self-proclaimed moral superiority: if we want to safeguard an open Internet and freedom of expression, the West argued, it is not possible to negotiate about information's content. Ironically, almost twenty years later, the West is forced to discuss with Moscow about the threat of manipulated online content, which probably is, in itself, a score on the Russian side.

The approach highlighted in the Resolution of 1998 reflects Russia's strategic thinking: cyber-attacks and information warfare (we could also add electronic warfare, hybrid warfare,…) are, in Moscow's view, on an operational continuum. Cyberspace, in Russia's view, is one part of the broader "information space", which includes also ICT hardware and software, data and human information processing. This is confirmed in the Russia's Information Security Doctrine of 2000, which identifies two types of so-called "informational attacks": technical and psychological ones. If we assume that the ultimate strategic objective of Russia is that of undermining the cohesion and the stability of NATO and the European Union in order to renegotiate - from a better position - a new European security architecture, then, in order to obtain this overarching strategic goal, it does not really matter to Russia whether it is more suitable, in a given tactical context, to hack the opponent's networks or, so to say, "hack his mind" ("cognitive hacking"), or do both. Russia has an integrated and holistic approach to the "information space": while digital sabotages (CNOs) aim to infiltrate, disorganize, disrupt or destroy a State's functioning, psychological subversion (information warfare) aims at deceiving the opponent, discrediting its decision makers, and disorienting and demoralizing its public and armed forces. This is reflected in the current 2014 Russia's Military doctrine, the "New Generation War" doctrine (also known as "Gerasimov doctrine", from the name of the Russian *pro tempore* Chief of General Staff, Valeriy Gerasimov). The "New Generation War" doctrine enshrines a combination of hard and soft power (encompassing also economic warfare, energy blackmailing and pipeline diplomacy, support to political oppositions and agents of influence abroad, and other active measures) across different domains and through a skillful application of coordinated military, diplomatic and economic tools. In this context, "informational attacks" become the "system integrator" of both kinetic and non-kinetic military means as well as of government and non-government actors; they are waged during peacetime and wartime in domestic, the adversary's, and international media domains, and they are perceived as one of the most cost-effective tools of non-nuclear coercion, and an essential instrument to minimize kinetic engagements.

A textbook example of "informational attack" (or, in our lexicon, "cyber-enabled information warfare" - CEIW), that clearly combines both offensive cyber capabilities and information warfare, is Operation "Grizzly Steppe": the US Intelligence community assesses with "high confidence" (notwithstanding President Trump's skepticism) that Russia's intelligence (GRU) gained access to the Democratic National Committee (DNC)

computer networks in July 2015, and maintained it until at least June 2016. By May, Russia's Intelligence had exfiltrated large volumes of data from the DNC. Someone under the name of "Guccifer 2.0" subsequently leaked to Wikileaks.com and DCLeaks.com the material stolen from the DNC. The scandal that followed was exploited by a massive PsyOps to discredit Hillary Clinton and, more importantly, to erode trust in US institutions.

Considering the relevance of the "information space" in Russia's security strategic thinking and the intrinsic ambiguity of cyberspace, "informational attacks" seems perfectly suited for the job of the intelligence community that is so relevant in Russia. Cyberspace provides both unprecedented access to compromising material (available online or "securely" stored in PCs…) and a safe, efficient, effective and global distribution platform for gaining maximum strategic effect from its use. In order for data to became weaponised information, it does not really matter whether the content is forged or non-attributable; it is instead crucial to "make the first impression", to create the "sense of doubt" in the public opinion, to trash the information space with multiple truths - ultimately, to hack the cognitive domain. Moreover, the State's control over the "information space" is critical also at the domestic level: everywhere in the world, autocratic governments view the Internet as a threat to their grip on power - an information platform that must be monitored, censored and manipulated. Social media servers located outside of the government's control are an intrinsic threat, as Moscow's strict control over the Internet in Russia shows. The relatively low impact among the Russian public opinion of the Panama Papers' leak - that uncovered the personal wealth hidden abroad by Russia's leadership - is probably the result of such a control.

What's at stake

If operations in the "information space" are so critical in Moscow's "New Generation Wars", what does the escalation in directness, level of activity and scope of effort of Russia's activism in cyberspace tell us from the point of view of international security? Truth is, we do not really know. But it is reasonable to assume that much of what is going on in cyberspace (military and intelligence cyber campaigns; reconnaissance of networks; signaling about cyber capabilities in order to establish deterrence; information warfare,…) is part of a much greater game. How does what happens on global ICT networks relate, for instance, with the signaling concerning the level of readiness of conventional and nuclear forces? Ironically, understanding the ongoing political-military confrontation in cyberspace would require decoding an ongoing heavily encrypted interaction taking place on multiple tables and at the global level, just like hackers do.

Our limited perception of the ongoing confrontation in cyberspace is worrisome, for two reasons. First, there is an actual risk of misperceptions and miscalculations involved in States' responses to CEIW campaigns, as the tensions following Moscow's meddling

in the US presidential elections' debate show. Second, the use of cyberspace for projecting a State's power is endangering a free and open Internet, is fuelling the proliferation of aggressive capabilities through reverse-engineering of cyber weapons, is providing motivation and resources for hackers and organized crime engaged in identifying zero-days vulnerabilities and in developing cyber weapons, and is hijacking trust both among common Internet users and within public-private partnerships – which typically take years to develop. Our individual freedom and our societies' independence will be increasingly relying on a free, open and resilient Internet, and it would therefore be of key importance to safeguard it as a critical global common. We are unfortunately drifting toward a different scenario: sovereign States will inevitably aim at establishing information superiority over potential adversaries for the achievement of their own national security. Therefore the crucial question becomes: what can we do if we want to preserve our open democracies and one of the greatest accomplishments in human history against the risk of cyberspace becoming a warfighting domain? The general lack of awareness and consideration about the dangers and the responsibilities involved in this dilemma is a question of serious concern.

Mounting a multi-faceted response

What can we do to protect our democracies from the threat posed by fake news and cyber-enabled information warfare? The answer is multi-faceted, in as much as CEIW is an emerging asymmetric threat that forces us to innovate our security approach in many ways. Investments in technological innovation and cyber capabilities aside, there are probably at least five major endeavors.

If foreign influence is the virus that attacks democracies, the first aspirin (or, if you will, the most effective firewall) is **awareness & education**. Awareness about the threat, the game at play and the price at stake, both among the general public and at the top institutional level, is the first line of defence. Education in dealing with the cyber threat, in particular, is a powerful ally against CEIW, as reducing cyber vulnerabilities, enhancing the resiliency of our ICT infrastructure, and encouraging cyber hygiene in the general public would drastically reduce the potential damages of cyber attacks (for instance: the malware "Wanna Cry", that affected so many computers in 2017, used a well-known vulnerability, that was patchable long time before the campaign was launched). Cyber hygiene would also greatly contribute to the fight against cybercrime, which is the gym, the ATM, the fog of war of a far more dangerous game entailing state-actors' attacks for espionage, intelligence, surveillance and reconnaissance (ISR), deterrence, targeting, war fighting prepositioning. We are not saying that cyber hygiene and a greater awareness about the cyber threat will, *per se*, protect countries from cyber advanced persistent threats (APTs), hybrid scenarios or "New Generation Wars", but they are an easy and relatively inexpensive measure that could allow us to devote our scarce financial and technological resources to face even more serious threats and

challenges. Explaining to the general public the dangers of manipulated information will also constitute an efficient cultural barrier against fake news, while our societies develop a healthy skepticism as they learn to manage, interpret and evaluate large volumes of non-intermediated information. Education, in other words, reduces the "eco-chamber effect" of social media, ultimately making us better citizens.

A second critical element for countering CEIW is **our societies' coherence with their core values**: information warfare represents an attack to an unavoidable vulnerability of open democracies, but this does not mean we shall question or negotiate our commitment in transparency, openness and the rule of law. While we must confront foreign information warfare head-on, and we must increase transparency in political funding in order to avoid foreign meddling in our democratic processes, we must also, at the same time, avoid a witch-hunt against whoever is ideological aligned with Moscow's stances: such a course of action would ultimately erode the legitimacy of our democratic institutions, with the effect of dissipating precisely what we wanted to preserve. Instead, open democracies should work on reinforcing their institutions and the public support they deserve. The best way to do this is proving how they are able to deliver innovative solutions to manage the complexity of today's world. In this context, one discussion that seems urgent is the one concerning the strategic relevance of public-owned ICT infrastructures and independent media. Revealing, in this sense, is the discussion underway at the global level (but not much in Italy…) about net neutrality. The new US administration's decision to abandon President Obama's choice on net neutrality reflects the idea that the Internet is primarily a commercial environment and that market forces are best suited for ensuring its growth. But the Internet is clearly much more than this: it is, primarily, an infrastructure that is essential for the functioning of modern societies. Not recognizing this role at the domestic level risks undermining our ongoing international efforts to ensure an open Internet at the global level. Coherence to our values means, also, that politicians should refrain from undermining public opinions' faith in the free press just because they are the objects of unflattering but genuine journalism, because disinformation works best precisely where there is a lack of trust.

Another important element in our response to Russia's CEIW is to **refrain from launching, at least in peacetime, retaliatory strategic communication** (Stratcom) on our own citizens or on citizens of allied countries, as this would ultimately undermine faith in the free press and trust in international relations. Likewise, retaliatory Stratcom would most likely reinforce (and, to a certain extent, even justify) Russia's perception that information campaigns have been and are implemented by the United States and the West in order to influence the course of a series of regime change over the last two decades ("Color Revolutions" and the "Arab Springs"). The danger, in other words, is that of fuelling an escalation in the conventional domain with relevant repercussions. Instead, a viable option, although a very challenging one, is to respond to information

warfare not retaliating in kind, but countering its desired effects. ISPI, for instance, is one of the many think-tanks that launched a fact-checking initiative to expose fake news; likewise, many institutions are focusing not on developing a counter-narrative, but rather on exposing the mechanism behind fake news, such as the "East StratCom Task Force" launched in 2015 to counter Russian propaganda in Eastern Europe, the "EU myth-buster" and the US State Department's Global Engagement Center, that do not. The new US National Security Strategy seems to point to this direction, where it declares (p. 35): "We will craft and direct coherent communications campaigns to advance American influence and counter challenges from the ideological threats that emanate from radical Islamist groups and competitor nations. These campaigns will adhere to American values and expose adversary propaganda and disinformation."

A fourth initiative to counter CEIW is **strengthening our governance and response-mechanisms at the institutional level**. Michael V. Hayden, who served as CIA Director under President George W. Bush, described the Russian interference in the last US presidential elections as the political equivalent of the 9/11 attacks - an event that exposed a previously unimagined vulnerability and required a unified American response. The transformation underway at NATO, which is actively involved in developing doctrines, structures and mechanisms to counter hybrid threats, shows that new institutional and operational arrangements are needed. As suggested by Prof. Adriano Soi in his contribution to the second ISPI's Dossier on cybersecurity, maybe it is time to update even at the domestic level our decision-making processes and to develop an *ad hoc* strategy and specific structures and procedures for countering the emerging threat of CEIW.

Finally, the West should build on the idea that, in order to counter an asymmetric threat, the best possible strategy is **partnering with those that are defending against the same menace**. At the international level, this means strengthening both at the strategic and at the operational level our cultural, political and military alliances, and working actively to establish confidence building measures (CBMs) and norms of States' behavior in cyberspace. At the domestic level, CEIW compels us to actively engage in a coordinated effort all relevant public-private stakeholders, key ICT infrastructures' owners and operators and, also, media outlets, building within this communities as much trust as possible. Private companies should not be the arbiters of truth, but they do, however, have an interest in preserving a safe space for genuine content, and this interest could and should be leveraged. The success in engaging Internet providers and social media operators in countering online jihadist propaganda and radicalization, gained by the G7 Ministries of Interior last October at the meeting organized by Minister Marco Minniti in Ischia (Italy), is an excellent example of what can be done to develop a shared responsibility among key stakeholders, and could be fruitfully pursued also in the response to cyber-enabled information warfare.