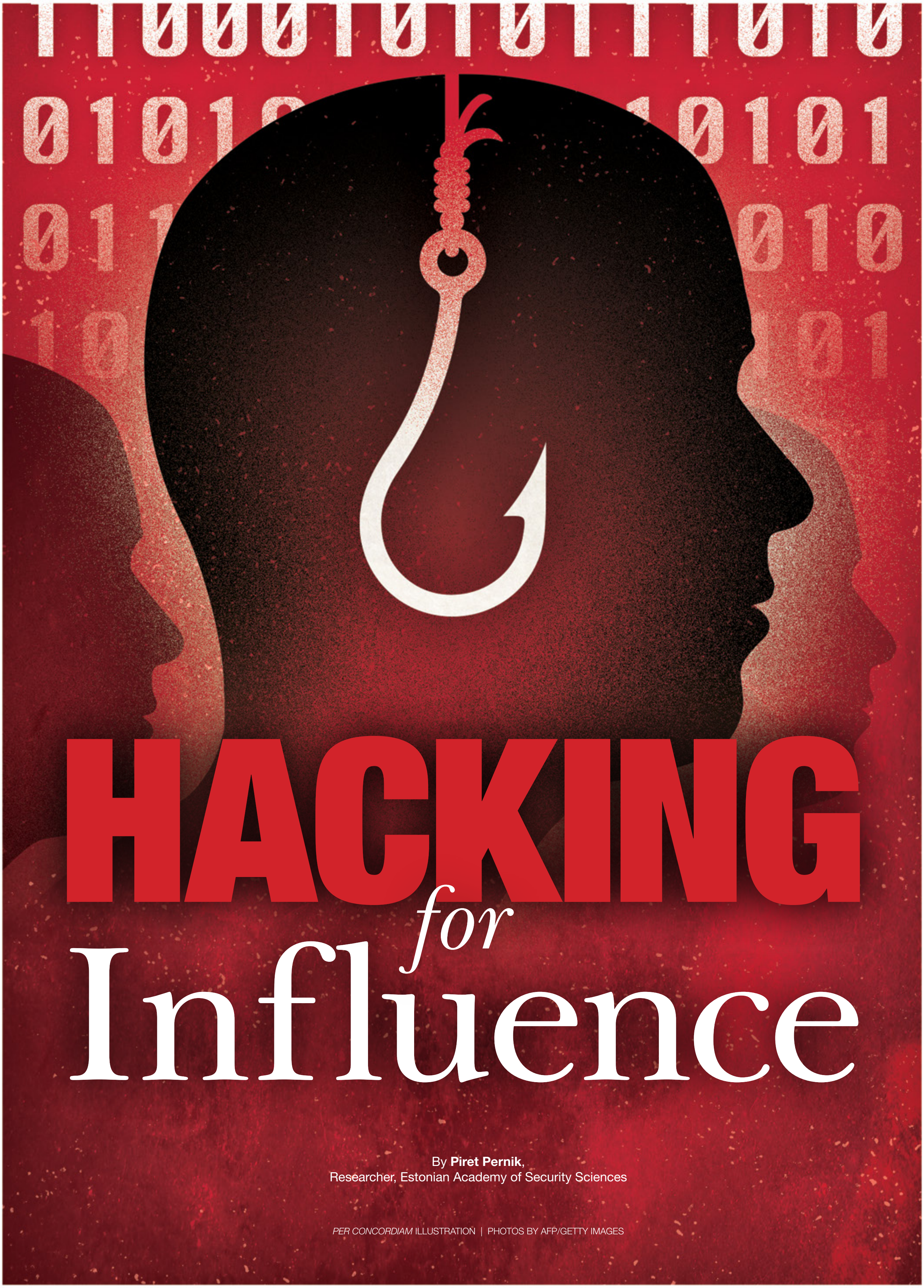


HACKING *for* Influence

By **Piret Pernik**,
Researcher, Estonian Academy of Security Sciences

PER CONCORDIAM ILLUSTRATION | PHOTOS BY AFP/GETTY IMAGES

Cyber attacks are key to Russian information warfare

In recent years, liberal democracies have found themselves increasingly subjected to nonkinetic attacks from authoritarian countries, especially in cyberspace. All nation states — democratic and authoritarian — have traditionally used cyber capabilities to gather intelligence in foreign countries, but today low-intensity political warfare in cyberspace has become more prominent. Unfortunately for democratic countries, cyberspace is an ideal environment in which to undermine democratic processes and institutions using diverse covert activities.

Authoritarian states and their proxies use cyber attacks in support of other influence activities. In cyberspace, the major state adversaries to democratic countries are China, Russia, Iran and North Korea. Among them, China and Russia have developed mature information warfare and information operation strategies and tactics, and Iran is effectively copying their activities. While the focus here is on Russian theory and practice in using cyber attacks for soft subversion, it should be emphasized that China's approach is similar. Both see free information and foreign technologies as threats to their "cyber sovereignty" and seek to control cyberspace and the information contained within. Similarly, neither distinguishes between peacetime and wartime information-related activities. They have long traditions of strategic thinking about the role of information in projecting national power and holistic understandings of the information space. It is unlikely that China's or Russia's strategies will change remarkably any time soon.

Russian and U.S. viewpoints

Russia's primary strategic documents (the Military Doctrine of the Russian Federation of 2014 and the Russian Federation's National Security Strategy of 2015) identify the use of information and communications technology for political and military purposes as a main security and military threat. They depict Russia's information counterstruggle as a defensive measure and a strategic priority in peacetime and wartime alike. Moscow perceives European Union and NATO enlargement and the "color revolutions" in former Soviet republics as threats to Russia's geopolitical interests and national security. Information of Western origin is consequently perceived as a security threat and the information environment as a domain of operations.

> Russia regards its information warfare against the West as a "threat-neutralizing measure" to deter what it perceives as hostile activities.

Against this backdrop, Russia regards its information warfare against the West as a "threat-neutralizing measure" to deter what it perceives as hostile activities. In this way, information freedom and its medium, the free and open internet, become Russian targets. This view, which may seem paranoid to some, is expressed frequently by senior Russian government officials and key leaders. For example, President Vladimir Putin's spokesman, Dmitry Peskov, claimed that

Russia is “in a state of information warfare with the trendsetters in the information space, most notably with the Anglo-Saxons, their media.” Sergey Kislyak, the former Russian ambassador to the United States, claims that the U.S. runs “a massive propaganda campaign … with the purpose of undermining the internal political atmosphere in Russia.” According to journalist and author Andrei Soldatov, the Kremlin genuinely believes it is under attack from the West, and Russia’s strategic activity is, therefore, always reactive. However, according to Dmitry Adamsky in a 2015 paper for the French Institute of International Relations, in the Russian view, deterrence in the information space can coerce an opponent’s behavior in the other domains of operations.

The Russian concept of information warfare can be described as *informatsionoye protivoborstvo* (information confrontation or counterstruggle). The Russian defense ministry defines its purpose as “to inflict damage on [an] opponent by means of information in [the] information sphere.” The main mechanisms to cause harm are divided into information-psychological and information-technical tools. Technical tools are low-level cyber attacks (for instance, unauthorized access to information resources). The end goal is a change in the strategic behavior of an adversary, which is achieved by manipulating their picture of reality and consciousness through technological and psychological components of the counterstruggle.

> “For Russia, the objective of psychological activities is to affect the will, behavior and morale of the adversary, and the more subtle emotions that impact rational thinking.” ~ V.A. Kiselyov, *Military Thought*

Psychological measures encompass anything that can be used to influence the general population and armed forces personnel. V.A. Kiselyov, in a 2017 article for the Russian journal *Military Thought*, tells us that, for Russia, the objective of psychological activities is to affect the will, behavior and morale of the adversary, and the more subtle emotions that impact rational thinking. Adamsky describes this activity, known as reflective control, as a state attempting to predetermine an adversary’s decisions in such a way that the adversary believes it is behaving in its own interests. According to Russia’s military doctrine, information warfare in modern conflicts does not solely target an adversary’s key decision-making, but extensively uses “the protest potential of the population.” U.S. military doctrine is much less nuanced in the area of psychological influence on the population. It states simply that the aim of information operations is to create doubt, confuse and deceive, and to influence decision-makers, militaries and various other audiences, but it is silent on the need to manipulate the sentiments of the population. According to Adamsky, Russia views the main battlefield as human consciousness, perceptions and strategic calculations. Prominent Russian information warfare expert Sergei Modestov says there are no borders in the battlefield of the cognitive domain. The borders are blurred between war and peace, tactical, operational and strategic levels of operations, forms of warfare (offensive and defensive) and coercion.

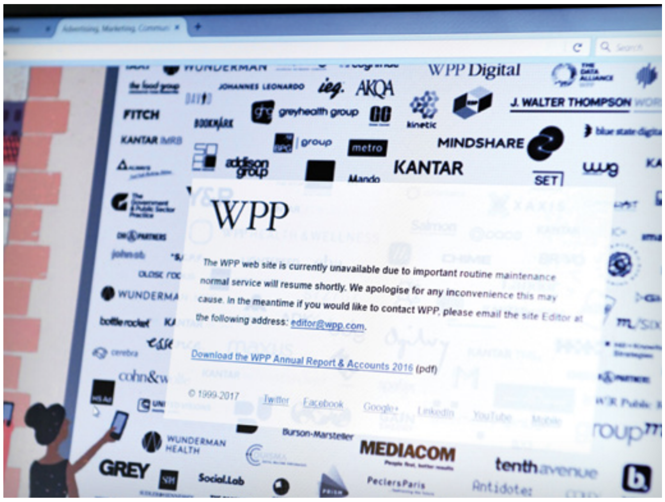
Two key aspects distinguish Russia’s understanding of the information confrontation from the U.S. military’s view of information operations. In the Russian view, it is first conducted constantly during peacetime and, secondly, it is a strategic-level activity executed by a whole-of-society response that recalls the Soviet-era concept of total defense, according to which all the resources of civil society were used for national defense. Russia expert Mark Galeotti, in a 2016 article for the European Council on Foreign Relations, described how the Kremlin carries out this holistic approach by outsourcing the policy implementation to volunteers, organized-crime groups, business, the Russian Orthodox Church, government-organized nongovernmental organizations, the media and other actors in the deployment of various active measures. By contrast, the U.S. military perceives information operations as a wartime activity executed by designated authorities whose action is legally constrained by their mandates. For the U.S., this activity is conducted at the operational level.

In several respects, the U.S. and Russian views also display similarities. For Russia, Kiselyov asserts, violent physical acts, such as “kidnapping adversary officials” and “physical destruction of adversary assets and targets,” are also psychological tools. Likewise, the U.S. includes physical destruction among information operations tools. Accordingly, actions in the domains of operations (land, air, sea, space and cyber) can have psychological effects. Both countries reckon that cyber attacks are part of the information warfare toolkit, and that information-related activities are to be conducted simultaneously in the cyber and physical spaces. Both countries include defensive activities (e.g., operational-level security, and protecting their own infrastructure, networks and forces) as part of information warfare, and they agree that the ultimate objective of information warfare is information superiority. Russia emphasizes information-psychological capabilities because the control of information, including internet content and physical infrastructure, is seen as security for the survival of the regime. In contrast, the U.S. emphasizes information-technological capabilities.

Asymmetric measures

Russian foreign policy instruments can be divided into six broad categories: governance, economics and energy, politics and political violence, military power, diplomacy and public outreach, and information and narrative warfare, as outlined by Robert Seely in a 2017 paper for *RUSI Journal*. In addition to the traditional tools of national power, Russia uses a mix of covert influence tools referred to as active measures. In a way, the Kremlin has weaponized every factor of modern life at the personal, organizational, nation-state and global level — culture, history, nationalism, information, media and social media, the

Customers try to enter a closed branch of Oschadbank in Kyiv, Ukraine, in June 2017. A wave of cyber attacks wreaked havoc on government and corporate computer systems as it spread to Western Europe and across the Atlantic.



WPP

The WPP web site is currently unavailable due to important routine maintenance normal service will resume shortly. We apologise for any inconvenience this may cause. In the meantime if you would like to contact WPP, please email the site Editor at the following address: editor@wpp.com.

Download the WPP Annual Report & Accounts 2016 (pdf)

© 1999-2017 Twitter Facebook Google+ LinkedIn YouTube Mobile

The homepage of British advertising giant WPP is pictured after it became one of several multinational companies targeted in a cyber attack that started in Russia and Ukraine before spreading to Western Europe in June 2017.

internet, business, corruption, electoral processes and globalization. In this struggle, information has been rendered a target, disinformation a weapon, and the internet a battlefield.

One of the principal threats posed by a democratic worldview to the Russian model of governance is the principle of freedom of expression, including its manifestation in a free and open internet. The internet can whip up protests and uprisings — the color revolutions, for example — and the Kremlin fears that an Arab Spring-like upheaval in Russia could sweep it from power. The Kremlin's fear of a free and open internet was expressed by Putin in 2014 when he claimed it was a "CIA project" from which Russia needed to be protected. For this reason, a multistakeholder internet governance model is perceived by Russia and many other authoritarian countries as inherently dangerous. These governments intend to increase their control over cyberspace content and physical infrastructure, as well as software and hardware. Whether for defensive or offensive purposes, or a mixture, Russia has used cyberspace to conduct political influence activities at the strategic level against many EU and NATO member states, as well as in the Western Balkans, the South Caucasus and Central Asia.

Each country is vulnerable to Russian active measures in different ways. Galeotti distinguishes seven types of Russian influence strategies that seek to exploit specific weaknesses and allegiances in individual countries. For example, Bulgaria and Greece have two types of vulnerabilities: a Russia-friendly political and business elite and weak democratic institutions. Russia cultivates a strategy of "state capture" by attempting to make these countries Trojan horses within the EU and NATO. Hungary, Romania and Montenegro also have weak institutions, but their affinity to Russian interests

> "The beginning of wisdom is to understand that the Russian pursuit of influence is a continuous, background effort not confined to 'influence operations.' It is labour as well as resource intensive, built on local knowledge, the cultivation of individuals and the long-term development of networks."
>
> ~ James Sherr, foreign policy expert

is moderate. Russia therefore seeks to influence them only on specific issues (e.g., EU sanctions) by cultivating a strategy that targets the state.

The remaining strategies are, according to Galeotti, exploitation (in the United Kingdom), demonization (in Estonia and Poland), disruption (in France, Germany, the Netherlands and Sweden), influencing (in the Czech Republic, Italy, Latvia and Lithuania), and social capture (in Slovakia). In the information environment, Russia has likewise cultivated specific memes and narratives to influence different countries. It has used social media bots to influence public opinion in the U.S., the U.K., the Netherlands and Spain. In Hungary, the Czech Republic and Austria, it used a multitude of local political, economic and disinformation actors, according to the 2017 paper "Does Russia Interfere in Czech, Austrian and Hungarian Elections?" Russian disinformation practices in Europe show that specific influence tools are chosen after considering particular strengths (e.g., free speech) and vulnerabilities to be exploited and the expected effects. Russia deemed social media to be an effective medium for covert disinformation activities in the U.S. That enabled it to target selected demographic groups in certain geographic areas over great physical distance with low risk of escalation. In several Central and Eastern European countries, physical influence activities (corruption and cultural, national and other allegiances) yielded better strategic-level effects than the abuse of social media platforms would have achieved.

Hence, Russia exacerbates various socio-economic and ideological grievances in Western societies related to processes such as globalization, technological innovation, nationalism, fundamentalism, immigration and climate change. In addition

A Russian aircraft arrives at Dulles International Airport outside Washington, D.C., in December 2016 to pick up Russian diplomats expelled as part of sanctions imposed on Russia for suspected cyber attacks during the United States elections.

to country-specific vulnerabilities, it exploits the openness and freedom of democratic systems. In the words of James Sherr, an expert on Russian foreign policy, "attributes of the liberal polity that normally are a source of strength, e.g., 'fairness,' can also be used to undermine liberal democracy and advance hostile objectives."

He writes: "The beginning of wisdom is to understand that the Russian pursuit of influence is a continuous, background effort not confined to 'influence operations.' It is labour as well as resource intensive, built on local knowledge, the cultivation of individuals and the long-term development of networks."

Many experts take the view that Russia's approach to the information confrontation has been constantly evolving, developing and adapting, and others believe that in the process it has become refined and tailored.

To sum up, the Soviet-era experience in the use of active measures and intimidation has been adapted and elaborated for modern use. Asymmetric tools that can be outsourced to various actors are attractive for projecting Russian national power due to their low cost and wide availability, a degree of anonymity and stealth, a low risk of escalation and great destabilizing potential, as described in a 2017 Atlantic Council report. What perhaps distinguishes Russia, according to Seely, is that asymmetric activities are highly integrated with one another and coordinated with conventional operations in early and defining phases of military conflict (e.g., kinetic operations in Georgia and Crimea).

The prison jacket of Enn Tarto, an Estonian former political prisoner who spent years in Soviet jails, hangs in the hall of Tallinn's Occupation Museum as a reminder of Russia's past subjugation of its neighbors.

Conclusion

The unique nature of cyberspace makes it an ideal domain for gray zone cyber attacks and other cyberspace-enabled political influence activities. Cyber capabilities differ from kinetic weapons in many respects, and conventional concepts fail to account for the dynamics in this complex domain. Cyber espionage seems to have strategic effects, while low-end cyber attacks tend to produce tactical and operational effects; however, together with psychological operations, they can have strategic effects on national security. Armed forces use cyber attacks in kinetic conflicts and also outside a conflict zone against civilian targets. They are conceived as force multipliers in support of operations in other domains and sometimes replace the kinetic use of force. In some cases, cyber attacks likely have psychological effects of their own, but there is still little understanding about the scope of possible impacts. There is also little understanding about the strategic effects of cyber attacks for national security and interstate relations. For this reason, past cyber attacks deserve better scrutiny.

Russia does not apply a uniform cyber-attack strategy across all targets but considers various opportunities innovatively as they emerge. Cyber attacks are ideal weapons for authoritarian states to project national power and support other political influence activities. They can be used for deterrence and coercion, but a better international relations theory for cyberspace should be developed to explain how cyber attacks translate into deterrent or coercive effects. Quantitative and qualitative methods, and operational and strategic level analysis, should be combined to develop a new theoretical and conceptual framework for understanding this fast-evolving domain and how authoritarian states are exploiting it. □

This is an abbreviated version of an article published by the International Centre for Defence and Security in Estonia.