Analytical Dossier 12/2020 ISSN 2704-6419

New Russian Deterrence Strategy

Andrej Il'nitskij

International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)
Analytical Dossier – N. 12/2020 – June 2020

First Edition: June 2020

Analytical Dossier – N. 12/2020

www.vision-gt.eu

New Russian Deterrence Strategy

The purpose of this article is to analyze the geopolitical threats that Russia faces in the context of the coronacrisis, global economic collapse, political chaos of the West and US military preparations.

How and what the USA is preparing for, how they see threats and future conflicts, how they determine their role in the world, who will be their enemies tomorrow – the answers to these questions are contained in published reports of RAND Corporation. It is a leading American analytical institute developing strategy for US and Pentagon.

It's worth starting with the RAND report, **Peering into the Crystal Ball. Holistically Assessing the Future of Warfare**, that was released on May 11, 2020.

The authors of the report specify ***the strongest political crisis in the United States***. The statement is based on analysis of the current geopolitical situation and probable scenario for the near future.

> *The American public is becoming increasingly polarized on many issues—including foreign and defense policy—which is producing political gridlock in the United States. This gridlock will limit the nation's ability to do the tasks needed to act effectively as a global superpower.*

The authors of RAND directly point to the option of finding solutions to overcome the crisis through the war!

> *Politicians might increasingly look for military solutions because the military is one of the few government institutions that Americans trust*

It is clearly indicated that the United States **will to try to maintain its position as the world's leading military superpower.**

> *The Chinese and Russian militaries are becoming increasingly capable, as both continue to modernize and professionalize.*
> *Both of these countries, along with Iran and North Korea, will increasingly turn to asymmetric capabilities such as cyber operations, missiles and weapons of mass destruction to counter the usual US superiority.*

Control of the cyber domain *will become increasingly central to domestic stability. The cyber domain becomes a tool for foreign subversion.*

US rivals – China, Russia, Iran, North Korea and terrorist groups *are likely to remain unchanged, but US allies may change as The European Union is becoming more fractured, less interested in expeditionary operations, and increasingly inward-looking.*

A revanchist Russia. *Although Russia is arguably a declining power, it is growing more aggressive, intervening in Georgia, Ukraine, and Syria and reaffirming its position as a great power.*

Thus, from a military point of view, Russia is clearly positioned as an adversary of the United States. Confrontation with the United States will increase not only on land, in sea and air space, but also in other areas, including space, information and cyberspace.

The most relevant external influence factors on Russia are information-ideological and cyber-threats. These threats cause mayhem and sow the seeds of doubt in the minds of people, undermining trust in relations between "power and society", destroying social infrastructure, and, as a result, weakening the state.

We will focus on these threats.

How will our potential adversaries act?

By 2023, a new form of war will be conceptually consolidated - virtual social warfare, as a mechanism for undermining sovereignty and destruction of states (according to RAND's report **The Emerging Risk of Virtual Societal Warfare. Social Manipulation in a Changing Information Environment - October 2019**). The methods of this warfare are very sophisticated. They may include political sanctions and covert operations aimed at creating the Fifth column in the target country with the help of Diasporas or ethnically related communities.

Today it is obvious that Russia is an object of large-scale informational campaign, and information warfare has been unleashed against it.

The purpose of the expanded campaign is to discredit Russia, show it as an aggressor / cyber-terrorist country. All possible means, all existing classical and digital Media are used to achieve this goal.

How will this war be waged / already waged?

The answer is contained in a recent analytical report of the JSC Kribrum made for the Center for Political Information - **"Information warfare against Russia. Designing the image of an enemy."** This issue is the first document in a series of studies of social networks and the Media, in order to identify the

tools and methods of our rivals. The specialists used unique, unparalleled, national technologies for working with information arrays of the global network.

The Twitter network was chosen for the first study. It is the service with the fastest response to current socio-political events, which accurately reflects the state of the information field as a whole. President Trump directly communicates with the people of the United States and the world with the help of this network.

The results of this study show how the negative image of the Russian special services (FSB, SVR, GRU, etc.) and Russia as a whole is being formed.

This image is transferred / exported to Russia through Russian-speaking platforms in Ukraine, Georgia, Poland, the Baltic states, Israel, etc., as well as the fifth column inside the country. Then the negative opinion is formed among Russians about the country's leadership.

Stages of the export process of the "image of an enemy"

The following statements frighten the ordinary people in the West:

- Aggressive Russian army hanging over the borders of the "free world"
- "Ominous and all-pervasive" Russian hackers serve in the special agencies of the Russian Federation.
- Russian hackers interfere in every social process, from elections to the functioning of the Media and public toilets.
- Hackers undermine the foundations of Western civilization.

Cynicism rolls over here. The reasons for criticizing Russia in the geopolitical arena are diverse, but technology is dull and uncreative. Scenario is always the same: The West blames "Russian special hackers" for every

possible incident, whether it is a sewerage breakdown or a failure of municipal power grids or major political revelation and scandal.

Here are recent examples.

"Accuse a Russian" special campaign. The West laid the blame on "Russian hackers" for the attack on Czech medical institutions committed between December 2019 and March 2020. Documents and databases of these institutions were published in the Web. It would seem a small and local event. However, this incident was used to form anti-Russian public opinion in the context of the demolition of the monument to Marshal Konev in Prague. The reason for such groundless accusations was the letter of Russian Minister of Defense Sergei Shoigu published on April 9, 2020, demanding the monument to Marshal Konev, which was dismantled in Prague on April 3, 2020, to be returned to Russia. Three days after, Czech President Milos Zeman called the dismantling of the monument "stupid and ridiculous action." Czech Defense Minister also supported the concern of his Russian counterpart.

And then the Bacchanalia began. Czech and Western Media reaction on "a warming of Russian-Czech relations" came immediately. On April 16, the first accusations against Russia of hacker attacks on Czech medical facilities appeared. Details were published in the Czech internet resource Seznam Zprávy with the headline: **"The source of cyber-attacks on Czech hospitals is unveiled."** The charges were based on Czech IP addresses that had been rented by a company with the office in Moscow. However, it seems unlikely that the authorities of the Czech Republic acted alone.

The United States and the pro-American part of the European establishment were also interested in updating the topic of the "Russian threat". The purpose was not only to "correct" the pro-Russian deviation of the Czechs, but also to undermine the positive media background around the Russian humanitarian aid to Italy and Serbia in the fight against the coronavirus pandemic.

The same scenario was used to explain cyber-attacks on British medical facilities. On April 22, the British ambassador to Russia, D.Broner, thanked the Russian Foreign Ministry and Aeroflot for their help in returning British citizens to their homeland. On May 3, the British National Cybersecurity Center accused Russia of trying to steal the development of British virologists searching for a coronavirus vaccine in early March 2020.

At the same time, anti-Russian propaganda campaign was launched in Germany accusing the "Russian military hackers" of breaching into the Bundestag servers and personal emails of Federal Chancellor A. Merkel in 2015. Moscow’s geopolitical rivals set out to undermine the initiatives to lift the sanctions regime against the Russian Federation, to prevent cooperation between the two countries in the fight against the pandemic, to block the commissioning of the Nord Stream-2 gas pipeline, as well as "reverse" the emerging "thaw" in Russian-German relations.

The Western media could not ignore the improvement in Russian-Polish relations. In April 2020, the foreign ministers of Poland and Russia announced the normalization of bilateral relations. The information agenda was "knocked down" by accusations against Russia of cyber-attacks on Polish educational institutions, committed in May 2019.

Those who wage the information warfare against Russia try to spin something out of nothing. No one cares about the lack of evidence.

Another prime example is the cyber-attack on Georgian websites and TV channels after an unacceptable tirade by Georgian TV presenter Giorgi Gabunia against President Vladimir Putin. Accusations against Russia are mainly based on the statement by the U.S. Embassy in Georgia. The BBC refers to the UK National Cyber Security Centre, which noted that British intelligence determined that it was GRU behind the cyber-attack on Georgia in 2019 with a probability more than 95%. However, there is no such information on the UK cyber-center website.

It’s an open secret that Western special services are able to imitate "hacker TTPs" (Tactics, Techniques, and Procedures) of Russian IT-specialists, including those who work in intelligence agencies and responsible for the information security of Russian Federation. To this end, the US and its allies use services of Russian-speaking hackers from the countries of the former Soviet Union. In addition, they developed their professional skills within the framework of the Soviet school of cryptography. That is why they may use instructions in Russian.

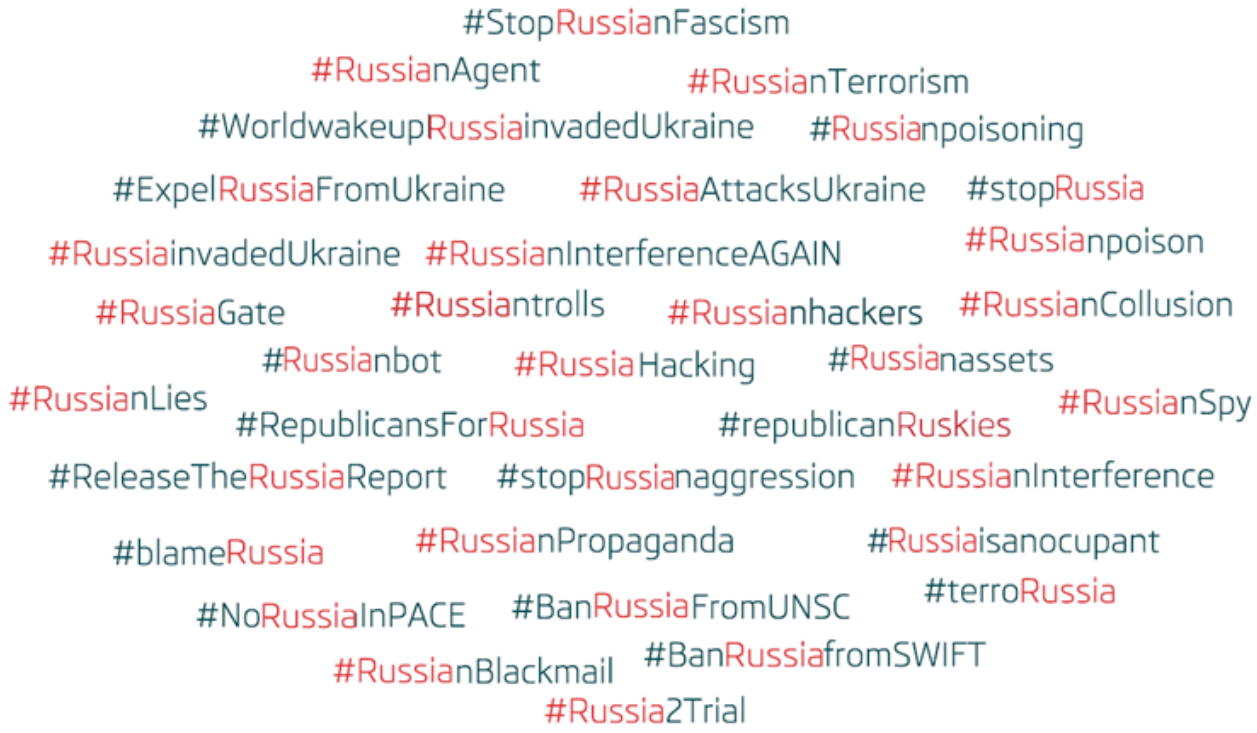
In some cases, the West may create a "false" hacker group that is used to organize provocations. It’s not difficult for a team of qualified specialists to disguise TTPs of "Russian hackers". Washington and its allies have been actively conducting such "false flag operation" of simulating cyber-attacks for several years.

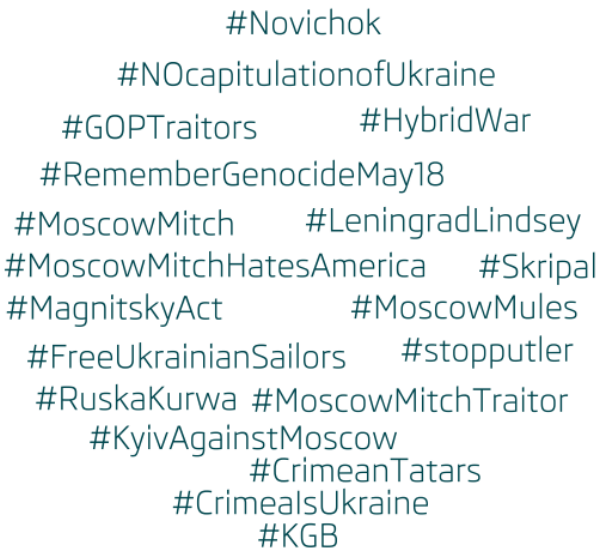
The myth of the omnipresent "Russian hackers", who can break into anywhere and turn off anything, has become the same horror story for Western politicians as the "Boogeyman" for American children. It’s amazing that photos of keyboards of Russian hackers with "Belomorkanal" cigarette butts and bottles of "Stolichnaya", as well as passports and ID cards of Russian officers, have not been published yet. According to Western opinion Russians even go to the toilet room only by presenting a passport to a representative of the totalitarian regime.

The same report of JSC Kribrum presented the algorithms of those information campaigns that are conducted in social networks against Russia. They are very revealing and interesting.

For the first time were identified and introduced clouds of tags and keywords of tags used in pro-Western microblogs and social networks to facilitate the search for messages by topic or content.

The logical sequence here is obvious - **the aggressor, interference, hackers, special services, Russia, Vladimir Putin** ... And as a conclusion, Russia is a cyber-terrorist country.



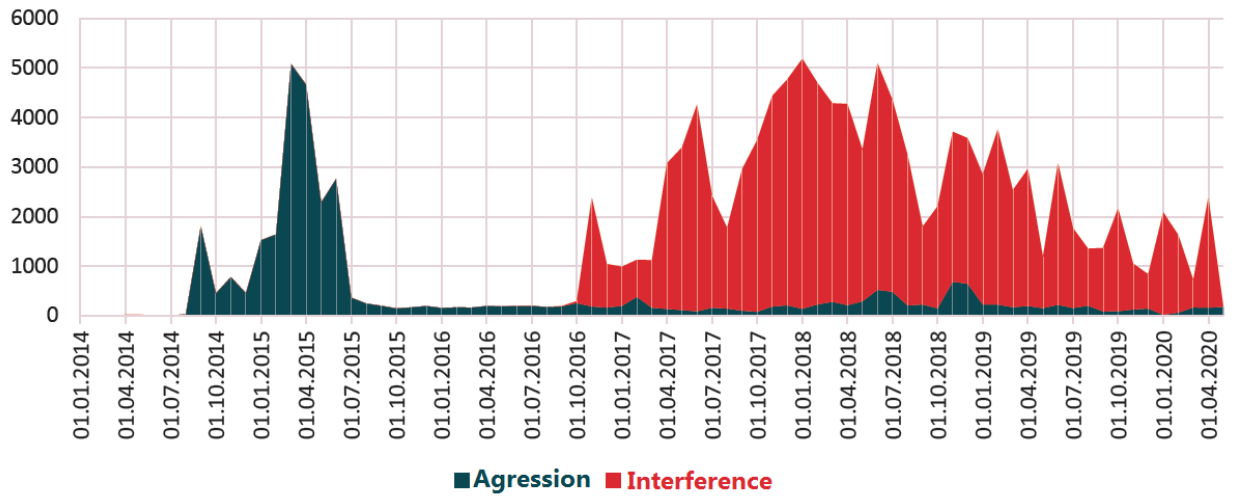


Tag cloud (The importance of each tag is shown with font size)

Analytical Report. Information warfare. JSC Kribrum

The diagrams below show a sharp increase of the activity of pro-Western networks at the end of 2016. This is related to the end of the election cycle and the emergence of a new thesis - "Russian interference." It is important to note that at the same time there was a change from "aggression" to "interference" in the main theme of the accusations against Russia.

Diagram 2. **Shift in agenda (English-speaking region)**



The number of reports accusing Russia of interfering in internal political issues of different states was growing during that period. At first, "Russian hackers" were accused of "interference" and their possible belonging to the Russian special services. Later the West begins to write about the existence of special cyber-units in FSB, SVR and GRU.

The charges were transformed from "Russian hackers, possibly related to the Russian special services" to "Russian special services".

Diagram 3. **Shift in agenda (English-speaking region)**

According to JSC Kribrum, a psychological and linguistic-semantic analysis of the foreign infosphere shows that 35% of western Twitter users associate Russia with its security services ("Military forces", "FSB", "SVR", "GRU", "special forces"). Non-media users show signs of "cyberphobia" flowing into "Russophobia". Foreign users are really afraid of cyber threats from Russia, despite the complete lack of evidence.

In Russian media the image of "Russian hackers" isn't as active as in western media. Moreover, it is ironic and loosely connected to Russian special services.

However, the Western policy and strategy towards Russians are based on methods such as described above.

The main goal of the anti-Russian provocations in cyberspace is to create in the Western public consciousness a kind of "cyberophobia" and to undermine Moscow's efforts to build a strategic balance of power, restore trusting relationships with foreign partners, and successfully combat the coronavirus pandemic.

It should be noted that the coronacrisis is going to end, but the West continues to inflame and distort.

The following is an excerpt from the article published by The New York Times on May 28, 2020.

> *Under a presidential order issued in 2018, Gen. Paul M. Nakasone, the head of the agency and the commander of the United States Cyber Command, can operate on his own authority in operations short of war, including the kind that involve pushing back on Moscow.*
>
> *They have launched an operation **to implement malicious software into Russian energy systems**, hinting at retaliation that Russia could expect if Moscow tried to attack the American critical infrastructure.*

Thus, according to this publication, **elements of direct cyber-aggression against Russia have already been implementing**. This is not even a threat. In general, this is a belligerent declaration.

Furthermore, China is also under intense scrutiny of the United States. The mentioned above RAND report states:

> *The power to use economic sanctions might decline because China makes its financial sector far more open and independent from the USA than it is now. If that happens, the United States might need to resort to more-kinetic forms of coercion*.
>
> To my opinion, it is a direct conflict.

Thus, the U.S. government is working on an economic warfare against China with the possibility of escalating into a kinetic war. At the same time it conducts the cyber-information warfare against Russia with the possibility of escalating into a kinetic war. Such an apocalyptic scenario is being prepared for the world by American strategists from the special services...

Russia should not only take these threats into account, but also be proactive. The ensuring of information and cyber-security is interdepartmental. It requires close cooperation and joint efforts of all special services and law enforcement agencies, civil authorities and society. Moreover, it requires a consolidated national policy to provide security.

A mobilization type socio-economic model inside the state system, which duplicates and insures in case of any kind of hybrid crises, such as coronavirus or cyber-technological failures in the future is required.

The amendments to the Constitution which we will vote for on July, 1 are aimed at forming such a strategy.

Namely, **Article 71**: *"The jurisdiction of the Russian Federation includes:*

*i) federal energy systems, nuclear energy, fissile materials; federal transport, traffic communications, information, **information technology and communications**; space activities;*

*m) defense and security; defense industry; determining the procedure for the sale and purchase of weapons, ammunition, military equipment and other military property; production of toxic substances, drugs and the procedure for their use; **ensuring the security of individuals, society and the state while applying of information technology, the circulation of digital data"...***

The significance of these articles is very high!

The state strategy should be ensured ideologically, technologically and professionally with ministry of defense leading the process. That's what we see in the United States that has seventeen intelligence services while the Ministry of Defense bolsters their efforts to guarantee national cyber and information security. China indeed operates the same way from the start.

To build the Russian state that ensures internal and external security, equal access to free medicine, fundamental education and advanced social infrastructure within walking distance is the vital matter of our time. Handling the issue will make Russia a role-model nation. This is hard, but it's a great historical mission.

Andrej Il'nitskij, Adviser to the Russian Minister of defense