America's "Offensive" Cyber Strategy. White House Authorizes Offensive Cyberwarfare

By Leonid Savin
Global Research, October 04, 2018
Oriental Review 2 October 2018

Region: USA
Theme: Intelligence, Militarization and WMD

On September 20, 2018 the White House released the US National Cyber Strategy, which was signed by ***President Donald Trump.***

It probably delighted both hawks and Democrats. The former were pleased that the strategy includes new components that clearly indicate an expansionist momentum. And the latter were gratified by the Trump administration's renewed interest in the subject of cyberspace, since Donald Trump eliminated the position of White House cybersecurity coordinator after his election and significantly reduced spending in this area. But the president now seems to have reconsidered, as indicated by the fact that the 40-page document is in many respects a rehash of efforts from the Obama era.

US **Secretary of Homeland Security Kirstjen Nielsen** (image above) noted in her statement that

> "[t]oday's National Cyber Strategy — the first in fifteen years — strengthens the government's commitment to work in partnership with industry to combat those threats and secure our critical infrastructure."

Her press release went on to say,

> "With respect to securing federal networks, for example, we have used our authorities to ensure agencies are updating and patching systems, strengthening their email security, and removing Kaspersky antivirus products from their systems."

Was this reference to the Russian company just a coincidence? Of course not. Even a cursory glance at this strategy drives home the point that Russia is being singled out as a militant enemy of the United States, and Washington is ready to start leaning hard on it.

It is also telling that several days before this document was released, an updated version of the US Department of Defense's cyber strategy was published, which suggests that the Pentagon and the Trump administration are working in tandem to a certain extent. Their mutual interests are also evident from a comparison of statements from the summary of the two documents.

Here is the Pentagon's strategy in a nutshell:

> "We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation."

And the introduction of the US National Cyber Strategy states:

> "Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and international national businesses and our allies and partners … China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft … The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. **Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners** … These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons." (emphasis added)

So, Russia is now being singled out in this very official way as an enemy of the US!

President Donald Trump walks to Air Force One on Sept. 19, 2018, at Andrews Air Force Base in Maryland. (Source: author)

And in order to combat these threats, both real and fictitious, **the leaders of the US intend to embark upon a course of risk management,** by introducing new information technologies, establishing priorities in business projects, and funneling government funds to cybersecurity contractors.

On pages 9 and 10 of the strategy, there are two subsections that refer to the global cybersecurity of maritime transportation and outer space. Since free and unfettered access to the sea, skies, and outer space is closely tied to America's economic and national security, US control over those domains and the use of various technical means — from ships to future satellite systems — is listed as one of the priorities.

The tasks enumerated also include updates to electronic surveillance, which will enable intelligence agencies to monitor streams of data, the transfer of new powers to investigative and prosecuting agencies, and the development of new ways to prosecute individuals outside the United States (i.e., the citizens of foreign countries), as well as other active

measures:

> "All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities."

In other words, responses to a cyberattack can now include the imposition of sanctions, the coordination of a propaganda campaign in the puppet media, or a missile launch.

Speaking at a press conference in Washington, the US president's National Security Advisor, **John Bolton**, noted specifically that **the White House had**

> **"authorized offensive cyber operations… not because we want more offensive operations in cyberspace, but precisely to create the structures of deterrence** that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear." (emphasis added)

However, America's historical approach to geopolitical (and military) deterrence is rife with interference in the affairs of other countries, including the orchestration of bloody coups and overt intervention under contrived pretexts (Haiti in 1993 springs to mind), which are precisely the ways in which the US operates.

By shifting these tactics into cyberspace, we can assume that DDoS attacks and the introduction of malware and spyware, as well as a variety of assaults against vulnerable "enemy" sites (and those could be anything from the servers belonging to banks and cellular service providers to databases belonging to private citizens, manufacturing infrastructure, or the various systems that provide essential social services), are the least of what we can expect from the Pentagon. It is possible that a few countries that have suitable experience in cybersecurity will manage to fend off such attacks. But it is more than likely that some states will be unable to effectively and painlessly deflect them.

And even a kinetic response is mentioned! And that is solely a military prerogative. This is why we are quoting an excerpt from the US Department of Defense's strategy.

The Pentagon's document clearly states how this strategy will be carried out.

"Our strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent."

The first item openly attests to these aggressive military intentions: "Our focus will be on fielding capabilities that are scalable, adaptable, and diverse to provide maximum flexibility to Joint Force commanders. The Joint Force will be capable of employing cyberspace operations throughout the spectrum of conflict, from day-to-day operations to wartime, in order to advance U.S. interests."

To put it more simply, **the US military is now literally getting a green light to launch cyberattacks and other cyber operations around the world.** You can even forget

about any formal declaration of war, because that is a rather complex procedure in the US, and for many recent years American soldiers have been sent to various destinations abroad as part of military operations that do not officially meet the criteria for either war or stabilization campaigns. But the US is up to all kinds of legal shenanigans. And given that no clear definition exists of what constitutes "malicious acts in cyberspace" and the fact that that label could thus be used to snare anyone or anything, this trend in the US military and political establishment might set a sobering precedent.

What's more, this is a clear signal for Washington to begin applying pressure through international organizations, primarily via the UN. Since the United Nations has for many years served as a platform for debates over the regulation of global cyberspace, and the US has clearly been on the losing side in numerous high-level discussions about national jurisdiction, sovereignty, and responsibility, Washington seems to be trying to take its revenge — now resorting to accusations and the techniques of preemptive diplomacy (i.e., threats and blackmail — the proven tools of US foreign policy).

In this regard, it is no coincidence that the Global Security website highlighted one point from that strategy, which reads:

> "ADVANCING AMERICAN INFLUENCE: The National Cyber Strategy will preserve the long-term openness of the internet [sic], which supports and reinforces American interests."

But how can the openness of the Internet promote US interests? Obviously that can only happen when the Americans set the rules of the game in cyberspace, like those the US has established that govern world trade through American control over banking transactions, stock exchanges, and other tools of the globalized economy. And if some countries refuse to follow Washington's orders, they will be once again be labeled as pariahs and accused of acting maliciously. The refusal to adopt US standards will be treated as an act of war by other means against American citizens. This is as serious as the statement made by George W. Bush after the terrorist attacks in New York in September 2001, at which time he declared, "whoever is not with us is against us."

And unsubstantiated allegations about the interference of "Russian hackers" in the US presidential election and about China's industrial espionage against American companies might someday look like a naive example of much ado about nothing, compared with what Washington is about to plunge into.

*

Note to readers: please click the share buttons above. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Leonid Savin *is a geopolitical analyst, Chief editor of Geopolitica.ru, founder and chief editor of Journal of Eurasian Affairs; head of the administration of International Eurasian Movement.*

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Leonid Savin**