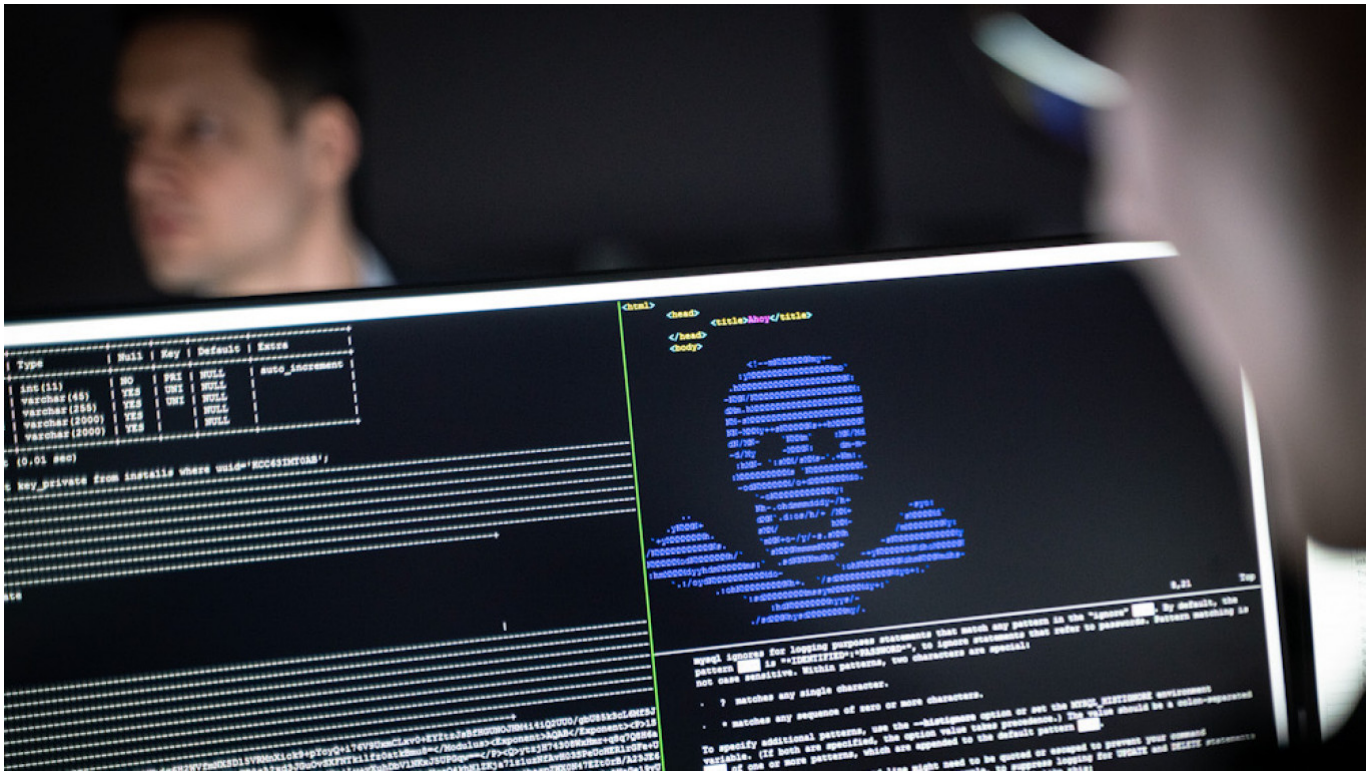
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

An 'Act of War?' Avoiding a Dangerous Crisis in Cyberspace

Unlike in the nuclear sphere, there are no rules governing the increasingly intense rivalry between the U.S. and Russia in the cyber sphere.

By Dmitry Trenin

December 24, 2020



Frank Rumpenhorst / DPA / TASS

There's a distinct feeling of deja vu. Just when some Russians were heaving a sigh of relief that this time, unlike four years ago, Russia was not accused of meddling in the U.S. presidential election, news came of a massive hack of several U.S. government agencies. Again, accusing fingers were almost immediately pointed at Russia. Some called it an invasion; others compared it to Pearl Harbor. Senior politicians demanded retribution.

Yet the present case is different to 2016. Essentially, the hacking was aimed at collecting information, rather than manipulating the target country or causing physical damage. Spying

is, of course, one of the world's oldest professions, and has been universally considered an inalienable part of statecraft. Everyone does it. Of all nations, the United States is perhaps best equipped for it, and is likely most active. Edward Snowden and Wikileaks have supplied mountains of evidence to support that.

Attribution of cyberattacks is notoriously tricky. Yet the Americans are certain that the origin of the current massive hack in the United States is the Russian Foreign Intelligence Service (SVR), which celebrated its centenary last Sunday. If—despite the official Kremlin denial—that is the case, it is indeed a major achievement for Moscow, and an indicator of its cyber power. But it comes with strings attached.

Tit-for-tat is an established modus operandi among hostile intelligence services. What is not clear is what kind of retaliation the United States will eventually decide upon. President-elect Joe Biden will probably be in charge by the time the U.S. response is launched, and it might go beyond sanctions. How far beyond? Ron Klain, the incoming White House Chief of Staff, has suggested that it could well be a cyberattack, going beyond a "mirroring" hacking operation.

Therein lies the problem. In the hybrid war now being fought between America and Russia, the information domain is a principal battlefield, and cyber tools are the weapons of first resort. Yet unlike in the nuclear sphere, there are no rules governing the increasingly intense rivalry.

The line between cyber espionage and cyber warfare is rather blurred. Latter-day Trojan horses can do much more than furnishing critical intelligence: like their ancient model, they can disable the adversary's defenses or even manipulate the enemy to their advantage. It's true that something of that kind was always possible: remember the World War II-era radio games. Yet now the scope, scale, and impact of such operations is incomparably greater.

Cyber intelligence, however intrusive, is one thing. Cyber war is another. A kinetic state-versus-state collision, traditionally known as a shooting war, is yet another category. Yet Democratic Senator Richard Durbin has already called the operation attributed to SVR an act of war. The United States policy does allow for the use of military force in response to hostile actions short of war, as is commonly understood. Of course, the decision will rest with the U.S. president.

This article was first published by the Carnegie Moscow Center.

Original url:
https://www.themoscowtimes.com/2020/12/24/an-act-of-war-avoiding-a-dangerous-crisis-in-cyberspace-a72430