Is Trump Capable of Launching an All-Out Cyberwar?

At the turn of the 21st century, a great many politicians, scientists, and military brass embraced the idea that humanity was approaching a new era, a world built upon the foundation of the US military superiority. Yet, this new world order would eagerly neglect the national sovereignty principle that has been the cornerstone of international politics ever since the 17th century. America would build increasingly more sophisticated means of warfare to immediately test them across various regions of the world. Moreover, by introducing new technologies and securing its dominance in the information space Washington received the impression that its world order has become unbeatable.

And it's hardly a secret that this world order is not being supported by regular weapons alone anymore, as the rapid development of the Internet led to the emergence of a new type of warfare - cyber warfare. We've seen it all - mysterious hackers, special cyber units, security breaches, DDoS attacks, and the use of social networks for the staging of “color revolutions” across the Middle East and those states that refuse to obey Washington's dictate. Further still, to undermine critical infrastructure objects in the so-called “revisionist states” Washington would launch cyber-attacks against those.

Thus, the World Wide Web has become a frontier in a hardening confrontation between the global superpowers. The Internet, GPS systems and quantum physics have been conscripted by governments and are being readied for battle.
As a matter of fact, an operation launched by the US Cyber Command disrupted Russia's access to the US segment of the Internet on the day of 2018 midterms. The attack was launched on the pretext that Russia would try to interfere in the US elections, yet no evidence has been presented to support this claim. In turn, Robert Mueller's investigation would fail to trace Russia's involvement in the hijacking of the US presidential election back in 2016. It was reported that this cyber attack that was nothing short of a war step was ordered personally by the sitting US president, Donald Trump.

Is it of any surprise then that the world's largest annual cyber-security military games dubbed Locked Shields were held in Estonia in early April. The exercise was supervised by the NATO headquarters, with dozens of NATO member states joining the US in the joint training effort, including the Estonian Ministry of Defense. According to various military experts, Locked Shields has nothing to do with deterring Russia's hypothetical aggression, instead it's a poisonous cyber-dagger aimed at its heart. Ever since it was first launched back in 2012, the number of participants of Locked Shields has been steadily increased. In 2016, 550 servicemen from 26 countries were involved in the military games, launching 1,700 attacks with the use of 1,500 virtual machines; in 2017 the number of servicemen participating reached 800 people from 25 countries, the number of attacks peaked at 2,500, and the number of virtual machines involved exceeded 3,000; in 2018, the exercise brought together a grand total of 1,000 servicemen from 30 countries, bringing the number of virtual machines to 4,000.

The United States, as the most advanced country in the field of cyber security and information technology, and each year it gets even more capable of unleashing a cyber onslaught upon its enemies. Ever since 2006, the United States has been conducting Cyber Storm military games once every two years. This exercise is designed to allow highly-trained teams of hackers to sabotage the energy, financial, transportation and IT capabilities of most any international players across both sides of the Atlantic. Since 2016, the DoD has been conducting all sorts of cyber exercises, including Hack the Pentagon, Hack the Army, Hack the Air Force, Hack the DTS, and Hack the Marine Corps. It's curious that Hack the Air Force 3.0 were held as recently as last November.

Considering the increasingly aggressive nature of Washington's actions on the international arena in recent years, its neglect towards the international law in its staging of armed conflicts in various parts of the world, its completely unwarranted withdrawal from a number of international treaties to curb the proliferation of weapons and armed conflicts, the international community has been following with increasing concern Washington's steps in cyberspace. Even today for a great many countries across the globe a possible massive cyber attack that would be accompanied by provocative statements in the media and mass-protests stirred by the social network specialists is not a theoretical threat anymore. For this reason, many countries have started to explore the possibility of cutting their national segment of the net from the World Wide Web.

It's been noted that so far, at least nine countries have cut off their national Internet connections to assert political control at critical moments, including Egypt, Libya, the Maldives, Myanmar, Nepal, Sierra Leone and Syria, according to the countersecurity fellow of the New America Foundation, Justin Sherman. Those state would deliberately shut down the Internet to contain people's protest, while Gabon and the Democratic Republic of Congo can be mentioned as the most recent examples.

As for China and Russia, they've been hard at work preparing for such a scenario for a reason. They want to be sure that should there be a crisis or conflict with the US when Washington tries to shut off their Internet, they would be able to maintain their IT infrastructure intact.

The standout success is China. China has long ago figured out how to cut off from attack locally. Beijing not only wants to keep sovereign control of its web and its people, it also wants to be able to survive a US Internet embargo, the equivalent of the trade embargo.

In turn, Moscow has recently approved a bill that would allow it to do precisely the same thing. It's been revealed that Russia is planning to change the configuration of its Internet so that it can be entirely self-contained and self-sustaining "to ensure the long-term stable function of Internet networks in Russia.

However, the most fascinating aspect of those preparations was Washington's reaction to the above mentioned steps that Moscow is taking. With the assistance of their numerous mouthpieces, the United States and Britain would launch a barrage of accusations against Russia for its alleged attempts to "usurp information democracy" (sic)! At the same time, nobody in the MSM would even dare to mention the fact that same exact preparations are being made in the United States. Somehow Washington that has started this whole mess isn't usurping information in the next major war.
security in the eyes of Western journalists.

And there's one perfectly logical explanation for all this, since Washington has spent an extensive amount of time, money and effort to prepare for waging cyber-wars on other states, but then the steps taken by Russia, China and a number of other states rendered all of these preparations useless.

Jean Périer is an independent researcher and analyst and a renowned expert on the Near and Middle East, exclusively for the online magazine “New Eastern Outlook“.