In recent years, the very term "cyber warfare" has evolved from something only the military brass would use into a hypeworthy piece of news, with politicians in different countries alleging that their ratings were plummeting due to "cyber attacks" launched by their opponents. With Russophobia rapidly becoming a new epidemic, there's nothing surprising in the fact that Russia would often be accused of committing “cyber attacks” against the United States, Britain, and a number of their satellites. However, it’s safe to say that those allegations are used as a smoke screen to provide cover to those operations in the cyber space that Washington and its allies have been conducting. However, when law enforcement agencies start investigating such shameful allegations, like the notion of Russia’s meddling in the presidential campaign in the United States, time and time again they fail to produce any evidence that could incriminate Moscow in actually committing something illegal.

However, such failures haven’t stopped a number of Western countries, namely the US, Great Britain, and a couple of NATO member states from creating massive cyber units and providing them with a constant stream of cash, which allows them to carry out high-profile cyber operations on the regular basis. After all, it has long become evident that national states can be hijacked without the use of conventional weapons, through the constant abuse of various networks alone.

Actually, the very possibility of conducting cyber war has been considered since the moment the Internet became a
truly global network. But even earlier, from about the end of the 1950s, the US started investigating the possibility of waging so-called “hybrid wars” as they were dubbed back then. Upon developing the tactics behind such operations, the Pentagon officially adopted them as an option under the name of network wars.

In 2013, a new branch of the armed forces was created in the US Armed Forces - the Cyber Command, as cyberspace was seen as a separate military operating environment, that was non less important than ground, air or sea operations. There's well over 19 thousand cyber “warriors” enlisted by the US military. In April 2018, the United States Cyber Command released a new revision of the US National Cyber Strategy, that was aimed at conducting proactive actions in cyberspace to maintain US primacy in this domain.

As it's been noted by a military analyst, Fred Kaplan:

> Cyberspace is now seen by officers and officials as just another “domain” of warfare—along with air, land, sea, and space. But there’s something different and more dangerous about this domain: It takes place out of sight, its operations are so highly classified that only a few people know what’s going on there, and it creates an inherently hair-trigger situation, which could unleash war in lightning speed with no warning.

It seems that all of the major cyber powers have been able to hack into one another’s “critical infrastructure,” thus inflicting a considerable amount of damage on its rivals, and Washington is the unannounced champion of this warfare.

According to the New York Times, US Cyber Command now feels less constrained about going on the offensive, as it has stepped up cyber offensive operations, in frequency and scale. The prime targets are China, Russia and Iran. And even though it's often said that the US ruling elite is not aware of such operations, as there's been reports that Donald Trump wasn’t even briefed on the US hacking of Russia’s power grid, in one of his interviews the sitting US President would boast about him ordering a cyber-attack on Russia back in 2018.

On June 11, 2019, United States National Security Advisor John Bolton, speaking at a forum of financial managers in Washington, openly stated that the sitting US administration has begun to actively conduct offensive operations in cyberspace. Thus Washington has officially recognized that the Pentagon's new cyber doctrine implies preemptive strikes on energy, industrial and government infrastructure nodes of the potential enemy. On top of crippling the infrastructure of other states, the Pentagon is involved in spreading misinformation on social networks and media platforms. And that's no theorycrafting, as it has already conducted a series of such attacks against Venezuela and Iran.

It must also be acknowledged that Bolton’s speech refers to the extension of Presidential Policy Directive 20, signed by Barack Obama in 2012, which for the first time since 2004 gave the US military the right to “act more aggressively” in the cyberspace.

Upon receiving the green light from Washington, its allies have actively joined the effort of developing offensive cyber capabilities. Last year London allocated some 331 million dollars on the creation of offensive British cyber units that were bound to enlist up to 2,000 men. Germany is planning to increase the number of its cyber “warriors” to 13.5 thousand people, while Lithuania, Estonia and several other NATO countries are also undergoing the process of modernization and buildup of their offensive cyber capabilities.

It's been revealed that the United States is planning to deploy additional cyber units to Eastern Europe in the near future. In addition, as Bloomberg recently reported, on the islands of the Philippines and Taiwan, the United States is planning to deploy a special cyber unit aimed at countering Russia and China.

As hostilities increasingly overtake the digital realm, the Pentagon has decided to transform its Cyber Command that is bound to become the Army Information Warfare Command, according to James McConville. It’s one of the several modernization efforts to counter "great power" opponents like Russia and China.

Vladimir Platov, Middle East expert, exclusively for the online magazine “New Eastern Outlook”.