GlobalResearch
Center for Research on Globalization

NATO Rolls Out Offensive Cyberweapons

By Ulson Gunnar
Global Research, December 26, 2017
New Eastern Outlook 25 December 2017

Theme: Intelligence, Media Disinformation, US NATO War Agenda

NATO members including the US, UK, Germany, Norway, Spain, Denmark and the Netherlands have begun taking public steps in defining guidelines regarding the deployment of offensive cyberweapons.

Reuters in its article, "NATO mulls 'offensive defense' with cyber warfare rules," would state:

> A group of NATO allies are considering a more muscular response to state-sponsored computer hackers that could involve using cyber attacks to bring down enemy networks, officials said.

Reuters would also report:

> The doctrine could shift NATO's approach from being defensive to confronting hackers that officials say Russia, China and North Korea use to try to undermine Western governments and steal technology.

The article also noted that the United States and its allies already possess and have threatened to use cyberweapons offensively, citing the 2010 Sutxnet virus deployed against Iranian nuclear infrastructure as a possible example. Other examples cited of possible applications included shutting down power plants with malware rather than bombing them.

Reuters also reported that NATO was setting up "cyber commands" including one in Estonia apparently intended to launch cyber attacks into Russia.

Extending NATO Aggression into Cyberspace

At face value, a nation developing the ability to defend itself and carry out counterattacks against foreign aggressors, including in cyberspace, appears as legitimate policy.

For NATO, however, its track record of serial aggression and expansion beyond its borders predicated on intentionally false pretexts indicate that the military alliance will simply carry its aggression into cyberspace as well.

The NATO invasion and occupation of Afghanistan followed the attacks on September 11, 2001 on Washington D.C. and New York City. Despite none of the alleged suspects involved in the attack actually coming from Afghanistan, and the government of Afghanistan having played no role in the attacks, NATO would invade and has since occupied the nation for the past 16 years.

The 2003 invasion of Iraq led by the US and other prominent NATO members was predicated entirely on falsehoods. Claims that the Iraqi government at the time possessed chemical and biological weapons later turned out to have been intentionally fabricated to justify an invasion that, by some estimates, cost the lives of over a million Iraqis and thousands of US and European soldiers. The invasion and occupation resulted in regional conflict that continues to this day.

In 2011 when terrorists affiliated with Al Qaeda moved against the government of Libya, NATO portrayed the resulting conflict as a crackdown on what it and Western media called "freedom fighters." NATO armed militants and eventually intervened in an air campaign that toppled the government, leaving Libya in ruins since.

Between 2013-2014 the US and its NATO partners openly fomented protests against the elected government of Ukraine. Supporting Neo-Nazi militias and their affiliated political parties, NATO succeeded in overthrowing the government and placing into power organizations and parties involved in the protests. NATO has since intervened on various levels, short of military intervention, to protect the regime in Kiev from both political challengers and a possible counter-coup.

In many ways, since the Arab Spring in 2011, the US and its NATO partners have already used cyberweapons of sorts to destabilize and attack targeted nations. Social media was manipulated in the opening weeks of protests, false information transmitted, technology and software distributed among US-NATO funded opposition groups, all in an effort to stampede targeted governments out of power.

Today, NATO members are involved in the bombing, invasion, occupation and drone warfare from Africa to Asia. They employ the tools of modern disinformation and propaganda to interfere and manipulate in the political processes of nations worldwide.

The notion that NATO will develop and deploy cyberweapons in an offensive capacity will not only enhance ongoing aggression, but because of the nature of cyberweapons and the possibility of attacks concealing their point of origin, might see it expand into areas where currently, conventional military means cannot be justified.

Considering the extensive experience NATO possesses in fabricating pretexts for aggression, and the perceived benignity of cyberwarfare versus conventional weapons, we can expect to see NATO use this new concept of "offensive defense" to further menace the nations and peoples of this planet with a degree and frequency far above and beyond its conventional military operations.

While Reuters cites Russia, China and North Korea as likely targets of NATO cyberattacks, it is likely that any and all actors, both state and non-state, will find themselves targets of NATO aggression should their interests conflict with those that underwrite the NATO alliance.

Developing the means to put these capabilities in check and prevent NATO from developing any sort of advantage in cyberspace will be a prerequisite for future peace and stability, online and off.

Ulson Gunnar is a New York-based geopolitical analyst and writer especially for the online magazine "New Eastern Outlook".

Featured image is from the author.

Articles by: Ulson Gunnar