GlobalResearch
Center for Research on Globalization

US-UK Accuse Russia of "NotPetya" Cyberattack, Offer Zero Evidence

By Ulson Gunnar
Global Research, February 19, 2018
Region: Europe, Russia and FSU, USA
Theme: Intelligence, Media Disinformation

The US and European press have both published stories accusing the Russian government, and in particular, the Russian military, of the so-called "NotPetya" cyberattack which targeted information technology infrastructure in Ukraine.

The Washington Post in an article titled, "UK blames Russian military for 'malicious' cyberattack," would report:

> Britain and the United States blamed the Russian government on Thursday for a cyberattack that hit businesses across Europe last year, with London accusing Moscow of "weaponizing information" in a new kind of warfare. Foreign Minister Tariq Ahmad said "the U.K. government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyberattack of June 2017." The fast-spreading outbreak of data-scrambling software centered on Ukraine, which is embroiled in a conflict with Moscow-backed separatists in the country's east. It spread to companies that do business with Ukraine, including U.S. pharmaceutical company Merck, Danish shipping firm A.P. Moller-Maersk and FedEx subsidiary TNT.

British state media, the BBC, would report in its article, "UK and US blame Russia for 'malicious' NotPetya cyber-attack," that:

> The Russian military was directly behind a "malicious" cyber-attack on Ukraine that spread globally last year, the US and Britain have said.

The BBC also added that:

> On Thursday the UK government took the unusual step of publicly accusing the Russia military of being behind the attack. "The UK and its allies will not tolerate malicious cyber activity," the foreign office said in a statement. Later, the White House also pointed the finger at Russia.

Yet despite this *"unusual step of publicly accusing the Russian military of being behind the attack,"* neither the US nor the British media provided the public with any evidence, at all, justifying the accusations. The official statement released by the British government would claim:

> The UK's National Cyber Security Centre assesses that the Russian military was

> almost certainly responsible for the destructive NotPetya cyber-attack of June 2017. Given the high confidence assessment and the broader context, the UK government has made the judgement that the Russian government – the Kremlin – was responsible for this cyber-attack.

Claiming that the Russian military was *"almost certainly responsible,"* is not the same as being certain the Russian military was responsible. And such phrases as *"almost certainly"* have been used in the past by the United States and its allies to launch baseless accusations ahead of what would otherwise be entirely unprovoked aggression against targeted states, in this case, Russia. The White House would also release a statement claiming:

> In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

Considering claims that this is the *"most destructive and costly cyber-attack in history,"* it would seem imperative to establish evidence beyond doubt of who was responsible. **No Evidence From Governments Confirmed to Possess the Means to Fabricate Attribution** Yet, so far, this has not been done. Claims that Russia's military was behind the attacks seems to be built solely upon private analysts who have suggested the attacks appear to have originated in Russia.

However, as it was revealed by Wikileaks in its Vault 7 release, exposing cyber hacking tools used by the US Central Intelligence Agency (CIA), the origin of attacks can be forged. USA Today in an article titled, "WikiLeaks: CIA hacking group 'UMBRAGE' stockpiled techniques from other hackers," would admit:

> A division of the Central Intelligence Agency stockpiled hacking techniques culled from other hackers, giving the agency the ability to leave behind the "fingerprints" of the outside hackers when it broke into electronic devices, the anti-secrecy group WikiLeaks alleges as it released thousands of documents Tuesday.

The article continues by pointing out:

> The documents also suggest that one of the agency's divisions – the Remote Development Branch's UMBRAGE Group – may have been cataloguing hacking methods from outside hackers, including in Russia, that would have allowed the agency to mask their identity by employing the method during espionage. "With UMBRAGE and related projects the CIA cannot only increase its total number of attack types, but also misdirect attribution by leaving behind the 'fingerprints' of the groups that the attack techniques were stolen from," Wikileaks said in a statement.

Not only does this ability allow the CIA to carry out espionage that if discovered would be attributed to other parties, it also allows the CIA to conduct attacks the US government and

its allies can then blame on foreign states for the purpose of politically maligning them, and even justifying otherwise indefensible acts of aggression, either militarily, or in the realm of cyberspace.

Evidence provided by the UK and US governments would have to establish Russia's role in the "NotPetya" cyberattack beyond mere attribution, since this is now confirmed to be possible to forge. The UK and US governments have failed to provide any evidence at all, likely because all it can offer is mere attribution which skeptics could easily point out might have been forged. **NATO Had Been Preparing "Offensive" Cyber Weapons**

As previously reported, NATO had been in the process of creating and preparing to deploy what it called an *"offensive defense"* regarding cyber warfare. Reuters in an article titled, "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.

It has been repeatedly pointed out how the US, UK and other NATO members have repeatedly used false pretexts to justify military aggression carried out with conventional military power. Examples include fabricated evidence of supposed "weapons of mass destruction (WMD)" preceding the 2003 US invasion of Iraq and the so-called "humanitarian war" launched against Libya in 2011 built on fabricated accounts from US and European rights advocates.

With UMBRAGE, the US and its allies now possess the ability to fabricate evidence in cyberspace, enabling them to accuse targeted nations of cyber attacks they never carried out, to justify the deployment of “offensive” cyber weapons NATO admits it has prepared ahead of time. While the US and European media have warned the world of a “cyber-911″ it appears instead we are faced with “cyber-WMD claims” rolled out to justify a likewise “cyber-Iraq War” using cyber weapons the US and its NATO allies have been preparing and seeking to use for years. Were Russia to really be behind the “NotPetya” cyberattack, the US and its allies have only themselves to blame for decades spent undermining their own credibility with serial instances of fabricating evidence to justify its serial military aggression. Establishing that Russia was behind the “NotPetya” cyberattack, however, will require more evidence than mere “attribution” the CIA can easily forge.

*

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

All images in this article are from the author.
