GlobalResearch
Center for Research on Globalization

US Cyberattacks on Russia Could Escalate to Real-world Conflict

By Drago Bosnic
Global Research, June 12, 2022
InfoBrics 8 June 2022

Region: Europe, Russia and FSU, USA
Theme: Intelligence, US NATO War Agenda
In-depth Report: UKRAINE REPORT

All Global Research articles can be read in 51 languages by activating the "Translate Website" drop down menu on the top banner of our home page (Desktop version).

To receive Global Research's Daily Newsletter (selected articles), click here.

Visit and follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

***

Carl von Clausewitz, a prominent Prussian general described war as "merely the continuation of policy by other means." This perfectly describes the political West's relationship with the world. However, against Russia, it is unable to conduct what the late Donald Rumsfeld euphemistically called "kinetic force." The phrase differentiates conventional warfare from "soft" force, limited to diplomacy, sanctions and cyber warfare. The latter is usually overlooked, despite often taking center stage in geopolitics.

The advent of the Digital Age gave rise to cyber warfare. While it was applied even during the 1990s, it became more prominent in the last 20 years. With nearly all organizations on the planet now being online, we got unprecedented access to information. However, this has its downsides, particularly in the form of hackers, who aren't necessarily just "lone wolves" motivated by money (or ideology). The data on hackers is questionable at best. However, there's publicly available information, especially that coming from state structures openly talking about the military usage of cyberspace.

General Paul Nakasone, the head of US Cyber Command, stated the US is conducting offensive operations in "support of Ukraine." In an exclusive for Sky News, he explained: "'Hunt forward' operations are allowing the US to search out foreign hackers and identify the tools they use against America." Nakasone, who is also director of the NSA, stated he is "concerned every single day about the risk of a Russian cyberattack" and that the "hunt forward" activities were an "effective way of protecting America." He confirmed for the first time the US is conducting offensive cyber-ops against Russia. "We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations," he stated. The general didn't give any specifics, but he claimed the activities of US military hackers were allegedly "lawful, conducted with complete civilian oversight of the military and through policy decided at the DoD." His job is to "provide a series of options to the secretary of defense and the president, and so that's what I do," he said, declining to give any further details.

> "We had an opportunity to start talking about what particularly the Russians were trying to do in our midterm elections. We saw it again in 2020, as we talked about what the Russians and Iranians were going to do, but this was on a smaller scale. The ability for us to share that information, being able to ensure it's accurate and it's timely and it's actionable on a broader scale has been very, very powerful in this crisis," the general said.

When asked about counterattacks in response to US offensive operations, Nakasone said: "We remain vigilant every single day. I think about it all the time. This is why we're working with a series of partners to ensure we prevent that." He delivered a speech at CyCon, a conference on cyber conflict, hosted by NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, and praised the cooperation as a "key strategic benefit."

> "Hunt forward is a key aspect of the Cyber Command's partnerships. It is so powerful… because we see our adversaries and we expose their tools. Cyber Command specialists have been deployed abroad to 16 other nations where they can seek intelligence from the allies' computer networks – always on a consensual, invitation basis," General Nakasone said.
>
> "Crucial to how hunt forward works is Cyber Command sharing the intelligence they find with the host nation. If you're an adversary, and you've just spent a lot of money on a tool, and you're hoping to utilize it readily in a number of different intrusions, suddenly it's outed and it's now been signatured across a broad range of networks, and suddenly you've lost your ability to do that," the general said. "In one such hunt forward deployment, US military specialists had been present in Ukraine very close to the date of the invasion. We went in December 2021 at the invitation of the Kiev government to come and hunt with them. We stayed there for a period of almost 90 days," he added.

A spokesperson confirmed this team left in a hurry after Russia intervened. There aren't many details regarding US cyber-ops, but what we know 100% is what Nakasone himself admitted – the US is actively conducting offensive cyber-ops against Russia. This may very well explain the strange blackouts in some Russian regions, as well as other unexpected disruptions of its key infrastructure. The issue is not just that Russia could respond to these attacks with its own cyber-ops, but also with "kinetic force", as Rumsfeld defined it. This is especially true as the consequences of cyber-ops aren't only limited to cyberspace. Blackouts result in very real damage. Schools, hospitals, state institutions, etc. all rely on critical infrastructure. If the result of these attacks is similar to armed aggression, Russia would be compelled to respond.

After all, the political West itself has been contemplating this approach. NATO is considering including cyber warfare in Article 5. The clause is the focal point of the "defensive alliance." Expanding its scope to cyber-ops could lead to uncontrollable escalation. It also reveals yet another instance of glaring hypocrisy of the political West – while the US and its satellites conduct offensive cyber-ops against Russia, and then openly brag about it, they're saying those same cyber-ops in response to US/NATO cyberattacks would trigger its infamous "collective defense" clause.

If the US/NATO insist(s) that Article 5 could be invoked, why doesn't the same apply to Russia? Well, as far as Russia goes, the "purely defensive alliance" doesn't get to decide what Russia defines as a security threat.

Thus, the political West might not only be facing Russia's cyber counteroffensive, but an actual, physical response. As Huntington defined it, "the West won the world not by the superiority of its ideas or values or religion (to which few members of other civilizations were converted) but rather by its superiority in applying organized violence. Westerners often forget this fact; non-Westerners never do."

Russia can also "apply organized violence" in a way superior to anyone else's. It hopes it won't need to, but it most certainly is capable of it. If the political West wants to prevent a world-ending conflict, it will stop its cyber, bioweapons or other operations against Russia. Otherwise, the "purely defensive alliance" will finally get the taste of its own medicine, facing the full might of the "defense" it has been conducting against the world. Only radioactive.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

Drago Bosnic is an independent geopolitical and military analyst.

Featured image is from InfoBrics

The original source of this article is InfoBrics
Copyright © Drago Bosnic, InfoBrics, 2022

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Drago Bosnic

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca