GlobalResearch
Center for Research on Globalization

China Concerned that US Cyber Aggression Against Russia Could Trigger Nuclear War

By Drago Bosnic
Global Research, July 04, 2022
InfoBrics

Region: Russia and FSU, USA
Theme: Intelligence

***

In early June, some news media outlets reported on an interview General Paul Nakasone, the head of US Cyber Command, had with Sky News, where he openly admitted the United States is conducting offensive cyber operations against Russia. General Nakasone explained:

> "'Hunt forward' operations are allowing the US to search out foreign hackers and identify the tools they use against America." Back then, 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 in order to "support" Ukraine. "We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations," US general stated. He didn't give any specifics, but 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," adding that his job is to "provide a series of options to the secretary of defense and the president, and so that's what I do," declining to give any further details.

> "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 during a speech at CyCon, a conference on cyber conflict, hosted by NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn.

> "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.

The revelation didn't catch much attention from Western state-run mass media, or at least not as one would expect for such a groundbreaking admission. What garnered even less attention was a statement by Zhao Lijian, China's Foreign Ministry Spokesman. When asked about the US cyber aggression against Russia, he responded:

> "We have noticed relevant reports and are concerned over the dangerous and irresponsible US behavior. The US needs to explain to the international community how these 'offensive hacking operations' are consistent with its professed position of not engaging directly in the Russia-Ukraine conflict.
>
> The US and NATO have said cyber-attacks can be considered an 'armed attack'. The US also declared earlier that it could respond to cyber-attacks with conventional means or even nuclear weapons. According to its own logic of policy-making, the above-mentioned US operations could lead to the possibility of escalating the Russia-Ukraine conflict situation and even triggering a nuclear attack.
>
> It's quite obvious that the US is conducting a dangerous experiment in the context of the Russia-Ukraine conflict. The US believes that with an unrivalled military cyber capability, it is able to unilaterally control the scale and consequences of offensive hacking operations. However, the reality might not necessarily follow the US's design. If the situation gets out of control, it will end up harming the common interests of the international community, the US included. Besides, the US has also declared repeatedly about 'Forward Deployment' of cyber military forces in some small and medium-sized countries. These countries need to keep their eyes wide open and beware whether such deployment could embroil them in a conflict they don't seek.
>
> Cyberspace is the common space of activities for mankind. We urge the US to change its dangerous and irresponsible behavior and join the international community in safeguarding peace and security in cyberspace."

Indeed, NATO is contemplating the inclusion of cyber warfare in the controversial Article 5, the "collective defense" clause considered to be its cornerstone. The sheer hypocrisy of the political West's actions and statements is nearly impossible to overstate. This has become so obvious that the world is plainly speaking sick and tired of it. Prior to the West's escalating actions which forced Russia's hand and the aggressive moves and rhetoric in regard to China, Mr. Lijian's statements were usually very reserved. However, ever since, China has become more direct in criticizing US aggression against the world.

This also includes Russia's former president and head of its Security Council, Dmitry Medvedev, who has lashed out at the West multiple times so far, including a call for Russia to stop negotiating with the political West, which has broken nearly all international treaties and laws.

In addition to Russia, NATO and its numerous vassals have openly targeted China during the

already infamous Madrid summit. The new policy will certainly result in further destabilization of the world. However, for the political West this is not merely an acceptable consequence, but also desirable, as their long-obsolete "purely defensive alliance" will finally get the "much-needed" reinvigoration.

*

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
