GlobalResearch
Center for Research on Globalization

Cyberspace Close to Become New Focus for NATO-Ukraine Joint Actions Against Russia

By Lucas Leiroz de Almeida
Global Research, January 18, 2022
InfoBrics 17 January 2022

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

***

Once again, the West seems to be creating arguments to justify the implementation of coercive measures against Russia. A cyberattack against Kiev allegedly occurred last week has been making headlines around the world. Now, the Ukrainian government claims to have proof that the attack has Russian involvement – although no details have been provided so far as to what such "proof" would be. Apparently, NATO and Kiev are ready to turn cyberspace into a new focus of their anti-Russian campaigns.

An alleged cyberattack against Ukraine took place in the early hours of Friday last week, leaving several official government systems inaccessible. For a few hours, the websites of several Ukrainian ministries were absolutely offline. On some of the hacked sites, some messages appeared warning Ukrainians to "expect the worst". In addition to ministries, virtual databases of many government offices were hacked, but according to information published by the Ministry of Digital Transformation, there was no leakage of personal data of government officials, being the damage limited to the operability of the websites.

The alleged "attack" generated immediate worldwide repercussions. Governments and international organizations around the world have published notes repudiating the hackers' attitude. The European Union, the US, pro-Western governments, and NATO reinforced their desire to "help" Kiev to strengthen its cyber defense system.

NATO's **Secretary Jen Stoltenberg** published the following words about the case:

> "I strongly condemn the cyber attacks on the Ukrainian Government. NATO has worked closely with Ukraine for years to help boost its cyber defenses (…) In the coming days, NATO and Ukraine will sign an agreement on enhanced cyber cooperation, including access to NATO's Ukrainian malware information sharing platform. NATO's strong political and practical support for Ukraine will continue".

In the same sense, White House Press Secretary **Jen Psaki** also commented on the case,

saying:

> "We are also in touch with Ukrainians and have offered our support as Ukraine investigates the impact and nature and recovers from the incident".

In Europe, on the other hand, the comments were more aggressive and tried to blame Russia. EU top diplomat **Josep Borrell** said:

> "We are going to mobilize all our resources to help Ukraine to tackle this cyber attack. Sadly, we knew it could happen (…) It's difficult to say (who is behind it). I can't blame anybody as I have no proof, but we can imagine".

By saying "we can imagine", Borrell was certainly referring to Russia. Also, something similar has been said by Swedish **Foreign Minister Ann Lind,** who commented directly on the possibility of Russian involvement, saying words in a threatening tone:

> "we have to be very firm in our messages to Russia: that if there are attacks against Ukraine, we will be very harsh and very strong and robust in our response".

Later, on Sunday, Kiev definitively adopted the rhetoric that had been previously promoted by Europeans, blaming Russia. Ukrainian digital transformation ministry **Mykhailo Fedorov** said that "all the evidence points to Russia being behind the cyber-attack". Evidently, this is a suspicion that could arise at any moment, considering that the attack took place amid tensions between Russia and Ukraine and that cyber operations are a common military tactic in contemporary warfare. The problem in this case is that no details were provided on what such "evidence" would be. Kiev simply believes that Moscow operated the attacks because it is a "plausible" suspect, considering the fact that these are rival countries, but no material evidence has been presented so far, which makes the narrative very weak.

If Kiev and the West accuse Russia of involvement in the attack, it is up to them to prove the allegations. The burden of proof for the accuser is a universal principle of justice that cannot be ignored in diplomatic relations. Furthermore, in the same way that cyber-attacks are common practice in contemporary warfare (which would make the Russian involvement narrative plausible), self-sabotage operations and "false flag attacks" are also constantly practiced in current conflicts between states, which makes it plausible that Kiev or some other western government operated the hacking attack in order to blame Russia and tighten security measures against Moscow – and the fact that there was no data leakage in the attack can be considered an evidence in this regard, as such leakage would not be of interest in a false flag operation.

Indeed, there are many possibilities, and it would be wrong to accuse either side without prior investigations. However, unfortunately, what we can expect going forward is that the anti-Russian narrative, despite being weak, will be considered sufficient for NATO to harden the measures against Russia and start a campaign of cyber warfare. Increasingly, cyberspace can be considered a new battlefield, as important as land, sea, air, and outer space.

*

Lucas Leiroz *is a researcher in Social Sciences at the Rural Federal University of Rio de Janeiro; geopolitical consultant.*

Featured image is from InfoBrics
