GlobalResearch
Center for Research on Globalization

The Online Bomb Hoaxes Against Russia Are Clear Cases of Cyber Terrorism

By Andrew Korybko
Global Research, February 02, 2020
Region: Russia and FSU
Theme: Intelligence, Law and Justice

Russians have been terrorized for the past several months by online bomb hoaxes spread throughout the country by anonymous email services based abroad, which represent a cutting-edge threat to the modern world's way of life and thus necessitates a concerted response by the international community if this scourge is to ever be fully defeated.

A new form of terrorism has been waged against Russia over the past several months through online bomb hoaxes spread across the country by anonymous email services based abroad. This cyber terrorism saw hundreds of public facilities evacuated since November 2019 out of an abundance of caution, only for each and every one of them to have been false alarms. The authorities discovered that the Netherlands-based Startmail.com was being used by the cyber terrorists and thus banned the service earlier this month, but it's since been reported that the Swiss-based Protonmail.com replaced it as the new method of conveying these false threats. It, too, has just been banned, but it's predictable that another one will once again take its place, and so and on so forth until the logical conclusion of the authorities' security campaign has been reached by banning all anonymous email services in the country.

Cyber terrorism of this sort is especially dangerous because it's intended to sow panic among the population and make them believe that they're living in a state of non-stop siege. Furthermore, it's also meant to test the authorities' responses in anticipation of what might eventually be a genuine bomb threat sometime in the future that could be perfected for maximum damage if the perpetrators manage to discern any shortcomings in the security services' method of handling these hoaxes. Even if none are discovered, then it goes without saying that the authorities might naturally grow fatigued having to respond to so many false alarms all the time, after which they might either become complacent or sloppy in their responses and thus miss an actual bomb in the event that one is ever really planted at a targeted facility. Of course, the argument can also be made that these hoaxes provide the security services with extra training, but they also become tiresome after so long too.

These online bomb hoaxes are a cutting-edge threat to the modern world's way of life even though this form of cyber terrorism is only being waged against Russia at the moment, and it'll require a concerted response by the international community if this scourge is to ever prevented from spreading and ultimately defeated. The problem, however, is that there's barely any foreign media coverage about this issue, making one wonder whether others abroad simply aren't all that aware of what's happening or if they fear that reporting on it could trigger copycat attacks against their own countries. It's therefore difficult to discern whether decision makers abroad are even really aware of the enormity of this threat and the

scale with which it's been waged against Russia or not. Of course, it can be speculated that a foreign intelligence agency or possibly even several might be somehow connected to these cyber terrorist attacks, but for the time being at least, that can't be proven.

In the spirit of good faith, Russia should therefore consider the wisdom of discussing this threat in prominent international fora, especially the UN, in order to make the world aware of what it's been facing over the past several months. Anonymous email services by their very nature make it difficult to trace who's sending what, so the natural solution is to shut them down worldwide. That, however, probably won't happen because of privacy concerns in some mostly Western countries and the fear that governments would be overstepping their authority by attempting to regulate this space. They likely won't act, if ever, unless they're one day targeted on a large scale like Russia presently is, but they could at the very least be politely dissuaded from potentially condemning the authorities' response of banning these services. Any politiczation of the government's policy of shutting down those sites' reach in Russia would suggest Machiavellian motives on their part.

After all, while it can't be proven (at least at this point in time) that any foreign intelligence agencies are involved in these cyber attacks, it would speak volumes about the self-interested and shameless opportunism of other countries if they use the Russian authorities' response as an excuse to continue with their infowar crusade against the country. There was already tremendous uproar in the foreign press over the state's internet survival exercise last month (inaccurately reported as a "shut-down"), so it's conceivable that some forces might seek to exploit Russia's latest cyber security moves to continue advancing the fearmongering narrative that the Kremlin is supposedly cracking down on cyberspace ahead of a so-called "power grab" by President Putin. Nothing of the sort is transpiring, though speculatively alleging as much serves to erode Russia's moral standing in the world by misportraying it as a "dictatorship" that's supposedly "scared of its own people" whereas it's really just a national democracy doing its utmost to protect its citizens from the threat of cyber terrorism.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

This article was originally published on OneWorld.

Andrew Korybko is an American Moscow-based political analyst specializing in the relationship between the US strategy in Afro-Eurasia, China's One Belt One Road global vision of New Silk Road connectivity, and Hybrid Warfare. He is a frequent contributor to Global Research.

Featured image is from OneWorld

Articles by: Andrew Korybko

About the author:

Andrew Korybko is an American Moscow-based political analyst specializing in the relationship between the US strategy in Afro-Eurasia, China's One Belt One Road global vision of New Silk Road connectivity, and Hybrid Warfare. He is a frequent contributor to Global Research.