GlobalResearch
Center for Research on Globalization

“The Russians Are Coming”, Again! Poorly Understood Cybercrimes Play Perfectly into Political Agendas

By Helen Buyniski
Global Research, July 17, 2020
RT Op-Ed 16 July 2020

Region: Europe, Russia and FSU, USA
Theme: Intelligence, Media Disinformation

Foreign hackers are determined as ever to steal technology, meddle in elections and skew foreign policy, but fear not! The CIA has apparently been authorized to deliver preemptive cyber-strikes based on partisan mythmaking.

US, UK and Canadian intelligence dropped a 16-page report on Thursday accusing *“Russian hackers”* – specifically APT29, the *“Cozy Bear”* hacking group of ‘Russiagate’ fame – of targeting unspecified entities involved in developing the (increasingly controversial) Covid-19 vaccine.

However, the report is fraught with the same factual pitfalls plaguing previous unsubstantiated *“Russian hacking”* tales, seemingly designed to capitalize on the general population’s ignorance about cyber-attacks – or vaccines, for that matter. While Democrat-linked cybersecurity firm CrowdStrike specializes in attributing state actors to malware attacks, more reputable companies avoid doing so based solely on the malware used, since hacking groups often exchange tools or even collaborate.

The best, or just best-funded hackers are able to not only cover their tracks effectively but create a fake trail leading to someone else. The WikiLeaks Vault 7 release in 2017 exposed the disturbing tools the CIA has at its disposal for simulating foreign cyberattacks, tools that allow the agency to make it seem like Moscow or Tehran is behind a hack when the real culprits are in Langley, Virginia.

Russia is far from the only country to be accused of such behavior, of course – China was accused of attempting to steal coronavirus vaccine research back in May, while US and UK intelligence agencies warned that same month that other *“threat groups”* were *“actively targeting”* local governments, pharmaceutical and research firms, healthcare facilities, and universities for virus-related hacking.

Nor is this latest outbreak of finger-pointing limited to the pandemic. On Thursday, UK foreign minister Dominic Raab denounced *“Russian actors”* for *“almost certainly”* seeking to meddle in the 2019 election – not by actually breaking any laws, but by *“amplifying”* documents leaked by other people on Reddit and circulated around social media in the run-up to December’s contest.

Raab didn’t name any of the Russians responsible for circulating the material, perhaps mindful of the embarrassment that befell his ideological brother-in-arms, Atlantic Council

bot-hunter Ben Nimmo, who accused several real people of being *"Russian bots."* Further covering his bases, Raab in the same statement acknowledged that there was *"no evidence of a broad-spectrum Russian campaign against the General Election."*

Even the most nonspecific shrieking about Russian hackers plotting to steal vaccine data, however, distracts from the inconvenient reality that the vaccines under development in the UK and US are performing abysmally. Neither the US company Moderna – initially hailed as the frontrunner despite never having brought a vaccine to market before – nor the UK's collaboration between Oxford University and pharma giant AstraZeneca have produced any encouraging results in their clinical trials.

That didn't stop the US from ordering 300 million doses of the Oxford jab, though the Trump administration's coronavirus czar Anthony Fauci has already begun lamenting the *"general anti-science, anti-authority, anti-vaccine feeling among some people in this country"* he fears will keep Americans away from the needle.

With regard to hacking, however, the world might be more concerned about the CIA than the Russians – especially following Wednesday's Yahoo News report that the agency had received carte blanche from Trump to wage preemptive (i.e. unjustified) cyber-warfare against any individual or organization it could link to a *"handful of adversarial countries."*

According to several former US officials, the CIA has been wielding unprecedented offensive powers against American civilians only tenuously connected to Washington's geopolitical rivals since 2018, checking off at least 12 cyber-attacks on its *"wish list"* already. Liberated from the tiresome need to provide *"years of signals and dozens of pages of intelligence"*justifying raining computer-borne chaos and destabilization on its victims, the CIA has wrought *"a combination of destructive things – stuff is on fire and exploding – and also public dissemination of data: leaking or things that look like leaking."*

News of the CIA being given carte blanche appears at the same point in the US election cycle as the 2018 report about a similar measure that freed the hands of the Pentagon to conduct its own cyberattacks without interference from the State Department or any intelligence agencies.

With a hotly anticipated election coming up in November, it's not hard to imagine how a few well-placed *"leaks"* or *"destructive things"* might convince voters to put aside their concerns about the administration's response to the pandemic – or to place it front and center, depending on whether the CIA has decided it can live with four more years of Trump.

One thing is certain: the *"Russian meddling"* narrative isn't going away anytime soon.

*

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.

Helen Buyniski is an American journalist and political commentator at RT Op-Ed. Follow her on Twitter @velocirapture23

The original source of this article is RT Op-Ed
Copyright © Helen Buyniski, RT Op-Ed, 2020

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Helen Buyniski

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