GlobalResearch
Center for Research on Globalization

Clamouring Against Russia: The Cyber Attack Platform

By Dr. Binoy Kampmark
Global Research, April 20, 2018

Region: Russia and FSU
Theme: Intelligence, Media Disinformation, US NATO War Agenda
In-depth Report: FAKE INTELLIGENCE

In a time when such revelations as those of Edward Snowden pass a person's lips with ease and awareness, political clamouring for action and measures against Russia on the subject of cyber attack seem risible. This is not to say that Russia does not engage in an energetic, state of the art program of surveillance and penetration. More significant is the sheer noise such acts generate from those who claim to have the book of ethics in one hand and the code of laws in the other – the international ones no less.

This is cyberwarfare writ large, its warriors on keyboards becoming a new feted aristocracy, digital knights fashioning the next theft, or the next destabilising virus. Singling out a monster can only come across as a vulgar, if convenient distraction. In another sense, it offers backhanded praise.

On April 16, the US Department of Homeland Security, Federal Bureau of Investigation and the UK's Cyber Security Centre released a "Technical Alert" citing "malicious cyber activity carried out by the Russian Government." The joint US-UK statement noted attacks on "network infrastructure devices worldwide such as routers, switches, firewalls, and the Network Intrusion Detection System (NIDS)."

Jeanette Manfra charged with cybersecurity and communications matters within the US National Protection and Programs Directorate was even dramatic on the scale of the assault.

> "Russian government activities continue to threaten our respective safety, security, and the very integrity of our cyber ecosystem."

Then came the Five Eyes chatterers, the small Anglophone grouping that was given some dressing down by the Snowden revelations in 2013. Four of them – Australia, New Zealand, Canada and the United Kingdom – got comfortable at the National Cyber Security Centre in London during the week. The only member missing before the picture shoot was the US colossus.

UK Prime Minister Theresa May accused Moscow of "using cyber as part of a wider effort to attack and undermine the international system." May was at pains with her colleagues to observe that,

> "We know what it's doing, and we should be in no doubt that such cyberwarfare is one of the greatest challenges of our time."

The others also added their contribution to the potluck luncheon of indignant warning. Canada's Justin Trudeau was confident in condemnation.

> "There are folks out there in the world, countries out there in the world who do not share our values and our approach to freedoms and mostly the rules-based order."

Trudeau was telling if inadvertently so.

> "So the importance of like-minded friends and partners like us four to stand together provides a response and a solidarity that is a clear message to those around the world who do not play by the same rules."

Whose rules you ask? The answer is clearly evident.

The Australians added their own version, claiming that up to 400 Australian businesses might have been the target of Russian sponsored hackers, though Cyber Security Minister Angus Taylor demonstrated the confused state of thinking by claiming no information had been "compromised". Keeping a brave face, Australia's defence minister Marise Payne reiterated the same theme: the attacks had taken place, but evidently without much consequence (in her words, without "any exploitation of significance").

At the National Cyber Security Centre gathering, Prime Minister Malcolm Turnbull rounded the assault on Russia in a job lot description:

> "The message to be sent in solidarity that this type of illegal conduct whether it is a chemical attack in Syria, the use of a nerve agent on British soil or the expanding cyber attacks across the internet across the whole digital domain on which all our businesses and economics depended. These must be resisted."

The rather seedy way of roping international values into a Five Eyes arrangement that insists on targets, surveillance and theft is a fairly rich thing to do. That very same gathering has done its fair share of spying on each other's citizens, blurring the line on plausible targets. The rules-based order so praised has been left wanting, and limping. The world of global surveillance is an unruly one indeed.

The case of New Zealand offers one such example of that limp, notably in the government handling of the Kim Dotcom case. Not only has the intelligence service there lost its head in monitoring him specifically for their American lords, the entire outfit had demonstrated that it is happy to spy on residents, something which it is legally barred from.

It was left to the High Court of New Zealand to find on a few occasions in 2017 that the operation conducted by the Government Communications Security Bureau against Dotcom, Bram van der Kolk and Mathias Ortmann, all associated with Megaupload, was illegal. Such spying constituted "illegal searches" in violation of the New Zealand Bill of Rights.

In targeting Russia, importance is elevated, the very thing that will be earning points on the Moscow tally board of realpolitik.

> “We have found the Russians in routers and deep inside networks for 20 years,” says Robert Hannigan, a person who knows a thing or two about hoovering and gathering intelligence from tapped transatlantic fibre-optic cables.

He was, after all, a former head of Britain’s GCHQ, the agency responsible for those very exploits.

The recent spike of interest in Russia’s cyber heft made the *New York Times* feel nostalgic, a sort of tunnel vision view about a revamped and rejigged Cold War that was gaining pace.

> “The sweep and urgency of the statements from both sides of the Atlantic called to mind a computer-age version of a Cold War air raid drill, but asking citizens to upgrade their passwords rather than duck and cover.”

The shaky ground upon which the argument against Russia is built on presumes harked international norms in the face of a new Wild West frontier of battles and appropriations. The exceptionalist language of devilry Russia is coated with ignores one brutal fact: cyber measures have become ordinary fare, boringly regular. The only response from connected citizens is rudimentary, if at times ineffectual common sense: change passwords regularly, and hope for the worst.

*

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

---