GlobalResearch
Center for Research on Globalization

Hacking for Vaccines. Intellectual Property and Espionage

By Dr. Binoy Kampmark
Global Research, May 18, 2020
Region: Asia, USA
Theme: Intelligence, Science and Medicine

If you cannot discover or create something, best steal it. It has been the operating principle for everything from wealth to technology. With the efforts to discover a vaccine to the novel coronavirus being all but bound by solidarity, the race on plundering secrets has already begun in earnest. No one party can claim particular innocence in this endeavour. All states engage in economic espionage and old-fashioned secret pinching to advance their interests. Finding the building blocks for a COVID-19 vaccine is proving no different.

As with such accusations, the cloak is procured with the dagger. The case is probable, and plausible enough, but confirmation tends to come in rations. In the business of hacking, what is acceptable in torrid love and hideous war tends to be a hard one to pin down.

In 2015, the US and China reached an accord to, in the words of **President Barack Obama**, refrain from conducting or knowingly supporting "cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage." At the time, an assessment by *Wired* came to the conclusion that the agreement did not prevent traditional, full blown espionage, focusing, instead, on such efforts as those to pinch company source codes for competitive advantage.

In addition to Obama's main point, Beijing and Washington agreed to furnish timely responses to requests for information and assistance dealing with malicious cyber activities; engage in "efforts to further identify and promote appropriate norms of state behaviour in cyberspace" and "establish a high-level joint dialogue mechanism on fighting cybercrime and related issues."

In 2018, the National Counterintelligence and Security Centre (NCSC) reported that "the Intelligence Community and private sector security experts continue to identify ongoing Chinese cyber activity, although at lower volumes than existed before the bilateral September 2015 US-China cyber commitments." Not all bad then, especially given that cyber activity designed to pilfer intellectual property for other non-competitive purposes continued to be de rigueur.

During the pandemic crisis, the niggles and pinches caused by cyberactivity have reportedly increased in number. Academic and research programs are being scrutinised. The US Justice Department has taken a particular interest in the PRC-sponsored Thousand Talents program. One of their latest targets is University of Arkansas' professor of engineering, Simon Saw-Teong Ang, accused of concealing his ties to the Chinese government and universities while he worked on projects with NASA funding.

The United States, while not exactly leading in its response to dealing with COVID-19, now

claims that its efforts to identify treatments and a vaccines are being targeted by others, with the PRC leading (naturally), the keen pack. "The PRC's behaviour in cyberspace," US **Secretary of State Mike Pompeo** argued in a statement last Thursday, "is an extension of its counterproductive actions throughout the COVID-19 pandemic." **Senator Marco Rubio**, one of the noisiest of China hawks, has also been squawking on what he claims is an adjustment in Chinese tactics. "Beijing has shifted its recruitment efforts for the Thousand Talents Program online, and it has increased efforts to hack US medical research institutes for COVID-19 information."

On May 13, a joint statement by the Federal Bureau of Investigation and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency was published. It alleged "the compromise of US organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors." Allegedly, such actors had "been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research."

The statement warned that organisations "conducting research in these areas" should "maintain dedicated cybersecurity and insider threat practices to prevent surreptitious review or theft of COVID-19-related material." Systems should be patched for "critical vulnerabilities"; web applications for authorised access should be actively sought out. Users "exhibiting unusual activity" should be suspended.

The warning is skimpy in details, notably on the issue of how treatments will be hampered. Nor are many researchers blind about similar pinching efforts from the US side of the fence. Jason Healey, a senior researcher at Columbia University's School of International and Public Affairs makes a few valid points on this. "If the US is wanting to argue for norms, I look forward to us doing it directly and saying here's what we think the playing field lies, because certainly we're being active in many of these areas as well."

China has also been the subject of cyber interest in this particularly busy playing field. In April, a Vietnamese hacking group known as APT32 is said to have taken interest in the PRC's Ministry of Emergency Management and the government of Wuhan. According to Ben Read of the cybersecurity firm FireEye, "These attacks speak to the virus being an intelligence priority – everyone is throwing everything they've got at it, and APT32 is what Vietnam has." Not a good time, it seems, to find a vaccine in solidarity.

*

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.

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*

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Dr. Binoy Kampmark**