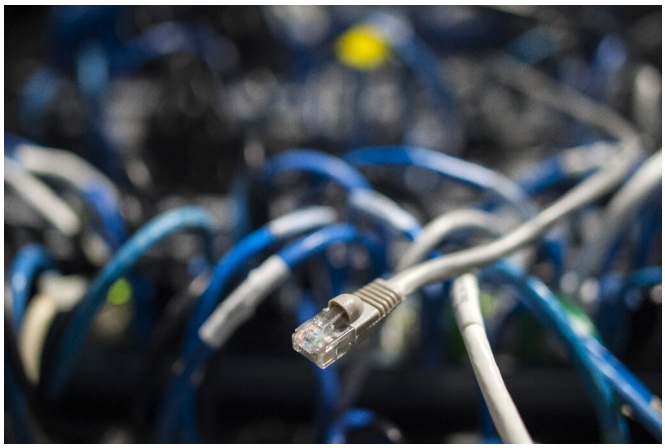
Coronavirus confinement challenges intelligence services

23 March 2020, by Didier Lauras



The pandemic has exposed the internet as both a tool and a potential target for malefactors

The home confinement of hundreds of millions of people worldwide to halt coronavirus contagion has presented intelligence services with a challenge: monitoring an explosion in internet traffic, above board and not, even as their own capacity is reduced.

The global health crisis has exposed the internet as both a tool and a potential target for malefactors, experts say, with agents—many themselves working from home—having to sift through the deluge looking for credible threats.

Criminals could take advantage of the disarray to launch attacks on government and nuclear systems, alter scientific or electoral data, paralyse servers, or spread fake news.

Developing countries and those with weak monitoring systems are most at risk, with Western nations better geared to pick up external cyber threats.

"If you want to make mischief in... some other part of the world, and try to do so in a low-profile way and try to escape attention, now presents an opportunity to do that," said Suzanne Spaulding of the Center for Strategic and International Studies (CSIS) in Washington.

In a bid to curb virus contagion among their ranks, intelligence services are alternating teams at the office, like many other essential businesses and services continuing to function amid the unprecedented global lockdown.

And while some officials are equipped to work on encrypted systems from home, these generally do not grant them access to the most sensitive information, a former agent of France's DGSE foreign intelligence agency told AFP on condition of anonymity.

"There is continuity, but strategic intelligence gathering will necessarily be lighter," he said.

Brian Perkins, a researcher at the Jamestown Foundation, a Washington intelligence think-tank, pointed to a breakdown in covert fieldwork capabilities.

"The biggest challenge posed by COVID-19 is... the inability of intelligence field officers to extract human intelligence in areas with active outbreaks, particularly areas with significant restrictions on public interactions or travel," he told AFP.

'Malign actors'

Such restrictions create fertile ground for organised disinformation campaigns and cyberattacks.

"Malign actors are actively exploiting these new challenging circumstances," cross-border policing agency Europol said last week.

And the World Economic Forum has warned that "broad-based cyberattacks could cause widespread

infrastructure failures that take entire communities or cities offline, obstructing healthcare providers, public systems and networks."

With the attention of governments around the world focused on a common, invisible enemy, one could have hoped for a drawdown of global hostilities.

But no such luck, experts say.

"Over the past six weeks, we've seen Chinese threat actors continue their operations against their usual external targets," said Ben Reed of the cybersecurity group FireEye.

"It's too early to see if there's been any quantitative decrease in activity, but what we're seeing matches previous patterns... no indication of a 'truce'."

He added that they have continued to see "cyber-espionage" activity from North Korea, Russia and South Asia despite the coronavirus activity.

Russia versus the West

Moscow is indeed also a focus for Western governments, which have accused it of stepping up a campaign of misinformation regarding the coronavirus outbreak.

"It does not take a lot of people nor resources to carry out these kind of attacks," Spaulding from CSIS said.

The European Union's East Stratcom anti-disinformation taskforce has pointed to more than 110 coronavirus-related campaigns between January 22 and March 19.

"Messages targeting domestic Russian audiences describe the virus as a form of foreign aggression", it said in a statement, while messages targeting international audiences "focus primarily on conspiracy theories".

"These messages are characteristic of the Kremlin's well-established strategy of using disinformation to amplify divisions, sow distrust and chaos, and exacerbate crisis situations and issues of public concern," East Stratcom said.

Moscow regularly denies such accusations, accusing the West of similar tactics in return.