malaymail Since 1896

17 July 2018

Cyberspace invaders

By Elina Noor

Last Friday, a grand jury in the US District of Columbia charged 12 Russians with 11 counts of aggravated identity theft, conspiracy to launder money, and conspiracy to commit an offence against the United States.

These federal crimes, as the indictment alleges, were knowingly and willfully conducted through large-scale and multi-layered cyber operations in order to interfere with the 2016 US presidential election.

The indictment is a bold and remarkable assignment of blame to the 12 defendants identified as officers of Russia's Main Intelligence Directorate of the General Staff ("GRU"). It goes into great detail about the complexity of the Russian operation and suggests impressive counter-intelligence tactics on the part of the United States. Significantly, it doubles down on a series of assessments over the past couple of years by both the private sector as well as security and intelligence services in the United States' of Russia's role in disrupting US political and electoral processes through cyber operations. With this indictment, the United States has technically, politically, and legally attributed responsibility of interference in its 2016 presidential election to Russia.

The question of attributing cyber attacks is difficult and controversial. While technical forensic investigations may yield significant and detailed footprints to convincingly attribute attacks to their perpetrators, they risk revealing valuable means, methods, and sources in the process. Understandably, governments almost never publicly share how they determine attribution. Often, attribution is not a singular determination but a cumulative analysis of behavioral patterns and motivations that, in the case of suspected state actors, may extend into the realm of a political judgement. This political call, if publicly unsubstantiated, however, leaves room for suspicion and dispute by others not privy to the evidence gathered.

But what do the geopolitics of major power competition, the intrigues of espionage, and the complexity of cyber operations have to do with small countries like Malaysia? Turns out, we sometimes unwittingly end up in the cross hairs as bit players.

In describing how the Russians attempted to cover their tracks in cyber space, Friday's indictment alleges that the defendants used cryptocurrency they had mined and bought to lease a server in Malaysia that they then used to host the dcleaks.com website. Stolen election-related emails and documents were released and publicized on the website, which was made to seem as if it had been created by American hacktivists.

There is no implication in the indictment that the server host in Malaysia knew how its services were going to be used or that Malaysia was somehow lax in allowing this to happen. A server in Arizona was also reportedly leased by the Russian defendants to monitor and surveil the computers they had hacked into.

What the allegation demonstrates is the inherent complexity of the public-private overlay in cyber space. With the exception of behemoth multinational corporations with interests in different countries, companies are typically driven by their bottomline rather than geopolitics. The cost-benefit calculations of ensuring servers are not commandeered to destabilize or interfere in the internal affairs of other countries, far outweighs any real motivation to do so. That so much of the public and national security interest intersects with infrastructure and services provided by the private sector raises important questions about how much of the latter should be regulated to preserve the former.

The references to Malaysia in the indictment also raise the hypothetical - though not completely far-fetched possibility - of how a small, third-party state might be caught in a difficult position if its territory were used to commit an offence against another state, as part of a sustained cyber campaign conducted during peacetime. If the operations violate national laws, then the perpetrators could be prosecuted accordingly. If the operations fall just short of offending any national or international laws, then the third-party state might be caught in a larger political fallout between the affected states. If the operations amount to a use of force, or an armed attack, and the aggrieved state concludes in the process that the third-party state did not do enough or had been unwilling to stop the cyber campaign from occurring within its territory, then there might be severe ramifications for the third-party state if the aggrieved state also decides to act against it in self-defence.

There is little, if any, support for the notion that the alleged Russian meddling of the 2016 US presidential election amounted to a use of force or an armed attack enough to justify a US response in self-defence under international law provisions. Lawyers could argue, however, that at a minimum, US sovereignty and the principle of non-intervention were breached. But without evidence of coercion, or tangible damage caused, by the alleged Russian interference, the law is presently unsettled and international legal precedents do not authoritatively point one way or the other. The legal ambiguity of this type of grey-zone operations in peacetime is exactly why the exploitation of cyber space holds strategic appeal.

In the absence of legal clarity on this and other forms of grey zone operations, there have been discussions over the years to promulgate certain norms of behaviour in cyber space. There is general agreement that international law applies in cyber space as repeatedly affirmed by consensus by the UN Group of Governmental Experts in 2013 and 2015. Closer to home, ASEAN leaders also recently vouched for a rules-based order to frame conduct in this emergent domain. What is hotly debated is how specific provisions of international law should apply, what kinds of rules and norms can be agreed on, and what role territorial borders have in cyber space.

However, between diplomatic intractability and the growing proliferation of attacks in cyber space, one priority should be borne in mind: that of preserving the availability and integrity of the Internet, and therefore, stability in cyberspace for all. This is crucial given how much of the Internet we rely on to conduct our daily lives, whether in furtherance of personal banking or national security. In 2017, the Global Commission on the Stability of Cyberspace issued a call to protect the public core of the Internet. All stakeholders, whether state or non-state actors, should commit at a minimum to non-interference with what underpins the functionality of the Internet: routing and naming systems, physical transmission infrastructure, and cryptographic mechanisms of security and identity.

It is inevitable for power dynamics to play out among states for domination of influence and domain in cyber space. In that light, it will be increasingly important for smaller states like Malaysia to carve out a balanced, principled position amid these dynamic, digital complexities. But let’s not lose sight of the low-hanging fruits for cooperation to maintain stability in cyber space even as we press on - and we must - with larger, more vexing discussions of international security in this arena.

Elina Noor is Visiting Fellow, Institute of Strategic and International Studies (ISIS) Malaysia and Commissioner, Global Commission on the Stability of Cyberspace