Russian election hacks exploited legal grey zone: lawyers

February 9 2017, by Paul Handley

Policymakers need a manual to assess and counter hacking attacks, according to lawyers specializing in cyber issues

Russia's alleged computer hacking to interfere in US elections was no act of war, but exploited a legal grey zone that makes justifying retaliation hard, international lawyers specializing in cyber issues said Wednesday.

Moscow's interference in the presidential campaign last year by hacking Democratic Party computers and leaking embarrassing communications was an act of espionage—legal under international law—and at worst a slight violation of US sovereignty, the lawyers said.

But it was definitely no act of war, as some American politicians have suggested, US lawyer Michael Schmitt said, adding that calling it such "is very destabilizing."

Self-defense standards

Speaking at the launch of a new manual on cyber attacks and international law, he said the reaction to the Russia-US hacking case heightens the need for accepted international standards for countries to assess and counter cyber attacks proportionately.

The new volume, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" was produced by 20 international lawyers led by Schmitt at the Estonia-based NATO Cooperative Cyber Defence Centre of Excellence.

A bid to create a framework for policymakers around the world, the manual lays out a number of situations and cases to which it applies established international law.

A glass wall featuring coding symbols at an Internet security firm in Moscow

"It was clear that states were grappling on a day-to-day basis" with peacetime cyber attacks, said Liis Vihul, an Estonian lawyer who was project manager for the manual.

A key thing they want to know is "when do states enjoy the right to self-defense?"

Stuxnet attack on Iran

The range of cyber-attacks in recent years makes it important to give leaders a framework for their choices, Schmitt said.

He referred to the North Korean hacking of Sony Corp; the possible Chinese theft of millions of US government employees' personal records

from the main civil service agency; the Stuxnet computer virus attack on Iranian nuclear installations; and the recent election hacks.

In each case, Schmitt said, it is crucial to assess the motives and targets of the attacks; the level of damage done beyond the simple theft of data in an act of spying; and be able to clearly identify the culprits.

US intelligence officials characterized the theft of US civil service data at the time as an act of war, simply because of the amount of stolen data.

The Stuxnet computer virus attack on Iranian nuclear installations could be categorized as an act of self-defense against a known threat, according to international lawyers specializing in cyber issues

But Schmitt said the lawyers behind the new manual generally agreed

that scale does not change the principles just because it takes place online. The theft "didn't interfere with the functioning of any inherently governmental act," a principle issue for assessing attacks.

Law and deterrence

In the Sony case, the hackers sought to damage a major corporation on US territory, which can be construed as an attack on US sovereign territory, he said—while stressing the need for a proportional response.

The Stuxnet case, widely blamed on the United States and Israel, could arguably be categorized as an act of self-defense against a known threat, he said.

But Iran could also have considered it equivalent to an armed attack. The lawyers were split on that point, Schmitt said, adding, "I am of the opinion that it reached that level."

The lawyers writing the manual had created a theoretical case of election interference by a foreign country well before the issue of Russian hacking of the Democratic Party communications surfaced, he added.

But in that case, the lawyers were split. Vihul said it was espionage that did nothing more than leak true information to inform US voters, not a violation of international law.

US politicians have promised to retaliate after Russia hacked the Democratic Party computers in 2016, with some calling Moscow's intervention an "act of war"

For Schmitt, Russia went over the line "a wee bit" to damage US election processes, which are protected under global legal standards.

"The Russians are masters at identifying grey zones in international law," he said.

"They look for these grey zones to operate in because they know that it will be difficult to characterize their actions as unlawful."

However, he said, Russia needs to understand that "if you play in the grey area, you're then creating precedent for other states to play in the grey area as well, vis a vis you."

The role of international law, he argued, sets standards for retaliation and deterrence.

"Clarity in the law leads to stability... Clear rules of the game diminish the possibility of escalation."