The New York Times

Putin Is Running a Destructive Cybercrime Syndicate Out of Russia

Every day, cybercrooks inflict immense harm on real victims across our country and around the world. Will Trump protest?

By John P. Carlin

Mr. Carlin, the former assistant United States attorney general for national security and chief of staff to the F.B.I. director Robert Mueller, is the author of the forthcoming "Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat."

July 16, 2018

The indictment of a dozen Russian military intelligence officers by my former boss, Robert Mueller, instantly reshaped the geopolitical backdrop of President Trump's summit meeting with Vladimir Putin. But the sad truth is that it's just more evidence of what we've known for years: Online, Russia is increasingly a rogue state, a country that plays by its own rules in cyberspace and today stands as the world's largest safe haven for cybercriminals — not just protected but also aided and abetted by the state.

Recent headlines have focused on the attacks of the 2016 election, but every day Russian crooks inflict immense harm on real victims across our country and around the world, causing billions of dollars in losses.

Why won't President Trump call out Mr. Putin for Russia's rogue behavior in cyberspace?

Russia today hosts a "who's who" of the world's most wanted hackers, and the list grows almost monthly. The scale of their theft and damage is staggering. In February, the United States indicted 36 individuals for running Infraud, an online criminal enterprise whose brazen name made clear its intentions: "In fraud we trust." The Infraud website, which trafficked in stolen identities, financial information and malware, facilitated more than $530 million in losses over its seven years in operation; its ringleader, a Russian named Sergei Medvedev, was arrested in Thailand.

Because Russia shields and supports the thugocracy operating within its borders, in order for law enforcement to capture them, they have no choice but to wait for the hackers and criminals to travel overseas. Even then, the Russian state fights tooth and nail to protect crooks.

Through exemplary international law enforcement cooperation, the notorious Russian spam king Peter Levashov — who was ranked sixth on a global most-wanted list of spammers — was arrested last spring when he traveled to Spain for vacation. Russia fought his extradition, issuing its own arrest warrant for him in a ploy to bring him back home safely and stop him from being brought to justice. (Spanish authorities resisted, and a Spanish court allowed him to be extradited to Connecticut to stand trial.)

Russian obstruction efforts often succeed: In recent years, Russia persuaded a Cyprus court to return a hacker wanted by the United States for attacking an American Fortune 100 company; it

also fought in Greece to bring home a hacker indicted in the United States for a $4 billion Bitcoin-laundering scheme.

One reason Russia likes to bring its hackers back home is that it looks to these actors as potential recruits for state business. Alexsey Belan, currently one of the F.B.I.'s most-wanted cybercriminals, faces multiple indictments in the United States for major fraud schemes. In 2012 and again in 2013, he was charged with identity theft and intrusions against e-commerce companies in the United States. Last year he was indicted on a charge of leading, along with two F.S.B. — a successor intelligence agency to the K.G.B. — intelligence officers, a devastating assault on Yahoo that saw the theft of billions of user names. As outlined in the charging documents, instead of responding to requests for law enforcement cooperation, Russia signed him up as an intelligence asset.

Mr. Belan is hardly the only criminal recruited by the government: Another most-wanted man, Evgeniy Bogachev, was indicted on a charge of running the GameOver Zeus botnet, which stole more than $100 million from United States banks and businesses, crippling some of the small businesses he targeted. In 2014, investigators watched with amazement as Mr. Bogachev, apparently in cooperation with Russian intelligence, used his botnet (a remote-controlled network of compromised computers) to target Ukraine, Turkey, Georgia and other Russian adversaries to steal classified information.

Given the increasing damage these activities inflict and the threat they pose to world commerce and order, in Helsinki, President Trump needs to call out Russia as the globe's worst actor online.

Both in my previous role in government and in my current practice, I am regularly approached by victims of this behavior — companies or individuals whose losses count in the billions. They can't defend themselves alone; they need the United States government to stand up for them.

President Trump has been silent on the issue, but not the rest of his administration, including his own White House. In February, Sarah Huckabee Sanders issued a statement attributing the "NotPetya" ransomware attack in June 2017 to Russia, saying, "The Russian military launched the most destructive and costly cyberattack in history," which caused "billions of dollars in damage across Europe, Asia and the Americas."

Damage from that cyberattack alone stretched into the billions; FedEx reported that it suffered more than $300 million in damage. Merck, which had to replace more than 45,000 computers and 4,000 servers after being hit by the ransomware, suffered about $310 million in damage.

If Russia physically attacked the corporate headquarters of either Merck or FedEx, causing an equivalent amount of damage, the president would not remain silent. In the past week, Mr. Trump has called out countries including China, Canada and our closest NATO allies for actions that he believes harm United States businesses and interests. So it's inexplicable that the president has remained silent in the face of Russian actions to enable actors who prey on the very American companies and their employees and customers whom the administration claims to champion.

Cyberspace remains a new frontier where global rules and norms are still being established. There is nothing inherent about cyberspace that makes it impervious to law and order. Hard work by investigators and prosecutors around the world has shown time and again that cybercriminals are not anonymous — a lesson underscored by Mr. Mueller's ability to name 12 Russian intelligence officers responsible for the 2016 election attacks — and that the perpetrators of such crimes can be brought to justice.

Mr. Putin's Russia is the obstacle standing between the world's most notorious cybercriminals and a prison cell. It's time to say stop.

John P. Carlin, the former assistant United States attorney general for national security and chief of staff to the F.B.I. director Robert Mueller, is currently chairman of the Global Risk & Crisis Management Group at the law firm Morrison & Foerster. He also serves as chairman of the Aspen Institute's Cybersecurity & Technology Program. He is the author of the forthcoming "Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat."