The ‘Global Cybercrime Problem’ Is Actually the ‘Russia Problem’

Convincing Putin that further attacks will trigger automatic, severe responses is the best path to deterrence.

Paul Abbate, the then–FBI assistant director of the Criminal, Cyber, Response, and Services Branch, speaks next to a poster of a suspected Russian hacker in 2017.YURI GRIPAS / REUTERS

A series of explosive Department of Justice filings—outside the special counsel’s probe—makes clear that Russia is a rogue state in cyberspace. Now the United States needs a credible system to take action, and to sanction Russia for its misdeeds.

Consider what we learned from last month’s criminal charges filed by the Department of Justice against the “chief accountant” for Russia’s so-called troll factory, the online-information influence operations conducted by the Internet Research Agency in St. Petersburg. The indictment showed how Russia, rather than being chastened by Special Counsel Robert Mueller’s detailed February indictment laying out its criminal activities, continued to spread online propaganda about that *very* indictment, tweeting and posting about Mueller’s

charges both positively and negatively—to spread and exacerbate America's political discord. Defense Secretary James Mattis later told the Reagan National Defense Forum in Simi Valley, California, that Vladimir Putin "tried again to muck around in our elections this last month, and we are seeing a continued effort along those lines."

In October, a 37-page criminal complaint filed against Elena Alekseevna Khusyaynova, who is alleged to have participated in "Project Lakhta," a Russian-oligarch-funded effort to deploy online memes and postings to stoke political controversy, came along with a similar warning, from the director of national intelligence. Those charges came in the wake of coordinated charges filed this fall by U.K., Dutch, and U.S. officials against Russia and its intelligence officers for a criminal scheme to target anti-doping agencies, officials, and even clean athletes around the world in retaliation for Russia's doping scandal and in an apparent effort to intimidate those charged with holding Russia to a level playing field. There's also new evidence that Russia has been interfering in other foreign issues, such as a recent referendum in Macedonia aimed at easing that country's acceptance into Europe.

Read: How to run a Russian hacking ring

At times, it's seemed like every week this year has brought fresh news of Putin acting as the skunk at the global internet party. This fall also saw a new reportfrom the security firm FireEye that concluded that the code used to attack a Saudi petrochemical plant came from a state-owned institute in Moscow.

Moreover, it's also become more clear that the "global cybercrime problem" is actually primarily a "Russia problem," as Putin's corrupt government and intelligence services give cover and protection to the world's largest transnational organized crimes, cybercriminals, schemes, and frauds that cost the West's consumers millions of dollars. Earlier this year, the Justice Department broke up one cybercrime ring based in Russia whose literal motto was "In fraud we trust." The Justice Department charged 36 individuals, many of whom live in Russia beyond the law's reach, and outlined a scheme by which they stole more than a half-billion dollars. It's hardly the only example from this year; last week, the FBI announced that it had dismantled two other cybercrime rings and charged eight people—seven of them Russian—with running a multimillion-dollar ad-fraud scheme. (Three of those charged were able to be caught overseas in friendly countries that respect the rule of law: Malaysia, Bulgaria, and Estonia.)

Ferreting out cybercriminal and intelligence operations and making them public are two prongs of a three-part strategy to change behavior. In recent years, we've gotten really good at the first two parts. In fact, while for years these cases were hidden away inside the government, we now release them routinely. This fall, Deputy Attorney General Rod Rosenstein announced that the Justice Department was changing its approach to election-meddling cases, with the default now to make such cases public as quickly as possible. The change coincided with the criminal complaint against Khusyaynova, detailing that the attacks on our elections are a problem of right now, not just a theoretical issue.

Read: What Putin really wants

As Rosenstein said earlier this year, "Exposing schemes to the public is an important way to neutralize them." Making public such charges helps us be more resilient and more savvy consumers of online content—Russia's attacks in 2016 succeeded in part because we weren't expecting them and because people weren't skeptical enough about consuming information online. Today, of course, we understand all too well that photos, images, and posts online could be the work of foreign trolls and bots.

While defaulting to public action is a good first step, it is not sufficient. The elusive third part of the strategy is what is most needed: making Russia pay a cost that deters the activity. The United States should move toward automatic retaliatory action, ensuring that in today's fast-moving information environment a response doesn't get bogged down in partisan politics or bureaucracy.

It was reported just before the November elections that U.S. Cyber Command was privately notifying Russian hackers that it's on to them—warning them that the United States is watching and that if their actions continue, they're likely to face personal retaliation, such as U.S. criminal charges or sanctions. While sanctions and criminal charges on operatives make it nearly impossible for targets to travel overseas and participate in global banking or commerce, and limit prospects, we can do more.

Read: The coincidence at the heart of the Russian hacking scandal

We should consider building more "dead man's switches" into our counter-foreign-influence work—such as automatic triggers that, when foreign efforts are detected and charged, would put in place new sanctions authority and even boost

our own government's spending on democracy-building efforts that counter Russia's influence campaigns. Russia might think twice about the value of investing the approximately $30 million allegedly spent on Project Lahkta if doing so would presumptively trigger tough new sanctions as well as a fivefold or tenfold American investment in democracy-building NGOs or institutions such as Voice of America and Radio Free Europe that beam free and independent news in the Russian language.

Too often, the responses to these incidents get caught up in political debates and bureaucratic stalemates. The dead man's switch would cut through the inertia by setting up our response in advance—putting Putin on notice that if our intelligence community concludes that a country has targeted our elections, either through online influence operations or direct attacks on the voting systems, that assessment would trigger automatic sanctions against the head of state personally as well as against senior government, intelligence, or foreign-business figures. One credible way to make Putin reassess the cost-benefit analysis of attacking our democracy would be to announce in advance that we'd target his personal wealth for sanctions or that his most powerful oligarch allies would have a harder time vacationing on their super-yachts in the Mediterranean.

After all, the greatest leverage we have is that as much as Putin seeks to undermine the West, his oligarchs, business associates, and even his country's economy all rely on the West to live their life. If the world responds in concert, we can raise the costs and make it safer for everyone.

We want to hear what you think about this article. Submit a letter to the editor or write to letters@theatlantic.com.

JOHN P. CARLIN is the author of Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat. He served as the assistant attorney general for national security at the Department of Justice and currently chairs the Aspen Institute's Cyber & Technology Program.

Source: https://www.theatlantic.com/ideas/archive/2018/12/how-trump-can-stand-russian-cybercrime/578185/

[Disclaimer]