Expect More Covert Action Under Trump

Katie Harbath ⋮ 13-16 minutes

Editor's Note: This newsletter is part of a collaboration between Lawfare *and Risky Business. You can find the full version of the Seriously Risky Business newsletter and previous editions on news.risky.biz.*

Expect More Covert Action Under Trump

Predicting Trump's second-term moves is a mug's game, but here's our best guess: Cybersecurity policy initiatives will be sensible but unambitious, while the intelligence community will be asked to carry out bold—and maybe even bonkers—operations.

This is based on our examination of Trump's first term, which, from a narrow cybersecurity perspective, was just fine.

In 2017, for example, Trump issued an executive order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and expanded on this in 2018 with the release of a National Cyber Strategy. These were both sensible efforts, not as ambitious as the Biden administration's 2023 strategy, but entirely appropriate for the time. In 2018, Trump issued an executive order intended to deter foreign actors from interfering with U.S. elections. Another sensible step, and President Biden continued this order in September this year.

These examples reflect Trump's lack of interest in cybersecurity issues. As long as they didn't cut across his vital concerns, experts in government could craft policy that was sensible, albeit pedestrian. At times this required careful wording. For example, in its second paragraph, Trump's 2018 executive order on imposing sanctions for interfering in a U.S. election said:

> Although there has been no evidence of a foreign power altering the outcome or vote tabulation in any United States election, foreign powers have historically sought to exploit America's free and open political system.

There is no evidence that foreign interference in the *vote-counting* machinery of elections has changed a result, but many people would argue that Russian interference on social media and via hack-and-leak operations swung the 2016 presidential election in Trump's favor. The truth here is unknowable, but this was certainly a sore spot for Trump. The key thing is that with some fairly straightforward wordsmithing, the order's authors were able to work around the president's sensitivities to get good policy implemented.

We expect that in Trump's second term there will be good people in the government continuing to push sensible, albeit incremental, policy reform.

However, from an intelligence community perspective, there is good evidence that the incoming Trump administration will push for far more audacious or maybe even outlandish operations. Partly, this is because it appears that the key selection criterion for political appointees in Trump's second term is personal loyalty coupled with the ability to defend Trump on television, rather than in-depth subject matter expertise. Nominations announced so far include Tulsi Gabbard as director of national intelligence, Pete Hegseth as secretary of defense, and John Ratcliffe as CIA director.

In his first term, at the more reasonable end of the spectrum, Trump issued National Security Presidential Memorandum-13 (NSPM-13), a policy intended to remove procedural barriers to the authorization of Department of Defense offensive cyber operations. In other words, more aggressive Cyber Command (CYBERCOM) offensive operations, more often.

Former CYBERCOM General Counsel Gary Corn said the policy prior to NSPM-13 was "a process that was notorious for reinforcing indecision[,]" and John Bolton, Trump's national security adviser, said the offensive cyber operations "interagency [consultation] process was frozen solid." When the Biden administration reviewed NSPM-13, it was dialed back slightly to give the State Department limited ability to provide input into cyber operations, so on balance this policy initiative was a positive.

However, there are a few stories from Trump's first term that are, frankly, bonkers.

One, reported by Zach Dorfman writing for Yahoo News in 2021, involved the Australian WikiLeaks founder Julian Assange when he was holed up in the Ecuadorian Embassy in London. After WikiLeaks published "Vault 7" documents sourced from the CIA, Trump-appointed CIA Director Mike Pompeo wanted aggressive action against the organization and designated WikiLeaks "a non-state hostile intelligence service." This designation formally allowed the CIA to take more aggressive actions against WikiLeaks, including disrupting the group. Per Yahoo News:

> At meetings between senior Trump administration officials after WikiLeaks started publishing the Vault 7 materials, Pompeo began discussing kidnapping Assange, according to four former officials. While the notion of kidnapping Assange preceded Pompeo's arrival at Langley, the new director championed the proposals, according to former officials…
>
> Some discussions even went beyond kidnapping. U.S. officials had also considered killing Assange, according to three former officials. One of those officials said he was briefed on a spring 2017 meeting in which the president asked whether the CIA could assassinate Assange and provide him "options" for how to do so.

The kidnapping and assassination ideas ultimately went nowhere, and there were reportedly serious concerns about them raised within the CIA.

Another example reportedly recently, also from Zach Dorfman, writing this time for Wired, described the Trump administration's efforts to get the CIA to conduct operations to overthrow Venezuelan president Nicolás Maduro. This resulted in a cyber operation to disrupt the payroll system for Venezuela's military, but Trump administration officials describe the CIA's efforts as half-hearted. Other operations

floated but not carried out included sabotage operations within Venezuela and remotely disabling oil tankers headed from Venezuela to Cuba.

At the time, Gina Haspel, a career intelligence officer, was CIA director. Per Wired:

> To some Trump-era officials, CIA executives—including CIA director Gina Haspel—were clearly opposed to the administration's directive. Haspel "never bought into doing anything aggressive in Venezuela because she was still of the mind that we were ugly Americans," says a senior Trump-era official. Haspel declined to comment.

Although it wasn't an intelligence community action, the Trump-ordered assassination of Iranian Gen. Qasem Soleimani by drone strike is consistent with this philosophy—strike at enemies without being paralyzed by the possible consequences.

This inclination to aggressively use covert operations won't disappear in Trump's second term. He actively employs state power, whether by sanctions, drone strikes, and military force or via covert action. And although the two first-term intelligence community thought experiments we cite—kidnapping or assassinating Assange and toppling Maduro—were driven at least partly by personal animosity (from Pompeo and Trump), there are plenty of people to hate in the world.

In Trump's first term, based on the available public reporting, we'd have to give the intelligence community top marks for behaving responsibly and pushing back on the bonkers ideas that were floated. The big question is whether those checks and balances will continue to hold?

Oh, and we wouldn't rule out creation of a cyber force, either.

U.S. and U.K. Back Flawed UN Cybercrime Treaty

A UN draft cybercrime treaty will be voted on in the UN General Assembly next month, and while the U.S. and U.K. governments recognize the treaty is flawed, they have decided to support it nonetheless.

The U.K. government said the treaty's "broad scope of international cooperation … and its intrusive procedural powers" could present risks to human rights and also recognized some member states were already trying "to deny or dodge" human rights obligations present in the text. A U.S. government statement echoed the U.K. government's concerns, and both countries committed to demanding accountability. Both said that countries should refuse requests from states that were violating the human rights provisions of the treaty. Jonathan Shrier, a U.S. representative to the UN, told reporters that part of the reason the U.S. backed the treaty was to have a future role in shaping the way it was implemented. The Record has further coverage.

Canada's TikTok Expulsion Order Is Baffling

Last week, the Canadian government ordered TikTok to close its offices in the country but otherwise left the app available for its citizens to use. The federal government innovation minister, François-Philippe Champagne, said the decision was based on information from a national security review and advice from Canada's security and intelligence community.

National security types are concerned about TikTok because of its China-based ownership coupled with its ability to collect data from its users, meaning it could be used for influence operations and political manipulation. Just this week, for example, The Information reported that TikTok had modified its moderation policies ahead of the U.S. presidential election to appeal to conservatives and the Trump campaign. That's not necessarily manipulation per se, but it does reflect a willingness by TikTok's management to pull levers when it needs to.

Both data collection and manipulation are possible because people use the TikTok app, not because TikTok happens to have offices and staff in Canada. So we can't see how closing these offices achieves anything.

Michael Geist, University of Ottawa law professor and Canada Research Chair in internet and e-commerce law, told Canada's CBC that shutting TikTok's offices might actually make it *harder* to enforce local laws. "You want to have someone that you can deal with, that you can sometimes serve legal papers to," Geist said. "That's much tougher if the company isn't even operating here."

We are bemused.

Three Reasons to Be Cheerful This Week:

1. **Progress on secure-by-design:** The Record summarizes the progress some major vendors are making toward the Cybersecurity and Infrastructure Security Agency's (CISA's) secure-by-design pledge. Here the good news is not so much the progress itself but that CISA plans to some extent to hold the companies accountable. The article itself points out, without any hint of snark, that Fortinet "says it's helping users of its old, end-of-life security products migrate to newer devices that still receive updates." We are more than a bit cynical about security commitments that boil down to "sell more of our stuff," so hopefully that help includes significant discounts.
2. **10 years for BEC scammer:** A Nigerian national who had been living in the U.K. has been sentenced to 10 years in U.S. prison for stealing almost $20 million in business email compromise scams targeting real estate transactions. Some victims lost all the money they'd saved to buy a home, and the victim impact statements are heartbreaking. Unfortunately, two of the scammers' co-defendants are still at large.
3. **Better security in Africa:** Microsoft has announced that it is expanding its cybersecurity service for at-risk, highly targeted organizations, AccountGuard, to three new markets in Africa: Nigeria, Kenya, and South Africa.

Shorts

Why Italy Is a Spyware Hub

The Record analyzes why Italy is a hub for spyware and is home to six major vendors and one supplier. One reason is that Italian

companies got involved early; the first company, RCS, entered the industry back in 1992. Italian firms also tend to be much smaller than more infamous enterprises such as NSO Group. And rather than selling expensive, high-end, zero-click capability such as NSO Group's Pegasus, Italian spyware is cheaper, more accessible, and more widely used. More Fiat than Ferrari.

Risky Biz Talks

In the latest "Between Two Nerds" discussion, Tom Uren and The Grugq talk about how ungoverned spaces on Telegram result in increasingly toxic and antisocial communities.

From Risky Biz News:

Most of 2023's top exploited vulnerabilities were initially zero-days: Ten of the 15 most frequently exploited vulnerabilities last year were initially zero-days, CISA said in a joint report published with cybersecurity agencies from Five Eyes countries on Tuesday.

This includes infamous zero-days, such as the one that forced Barracuda to tell customers to replace all email security gateway (ESG) appliances, the zero-day used in the MOVEit hacking spree, and the CitrixBleed vulnerability.

Because zero-days dominated last year's Top 15, 2023 marks the first time CISA's Top Exploited Vulnerabilities list is dominated by new common vulnerabilities and exposures (CVEs).

Chinese hackers target Trump lawyer: The FBI has notified Donald Trump's lead attorney Todd Blanche that his phone was tapped by Chinese hackers. The hackers allegedly obtained voice and text messages, but none were related to President-elect Trump. The hack is the work of Salt Typhoon, a Chinese APT group that breached U.S. telecommunications company wiretapping systems earlier this year. The Blanche hack is part of a larger series of hacks that targeted politicians across both U.S. parties. [Additional coverage in *ABC News*]

Russia blocks Cloudflare ECH connections: Russia's internet watchdog agency, the Roskomnadzor, has blocked traffic to Cloudflare-hosted websites that use the new Encrypted Client Hello (ECH) technology.

Users in Russia and abroad started reporting issues with accessing a large number of websites on Nov. 6.

Roskomnadzor, through its Center for Monitoring and Control of Public Communications Networks department, says it took the action after Cloudflare enabled ECH by default for customer accounts in October.

The agency said ECH was being used by Russian citizens to bypass its censorship measures and access restricted resources.