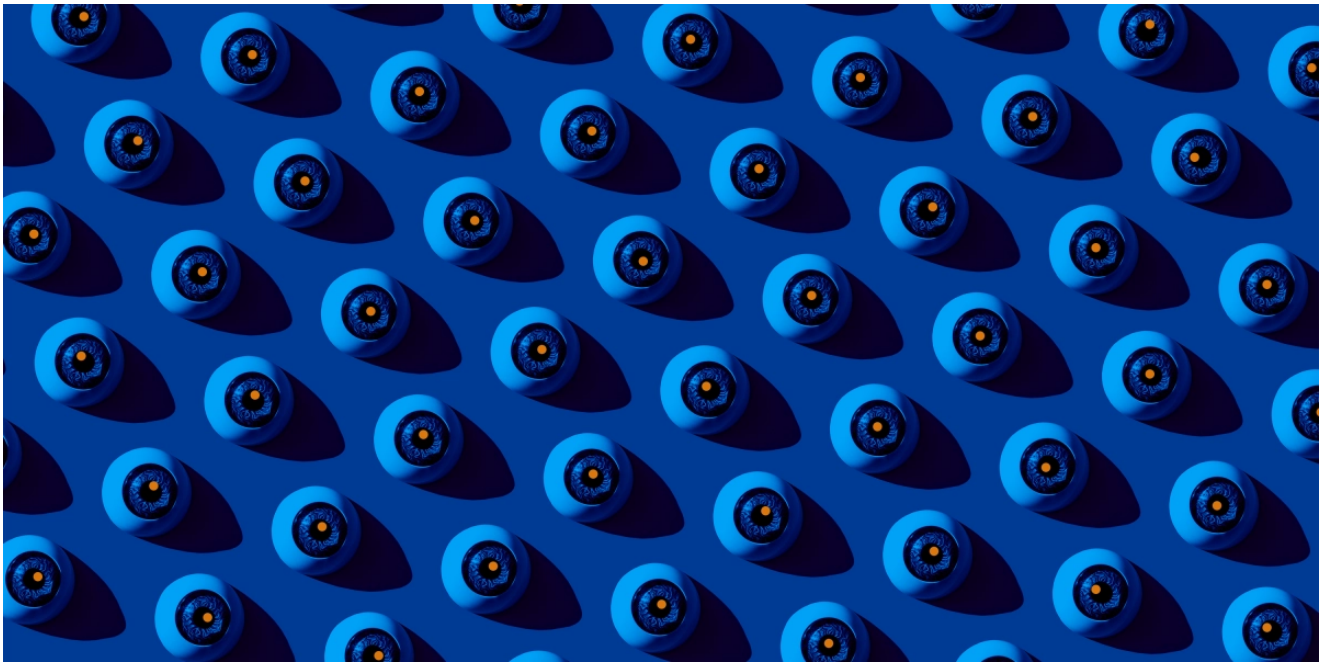
“A grim outlook”: How cyber surveillance is booming on a global scale

technologyreview.com/2021/11/08/1039395/grim-outlook-cyber-boom-atlantic-council-report/

Patrick Howell O'Neill

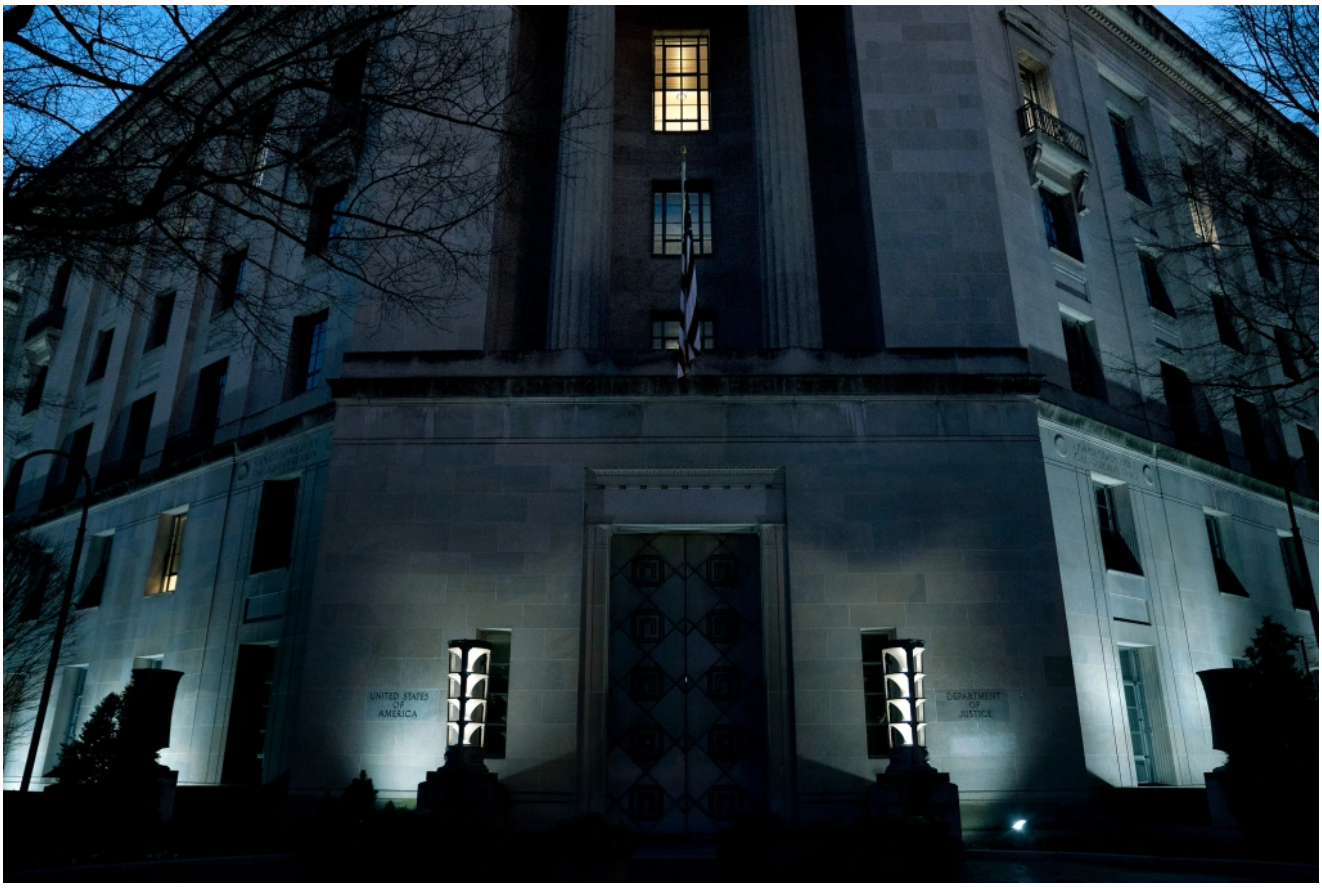


The increasing overlap between the world’s arms trade and the secretive surveillance industry risks damaging US national security and will create the potential for even more abuse unless more accountability is introduced, according to a new study.

The research, from the American think tank the Atlantic Council, offers one of the most thorough accountings ever assembled of a booming, cross-continental surveillance industry that makes billions of dollars and yet mostly manages to stay out of the limelight. After years of rising demand for hacker-for-hire products and an increase in reported abuses by companies like NSO Group, countries around the world are now trying to deal with this largely hidden industry.

The report is based on 20 years of data collected from the cyber surveillance trade show ISS World and arms fairs like France’s Milipol, where hacking is the fastest-growing business segment alongside more traditional wares like guns and tanks. Its authors examined 224 surveillance companies present at these shows, looked at their marketing material, examined where in the world they advertised their products, and detailed the known sales of surveillance and hacking tools.

Related Story



This US company sold iPhone hacking tools to UAE spies

An American cybersecurity company was behind a 2016 iPhone hack sold to a group of mercenaries and used by the United Arab Emirates.

They also argue that numerous companies that market internationally, especially to adversaries of NATO, are “irresponsible proliferators” and deserve more attention from policymakers.

These companies include Israel’s Cellebrite, which develops phone hacking and forensics tools, and which sells around the world to countries including the US, Russia, and China. The company has already faced significant blowback because of, for example, its role during China’s crackdown in Hong Kong and the discovery that its technology was being used by a Bangladeshi “death squad.”

“When these firms begin to sell their wares to both NATO members and adversaries,” the report says, “it should provoke national security concerns by all customers.”

The trade is increasingly global, according to the report, with 75% of companies selling cyber surveillance and intrusion products outside their own home continent. Lead author Winnona DeSombre, a fellow with the Atlantic Council’s Cyber Statecraft Initiative, argues that such sales signal potential problems with oversight.

“There does not seem to be a willingness to self-regulate for a majority of these firms,” she says.

By marking such firms as “irresponsible proliferators,” DeSombre hopes to encourage lawmakers around the world to target some companies for greater regulation.

> “When these firms begin to sell their wares to both NATO members and adversaries, it should provoke national security concerns by all customers.”

Governments have recently made moves toward some forms of control. The EU adopted stricter rules on surveillance tech last year, with the goal of increasing industry transparency. And within the last month, the US has enacted stricter new licensing rules for selling intrusion tools. The notorious Israeli spyware company NSO Group was one of several companies added to a US blacklist because of allegations that spyware it supplied to foreign governments was then used to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. NSO has consistently denied wrongdoing and argued that it strictly investigates abuse and shuts off offending customers.

Nevertheless, one of the report’s authors says it is important to realize the true scale of what is happening.

“The most basic takeaway from this paper is that we are dealing with an industry,” says Johann Ole Willers, a fellow at the Norwegian Institute of International Affairs (NUPI) Centre for Cyber Security Studies. “That is a fundamental insight. It’s not enough to target NSO Group.”

UN warning

United Nations human rights experts recently raised alarms about what they called “growing use of mercenaries in cyberspace.”

“It is undeniable that cyber-activities have the ability to cause violations both in armed conflicts and in peacetime, and thus that a whole variety of rights are engaged,” Jelena Aparac, chair of a United Nations working group on the issue, said in a statement. The group called on international lawmakers to more effectively regulate the industry in order to protect “the right to life, economic social rights, freedom of expression, privacy, and the right to self-determination.”

One obstacle is that the cyber surveillance industry is rife with obfuscation: shell companies and resellers are common, and both sellers and buyers use a host of tools to hide their interactions.

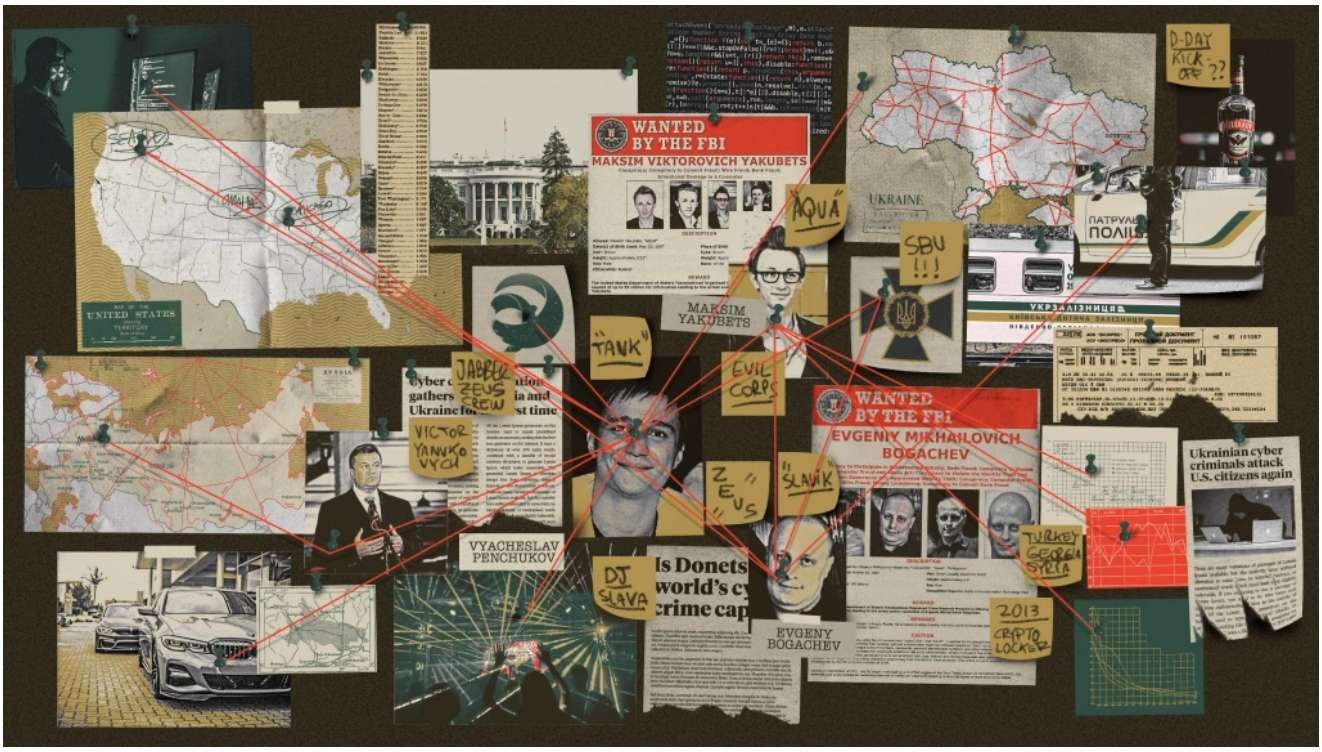
“There is not enough knowledge about the industry in the public, where you can delineate the irresponsible firms from the responsible,” says DeSombre.

The report points to the recent indictment of former US intelligence personnel who had been working for the United Arab Emirates as evidence that capabilities first developed by friendly governments can end up being used for other spying purposes. The hacking tools and expertise developed by US agencies were then used by the UAE to spy on hundreds of targets, including Americans.

Use and abuse

The researchers have some suggestions for how governments might learn to understand and control this growing ecosystem. They recommend enacting stronger "know your customer" requirements for the industry, so that every seller will better understand how potential customers might use—or abuse—a hacking tool.

Related Story



Inside the FBI, Russia, and Ukraine's failed cybercrime investigation

Russia and Ukraine promised to cooperate and help catch the world's most successful hackers. But things didn't quite go to plan.

The researchers argue that NATO countries, which host many prominent cyber surveillance trade events, should limit the attendance of irresponsible vendors at arms fairs. They also encourage more international cooperation to rid export laws of loopholes that allow vendors to evade controls and sell to authoritarian regimes. Finally, they encourage naming and shaming irresponsible sellers and buyers.

“Our analysis indicates that there exists a significant group of private companies willing to act irresponsibly: marketing capabilities that carry the risk of becoming tools of oppression for authoritarian regimes or strategic tools for non–NATO allies,” the report concludes.

Without such actions, it warns, the world faces a “grim outlook”: “a growing number of private corporations who see few consequences to bolstering the cyber arsenals of major Western adversaries, only profit.”