The hacker-for-hire industry is now too big to fail

technologyreview.com/2021/12/28/1043029/the-hacker-for-hire-industry-is-now-too-big-to-fail/

Patrick Howell O'Neill

A shock has reverberated inside Israel in the last few months. NSO Group, the billion-dollar Israeli company that has sold hacking tools to governments around the world for more than a decade, has drawn intense scrutiny after a series of public scandals. The company is in crisis. Its future is in doubt.

But while NSO Group's future is uncertain, governments are more likely than ever to buy cyber capabilities from the industry NSO helped define. Business is booming for "hackers for hire" firms. In the last decade, the industry has grown from a novelty into a key instrument of power for nations around the world. Even the potential failure of a major firm like NSO Group isn't likely to slow the growth.

Just this month, Facebook reported that seven hacker-for-hire firms from around the world had targeted around 50,000 people on the company's platforms. The report spotlighted four more Israeli companies alongside operations from China, India, and North Macedonia. The fact that the investigation didn't even mention NSO Group shows that the industry and its targeting are far more vast than what the public can typically see.

NSO Group has been besieged by criticism and charges of abuse for years. In 2016, the United Arab Emirates was caught targeting human rights activist Ahmed Mansoor using NSO Group's Pegasus, a tool that leverages software flaws to hack iPhones and turn control over

to NSO Group's customers. In that case, the UAE government was seen as the culprit, and NSO walked away unscathed (Mansoor is still in prison on charges of criticizing the country's regime).

The pattern repeated for years–over and over again, governments would be accused of using NSO hacking tools against dissidents but the company denied wrongdoing and escaped punishment. Then, in mid-2021, new reports emerged of alleged abuse against Western governments. The company was sanctioned by the US in November, and in December Reuters reported that US State Department officials had been hacked using Pegasus.

Now NSO Group faces expensive public lawsuits from Facebook and Apple. It has to deal with debt, low morale, and fundamental threats to its future. Suddenly, the poster child for spyware is confronting an existential crisis.

All of this is familiar territory. The secretive hacker-for-hire industry first splashed across international newspaper headlines in 2014, when the Italian firm Hacking Team was charged with selling its "untraceable" spyware to dozens of countries without regard for human rights or privacy violations.

Hacking Team opened the world's eyes to a global industry that bought and sold powerful tools to break into computers anywhere. The resulting storm of scandals seemed to eventually kill it. The company lost business and the ability to legally sell its tools internationally. Hacking Team was sold and, in the public's mind, left for dead. Eventually, however, it rebranded and started selling the same products. Only this time, it was a smaller fish in a much bigger pond.

"The demise of Hacking Team did not lead to fundamental change in the industry at all," says James Shires, assistant professor at the Institute of Security and Global Affairs at Leiden University. "The same dynamic and demand still exists."

The industry's earliest customers were a small set of countries eager to project power around the world through the internet. The situation is far more complex today. Many more countries now pay for the instant capability to hack adversaries both internationally and within their own borders. Billions of dollars are at play, but there's very little transparency and even less accountability.

While public scrutiny of firms that provide hackers for hire has grown, the global demand for offensive cyber capabilities has escalated too. In the 21st century, a government's highest-value targets are online more than ever—and hacking is usually the most effective way to get to them.

The result is a growing crowd of countries willing to spend large sums to develop sophisticated hacking operations.

For governments, investing in cyber is a relatively cheap and potent way to compete with rival nations—and develop powerful tools of domestic control.

“Especially in the last five years, you have more countries developing cyber capabilities,” says Saher Naumaan, a principal threat intelligence analyst at BAE Systems.

And more of those countries are looking outside for help. “If you don’t have a way to harness the skills or talent of the people in your country but you have the resources to outsource, why wouldn’t you go commercial?” she says. “That’s an option in a lot of different industries. In that way, cyber is not that different. You’re paying for something you’re not going to build yourself.”

For example, oil-rich countries on the Persian Gulf have historically lacked the considerable technical capability needed to develop domestic hacking power. So they spend on a shortcut. “They don’t want to be left behind,” Naumaan says.

Military contracting giants across the world now develop and sell these capabilities. These tools have been used to commit egregious abuses of power. They’re also increasingly used in legitimate criminal investigations and counterterrorism and are key to espionage and military operations.

The demand for what private hacking companies are selling isn’t going away. “The industry is both bigger and more visible today than it was a decade ago,” says Winnona DeSombre, a security researcher and fellow at the Atlantic Council. “The demand is rising because the world is becoming more technologically connected.”

DeSombre recently mapped the famously opaque industry by charting hundreds of companies selling digital surveillance tools around the world. She argues that much of the industry’s growth is hidden from public view, including Western companies’ sales of cyber weapons and surveillance technology to geopolitical adversaries.

“The biggest issue comes when this space is primarily self-regulated,” she explained. Self-regulation “can result in widespread human rights abuses” or even friendly fire, when hacking tools are sold to foreign governments that turn around and use the same capabilities against the country of origin.

Alerted to the industry’s increasing impact, authorities around the world now aim to shape its future with sanctions, indictments, and new regulations on exports. Even so, the demand for the tools grows.

Ultimately, the most meaningful change may come when there’s an impact on companies’ revenue. Recent reports show that NSO Group is saddled with debt and struggling to court Wall Street investment.

“This is a commercial industry, after all,” Shires says. “If venture capital firms and big corporate investors see this as a risky bet, they’ll choose to pull out. More than anything else, that can change the industry radically.”