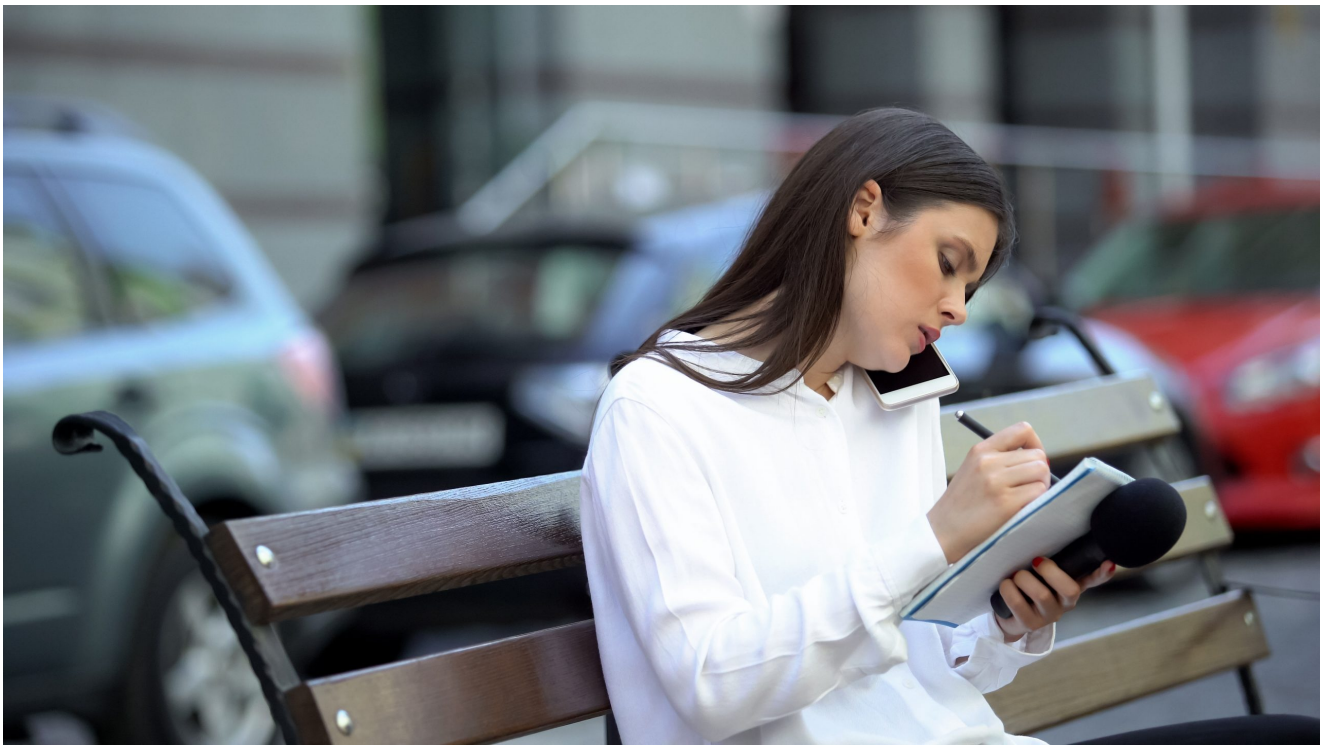
# Cyber mercenaries don’t deserve immunity

blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/

December 21, 2020



A growing industry of companies called private-sector offensive actors – or PSOAs – is creating and selling cyberweapons that enable their customers to break into people’s computers, phones and internet-connected devices. Now, one of these 21st-century mercenaries, called the NSO Group, is attempting to cloak itself in the legal immunity afforded its government customers, which would shield it from accountability when its weapons inflict harm on innocent people and businesses. The firm also contributes to the urgent cybersecurity challenges discussed by our president Brad Smith last week. We believe the NSO Group’s business model is dangerous and that such immunity would enable it and other PSOAs to continue their dangerous business without legal rules, responsibilities or repercussions. That’s why today we filed an amicus brief – along with Cisco, GitHub, Google, LinkedIn, VMWare and the Internet Association – in a legal case brought by WhatsApp against the NSO Group.

The NSO Group sold governments a program called Pegasus, which could be installed on a device simply by calling the device via WhatsApp; the device’s owner did not even have to answer. According to WhatsApp, the NSO Group used Pegasus to access more than 1,400 mobile devices, including those belonging to journalists and human rights defenders. We believe companies like NSO Group selling tools like Pegasus are concerning for three reasons.

First, their presence increases the risk that the weapons they create fall into the wrong hands. Previously, sophisticated nation-state hacking capabilities resided in a small number of governments with well-funded agencies focused on developing these weapons. Even then, government-created espionage tools got into the hands of other governments who used them in attacks like WannaCry and NotPetya that spread like wildfire beyond the targeted victims and ultimately devastated lives and disrupted businesses around the world. Lowering the barrier for access to these weapons would guarantee that such catastrophes would be repeated.

Even if the tools are sold to governments who use them for narrowly targeted attacks, there are a variety of ways they can still fall into the wrong hands. For example, private actors like the NSO Group and their less sophisticated customers may lack the defenses some governments use to protect the weapons, making them more susceptible to cyber-theft. For example, an Italian company called Hacking Team – one of NSO's competitors – was itself hacked in 2015. Additionally, targets of these weapons can observe, reverse-engineer and then use these tools for their own purposes.

Second, private-sector companies creating these weapons are not subject to the same constraints as governments. Many governments with offensive cyber capabilities are subject to international laws, diplomatic consequences and the need to protect their own citizens and economic interests from the indiscriminate use of these weapons. Additionally, some governments – like the United States – may share high-consequence vulnerabilities they discover with impacted technology providers so the providers can patch the vulnerability and protect their customers. Private actors like the NSO Group are only incented to keep these vulnerabilities to themselves so they can profit from them, and the exploits they create are constantly recycled by governments and cybercriminals once they get into the wild.

Third, companies like the NSO Group threaten human rights whether they seek to or not. An analysis of recent cyber-attacks was able to identify five countries using offensive cyber capabilities between 2012 and 2015: Russia, China, North Korea, France and Israel. Between 2016 and 2018, however, the cast of characters changed to include countries like the United Arab Emirates and Uzbekistan. And public reporting has identified clients of cyber-surveillance companies like the NSO Group to include Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Mexico, Morocco, Nigeria, Oman, Saudi Arabia and Sudan. Reporting also shows foreign governments are using those surveillance tools, bought from PSOAs, to spy on human rights defenders, journalists and others, including U.S. citizens. These tools allow the user to track someone's whereabouts, listen in on their conversations, read their texts and emails, look at their photographs, steal their contacts list, download their data, review their internet search history and more. Just yesterday The Citizen Lab reported that between July and August of this year NSO's Pegasus program was used to hack 36 phones belonging to journalists, producers, anchors and executives at Al Jazeera. Privacy is fundamental to the ability of journalists to report, of dissidents to speak their voices and of democracy to flourish and these tools threaten their rights and their lives.

The expansion of sovereign immunity that NSO seeks would further encourage the burgeoning cyber-surveillance industry to develop, sell and use tools to exploit vulnerabilities in violation of U.S. law. Private companies should remain subject to liability when they use their cyber-surveillance tools to break the law, or knowingly permit their use for such purposes, regardless of who their customers are or what they're trying to achieve. We hope that standing together with our competitors today through this amicus brief will help protect our collective customers and global digital ecosystem from more indiscriminate attacks.

Tags: amicus brief, cybersecurity, NSO