Written testimony of Cristin Flynn Goodwin, General Manager & Associate General Counsel, Microsoft
House Permanent Select Committee on Intelligence
Hearing on "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware"

July 27, 2022

Introduction

A world where private sector companies create and sell cyberweapons is more dangerous for consumers, businesses of all sizes, and governments. These tools can be used in ways that are inconsistent with the norms and values of good governance and democracy. Microsoft believes that the protection of human rights is a fundamental obligation, and one that we take seriously and support globally.

While governments were the first to develop these types of technologies and capabilities for use in clandestine intelligence operations, the number of governments doing so was small. As security and encryption improved, governments needed to continue to evolve their tools to maintain access. This evolution required financial and engineering resources beyond the capabilities of most government intelligence organizations.

Microsoft has been outspoken about the risks of harm posed by foreign companies that develop and sell surveillance and intrusion capabilities to governments. Over a decade ago, we started to see companies in the private sector move into this sophisticated surveillance space as autocratic nations and smaller governments sought the capabilities of their larger and better resourced counterparts. In some cases, companies were building capabilities for governments to use consistent with the rule of law and democratic values. But in other cases, companies began building and selling surveillance as a service to governments lacking the capabilities to build these technically complex tools, including to authoritarian governments or governments acting inconsistently with the rule of law and human rights norms. The NSO Group is the canonical example here, but there are other companies included on the US Department of Commerce Entities List and a myriad of others that are selling these services that are not yet included on the List. Many of the technologies and services being sold by these companies are associated with attacks against government officials, human rights advocates, journalists, dissidents, and others involved in civil society – people who are often also our customers.

Microsoft has long advocated for clear legal and normative regimes to regulate these technologies so that human rights abuses are prohibited, and legitimate security research can flourish. Cyber espionage not only erodes the rights of the targeted individual, but it also frequently places the security of the online ecosystem at risk. We see private sector companies pursuing acquisition of newly discovered and privately developed vulnerabilities (zero-day vulnerabilities) and then using those to develop unique capabilities to gain access to systems without user consent. These companies then either sell these exploits or provide related exploit and surveillance services to governments or potentially offer these services to companies for the purpose of industrial espionage. Once new vulnerabilities are exploited or capabilities to gain access to systems without user consent are developed, other actors can quickly repeat the exercise.

As Microsoft President Brad Smith noted in December 2020:

> This represents a growing option for nation-states to either build or buy the tools needed for sophisticated cyberattacks. And if there has been one constant in the world of software over the past five decades, it is that money is always more plentiful than talent. An industry segment that aids offensive cyberattacks spells bad news on two fronts. First, it adds even more capability to the leading nation-state attackers, and second, it generates cyberattack proliferation to other governments that have the money but not the people to create their own weapons. In short, it adds another significant element to the cybersecurity threat landscape.[1]

Indeed, the European Network Security Agency (ENISA) recently listed these private sector "hackers for hire" on their 2021 Threat Landscape of major risks in Europe, recognizing customers of these services are "usually governments", but also recognized sales to corporations and individuals as a threat.[2]

We welcome Congress's focus on the risks and abuses the world faces from the unscrupulous use of surveillance technologies. The commercial spyware industry has grown into an industry estimated at over $12 billion in value and will likely increase.[3] Cybersecurity researchers, NGOs, journalists, and companies have uncovered disturbing and sometimes tragic abuses of technology, including the targeting of dissidents, journalists, human rights lawyers and workers, politicians, and even family members of targets – including children.[4] The progression from tools used by government agencies for national security purposes to tools abused by governments to gain access to tools now being sold for commercial surveillance, personal surveillance, and industrial espionage only increases the pressure on democratic governments to engage on this growing problem. Below we share some of Microsoft's actions to combat these threats to date, and recommendations to consider for future action.

Microsoft actions against private sector offensive actors

Microsoft has lived up to our commitments made through the Cybersecurity Tech Accord[5] and used both technical and legal means to disrupt attack activity or tactics from advanced actors. Private sector offensive actors (PSOA), sometimes referred to as cyber mercenaries, are no exception. To protect our customers, we engage technical and legal means, depending on what is most appropriate to mitigate the harm.

Technical Actions

Microsoft proactively monitors PSOA activity and partners with others in the security community on this activity. When we have information that a PSOA is using previously unknown vulnerabilities in a Microsoft product or service (commonly known as a "Zero Day") we will develop and issue patches for those

---

[1] Brad Smith, *A moment of reckoning: the need for a strong and global cybersecurity response*, Microsoft On the Issues (July 23, 2022, 5:30 PM), https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

[2] E.U. Agency for Cybersecurity, ENISA Threat Landscape (2021).

[3] Ronan Farrow, *How Democracies Spy on Their Citizens*, The New Yorker (2022), https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens (last visited Jul 23, 2022).

[4] Mark Mazzetti et al., *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*, N.Y. Times (July 23, 2022, 4:50 PM), https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html?searchResultPosition=1; Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. Times (July 23, 2022, 4:53 PM), https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html.

[5] Cybersecurity Tech Accord commitment, https://cybertechaccord.org/accord/.

vulnerabilities. When we identify or learn about malware involved in these types of attacks, we write detection signatures that can help ensure that the malware in question is blocked. We also make the signatures public so that other vendors can incorporate them into their security products and services, thereby making the online ecosystem safer.

Our first disruption was in July 2021 against a PSOA that we call SOURGUM and that the Citizen Lab has identified as the Israeli-based firm Candiru.[6] SOURGUM enabled the compromise of over 100 victims, which included human rights defenders, dissidents, journalists, activists, and politicians. Approximately half of the victims were found in the Palestinian Authority, with most of the remaining victims located in Israel, Iran, Lebanon, Yemen, Spain (Catalonia), United Kingdom, Turkey, Armenia, and Singapore. These attacks have largely targeted our consumer rather than enterprise accounts, indicating SOURGUM's customers were pursuing specific individuals.

Today, we are announcing publicly that Microsoft has disrupted the tools of another PSOA, which we refer to as KNOTWEED.[7] KNOTWEED is an Austria-based PSOA called DSIRF. Multiple news reports have linked the company to the development and attempted sale of a malware toolset called Subzero.[8] The Microsoft Threat Intelligence Center (MSTIC) found the Subzero malware being deployed through a variety of methods, including zero-day exploits in Windows and Adobe Reader, in 2021 and 2022.

Microsoft is publicly releasing the details of its investigation on our relevant blog pages. MSTIC has found multiple links between DSIRF and the exploits and malware used in these attacks. These include command-and-control infrastructure used by the malware directly linking to DSIRF, a DSIRF-associated GitHub account being used in one attack, a code signing certificate issued to DSIRF being used to sign an exploit, and other open-source news reports attributing Subzero to DSIRF. Victims include law firms, banks, and strategic consultancies in countries such as Austria, the United Kingdom, and Panama.[9]

Legal actions

Microsoft actively supported Meta when WhatsApp brought its lawsuit against NSO Group for its exploitation of vulnerabilities that enabled attacks against "at least 100 human rights defenders, journalists, and other members of civil society across the world."[10] When NSO Group asserted that it was entitled to sovereign immunity – to receive the protections of a state – because it accessed WhatsApp as an agent of its foreign government customers, Microsoft helped build a coalition of companies to challenge that presumption. In December 2020, Microsoft, Google, Cisco, GitHub, LinkedIn, VMWare, and the Internet

---

[6] *Hooking Candiru*, CitizenLab (2021), https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[7] Microsoft uses elements from the Periodic Table to refer to nation state actors and uses names of trees to refer to PSOAs.

[8] Jan-Philipp Hein, *In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin*, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, *We unveil the "Subzero" state trojan from Austria*, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, *We unveil the state Trojan "Subzero" from Austria*, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.

[9] As noted in our technical blog, the identification of targets in a country does not necessarily mean that a DSIRF customer resides in the same country, as international targeting is common.

[10] Will Cathcart, *Why WhatsApp is pushing back on NSO Group hacking*, Washington Post (Jul 23, 2022 5:57 PM), https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/.

Association filed an amicus brief before the Ninth Circuit Court of Appeals in support of WhatsApp.[11] The companies argued that the risk to the computing ecosystem was too great to allow offensive actors like NSO Group to be granted the immunity afforded to nations for its harmful software. Almost a year later, the Court ruled against NSO Group, arguing that "if an entity does not fall within the [Foreign Sovereign Immunities] Act's definition of 'foreign state,' it cannot claim foreign sovereign immunity. Period."[12] The case continues as WhatsApp pursues its claims against NSO Group in the lower court,[13] and NSO Group filed a petition for a writ of certiorari in the US Supreme Court which remains pending.[14]

A decade of debate

Governments around the world have been aware of the problem this market poses for a decade or more. In 2013, the Financial Times ran an article with the headline "*Cyber war technology to be controlled in same way as arms*" and discussed that 41 countries were close to setting "new controls on complex surveillance and hacking software and cryptography" through an export control process known as the Wassenaar Arrangement.[15] The article reflected the fact that governments had been discussing what measures should be taken to control the risks arising out of surveillance software or the "*surveillance as a service*" capabilities provided by companies like NSO Group, Hacking Team, FinFisher, Candiru, and others through the secretive Wassenaar Arrangement export control process. The United Kingdom identified and had led the effort to use export controls to regulate a type of technology known as "*intrusion software*". While a worthy attempt, the fact that the first attempt at regulating this market was through a non-public, multi-national export control group, which left no room for public debate, meant that the original proposals were riddled with challenges. The controls introduced were overbroad and encompassed a wide range of other technologies and scenarios designed to support cybersecurity, cybersecurity research, and incident responders. Years passed before, following bipartisan support from Congress and industry pressure, the export control measures were re-written in Wassenaar and implemented in the United States in 2022.

The Need for Action

While export control and international dialogues have been progressing in the United States and Europe, the market for offensive cyberweapons has taken off. Recently, NSO Group testified before an EU parliamentary investigation that 5 EU nations had purchased the company's Pegasus surveillance software.[16] In addition, the development of "surveillance as a service" offerings continue to grow outside of Wassenaar

---

[11] Tom Burt, *Cyber mercenaries don't deserve immunity*, Microsoft On the Issues (July 23, 2022, 6:00 PM), https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/; Brief for Appellees at 19, NSO Group Technologies Ltd. et al. v. WhatsApp Inc. et al., 17 F.4th 930 (9th Cir. 2021) (No. 20-16408).

[12] *NSO Group Technologies Ltd. et al. v. WhatsApp Inc. et al.*, 17 F.4th 930, 937 (9th Cir. 2021).

[13] Jonathan Stempel & Elizabeth Culliford, *Facebook can pursue malware lawsuit against Israel's NSO Group -US appeals court*, Reuters (July 23, 7:29 PM), https://www.reuters.com/technology/facebook-can-pursue-malware-lawsuit-against-israels-nso-group-us-appeals-court-2021-11-08/#:~:text=In%20a%203-0%20decision%20on%20Monday%2C%20the%209th,foreign%20government%20agent.%20Advertisement%20%C2%B7%20Scroll%20to%20continue.

[14] *NSO Group Technologies Ltd. et al. v. WhatsApp Inc. et al.*, 17 F.4th 930 (9th Cir. 2021), *petition for cert. filed* (May 3, 2022)(No. 21-1338).

[15] Sam Jones, *Cyber war technology to be controlled in same way as arms*, Financial Times (July 23, 2022 5:00 PM), https://www.ft.com/content/2903d504-5c18-11e3-931e-00144feabdc0#axzz2mcmODFSm.

[16] Antoaneta Roussi, *Pegasus used by at least 5 EU countries, NSO Group tells lawmakers*, POLITICO (July 23, 2022 7:30 PM), https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/.

member states, with a New York Times article from 2019 noting that "the Middle East is the new epicenter of this era of privatized spying."[17]

Microsoft believes that as governments consider the appropriate use of cyberweapons, it is important to include surveillance as a service in that debate.

PSOA Technologies are Cyberweapons

It is important for the United States to consider how these offensive technologies are used as cyberweapons. Given that these offensive surveillance capabilities are no longer highly classified capabilities created by defense and intelligence agencies, but commercial products now offered to companies and individuals, any regulatory regime for cyberweapons needs to move beyond export control. There's been much discussion in the security community about what constitutes a cyberweapon and whether a piece of software can be a weapon at all. Over the years, courts have found a range of implements– a pillow,[18] duct tape,[19],even the surface of a parking lot[20] – all deemed weapons because of the way in which the implements were used was intended to cause harm.

Cyberweapons are tools that, depending on how they are used, can cause harm. In 2021, Indian privacy and civil society advocates argued that there was evidence of the Indian government's use of NSO Group's Pegasus software against "human rights defenders, journalists, lawyers, government officials, and opposition politicians" and the advocates further argued that "The disproportionate, illegal, or arbitrary use of spyware, like Pegasus, for surveillance violates the right to privacy, undermines freedom of expression and association, and threatens personal security and lives."[21] It is time to contemplate new and broad-based solutions to the problem of commercially available surveillance software in order to put necessary guard rails around cyberweapons and the rapidly growing commercial surveillance industry.

New steps against cyberweapons

The Biden Administration's decision to place known PSOAs NSO Group and Candiru on the Entities List was a sound decision recognizing that:

> These entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order.[22]

Continuing to identify companies involved in the surveillance as a service industry and reporting on those companies to Congress is a helpful step. Microsoft appreciates the efforts by Congress, including Section

---

[17] Mark Mazzetti et al., *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*, N.Y. Times (July 23, 2022, 4:50 PM), https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html?searchResultPosition=1.

[18] *State v. Wagner*, 319 Or. App. 399, 409 (2022).

[19] *Commonwealth v. Rodriguez*, 182 N.E.3d 986, 992 (Mass. App. Ct. 2022).

[20] *Burgh v. State*, 79 N.E.3d 955, 956 (Ind. Ct. App. 2017).

[21] *India: Spyware Use Violates Supreme Court Privacy Ruling*, Human Rights Watch (July 23, 2021, 8:00 PM), https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling#:~:text=The%20disproportionate%2C%20illegal%2C%20or%20arbitrary%20use%20of%20spyware%2C,threatens%20personal%20security%20and%20lives%2C%20the%20groups%20said.

[22] U.S. Dept. of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (2021).

309 of the House Intelligence Authorization Act of 2023, to shine a light on and address the increasing cybersecurity and national security risks posed by the foreign commercial spyware industry.

Contemplating options in the US and worldwide

For there to be real change, the United States will need to help advance global norms on surveillance software and the protection of human rights and privacy. We are committed to working with others in industry and civil society and with politicians and governments to help curb this dangerous market. Actions to address these risks might include:

- Continued efforts by the US Government to identify companies and governments leveraging cybersurveillance tools against Americans and adding new private sector offensive actors to the Entity List.
- Advocating for responsible government action, including making the procurement of these technologies more transparent and the control of their use subject to regulation.
- Establishing greater transparency of business practices for these PSOAs, which function as cyber mercenaries: given the opaque nature of this market, the information regarding the relationship between governments should demand standards and transparency procedures that are clear and unambiguous, preventing the use of these tools without lawful process and clear guidelines that adhere to human rights protections.
- Urging all private sector actors, including cyber mercenaries, to respect human rights. Cyber mercenaries frequently threaten human rights, spanning from the right to privacy to freedom of expression. Encouraging all private sector entities to have a corporate responsibility policy in place would help clarify their obligations to human rights, and their processes for due diligence, transparency, and remedy.
- Determining accountability frameworks: We urge states to highlight norm violations to establish appropriate legal standards and pursue multilateral consequences for particularly egregious acts.

Conclusion

In the past ten years, surveillance as a service has enabled governments around the world to exceed their technical capabilities or legal authorities. The exponential growth of the market and the tools themselves indicate that without creative regulation and global disincentives, we will continue to see governments, companies, criminal groups, and individuals use surveillance software to obtain information without the consent of the victim. The invasion of privacy, risk to human rights, and flaunting of the rule of law means that Americans domestically and abroad will be at risk, as well as countless others who work to enable democracy, human rights, and civil society around the world. Microsoft will continue to take action to protect our customers, as we are doing today in announcing our investigation and protections against KNOTWEED. We welcome the opportunity to collaborate with Congress, the Administration, national security agencies, cybersecurity researchers and other responders, as well as like-minded governments around the world to address the risks and harms posed by surveillance unguided by rule of law and democratic principles.