Written Testimony of Tom Burt
Corporate Vice President
Customer Security & Trust
Microsoft Corporation

to the Senate Judiciary Committee
Subcommittee on Crime and Terrorism

November 5, 2019

Chairman Hawley, Ranking Member Whitehouse, and Members of the Committee, thank you for the opportunity to testify today on the important topic of protecting information from criminals, terrorist organizations, and nation-state actors.

My name is Tom Burt and I am the Corporate Vice President of Customer Security and Trust (CST) at Microsoft, a cross-disciplinary team made up of engineers, lawyers, policy advocates, business professionals, data analysts, and cyber-crime investigators who are collectively responsible for ensuring customer trust in Microsoft's products and online services. We focus on ensuring compliance and enhancing security and transparency to protect our customers and promote global trust in Microsoft. Specifically, we work with a variety of governmental and nongovernmental stakeholders to:

- Fight cyber-crime and nation-state compromises;
- Advocate for and contribute to cyberpeace and the stability and security of democratic institutions globally;
- Advance safety on our online services; and
- Ensure Microsoft's products and online services comply with our internal security engineering policies.

Though my team has a broad mission, in my testimony I will focus specifically on the work that we do to combat cyber-crime and nation-state compromises and our approach to encouraging global cyberpeace.

There are two characteristics of the Internet that make it essential that private enterprise, governments, and civil society work collaboratively if we hope to ever find effective and durable approaches to combatting cybercrime and reducing nation-state attacks. First, the Internet is almost entirely the product of private sector innovation and ownership. The physical and virtual assets that form the backbone of the on-line community were created by, and are maintained, evolved and secured by, the private sector. Thus, the private sector has unique data access and systemic controls not available to government. Second, the Internet is largely borderless – and is especially so when cybercrime and nation-state attacks are considered. This means that traditionally sovereign approaches to the investigation and prosecution of crimes, and other disruptions, will not work. Indeed, sophisticated cybercriminals and nation-state actors use deep understanding of jurisdictional differences and legal authority restrictions to

enable their activities. Neither government nor the private sector can address these challenges alone.

Microsoft is committed to this partnership. We advocate with governments and through policy initiatives around the world for all stakeholders to adopt rules of conduct in cyberspace to protect governments, enterprises, and consumers. We collaborate with law enforcement, the intelligence community and other government agencies so that our efforts can yield maximum protection for the global online ecosystem and our customers throughout the world.

Nation-State Threats

Microsoft's work to protect our customers and the security of the online ecosystem builds upon the company's experience in both assessing and tracking cybersecurity threats and in fighting cybercriminal activity. The Microsoft Threat Intelligence Center (MSTIC) has focused on tracking nation-state actors for more than a decade, and Microsoft's Digital Crimes Unit (DCU) has used creative techniques and Microsoft technology to fight cyber-crime and improve cybersecurity since 2008. Our robust experience in tracking nation-state threats enhances Microsoft's ability to fight cybercriminal activity and increase the cybersecurity of the global online community. Combined, these actions help Microsoft customers stay ahead of new and evolving threats and challenges.

In the past year, Microsoft notified nearly 10,000 customers[1] that they have been targeted or compromised by nation-state attacks. About 84% of these attacks targeted our enterprise customers, and about 16% targeted consumer personal email accounts. This data demonstrates the significant extent to which nation-states continue to rely on cyberattacks as a tool to gain intelligence, influence geopolitics or achieve other objectives.

Most of the nation-state activity in recent months originated from actors in three countries: Iran, North Korea, and Russia. Specifically, we have seen extensive activity from: the actors we call Holmium, Phosphorus, [2] and Mercury operating from Iran; Thallium operating from North Korea; and two actors operating from Russia we call Yttrium and Strontium.[3] We have also seen activity by actors operating from China, but not at the same volume as the actors in these three nations. We continuously track these global threats, building this intelligence into our security products to protect customers and using it in support of our efforts to disrupt threat actor activities through direct legal action or in collaboration with law enforcement. Each nation has its own targets of primary interest. For Russia's Strontium actor, for example, we see them targeting information technology firms and think tanks, democratic processes and

---

[1] New Cybersecurity Threats require new ways to protect democracy. https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/

[2] Recent Cyberattacks Require Us All To Be Vigilant. https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/

[3] New Cyberattacks Targeting Sporting and Anti-Doping Organizations. https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

most recently antidoping and national sporting organizations. Iran's Mercury actor has been pursuing targets in the oil and gas sector. North Korea's Thallium actor has been targeting universities and diplomatic entities, especially individuals and organizations active in nuclear non-proliferation policy. Given the breadth and increasing frequency of these nation-state attacks, Microsoft has had to bring automation and machine learning to help address these problems at scale.

Combatting cybercrime and nation-state compromises require a joint effort. To that end, we monitor evolving cybercrime threats and work closely with law enforcement on a number of initiatives to help devise and execute strategies that disrupt cybercrime threats targeting enterprises, consumers, and governments. Microsoft's work with law enforcement agencies on malware disruptions demonstrates the value of private-public partnerships.

Microsoft Combats Botnets and Business Email Compromise

Microsoft plays offense against online threats. Working through robust partnerships, we work to take down criminal infrastructure and pursue financially motivated cybercriminals and nation-state actors. This work helps us to protect our customers and to improve the safety of the global internet community so that all users – enterprises, consumers, and governments – can trust the technology and online services on which we rely for commerce and communication.

Microsoft has been driving a sustained fight against botnets for over a decade using novel legal and technical countermeasures to protect our customers and internet users across the globe. "Bots" are software that infiltrate computers and other devices without detection. Typically, the infiltrated systems belong to a government agency, business, or individual. The bot software gives the person who infected the device, known as the "bot-herder," the ability to control the infiltrated systems remotely. These botnets can range from a few hundred to tens of millions of compromised systems. They are used by cybercriminals to conduct distributed denial of service (DDOS) attacks, launch massive spam campaigns, proliferate malicious software, and steal data. Whether using common law property or tort causes of action in civil cases to seize malicious domains, or applying Racketeering Influenced and Corrupt Organization (RICO) and Lanham Act provisions to physically seize command and control servers used by cybercriminals, Microsoft's efforts in this sustained campaign against cyber-crime enabling botnets can be seen in the 17 operations we've engaged in over the past several years against prominent botnets like Rustock,[4] Dorkbot[5] and more recently Gamarue.[6] Each operation is an exercise in collaboration, bringing together the unique abilities and assets of our private

[4] Rustock is a botnet that was responsible for significant amounts of spam in Hotmail consumer accounts. https://www.wired.com/2011/03/microsoft-versus-rustock-botnet/

[5] Dorkbot is a botnet that is used to steal online payments and cause distributed denial of service attacks. https://www.us-cert.gov/ncas/alerts/TA15-337A

[6] Gamarue is a botnet that was available for sale on the black market to enable a wide variety of cyber-crime. https://www.geekwire.com/2018/microsoft-releases-new-details-gamarue-malware-botnet-sprawling-infrastructure/

industry, academic, and public sector partners all striving to find new ways to protect people from cyber-crime across the globe.

Microsoft then works to clean the computers that were infected with botnet software. Our success in this effort is due to close collaboration with security industry partners, internet security providers (ISPs), and government computer emergency readiness teams (CERTs) that are tasked with protecting infrastructure and work with partners to defend against cyberthreats around the world to help affected computer owners regain control of their malware-infected computers. Microsoft shares the information acquired through our investigative efforts and disruptive actions primarily through our threat sharing program. By sharing our botnet takedown data with customers, ISPs, and CERTs, Microsoft has been able to provide the information necessary to inform affected computer owners as well as offer free tools to help them clean their systems. This effort has already helped drastically reduce the global infection of the 17 botnets Microsoft has tackled so far.[7] In fact, since 2012 Microsoft's efforts has rescued computers identified on 423 million distinct internet protocols (IPs) covering 15 malware families.

Building on the success of this effort, Microsoft is continuing to explore new ways to better engage with our partners. For example, we are working on incorporating new data into our threat sharing program in addition to the infected IPs collected during our botnet disruptions that we currently share. This new data will seek to include known or suspected malicious servers, domains, and internet of things (IOT) devices being leveraged by cybercriminals. Collecting and sharing this data will enable Microsoft and our partners to identify and block malicious traffic emanating from criminal infrastructure located in parts of the world beyond our collective reach, thereby allowing us to counter the changing tactics criminals deploy as they attempt to protect their infrastructure.

We have also developed a new threat sharing platform called the Command and Control Observer, a business intelligence-based dashboard delivering reliable, secure, and near real-time actionable intelligence on threats. The Command and Control Observer dashboard was designed to strengthen public-private collaboration in the investigation and disruption of cybercriminal infrastructure. It is being used by over 20 different entities including the Financial Services Information Sharing and Analysis Center (FS-ISAC), a financial industry consortium, and government agencies, ISPs, and CERTs in 13 countries today. It provides law enforcement, CERTs, and government agencies responsible for the enforcement of cyber laws and the protection of critical infrastructure with better telemetry related to criminal cyber infrastructure located within their jurisdiction regarding specific threats, as well as a view of compromised computers and victims impacted by such criminal infrastructure.

[7] We have seen a 49.56% decrease in distinct IPs since our highest peak in 2014. Each distinct IP can represent one device, or if associated with a small to medium business, several hundred devices. In the case of a US consumer home, one consumer home IP has on average five devices associated with it

In addition to its work combatting botnets, Microsoft is also fighting against Business Email Compromise (BEC) crimes. This crime impacts both individuals and enterprises around the world. The FBI reported that in the past three years there have been at least 160,000 victims, who have lost in total more than $26 billion to these crimes.[8] Microsoft is working to combat BEC by: 1) disrupting the technical infrastructure utilized by cybercriminals to facilitate BEC attacks – in the last year we have removed over 300,000 malicious phishing URLs, which helped prevent unsuspecting customers from inadvertently accessing phishing pages and falling victim; 2) deterring future BEC attacks by identifying the responsible individuals and referring cases and evidence to the FBI and international law enforcement agencies—most recently Microsoft provided evidence and referred cases in support of Operation ReWired, a coordinated international enforcement action against cybercriminals engaged in BEC; and, 3) communicating timely and relevant information regarding emerging BEC threats to customers and industry partners.

Private Sector Experience: Sharing Insights and Developing Tools

The private sector – as the owner and steward of the Internet – has the first responsibility to protect our customers. To that end, we work in a number of ways to increase the private sector's ability to prepare for, defend against, and become resilient to cyber-attacks. Among other things, we have worked with others to create tools for small and medium enterprises to manage cyber risk, formed coalitions of technology leaders to enhance the stability of cyberspace, and collaborated on surveys of private sector resilience.

In collaboration with Marsh, we recently surveyed the cyber risk management maturity of the private sector.[9] Overall, we found that the firms with the best cyber risk management strategies are increasing their focus on cyber resilience over prevention. Some of the key recommendations emerging from the survey are:

- Create a strong organizational cybersecurity culture, with clear, shared standards for governance, accountability, resources, and actions.
- Quantify cyber risk to drive better informed capital allocation decisions, enable performance measurement, and frame cyber risk in the same economic terms as other enterprise risks.
- Evaluate the cyber risk implications of new technology as a continual and forward-looking process throughout the lifecycle of the technology.
- Manage supply chain risk as a collective issue, recognizing the need for trust and shared security standards across the entire network, including the organization's cyber impact on its partners.
- Pursue and support public-private partnerships around critical cyber risk issues that can deliver stronger protections and baseline best practice standards for all.

---

[8] *Business Email Compromise A $26 Billion Scam.* https://www.ic3.gov/media/2019/190910.aspx

[9] *2019 Global Cyber Risk Perception Survey.* https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Consistent with these findings, Microsoft works with other private sector entities, governmental organizations, and international bodies to raise the standard of cybersecurity. The Cybersecurity Framework produced by the National Institute of Standards and Technology (NIST) has proven to be a useful baseline for firms to evaluate their cybersecurity maturity and the effectiveness of available processes to manage cybersecurity risk. The Framework has been widely adopted and reportedly is increasingly used by Boards of Directors and enterprise management. We were an industry contributor to the development of the NIST Cybersecurity Framework and use it as one means of assessing our own cybersecurity maturity. Microsoft enjoys a vibrant relationship with NIST in our partnership to advance Cybersecurity Excellence. We are a National Cybersecurity Excellence Partner (NCEP) and regularly engage with leaders and members of NIST's National Cybersecurity Center of Excellence to advance thought leadership and the provision of hardware and software to support the rapid adoption of secure technologies. Just this past month, during National Cybersecurity Awareness month, Microsoft sponsored a multi-day exchange with NIST at our headquarters to discuss emerging trends in artificial intelligence security, IoT standards, quantum computing, election system protection, and privacy. In addition, my team joined NIST in Maryland for NCEP roundtables for DC Cyber Week. Our engagement with NIST is a successful representation of effective public-private collaboration.

In addition, Microsoft, in collaboration with other private sector companies, launched the Cyber Readiness Institute (CRI), a non-profit initiative that convenes senior leaders of global companies—including Mastercard, Microsoft, ExxonMobil, Maersk, General Motors and others—to develop tools and resources to improve the cyber readiness of small and medium-sized enterprises.[10] The CRI uses the NIST cybersecurity framework as a baseline for its work in developing targeted programs such as the Cybersecurity Readiness Program. Though it rarely recommends non-governmental tools to consumers, NIST recently featured the Cybersecurity Readiness Program on its website as a tool for small and medium enterprises to increase the safety and security of enterprises against cybersecurity threats.[11]

Encouraging good cyber risk management practices for firms domestically and internationally enhances the ability of firms to prevent, protect, and recover from attacks. Most importantly, public awareness directly impacts the resilience of the private sector against cyber-crime and nation-state compromises. But industry leaders cannot do this alone, it requires collective effort by civil society, governments, and international bodies.

Collaboration with the Federal Government

In combatting cybercrime and nation-state compromises, we know that strong partnerships with the federal government are essential. We value our collaboration with the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency in particular, the

[10] https://www.cyberreadinessinstitute.org/cyber-readiness-news/national-institute-of-standards-and-technology-adds-cyber-readiness-institutes-cyber-readiness-program-to-small-business-cybersecurity-resources
[11] https://www.nist.gov/itl/smallbusinesscyber/training

Federal Bureau of Investigation, the Department of Justice, and other agencies, including the intelligence community, that are involved in combatting nation-state activity. We welcome the new mission of the National Security Agency's Cybersecurity Directorate and we look forward to deeper collaboration with the Directorate to help protect against nation-state attacks and advance the public private partnership required to achieve meaningful solutions.

The federal government, however, can help advance our shared goals by increasing transparency around nation-state activity it observes. Although it may appear counter-intuitive, that transparency will help eliminate more nation-state activity. Often, nation-state activity is a "stepping-stone" for further action by other nation-states or cybercriminals, recycling advanced tools to pursue their objectives cheaply and effectively. Law enforcement and intelligence agencies should more frequently share attribution, but also indicators of compromise or other threat intelligence from cases or matters that did not go to prosecution, so that they can be used by others to defend against attacks and improve resiliency.

Though the success of our efforts to disrupt nation-state compromises and cybercrime is due in significant part to our relationship with law enforcement agencies around the world, we recognize the special challenges law enforcement faces. A traditional approach of investigating in order to identify and prosecute is increasingly challenging in the virtual world, which enables cybercriminals to act anonymously, hide in jurisdictions with no qualms about their activities, and operate through resources located around the globe, thereby significantly frustrating efforts to identify and prosecute these individuals. Many cybercriminals are located within jurisdictions with no extradition treaties in place, so even when attribution is possible, arrest is not. This requires us to work together to balance the objectives of the public and private sector. We need to work together to effectuate systematic change, to take down criminal infrastructure globally, and improve the recovery and resilience of victims at scale.

To improve its effectiveness in combatting these crimes, the United States needs to work with allies in new ways while using existing authorities to make a meaningful impact. The recently announced agreement between the United States and the United Kingdom – the first international agreement concluded under the parameters of the Clarifying Lawful Overseas Use of Data (CLOUD) Act – is a significant step forward. But the United States, the United Kingdom, and governments around the world must continue to engage with each other to modernize digital evidence and privacy laws, resolve conflicts, and set forth concrete international frameworks that properly protect their citizens from cybercrime and insidious attacks in this digital age. We are encouraged by the start of negotiations between the United States and the European Commission toward a CLOUD Act agreement, and hope the Department of Justice increases their engagement with other governments to negotiate and conclude agreements envisioned by the CLOUD Act.

International Norms and Multi-Stakeholder Collaboration

Increasing numbers of sophisticated attacks in cyberspace today are being driven by nation-state investment in the development and deployment of offensive cyberweapon capabilities.

Nation-state cyberattacks have over the last decade increased dramatically in frequency, proliferation, and impact. Observers have also highlighted the risks posed by the laws of authoritarian governments like China's Cybersecurity Law, which requires that companies provide the Chinese government with carte blanche access to their networks. Other nations are starting to follow that lead. The U.S. must focus on the threats that such policies pose to the security of technologies, whatever their origin. We must invent 21st Century solutions to this uniquely 21st Century threat and this will require new forms of collaboration.

As Microsoft has worked to advocate for multi-stakeholder approaches to addressing these issues, we recognized that the private sector needed itself to commit to core principles to advance global cybersecurity. To that end, we joined with 34 other global technology companies in founding the Cybersecurity Tech Accord in 2018. This Accord asks members to endorse four foundational principles:

- Protecting all of our users and customers everywhere;
- Opposing cyberattacks against innocent civilians and enterprises;
- Empowering users, customers and developers to be more secure; and
- Partnering with one another to enhance cybersecurity and resilience.

Since its launch, the Cybersecurity Tech Accord has grown to include more than 120 global technology companies from 25 countries. We meet regularly to pursue new initiatives to protect cyberspace including awareness-raising activities, consultations with governments, promoting international norms, and committing to have every signatory adopt a vulnerability disclosure policy. The Cybersecurity Tech Accord has by its collaboration and actions become the global voice of the technology industry on cybersecurity policy.

Most recently, the Hewlett Foundation, Mastercard and Microsoft, along with others, founded the CyberPeace Institute as an independent NGO to be based in Geneva, Switzerland. The CyberPeace Institute seeks to enhance the stability of cyberspace by decreasing the frequency, harm, and scale of cyberattacks on civilians and civilian infrastructure and by increasing the resilience of vulnerable populations.

It seeks to accomplish this by:

- raising public awareness of the occurrence and impacts of sophisticated cyberattacks, including those led or sponsored by states, on civilians and civilian infrastructure;
- promoting transparency of, and accountability for, cyberattacks that are perpetrated by sophisticated actors and result in significant, direct harm to civilians or civilian infrastructure;
- reinforcing existing norms and practices related to increasing the stability of cyberspace, including by supporting institutions and mechanisms that seek to restrain the use, spread, or harm of cyberattacks on civilians and civilian infrastructure;
- highlighting any perceived normative or legal gaps that may exist by examining how rules regarding state behavior are being applied in an operational context;

- building and enhancing expert networks to assist vulnerable populations in recovering from cyberattacks that are perpetrated by sophisticated actors and have significant, direct harm; and
- providing capabilities to increase the resilience of vulnerable populations against cyberattacks.

The leadership of the Institute is assisted by both an executive board and an advisory board, comprised of leading experts from across industry, academia, civil society, and government. The Institute is to be based in Geneva, Switzerland, to capitalize on its history of neutrality and as the home of international institutions and non-profits related to peace and security, including the International Committee for Red Cross (ICRC), the UN Institutions, International Campaign to Abolish Nuclear Weapons (ICAN), Land Mine Ban Treaty Organization, and others.

On the global stage, the U.S. government can and should play a leading role in advancing meaningful international norms to limit escalating nation-state attacks in cyberspace. Although there are perhaps a handful of well-known and advanced cyber powers responsible for much of this activity, independent assessments suggest that more than 60 nations[12] are now actively developing such offensive capabilities in an apparent new "cyber arms-race," all in the absence of clear rules or expectations for responsible behavior. In fact, "cyber" is now the first global threat listed in the most recent *Worldwide Threat Assessment*, from the U.S. Intelligence Community.[13]

This weaponization of cyberspace also has important downstream consequences as cyberweapons developed by governments can be stolen, sold, reused or repurposed to devastating effect by malicious actors and cybercriminals with a wide range of objectives. Such consequences were on full display when nation-state developed exploit software was leaked and repurposed in the WannaCry and notPetya attacks of 2017 – which caused massive economic harm, spread autonomously to computer systems across dozens of countries and hundreds of enterprises in a matter of hours, and in the case of WannaCry disabled the United Kingdom's National Health System, putting lives at risk in the process.

As with other domains of conflict, long-term solutions for protecting cyberspace will require clear and binding international commitments to articulate what is and is not tolerable behavior for states online. The age of ambiguity, where many actors exploit perceived gaps or grey areas in international law, is no longer tenable, desirable, or acceptable for anyone.

Establishing these rules and making them truly effective must inherently require collaboration of governments and the private sector with the participation of civil society. Multi-stakeholder solutions are essential to what is necessarily a multi-stakeholder problem. We must indeed invent 21st Century solutions to this uniquely 21st Century threat and this will require new forms

[12] Council on Foreign Relations. https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities
[13] Worldwide Threat Assessment of the US Intelligence Community. 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

of collaboration. That is why Microsoft was proud to join in supporting the Paris Call for Trust and Security in Cyberspace last year, along with what are now more than 65 governments and over 350 companies and 135 civil society organizations. The Paris Call is a voluntary commitment to 9 foundational cybersecurity principles including protecting the public core of the internet, critical infrastructure, elections and intellectual property from cyberattacks. The Paris Call has widespread support from these 550 organizations and countries —including every government of the European Union, almost all NATO countries and every one of the "Five Eyes" governments -- all with the exception of the United States. For the sake of the security of American citizens, and those around the world endangered by escalating and sophisticated attacks online, Microsoft encourages the United States to join with so many other countries and organizations in supporting this multi-stakeholder agreement – the most widely endorsed multi-stakeholder commitment in history.

While the Paris Call is a significant step toward the required solutions the world needs, much more needs to be done and there are other processes in motion. Two ongoing dialogues under the auspices of the United Nations – the Group of Governmental Experts and an Open-Ended Working Group – have the potential to advance new and more binding commitments for responsible state behavior in cyberspace. The success of these initiatives will hinge in no small part on the willingness of the United States to push for consensus outcomes that recognize the importance of human rights, international law, multi-stakeholder input and rules for responsible state behavior online.

Governments, including our own, must continue to use diplomatic processes that include the private sector and civil society to advance cyber norms and drive for meaningful rules governing government conduct in cyberspace.

CONCLUSION

Microsoft believes strongly in the importance of protecting our customers in the United States and around the world from nation-states and cybercriminals. Nation-states are still exploring the boundaries of offensive cyber tactics and capabilities, and development of clear laws and policies have been slow. The safety and security of our customers and all participants in the global on-line community are at increasing risk, threatening the evolution and utility of our modern age's most transformative invention. To this end, Microsoft is working to raise industry standards for achieving better cyber risk management, encouraging increased transparency, improving collaborative public-private relationships, and advancing a multi-stakeholder approach to establishing meaningful international norms.

While public/private collaboration has yielded significant success in combatting cyber-crime and disrupting nation-state compromises, there is much more to be done. While we commend the government for its work disrupting criminal infrastructure, we hope that Congress will provide new incentives for law enforcement to prioritize the disruption and dismantling of criminal networks. We are supportive of the agreement between the United States and the United Kingdom implementing the CLOUD Act and encourage the Department of Justice to

increase their engagement with other governments to negotiate and conclude CLOUD Act agreements. We also encourage the United States to support the Paris Call and to support the adoption of clear and binding international commitments to rules of conduct in cyberspace. Governments, including the United States, must continue to use diplomatic processes to advance cyber norms and drive for multi-stakeholder solutions.