Statement of

Brandon Wales
Vice President, Cybersecurity Strategy, SentinelOne

"Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"

Before the
Committee on Homeland Security
United States House of Representatives

January 22, 2025

Chairman Green, Ranking Member Thompson, and members of the Committee, thank you for the opportunity to testify today on global cyber threats, a subject that I have worked as the Executive Director of the Cybersecurity and Infrastructure Security Agency (CISA) and now as Vice President of Cybersecurity Strategy as SentinelOne.

Introduction

The past few years of publicly-acknowledged intrusions by China, Russia, Iran, North Korea and cyber criminal organizations make clear that the U.S. is facing increasingly sophisticated adversaries in ongoing cyber warfare. The intensity of the threat is at an all-time high, driven by a combination of increasing geopolitical tension and the rapid pace of technological change. Defenders in the government and the private sector are learning from each breach and adapting to offender tactics. However, threat actors are learning and innovating as well. Maintaining a strategic edge and building national cyber resilience in the face of this onslaught remains a critical challenge and will require a collaborative whole of government and whole of industry response.

Russia

Russia's security services are an acute and malign cyber threat, willing to take increasingly aggressive cyber and sabotage operations to undermine western resolve in support of Ukraine. They maintain exceptionally skilled hacking teams that operate globally in support of Russian national interests, leveraging supply-chain attacks and access to sensitive national critical infrastructure to hold western security interests at credible risk.

Russian security services are conducting brutal sabotage campaigns across Europe in support of their illegal war and other geopolitical goals. Intelligence collection through cyber espionage plays a role in selecting targets for disruption. In addition to conflict-related targets, Russia's security services remain keen intelligence collectors against the US government. Political intelligence collection on personnel, the Department of Defense, and other US government

elements are a high priority. They remain very skilled at combining cyber and psychological operations to interfere in elections, inflame social divisions, and undermine democratic systems across the world, and have baked these operations into their doctrine for warfare against the West.

Beyond disruption, these groups engage in economic espionage, stealing sensitive data from critical sectors to bolster Russia's strategic interests. Ransomware gangs with tacit support from the state wreak havoc on U.S. businesses and institutions. The combined effect is deniable disruption and hybrid warfare that throws the security balance off kilter while imposing growing costs on our society.

Russia takes a mercenary approach to its foreign policy and cyber operations. According to public reporting from the Associated Press, Russian security services are improving their ties with the security services of the UAE.[1] Across Central Asia and Africa, Russia and the Emirates find common cause in stirring the pot in unstable countries to control gold mines and other precious resources. Their combined activities in Libya and Sudan make clear their goal to extract precious metals that help Russia blunt the impact of western sanctions.

Iran

Iran continues to dedicate its most capable teams to attacks against Israel and Israeli targets while also actively monitoring its own dissidents internally and abroad, in some cases to target them for assassination.[2] Iranian attacks against Unitronics PLCs in 2023 demonstrated the intent of the Iranian regime to target Israeli companies even outside of Israel and their willingness to target industrial control systems operating critical infrastructure.[3]

In the lead-up to the 2024 U.S. presidential election, the Islamic Revolutionary Guard Corps (IRGC) orchestrated a sophisticated "hack-and-leak" operation targeting President Donald Trump's re-election campaign. Employing spear-phishing techniques, IRGC cyber operatives infiltrated campaign email accounts, exfiltrating sensitive documents, including a 271-page vetting report on then vice-presidential candidate J.D. Vance. These stolen materials were subsequently disseminated to media outlets and individuals associated with rival political campaigns, aiming to undermine President Trump's candidacy and sow discord within the U.S. electoral process. The IRGC's efforts were, however, effectively neutralized by the broad unwillingness to publicize the stolen material.

North Korea

---

[1] https://apnews.com/article/intelligence-leak-russia-uae-pentagon-9941a3bb88b48d4dbb5218649ea67325

[2] https://www.reuters.com/world/middle-east/us-uk-taking-action-against-network-that-targeted-iranian-dissidents-us-treasury-2024-01-29/

[3] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Multiple federal indictments demonstrate how the North Koreans are trying to get their cyber operators hired into American companies so they can wreak havoc from the inside–looting companies to pay for their rapidly advancing nuclear weapons program.[4]

Late in 2024, research by SentinelLabs showed how a web of shell companies based in China were serving as fronts for DPRK remote IT workers seeking jobs at US firms.[5] These companies were registered in China as legitimate businesses with local government through individuals in China, though it is unclear the extent to which the PRC knew of and supported these operations. Our SentinelLabs researchers tracked these registrations back to Shenyang Province in China. Reporting by CNN a decade earlier identified DPRK Military Bureau 121 operating a hotel as a front for hacking operations in the same province.[6]

Unfortunately, DPRK's IT worker scam is still in full-swing. America's front line of defense is the HR department of enterprises big and small, many of which are not technically capable enough to identify discrepancies that may indicate an issue. North Korea's effective use of mules and laptop farms create issues in detecting worker scams before these "new employees" are hired into a company.

The DPRK is also unique in that their security services are expected to turn a profit, and they do so to the tune of several billion dollars a year. These days, most of their ill-gotten gains are generated via the theft of cryptocurrencies, and many observers estimate that the North Korean government is, collectively, the largest thief of cryptocurrencies in the world. These highly fungible digital assets are then used to fund their nuclear program and evade other sanctions placed on the regime.

Cyber Criminals

Cyber criminals continue to make use of a robust ecosystem of infrastructure providers, money launderers, and tool developers to attack businesses through ransom of systems, the blackmail of leaking data, and the sale of stolen data. Ultimately, the cyber criminal ecosystem relies on three core factors: (1) a vulnerable and misconfigured install base here in the U.S. and elsewhere; (2) a cryptocurrency ecosystem outside the oversight of the traditional fiat economy by which criminals can monetize those vulnerabilities and misconfigures to extract wealth from the west; and (3) a safe harbor in Russia and its sphere of influence from which the criminals can conduct their operations without fear of consequence.

---

[4] https://www.justice.gov/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information
https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and

[5] https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china/

[6] https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html

The US and allied governments have conducted effective joint operations to reduce the trust between actors, seize criminal infrastructure, and disrupt criminal networks. Still, many criminal actors persist and profit from poor cybersecurity practices in the public and private sectors. Our research and reporting will show in 2024 that the groups Akira, BlackBasta, and Play topped the metrics for frequency and profitability of their attacks. Cybersecurity companies, such as SentinelOne, are on the front line of stopping such attacks and we continue to work alongside our law enforcement partners in disrupting these operations.

China

But one threat actor, the People's Republic of China, stands out among the rest for its persistence, breadth of operations, and capabilities.

In our public conscience, the words "OPM hack, Google, Experian, Microsoft, Marriott" are anchors in our minds of China's large-scale data theft campaigns against the US. Many now more than a decade old, we can look back on China's hacking teams and see the lack of expertise and professionalism in their old trade craft. They were noisy, easy to track, and effective.

Things have changed, though. China's hacking teams have grown significantly in size and capability over the last decade.

After Xi Jinping came into power in 2013, he quickly established the Leading Small Group on Cybersecurity and Internet Management.[7] Within a year, he would transform that Leading Small Group into one of a handful of standing committees of the Chinese Communist Party Central Committee. It was a significant step for China and signaled Xi's personal interest in the issue.

Shortly thereafter in 2015, China revamped its cybersecurity degree requirements for universities, using the U.S.'s own National Initiative for Cybersecurity Education as a model to replicate.

In 2016, after hearing about a project in Wuhan to establish a National Cybersecurity Talent and Innovation Base, with its own National Cybersecurity School, the CCP Central Committee on Cybersecurity and Informatization deputized it as a national project. The school graduates around 2000 students each year that are trained in offensive and defensive cybersecurity techniques.

A year later, in 2017, China began certifying some schools as World-Class Cybersecurity Schools–a designation again meant to copy from the US system. This time, the inspiration was the joint DHS-NSA Centers for Academic Excellence in Cyber Operations.

The following year in 2018, China outright banned its best vulnerability researchers from traveling abroad for 0day competitions, where they burned vulnerabilities for cash. Instead,

[7] https://www.cfr.org/blog/chinas-new-small-leading-group-cybersecurity-and-internet-management

these vulnerabilities–which China's policy community consider a "national resource"–were forced to remain in the country and surrendered to the security services at competitions like Tianfu Cup.

By 2021, China decided to do something no other government had done–they mandated the collection of software vulnerabilities, a key tool in hacking operations, be reported to the government within 48 hours of discovery by companies "doing business in China."
It should come as no surprise that we see China's hacking teams repeatedly accessing critical infrastructure, corporate trade secrets, and sensitive national security systems.

As a result of these efforts, over the past decade, China has evolved from being one of the noisiest attackers–acting without regard for being caught, while still stealing massive amounts of data–to some of the best and most stealthy hackers on the planet.

In recent years, the People's Liberation Army has tasked a group of its hackers to target American critical infrastructure and develop persistent access to those systems.

This persistent access is all too easy to procure. It will only ever take a few people, with normal laptops and the knowledge of how their targets are vulnerable, to gain and retain persistent access. Deterring this behavior may not be possible.

It is also important to note the sheer scale of Chinese malicious cyber activity is unparalleled anywhere on the globe. Each intrusion is a warning, but the vast size and pace are the true concerns.

China's view that the U.S. military is superior to the People's Liberation Army drives them to pursue asymmetric tools to weaken the U.S., including cyber attacks against our critical infrastructure. The PLA believes cyber, information operations, and anti-satellite weapons are key to winning any military conflict including preventing the United States from intervening on behalf of Taiwan. So while we may be able to deter China from using these capabilities, we are not likely to deter China from preparing for conflict by prepositioning in our critical infrastructure.

Network Complexity

As adversaries grow more sophisticated, our networks have become increasingly complex. The adoption of cloud computing and expansion of remote workforces have further burdened already overextended defenders. In pursuit of constant availability, businesses have pushed technologists to deploy and maintain more tools with less downtime, resulting in poor hygiene. Additionally, the rapid emergence of AI is creating vast new data repositories which carry forward these same challenges.

As a result, our networks evolved into a patchwork of interdependent services and providers, frequently built on legacy technologies predating many current defenders and defenses. These outdated foundations, central to many businesses, have become easy prey for malicious actors.

Over the past decade, a surge in zero-day vulnerabilities targeting these systems has given adversaries a significant advantage. Tools and systems previously considered best-practice for security have quickly been turned against us.

Once-trusted solutions, such as VPN appliances, have become prime targets. Originally intended to protect remote workforces, these devices now represent a significant attack surface due to vulnerabilities and misconfigurations that go undetected or remain unpatched. As adversaries evolve their tactics, widely adopted security measures can be weaponized against any organization slow to adapt.

Vendors responding to market forces have been pushed to deliver new features, to maintain a competitive edge, at the expense of comprehensive testing and secure coding practices. As a result, old classes of vulnerabilities continue to be delivered to customers, providing an avenue for threat actors to gain a foothold. This relentless pressure to innovate often backfires, putting their customers and our infrastructure at even greater risk.

Addressing these gaps calls for a collective effort by businesses, vendors, and both the public and private sectors. There is no single, foolproof solution. As defenders strengthen their controls, attackers will evolve their methods. Emerging technologies like generative AI lower the bar for malicious actors while simultaneously providing defenders with advanced tools to detect and thwart these threats.

Driving meaningful change across the industry demands unified initiatives, such as CISA's Secure By Design, the Known Exploited Vulnerabilities catalog, Zero Trust architectures, and the NIST Cybersecurity Framework. Yet these efforts alone are insufficient. We must empower our defenders with the training and resources to counter modern threats, ensuring they possess the skills necessary to match, and surpass, those of our adversaries.

Policy Recommendations

There are steps that the government and industry must take to weaken our adversaries, bolster U.S. cyber defenses and enhance our resilience.

First, the gravity of this moment - the continually compounding risk posed by an exploding set of cyber threat actors, highlighted by the preparation for war by the Chinese Communist Party - requires serious, straightforward conversation amongst policy makers, elected officials, business leaders, and the American public. We must call our adversaries' activities what they are - preparation for war. Accordingly, we must call them by their names, plainly, and without fanciful marketing terms that only benefit cybersecurity vendor marketing teams and the adversary themselves, by mythologizing and obfuscating. Foreign government hackers positioned to take hospitals offline and turn off the water supply don't deserve flashy codenames, they deserve disdain and confrontation. No more typhoons or blizzards. Instead, we must speak to the American people about the provocations of the Chinese military and the

Russian security services. In no other theatre of conflict do we willingly throw a veil over our adversaries and their malign activities. It must end now.

Second, to ensure that industry retains its ability to share cyber threat information without fear of liability, Congress should reauthorize the Cybersecurity Information Sharing Act of 2015, which expires later this year. This Act is an important tool to facilitate the flow of critical cyber intelligence between industry and government, and letting it expire would be a huge step back. At the same time, the executive branch, led by CISA, should continue to look for ways to enhance public-private operational collaboration. While CISA's Joint Cyber Defense Collaborative is a great tool, there is more that needs to be done to ensure these efforts can achieve the scale and consistency to match the intensity of today's threats.

Third, we need a whole-of-nation effort to engage and encourage our critical infrastructure to improve their security and enhance their systemic resilience. We are never going to stop every cyber attack so our infrastructure needs to be capable of operating in a degraded state and getting back up and running quickly. The Federal Government should be supporting our infrastructure with information, guidance, technical assistance and, in some cases, with funding. That is why Congress should reauthorize and fund the State and Local Cybersecurity Grant Program, so that our resource constrained State and local government agencies can build and sustain minimum cybersecurity capabilities.

Fourth, the federal government should actively promote competition and avoid monoculture in our technology ecosystem, starting with federal networks. Not only will this spur more innovation, but it will help create more robust systems that minimize opportunities for broad systemic failure and disruption. In part, this can be done by maintaining the momentum in recent years of investing in and centralizing cybersecurity capabilities in CISA. The establishment of CISA in 2018, a key cybersecurity win of the first Trump Administration, combined with authorities granted by Congress in 2021 (e.g., persistent threat hunting on federal networks, administrative subpoena, Joint Cyber Planning Office, etc.) and 2022 (Cyber Incident Reporting for Critical Infrastructure Act) have steadily advanced the nation's cybersecurity capabilities. As we all recognize, however, in the modern digital economy, defenses must keep pace with the threats. Therefore, we must continually adapt and improve our defensive posture, including how we are organized, how we are resourced, how we interact across stakeholder groups, and how we respond. In that spirit, we believe elements of last week's Executive Order on cybersecurity and artificial intelligence continue much-needed forward progress on defending federal networks, such as the accelerating persistent threat hunting and strengthening the security of internet routing. I encourage the Administration and Congress alike to carefully evaluate the positive advances of the prior Administration's cybersecurity executive actions and retain those that put Federal networks and the private sector alike into the best possible position to defend against constantly evolving cyber threats.

Fifth, the U.S. government should continue to foster our global edge in innovation in emerging and next generation technologies such as Artificial Intelligence (AI), particularly in the cybersecurity space and quantum computing. Today, AI is being more quickly integrated into

cybersecurity tools, such as SentinelOne's PurpleAI, than our adversaries are able to integrate AI into their cyber weapons. In cybersecurity, speed kills, and AI-powered tools give defenders the ability to identify, investigate, and mitigate threats faster than ever before. If we want that to persist, we will need to ensure that the U.S. and its allies continue to lead the growth and development of AI, and that attempts to address potential AI risks don't create barriers to broader AI adoption. The PRC's enormous investments in quantum-related research and development threatens U.S. leadership as we look ahead to the emergence of quantum computing with the potential to revolutionize fields, from medicine to material science to AI, while putting much of today's encryption at risk. Congress and the executive branch must work together to ensure that not only does the U.S. win the race for supremacy in quantum computing, but that American businesses and government agencies are ready to upgrade systems to post-quantum cryptographic standards now that the National Institute of Standards and Technology (NIST) has released its first set of quantum resistant algorithms.

Sixth, the U.S. government should aggressively pursue and counter adversary activity wherever it originates from. The takedown of LockBit in early 2024 is an excellent case study. In February of last year, Operation Cronos demonstrated to LockBit affiliates and would-be victims that the group cannot be trusted to delete data after ransoms are paid–this hit a key component of the attacker-victim relationship, trust.[8] More recently, the operation against the Chinese actor, Twill Typhoon, by the DOJ and the FBI demonstrates the opportunities to disrupt nation state cyber threats.

Seventh, our alliances provide tremendous value in cyber space. Takedown after takedown of ransomware operators and criminal groups make clear the value of intelligence sharing and operational coordination across allied nations. More importantly, when attempting to address the intrusions by nation state actors, such as China and Russia, intelligence sharing agreements between like-minded nations, information sharing on adversary tactics, unified messaging and joint action are all critical in preparing for, stopping and countering adversary action.

Conclusion

Our nation continues to face unprecedented risks in cyberspace and our success in addressing this challenge is dependent on how effectively the government, industry and allies work together. No one organization or company can do this on their own. We need the unique expertise, skills and authorities resident across these communities, and time is not on our side. I applaud the Committee for making this subject its first hearing of the 119th Congress, and I look forward to working with the Committee in the months ahead.

[8] https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/