2020

NSA CYBERSECURITY YEAR IN REVIEW

WELCOME

Building on its information assurance legacy, the National Security Agency (NSA) created a Cybersecurity Directorate in October of 2019 to prevent and eradicate threats to our nation's most sensitive systems and critical infrastructure, with an initial focus on the Defense Industrial Base and its service providers.

The new directorate integrated NSA's threat intelligence, vulnerability analysis, cryptographic knowledge, defensive operations, and diverse technical expertise into one outcome-oriented, public-facing organization: an organization committed to driving combined threat and cybersecurity results that scale across government and industry.

While not all-inclusive, this Year in Review outlines key milestones and mission outcomes achieved during NSA Cybersecurity's first year.

Thank you for your support. We welcome your questions and comments at cybersecurity@nsa.gov.

Contents

LETTER FROM THE NSA CYBERSECURITY DIRECTOR

Eighteen months ago, several colleagues and I discussed the results of an internal study to examine the state of the cybersecurity mission at NSA. The findings were grim. As technology and the cyber threat had rapidly evolved, it was clear we had not always kept pace.

We left the room with a sense of urgency and purpose. A few months later, the Director of NSA, GEN Paul M. Nakasone, announced the establishment of the NSA Cybersecurity Directorate, with a mission to prevent and eradicate cyber actors from systems critical to national security and critical infrastructure, with a focus on the Defense Industrial Base. These systems need particular focus because they hold many of our nation's capabilities and secrets.

NSA's code-making and code-breaking capabilities, cyber intelligence and technical cybersecurity expertise offer distinct contributions to the cybersecurity mission across the U.S. Government, as encryption is the root of trust and a powerful component of every organization's cybersecurity. We generate mission outcomes through combining these with the power of our partnerships – government, private sector, foreign and academia. We aren't alone in the fight against adversary cyber actors, nor do we want to be.

As we began our first year, we took a deliberate approach to building trust by sharing unclassified threat and cybersecurity advice. We forged deeper relationships with our U.S. government and industry partners to deliver better outcomes than any of us could achieve alone.

What's at stake has become even clearer over the past year as connectivity between personal and enterprise networks increased exponentially with COVID, expanding the attack surface malicious cyber actors can leverage. We surged to rapidly deliver capacity for secure telework, and provide intelligence and cybersecurity advice to protect networks used in developing and approving a coronavirus vaccine.

BUILDING TRUST
by sharing unclassified threat and cybersecurity advice.

In the midst of the pandemic, we also worked alongside our partners at CISA, the Federal Bureau of Investigation, and U.S. Cyber Command to secure the 2020 Presidential Election from foreign interference and influence.

This Year in Review describes those efforts. It is a testament to the skill, dedication and resilience of our people - and our partners across the public and private sectors - who worked together throughout the year to defend the United States in cyberspace.

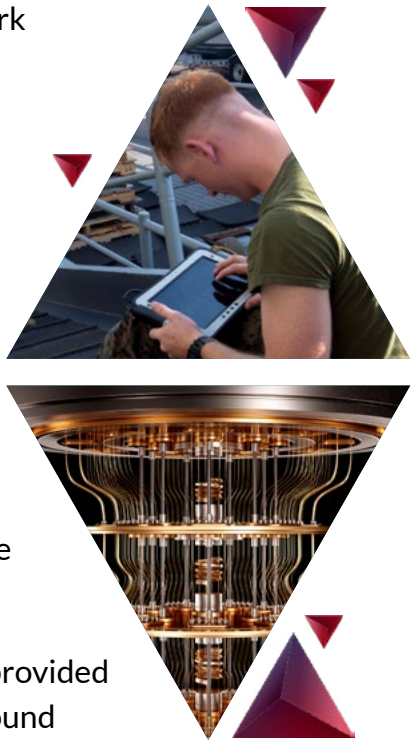
Be well,
Anne Neuberger

KEYS, CODES AND CRYPTOGRAPHY

In our "prevent and eradicate" mission statement, "prevent" is an explicit reference to our production of cryptography that protects the nation's most critical secrets from our most capable adversaries. NSA cybersecurity's code-making mission is complemented by NSA's code-breaking mission. Our ability to build strong cryptography is informed by NSA's complementary Signals Intelligence mission to break foreign adversaries' cryptography.

NSA DROVE MODERNIZATION OF ENCRYPTION working closely with the Joint Staff and Services.

In 2020, NSA focused on modernizing encryption across the Department of Defense (DoD). It began with a push to eliminate cryptography that is at risk from attack due to adversarial computational advances. **This applied to several systems commonly used by the Armed Services today to provide command and control, critical communications, and battlefield awareness.** It also applied to operational practices concerning the handling of cryptographic keys and the implementation of modern suites of cryptography in network communications devices.



More significantly, NSA has now embarked upon a broad effort to modernize the Department's cryptography to make it resistant to exploitation by a quantum computer. **Such a computer is still theoretical, but its development could render large swaths of the U.S. cryptographic inventory obsolete.** Thus, the DoD and the Intelligence Community (IC) are relying heavily on NSA, with substantial fiscal investments to field next-generation encryption. **To this end, NSA has approved a new suite of quantum-resistant cryptographic algorithms** for use in National Security Systems that address a range of potential threats for future use in equipment supporting the warfighter.

Modernizing encryption even extends to the nuclear arsenal. NSA provided the cybersecurity architecture and security engineering for the Ground Based Strategic Deterrent (GBSD). The GBSD is slated to replace the nation's aging intercontinental ballistic missiles.

Foremost in NSA's code-making mission is the production of the nuclear "launch codes" and related materials that would be used should the president ever authorize the launch of U.S. nuclear weapons. NSA also provides the encryption in the communications systems used to convey those orders. NSA's code-making mission extends to the production and distribution of keys, codes, and cryptographic materials used by the U.S. Government and U.S. military to protect communications from adversary eavesdropping and data/information from adversary intrusions.

NSA's keys, codes, and crypto mission rekeyed the entire U.S. Air Force (USAF) F-22 fighter jet fleet, as they do each year. The F-22 fleet of approximately 165 jets is a critical asset in the Air Force arsenal and the cryptographic devices on each jet secure communications and telemetry on and off the aircraft. This is typical of the kind of work NSA does for the Armed Services in their entirety.

Lastly, NSA's role in cryptography also includes the development and deployment of protective technologies. These technologies are important in preventing or detecting adversaries from physically exploiting cryptographic equipment and classified material while they are deployed or shipped around the world. These anti-tamper and tamper-indicating solutions prevent or provide a clear indication if equipment or material has been tampered with or exploited. In 2020,
NSA fulfilled 707 orders delivering 108,421 tamper-indicating products to customers around the world.

CYBERSECURITY PRODUCTS

2020 was notable for the number of Cybersecurity Advisories (CSAs) and other products NSA cybersecurity produced and released. These products are intended to alert network owners, specifically National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB), of cyber threats and enable defenders to take immediate action to secure their systems.

NSA has attributed threat activities to foreign adversaries in detail; calling attention to adversary activity to help network defenders prioritize patching and mitigation efforts, which imposes cost and makes foreign adversary cyber actors less successful across the board. In addition to supporting U.S. and allied network defenders, CSAs also expose foreign adversaries' tools, infrastructure, and tactics, eroding their ability to use the same tradecraft in the future.

While the primary purpose of publicly releasing CSAs is to benefit NSS, DoD, and DIB owners and repel foreign adversaries, a positive byproduct is that the private sector in the U.S. and across the globe can also benefit from this information and can leverage it to better secure their own enterprises for cybersecurity that scales.

NSA CYBERSECURITY CALLED ATTENTION TO ADVERSARY ACTIVITY to help network defenders prioritize patching and mitigation efforts, impose cost, and make foreign adversary cyber actors less successful across the board.

Since its creation, **NSA cybersecurity has publicly released 30 unique, timely, and actionable cybersecurity products. The success of every CSA** is measured by the outcomes it drives, more specifically three factors:

- **A quantitative increase in patching** for our customers
- Impacts to adversary behaviors (i.e. changes in tools, tactics, and procedures)
- **Qualitative assessments of the value-added** to the cybersecurity community (based on feedback received from our customers and observed via open source)

In October 2019, upon discovering that Russian actors were obfuscating their identity by leveraging Iranian implants and infrastructure for cyber operations, NSA and the UK's National Cyber Security Centre partnered to release a first-ever, dual-seal advisory highlighting this activity and providing indicators of compromise.

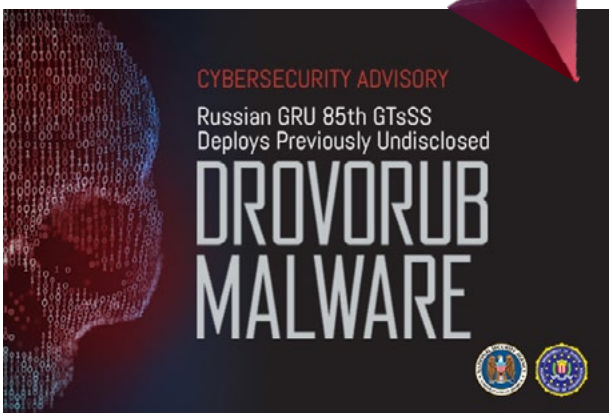
In January 2020, Microsoft released a patch for a critical cryptographic vulnerability in Windows 10 that was discovered and disclosed by NSA. The vulnerability affected millions of users around the world and, if it had been discovered by foreign adversaries, could have been used to undermine cryptographic trust across vast numbers of networks. In a significant departure from past practice, NSA accepted public recognition for this discovery and disclosure. Prior to the patch's release by Microsoft, NSA coordinated a rapid patching strategy for key components within DoD, including U.S. Cyber Command. Due to these efforts, DoD was able to rapidly patch the vulnerability in its enterprise networks. NSA's Cybersecurity Advisory, which was released concurrent with Microsoft's patch, has been downloaded approximately 2 million times.

In May 2020, to communicate technical guidance directly with network defenders, NSA launched its new Twitter handle @NSAcyber. The launch of the Twitter handle was aligned with the release of NSA's CSA on a vulnerability in Exim Mail Transfer Agent. This CSA warned of ongoing exploitation of a known vulnerability in Exim Mail Transfer Agent by a Russian cyber actor, the Russian General Staff Main Intelligence Directorate's (GRU) Main Center for Special Technologies, publicly known as Sandworm.

This advisory was significant for the outcomes it generated. Immediately following the CSA's release, there was an uptick in patching of this vulnerability by NSA customers. Additionally, multiple threat intelligence firms pivoted off the data to write substantive publications, and a variety of information security researchers used the provided indicators of compromise to uncover additional adversary activity. Most importantly, NSA's direct action denied the GRU their tools, infrastructure, and existing accesses, safeguarding a wide array of their intended targets.

NSA launched its new Twitter handle **@NSACYBER.**

In July 2020, **NSA partnered with DHS CISA** to release guidance on how National Security Systems owners, the Department of Defense, the Defense Industrial Base, and other critical infrastructure stakeholders should **secure their operational technologies and industrial control systems**. This CSA was written in response to malicious cyber actors' targeting of critical infrastructure. Public and private sector partners took immediate action, enhancing the security of the nation in cyberspace.



In August 2020, NSA exposed previously undisclosed Linux malware called "Drovorub." Drovorub was developed for use by the Russian GRU 85th GTsSS. Called "truly stunning" and "a major flex" by the cybersecurity community, the comprehensive CSA provided detailed technical analysis, detection techniques, and actionable mitigations, and its public exposure dealt a setback to the GRU's cyber operations.

In October 2020, NSA released a CSA on 25 publicly known common vulnerabilities and exposures. This release was designed to encourage network defenders to prioritize patching and mitigation efforts to defend against cyber adversaries deemed to be the most immediately threatening.

These advisories and more can be found on NSA.gov/cybersecurity-guidance.

ELECTION SECURITY

2020 was notable not just because it was the NSA Cybersecurity Directorate's first year nor because of COVID-19, but also because it was an election year in the United States. Drawing on lessons learned from the 2016 presidential election and the 2018 mid-term elections, NSA was fully engaged in whole-of-government efforts to protect 2020 election from foreign interference and influence. **Cybersecurity was a foundational component of NSA's overall election defense effort.**

NSA's cybersecurity insights supported the Department of Homeland Security (DHS), U.S. Cyber Command, the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) by sharing insights on adversary cyber actors and activities, particularly regarding any indicators of intent to interfere. NSA coordinated across the USG to identify potential threats and vulnerabilities to better understand our adversaries' intent and capabilities, impose costs through campaigns aimed at eradicating foreign adversarial activity, and enable the defensive actions of U.S. domestic agencies by collaborating with key partners including DHS and FBI on sharing indicators of compromise, victim notifications, and release of public Cybersecurity Advisories.

NSA's cybersecurity contributions to sharing knowledge and mitigating election threats included:

Providing almost
4,000
INDICATORS OF COMPROMISE
to partner agencies for subsequent action

Tipping approximately
200
NOTIFICATIONS OF COMPANY/AGENCY COMPROMISE
to partner agencies

Responding to more than
250
INQUIRIES
for additional reporting

Evaluating more than
25
LEADS/TIPS
from partners

RESPONDING TO COVID-19

COVID-19 impacted almost every aspect of American life in 2020: NSA cybersecurity was no exception. In response to this challenge, NSA engaged in several activities of significance, to include providing cybersecurity support to the development of a COVID-19 vaccine, and supporting the Department of Defense's (DoD) shift to telework.

SUPPORT TO OPERATION WARP SPEED

Operation Warp Speed (OWS) is a whole-of-government effort to accelerate the development of a COVID-19 vaccine. Led by the DoD and the Department of Health and Human Services, the OWS team was charged to produce and deliver 300 million doses of safe and effective COVID-19 vaccines.

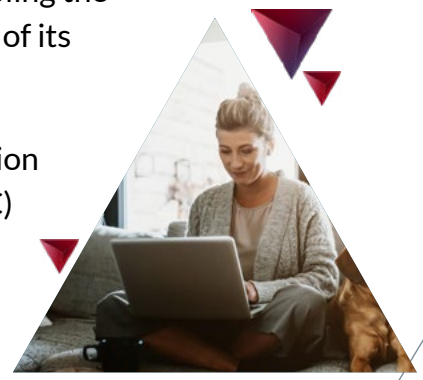
In support of OWS, NSA provided cyber threat intelligence, cybersecurity assessments, and foundational cybersecurity guidance. This included insights on foreign cyber threats to networks, systems, and data related to the development of a vaccine, as well as actionable cybersecurity guidance to protect against these threats. Our nation's vital vaccine production is safer as a direct result of NSA contributions.

The most public aspect of NSA's support to protection of the COVID-19 vaccine development efforts was a joint product issued by NSA, Department of Homeland Security's Critical Infrastructure Security Agency (CISA), and partners in the United Kingdom (UK) and Canada to warn of Advanced Persistent Threat (APT) 29's targeting of organizations engaged in COVID-19 vaccine research in the U.S., UK, and Canada.

APT29, also known as Cozy Bear and other industry identifiers, is almost certainly part of the Russian Intelligence Services, and is trying to steal information and intellectual property. APT29's activities were conducted using custom malware known as WellMess and WellMail. The joint advisory provided indicators of compromise, detection techniques, and actionable mitigations, again, knocking back the efforts of the Russians.

CYBERSECURITY FOR TELEWORK

The COVID-19 pandemic resulted in major changes to the way the DoD operated in 2020, including a rapid shift to secure telework, enabling the Department to continue with vital missions while a good portion of its personnel worked from home.



NSA enabled this transition by reviewing and approving 16 solution registrations based on Commercial Solutions for Classified (CSfC) capability packages, which layer commercial cryptography to protect classified data, enabling approximately 100,000 users to telework securely.

And as more employers across government and industry alike transitioned to working from home, NSA rapidly released multiple written products on how to telework securely and shared them on NSA.gov. These products included an evaluation of how commonly used commercial capabilities implement security such as end-to-end encryption within commercial collaboration services or making source code publicly available. Due to overwhelming feedback from the broader cybersecurity community with regards to the product's value, it was updated three times after its release to incorporate additional assessments of new platforms by customer request.

NSA enabled approximately **100,000 USERS TO TELEWORK SECURELY.**

In further support to U.S. government teleworkers, NSA cybersecurity released products on telework best practices, as well as how to identify and mitigate compromises to personal home networks as more end users began to use them for official business.

STRENGTHENING PUBLIC-PRIVATE PARTNERSHIPS

This past year, NSA cybersecurity prioritized public-private collaboration, invested in cybersecurity research, and made a concerted effort to build trusted partnerships with the cybersecurity community.

NSA's new Cybersecurity Collaboration Center worked throughout 2020 to forge the foundation for new bi-directional cybersecurity partnerships between industry and government. NSA's Cybersecurity Collaboration Center worked with DHS to refocus Enduring Security Framework (ESF) efforts solely on 5G security. To date, ESF has stood up three working panels focused on 5G: cloud security and analytics, standards, and threats to known vulnerabilities in 5G security. The ESF brings members of the Defense Industrial Base and IT SCCs, as well as governmental entities together on areas where a public-private partnership can enhance the security of the nation in cyberspace. These efforts directly support the president's National Strategy to Secure 5G.

Research partnerships keep NSA at the cutting edge of cybersecurity. NSA conducted research on the current and future machine learning needs of cyber defenders. NSA also partnered with universities in the Hacking for Defense program to study hard problems and propose solutions related to Defense Industrial Base cybersecurity and identification of malicious command-and-control infrastructure. Active collaborations with other universities explored the technical and non-technical hard problems in cyber, from trusted computing to cyber threat intelligence. Technical experts from NSA spoke at research conferences and published peer-reviewed papers which advanced the field of cybersecurity.

NSA also shared guidance on algorithms in communitywide post-quantum standardization efforts publicly on NSA.gov. **Sharing such guidance publicly—that would have previously been only shared with government customers—represents just one aspect of NSA efforts to be more transparent and open about the way it secures the nation.**

RESEARCH PARTNERSHIPS KEEP NSA AT THE CUTTING EDGE OF CYBERSECURITY.

NSA also recently received a patent related to Control Flow Integrity (CFI), an NSA-designed, hardware-based advancement to address memory corruption exploits.

Memory corruption exploits allow an attacker to remotely "hijack" code execution, allowing privilege escalation and remote control of administrative functions, giving the attacker complete control of the platform. There have been many attempts to mitigate these memory corruption attacks through software, but the principle of CFI proved that hardware-based mitigations could be cost-effective, efficient, and result in very little performance impact.

CFI development was adopted for incorporation into the x86 and ARM architectures, spanning much of the commodity computation market. This will result in effective hardware-based mitigation that unobtrusively and significantly strengthens the security of the commercial CPU market without user burden. **This multi-year research and development effort highlights NSA's long-term impact on cybersecurity and rich industrial partnerships.**

This year, NSA launched the Center for Cybersecurity Standards (CCSS) to engage with standards bodies on security requirements. As the government increasingly relies on commercial products to secure National Security Systems, this partnership will help ensure requirements are baked into development processes. Currently, CCSS is participating in standards development related to security protocols, cryptographic algorithms, cybersecurity automation, and platform resilience. This work and the center's strategic priorities have been publicly shared on NSA.gov.

As part of a concerted effort in 2020 to be more open in the work that it does, NSA cybersecurity leaders participated in more than 50 speaking engagements, 10 media interviews, and released six videos on topics ranging from the cybersecurity mission to the International Day of the Girl. **NSA Cybersecurity's Twitter handle @NSAcyber was launched to communicate cybersecurity guidance directly to technical audiences and has gained more than 30,000 followers to date.**

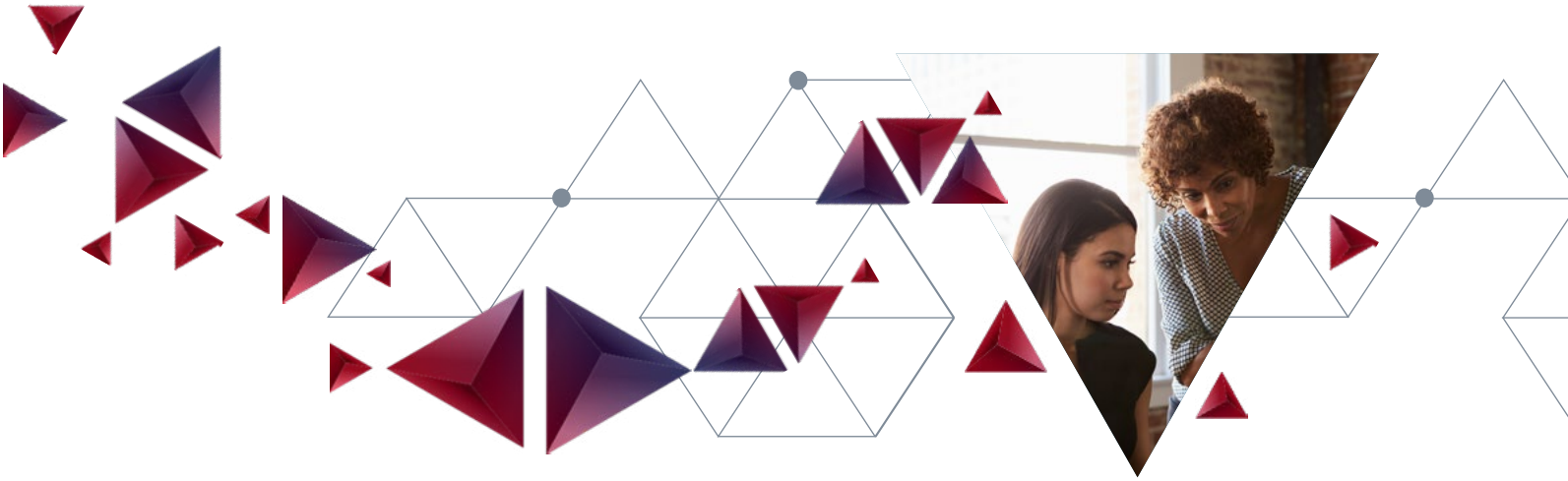
NSA also continues to discover and release cybersecurity vulnerabilities to private industry through an approved, intra-government process. For the past three years, vulnerability disclosures by NSA have trended upward, as the Agency commits to enabling the security of commercial technologies that the U.S. Government, our military, our businesses, and our citizens rely upon.

BUILDING A DIVERSE AND RESILIENT WORKFORCE

2020 was a tough year in several respects. To protect the health and safety of the workforce while continuing to achieve mission success, NSA embraced telework for employees. NSA's cybersecurity workforce shifted what could be worked at an unclassified level to work-from-home, including 100% of its standards and future technologies organization. **NSA's cybersecurity workforce maintains 11 other active use cases approved for unclassified telework**, enabling additional employees to work from home on unclassified activities.

This year, NSA came together to have candid conversations and reinforce our commitment to diversity and equality for each employee. In June, NSA Cybersecurity leaders hosted a series of informal talks to learn more about employees' personal experiences with inequality. Following these engagements, we also launched five diversity and inclusion initiatives focused on advocacy, sponsorship, and hiring. **We also increased outreach and recruiting at historically black colleges and universities.** We're excited about the potential that this brings to recruit diverse talent into our cybersecurity mission.

Despite the challenges of COVID-19, NSA executed an aggressive hiring and recruitment campaign to fill skill gaps and maintain the technical health of NSA's cybersecurity workforce with diverse, top-notch technical talent. The campaign included virtual recruitment panels and events.



NSA cybersecurity is comprised of people with many different backgrounds–and we know that cybersecurity is most effective when we bridge disciplines. So, we closed the year by **launching a peer mentoring program to foster professional networks and development** across our cybersecurity workforce. This program gives employees opportunities to shadow their peers elsewhere in NSA's cybersecurity mission, gaining insights into work they may not be familiar with in their home organizations. Not only does this program foster a stronger esprit de corps within NSA, it also enhances employees' understanding of how their own work is vital to other parts of NSA's cybersecurity mission.

All of these efforts were underpinned by extensive communications campaigns to connect, celebrate wins, and drive modernization efforts. NSA cybersecurity leadership published weekly blogs and videos, with followership that spanned the NSA workforce, the Intelligence Community, and Five Eyes partners.

NEW IDEAS MOVING US FORWARD

In partnership with the Department of Defense (DoD), NSA cybersecurity worked on a number of initiatives in 2020 to revolutionize how DoD addresses cyber threats to the Defense Industrial Base (DIB), weapons and space systems critical to the lethality of the Joint Force, and Defense Critical Infrastructure.

CYBERSECURITY OF THE DEFENSE INDUSTRIAL BASE

The U.S. Defense Industrial Base (DIB) encompasses more than 100,000 companies that produce all of the systems and services upon which DoD and the nation rely to underpin U.S. national security. These companies range from prime contractors with hundreds of thousands of employees to small businesses with just a handful of employees. While they are an attractive target for foreign intelligence services interested in stealing R&D or learning how to compromise weapons and space platforms, these entities vary widely in the resources they invest in cybersecurity. This has left the DIB extremely vulnerable to cyber intrusion and intellectual property theft, and cyber adversaries including China, Russia, and Iran have actively infiltrated the DIB for years.

Stakeholders across the U.S. government recognized that the U.S. DIB was hemorrhaging secrets to foreign adversaries. Something had to change and NSA cybersecurity piloted several new approaches in its first year.

In November 2019, NSA began laying the groundwork to conduct a pilot with the Defense Cyber Crime Center and five DIB companies to monitor and block malicious network traffic based on continuous automated analysis of the domain names these companies' networks were contacting. The pilot's operational phase commenced in March 2020. Over six months, the Protective Domain Name Service (PDNS) examined more than 4 billion DNS queries to and from these companies. The PDNS provider identified callouts to 3,519 malicious domains and blocked upwards of 13 million connections to those domains. The pilot proved the value of DoD expanding the PDNS service to all DIB entities at scale.

The PDNS pilot was just a scenesetter for a much larger game-changer; this past year, NSA began more fully utilizing DoD authorities to rapidly share bi-directional information with DIB entities and their

The DIB is extremely vulnerable to cyber intrusion and intellectual property theft.

NSA CYBERSECURITY IS TAKING ACTION TO PROTECT IT.

service providers. Threat information is only useful if acted on quickly – and if network defenders and threat analysts work directly to connect the dots each can uniquely see. NSA now shares threat intelligence directly with those companies, at classified or unclassified levels, to tip about the threat and most importantly, how to protect against it. The threats to the DIB are some of the most sophisticated the nation faces, and NSA is focusing on sharing information to the "left of theft."

NSA regularly participates in several channels to conduct this information sharing. **One channel of note features over 420 analysts representing 36 DIB companies, significantly expanding the collective ability of the DoD and the DIB to rapidly defend against cyber intrusions by adversary nation-state cyber actors.**

STRATEGIC CYBERSECURITY PROGRAM

How cyber secure is cyber "ready" for combat? In response to legislation that recognized the imperative of protecting key weapons and space systems from adversary cyber intrusions, NSA partnered closely with the DoD CIO, Joint Staff, Undersecretary of Defense for Acquisition & Sustainment, and the Military Services to structure, design, and execute a new cybersecurity program, focused on the most important weapons and space systems, known as **the Strategic Cybersecurity Program (SCP), with the mindset of "stop assessing and start addressing."**

The program initially identified 12 key weapons and space systems that must be evaluated for cybersecurity vulnerabilities that need to be mitigated. This is either due to the existence of intelligence indicating they are being targeted by cyber adversaries or because the systems are particularly important to warfighting. These systems cover all warfighting domains (land, sea, air, cyber, and space). Under the auspices of the SCP, NSA and military service partners will conduct cybersecurity evaluations, and, most importantly, maintain cyber risk scoreboards and mitigation plans accountability in reducing cyber risk to acceptable levels.

ON THE HORIZON

NSA is responsible for ensuring that U.S. Government (USG) IT owners can secure their most valuable information that resides on National Security Systems (NSS) — systems that handle classified information or are otherwise critical to intelligence and military operations. This is accomplished by sharing information on cyber threats and vulnerabilities, assessing cybersecurity posture, and connecting system operators with the mitigation guidance they need. In October 2020, NSA launched an expansive effort across the Executive Branch to understand how we can better inform, drive, and understand the activities of NSS owners to prevent, or respond to, critical cybersecurity events, and cultivate an operationally-aligned community resilient against the most advanced threats. These efforts across the community will come to fruition during the first quarter of 2021 and are expected to unify disparate elements across USG for stronger cybersecurity at scale.

NSA Cybersecurity is also focused on combating ransomware, a significant threat to NSS and critical infrastructure. Ransomware activity has become more destructive and impactful in nature and scope. Malicious actors target critical data and propagate ransomware across entire networks, alarmingly focusing recent attacks against U.S. hospitals. In 2020, NSA formed multiple working groups with U.S. Government agencies and other partners to identify ways to make ransomware operations more difficult for our adversaries, less scalable, and less lucrative. While the ransomware threat remains significant, NSA will continue to develop innovative ways to keep the activity at bay.

CLOSING

While we celebrate the successes of 2020, as we head into 2021 we are going to remain laser-focused on the threat.

China is notable for the scope and scale of its hacking operations. China is using widespread intellectual property theft to build its economy and military. Russia is using cyber operations as a corrosive and destabilizing force across multiple geographic regions. They've waged a disinformation war, often using U.S. infrastructure and technologies, to sow and amplify divisions in society.

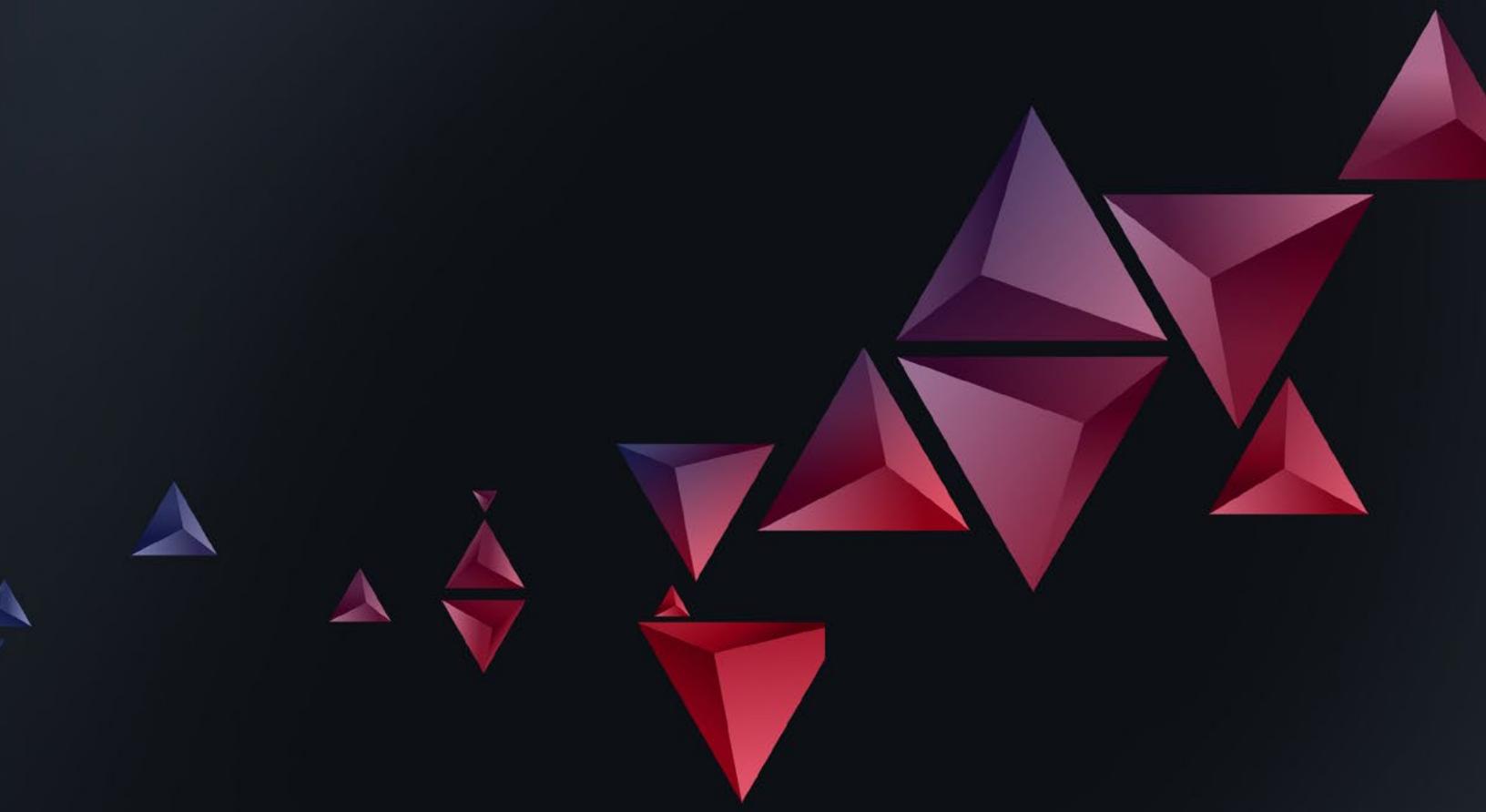
Iran is also a volatile threat and has demonstrated the ability and willingness to launch disruptive cyber operations on critical infrastructure across their region.

In response, NSA will relentlessly pursue our adversaries to keep them out of U.S. networks. We're going to share our threat insights and technical expertise to the fullest extent possible so you can do the same.

Information sharing is only as good as the action it compels. This year, take action. Prioritize cybersecurity investments against the greatest threats to drive down risk. Join us in advocating for innovative public-private partnerships.

Cyber threats will only be countered by the urgency with which we work together to defend against them.

Information sharing is only as good as **THE ACTION IT COMPELS.**



2020 YEAR IN REVIEW

www.NSA.gov/cybersecurity | @NSAcyber | cybersecurity@NSA.gov