U.S. Cyber Command 2022 Year in Review

CODE Wallpaper Widescreen 2

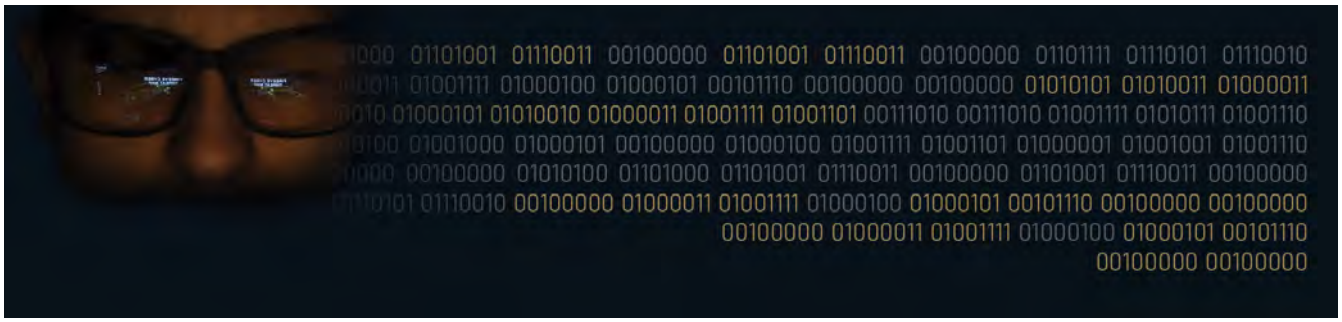
CODE Wallpaper Widescreen 2

By U.S. Cyber Command, Public Affairs / Published Dec. 30, 2022

Fort George G. Meade, Md,

2022 was a banner year for U.S. Cyber Command. Here are some of the year's most important moments:

OWN THE DOMAIN



CYBERCOM defends the nation, countering foreign malicious cyber actors alongside our interagency, industry, and international partners. We are always ready to fight and win as part of the Joint Force. Our ability to defend the nation, operate Department of Defense networks, and support the Joint Force is unmatched.

As the world's premier cyberspace operations force, we are unrelenting in our obligation to Own the Domain of cyberspace. Our actions are informed by our values – a recognition that CYBERCOM wins with its people, seizes the initiative, is always in the fight, goes where others cannot, and partners, empowers and delivers to defend the nation in cyberspace.

Learn more about the CYBERCOM's CODE and efforts to own the domain of cyberspace here.

Cyber Operations

CYBERCOM spent 2022 strengthening relationships with partners and allies across a range of cyber-related capabilities and development opportunities to help meet challenges, get out in front of threats and continue our mission of defending the nation.

CYBERCOM conducted a new global cyberspace defensive operation that exercised information and insight-sharing capabilities across our enterprise and with unified action partners globally. This operation was designed to improve the security and stability of national networks and systems from malicious cyber activities.

The 10-day operation used a library of publicly known malware and all its associated variations as the search criterion. This information was used to assess the integrity of the data, systems, and programs used by the joint force and our key partners. The output from this effort was improving the information-sharing channels across our stakeholders and seeking to mitigate and terminate any threats before they can adversely impact our cybersecurity.

Through such actions, CYBERCOM remains persistently engaged and ensures our nation's cyber defensive capabilities maintain an enduring advantage in cyberspace.

Learn more about here.

Hunt Forward Operations

2022 marked an essential step in the evolution of CYBERCOM when, with the consent of Ukraine, Cyber National Mission Force deployed its largest-ever hunt forward team. The joint CNMF team of U.S. Navy and U.S. Marine Corps operators hunted for malicious cyber activity on Ukrainian networks.

Before Russian forces launched their invasion, the Ukrainian government provided the hunt forward teams access to multiple networks. Working side-by-side with Ukrainian cyber professionals, the hunt forward teams initiated a multifaceted assessment of critical Ukrainian systems to identify suspected malicious cyber activity.

This effort allowed our Ukrainian counterparts to identify and address potential threats on their networks and proactively mitigate any potential adverse effects. When Russia launched what otherwise may have been a crippling cyber-attack in mid-January, Ukrainian cyber professionals, along with the hunt forward team, were able to disrupt or halt the malicious cyber activity before it was able to cause harm.

At the same time, valuable insights into adversarial tools and capabilities were shared with U.S. domestic interagency and public/private industry partners to improve U.S. homeland cyber defenses.

CNMF routinely conducts hunt forward operations as part of CYBERCOM's "Defend Forward" global strategy. Persistent engagement in foreign spaces allows the command to be positioned with unique capabilities and insights not only to learn and understand adversary cyber activities but to respond to threats before they can adversely impact the collective cybersecurity of the U.S. and its partners.

Learn more about Hunt Forward Operations here.

Multinational Cyber Exercises

This year saw two iterations of CYBERCOM's annual exercise, CYBER FLAG: CF22 and CF23-1. CYBER FLAG enhances readiness and interoperability as national and multinational cyber teams must collaborate to navigate various real-world cyber threat scenarios. CF22 included Cyber Protection Teams from every "Five Eyes" nation. It focused on the European Theater, while CF23-1 concentrated on the Asian Pacific Theater and saw the inclusion of cyber teams from France, Japan, the Republic of Korea, and Singapore in addition to Australia, the United Kingdom, and the United States.

In conjunction with the CYBER FLAG exercise activities, CYBERCOM hosted a Multinational Symposium and Tabletop Exercise, in which partner nation representatives and interagency partners collaborated in discussions and working groups to reinforce the impact that training, partnerships, and information sharing have on interoperability.

This once again reinforces the idea that cyber is a team sport!

Read more about CF22 here and CF23-1 here.

Partnerships

CYBERCOM sees partnerships as the lifeblood that differentiates us from our adversaries.

Our Commander, Gen. Paul M. Nakasone, emphasized this during an engagement with more than 230 students, faculty, and staff at a CYBERCOM Academic Engagement Network event in February. Additionally, throughout the year, he participated in more than a dozen engagements with students at universities and colleges across the country, continuing to echo, why partnerships command is key.

“It’s only through these partnerships and collaboration that we continue to make it increasingly difficult for our adversaries to operate," Nakasone said.

In November, CYBERCOM participated in the eleventh bi-annual Cyber Commanders Forum CCF11, hosted by the Estonian Defense Forces Cyber Command. CCF11 was a strategic event in which Cyber Commanders from around the globe came together to exchange ideas in the pursuit of cyber defense. The theme for CCF11 this year was partnerships among public and private entities.

Read more about CCF11 here.

Election Security

For this year’s mid-term elections, we continued our enduring, no-fail mission for CYBERCOM and the National Security Agency, alongside interagency partners at the Department of Homeland Security and the Department of Justice. This whole-of-government effort ensured millions of Americans could cast their votes free from foreign malicious cyber threats. We stood up the joint CYBERCOM-NSA Election Security Group to oversee and direct our efforts to disrupt, deter and degrade foreign adversaries' ability to interfere with and influence our elections. We also partnered with the private sector and U.S. allies, sharing information and building up insight gained from previous election cycles.

“Rest assured, we were doing operations well before the midterms began, and we were doing operations likely on the day of the midterms,” said Nakasone. “This is what persistent engagement is. This is the idea of understanding your foreign adversaries and operating outside the United States.”

Nakasone added, “we see our adversaries’ influence tradecraft overseas, and we are able to share that with the FBI, who's talking with social media companies to say, this is what your foreign adversaries are doing. That's the power of what we can bring to election defense.”

After this year’s successful election season, our vigilance did not end on Nov. 8th. It continues every day into 2023 and beyond.

Learn more here.

Integrated Deterrence

The U.S. National Defense Strategy relies on integrated deterrence: a seamless combination of capabilities designed to convince all potential adversaries that the cost of any hostile activities will significantly outweigh their benefits. Since our efforts in cyberspace touch almost every aspect of what our nation and the military does, CYBERCOM plays an important role in integrating capabilities across the DoD, across domains, and across the spectrum of conflict.

Innovation is paramount for CYBERCOM to remain agile and ready in cyberspace. By enabling the flow of new cyber capabilities developed through science and technology (S&T) research processes, we can create a user-directed pipeline to accelerate the tools our cyber operators need.

In November, we announced a partnership with DARPA aimed at placing new cyber capabilities into operators' hands rapidly.

"Innovation is core to the command's strategy, which is why CYBERCOM and DARPA are working more closely than ever to mature emerging tactical and strategic cyber capabilities and integrate them into operational warfighting platforms," said Mike Clark, director of Cyber Acquisition & Technology, J9 Directorate, at U.S. Cyber Command.

Ultimately, we are finding optimal ways to innovate and integrate our tailored cyber capabilities into specific settings as we work across the DoD and U.S. government along with U.S. partners and allies.

Learn more about the constellation pilot program here.

Cyber National Mission Force Sub Unified Establishment

In December, the Cyber National Mission Force (CNMF) was officially elevated to the Department of Defense's newest subordinate unified command, reflecting the evolution and need for a dedicated, persistent, and professional cyber force. CNMF is the U.S. military's joint cyber force charged with Defending the Nation in cyberspace through full-spectrum operations, including offensive, defensive, and information operations.

The establishment of CNMF as a sub-unified command recognizes the enduring mission to combat foreign malicious cyber actors, reflects CNMF's ongoing success in support of national priorities, and formalizes its organizational structure. Elevation to sub-unified command will drive how forces are presented to CNMF, how personnel will train, and the authorities CNMF will have.

Speaking at the elevation ceremony, Maj. Gen. William J. Hartman, commander of CNMF, said, "the elevation of CNMF to a sub-unified command reflects the incredible dedication, professionalism, and commitment of unit members, past and present."

Read more about CNMF's elevation to sub-unified command here.