



Operation Warp Speed

Security & Assurance

Threat Briefing

(U) Agenda

- OPERATION WARP SPEED (OWS) overview
- Foreign Threats
- Foreign Entities Operating in Cyberspace
- Recommendations

(U) Operation Warp Speed

(U) Our Mission

OWS S&A conducts integrated and synchronized activities across seven security pillars to protect the development, manufacturing, distribution, and administration of U.S. and partner COVID-19 vaccines, therapeutics, and diagnostics while preserving the integrity, stability, and availability of collected data.

(U) Mission Scope

- **Deliver timely and relevant multi domain information to promote threat awareness**
- Threats manifest in the cyber, physical, counterintelligence, and supply chain domains
 - Threats are complimentary and interrelated
 - Example: insider threat provides insight that facilitates cyber espionage operations leveraged to steal intellectual property
- OWS-sponsored participants provide a lucrative target for threat actors
 - Threat actors - cyber criminals, foreign nation-states, and criminal hacktivists

(U) Trusted public-private sector partnerships and cross-sector collaboration pose unique security challenges, which malicious actors will seek to exploit.

(U) Foreign Threats

(U) Principal Adversaries – Strategic View

(U) Russia targets the United States seeking to collect intelligence; erode U.S. democracy; undermine national policies and our foreign relationships; and increase Moscow's global position and influence.



(U) China exploits the openness of American society, especially academia and the scientific community, using a variety of means.

(U) Cuba continues to target the United States, which they see as a primary threat, while Iran continues to unjustly detain U.S. Citizens.



(U) Non-state actors including hacktivist groups, transnational criminals, and terrorist groups attempt to gain access to classified information to support their objectives. They are improving their intelligence capabilities, including recruiting sources and physical and technical surveillance.



(U) While OSINT research has definitively exposed Chinese, Russian, and Iranian targeting of Operation Warp Speed biotechnology research, we have not detected unclassified reports of such activity from Cuba or non-state actors.

(U) What is Beijing Targeting?

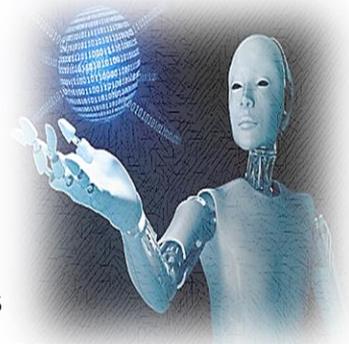
- **(U) Biotechnology**
- (U) Materials and Manufacturing
- (U) Information and Communications
- (U) Artificial Intelligence and Autonomy
- (U) Space and Counterspace Capabilities
- (U) Weapon Systems and Associated Technologies



(U) "Made in China 2025" plan calls for China to be a world leader in the most important technologies of the 21st century — AI, renewable energy, quantum computing, driverless cars, and a wide range of medical technologies.

(U) Technology Pursuits Driving the Threat

- (U) Cultivating talent in advanced machine learning and leading in machine learning theory are cornerstones of China's strategy to dominate AI by 2030.
- (U) China's military modernization is targeting capabilities with the potential to degrade core U.S. military-technological advantages.
- (U) To support modernization, China uses a variety of effective methods to acquire foreign military and dual-use technologies.
 - (U) Cyber espionage and theft
 - (U) Open source information
 - (U) Targeted foreign direct investment
 - (U) Exploitation of Chinese nationals with access
 - (U) Military-to-military exchanges with DoD services



(U) Since 2016, several cases emerged about China using intelligence services and employing other illicit approaches, which violate U.S. laws and export controls, to obtain U.S. national security information and export-restricted items.

(U) China's Theft of U.S. Research

- (U) May 2020: U.S. authorities charged a Chinese national with grant fraud and failing to disclose his employment in China. This Chinese national sought to defraud approximately \$4.1 million in grants from the National Institute of Health to develop China's expertise in the areas of rheumatology and immunology.
- (U) Aug 2020: While working at a U.S. university, a Chinese national was arrested for possibly transferring sensitive U.S. technical data to China's National University of Defense Technology and for failing to disclose his affiliation to the Chinese military, People's Liberation Army. Upon arrest the suspect destroyed the computer hard drive and concealed digital storage devices.



(U) Chinese Espionage Vectors

(U) China's Technology Development Strategy

(U) China takes a multifaceted, long-term, whole-of-government approach to foreign technology acquisition and indigenous technology development.



(U) Human Intelligence

- (U) Employ overt, covert, and clandestine operations.
- (U) Have not been significantly observed using “dead drops.”
- (U) Who are they in CONUS?
 - (U) Diplomats
 - (U) Academics
 - (U) Attachés
- (U) Strong track record of recruiting ethnic Chinese
- (U) Recruit agents from a variety of backgrounds.
- (U) Seek those with both direct and indirect access to sources of U.S. national security information.



(U) Chinese Cyber Espionage

- (U) China has a large, professionalized cyber espionage community.
- (U) They have demonstrated broad capabilities to infiltrate a range of U.S. national security and commercial actors with cyber operations.
- (U) Cyber employed to support intelligence collection against U.S. diplomatic, economic, and defense industrial base sectors.
- (U) Targeted information could benefit China's defense and high-tech industries; insight into U.S. perspectives on key China issues



(U) Foreign Entities Operating in Cyberspace

(U) Advanced Persistent Threat Actor Programs



- Can compromise or remotely access and manipulate control systems, hardware and software across critical infrastructure
- History of disruptive and destructive attacks; assertive even when detected
- Robust and highly adaptable information ops/influence program



- Able to gain access to networks without using advanced capabilities
- Can facilitate localized, temporary disruptive effects on US critical infrastructure—such as disruption of a natural gas pipeline for days-weeks
- Supply chain/insider threat implications for critical infrastructure components
- Aggressive information ops/influence program



- Cyber operations fully integrated into Tehran's national security strategy; espionage
- "Eye for an eye" approach in responding to cyber operations against its interests
- Previously associated with high profile disruptive/destructive cyber attacks abroad
- Uses social media platforms to target US and allied audiences



- Remains a cyber espionage threat; able to conduct disruptive, potentially destructive cyber attacks
- Cyber operations have previously supported regime priorities
- Cyber crime
- Data deletion attacks
- Associated with 2017 "WannaCry" ransomware attack; affected critical infrastructure sectors

(U) Deny...Degrade...Disrupt...

- Adversaries seek to
 - **Delay or inhibit** our ability to produce & deliver viable countermeasures
 - **Disrupt critical systems** for illicit financial gain
 - **Undermine confidence** in the U.S. COVID response efforts and trust the final vaccines or countermeasures
- Adversaries are trying to
 - **Steal Intellectual Property**
 - Research, clinical trials, manufacturing & scale-up
 - **Tamper with, destroy, or deny access** to data & systems
 - Clinical data, Supervisory control and data acquisition (SCADA) systems
 - **Discredit** the veracity of scientific research and related organizations, persons

(U) Cyber Exploitation Methods

- Social Engineering- is the practice of manipulating people in order to get them to divulge information or take an action.
 - Phishing: Cyberactors send emails to elicit information or to gain unauthorized system access
 - Spear-phishing: Cyberactors send emails targeting a specific individual, company, or industry
 - Actors Masquerade as CDC, WHO official communications or colleagues
- Unpatched vulnerabilities on web-facing systems
 - Primarily exploit remote-access
 - Virtual Private Network (VPN) , Remote Desktop Protocol (RDP)
- Third-parties services (e.g. managed services)
 - Home networks or applications of employees teleworking or family members
- Webshells
 - A piece of code or script running on a server that enables remote administration
- Remote / collaboration platforms
 - Office 365, Webex, Google Drive credentials
- Insider Threat

(U) Cyber defense requires vigilance and awareness of vulnerabilities.

(U) Data of Interest

- **R&D for vaccines** (Vx), therapeutics (Tx,) and diagnostics (Dx)
- R&D for **technology, manufacturing, and scaling** of Vx, Tx, and Dx
- Vaccine **components** and **manufacturing techniques**
- **Cyber-Physical systems** for manufacturing & fill finish
- **Clinical trial data** and results
- Candidate **submission data** & communications
- Personal devices & accounts of **high-value individuals**

(U) Organizations Targeted

- Academic institutions & labs
- Biological facilities
- Pharmaceutical companies
- Contract Research organizations (CROs)
- Contract Manufacturing organizations (CMOs)
- Fill/Finish facilities
- Trusted third-parties (esp. IT & security services)
- Hospitals
- Supply chain

(U) Targeted COVID-19 Research

(U) "...U.S. officials accused China sponsoring criminal hackers who are targeting biotech firms around the world working on corona vaccines and treatments. As the FBI, said the Chinese government was acting like 'an organized criminal syndicate.'"



(U) "...The defendants hacked for their own profit but also for the Chinese Ministry of State Security (MSS), a civilian spy agency responsible for counterintelligence, foreign intelligence, and domestic political security, the indictment says. They were aided in that effort by an MSS officer..."

(U) "...China, far more than any other country, has been aggressively stealing valuable medical technology for years. Information on a possible vaccine would be a huge prize..."



(U) "...Reuters reported that hackers linked to Iran tried to break into email accounts at the U.S. drug-maker Gilead Sciences, which has a potentially promising drug to treat the COVID-19 virus..."



(U) "...The National Security Agency, as well as counterparts in Britain and Canada, are seeing persistent attempts by Russian hackers to break into organizations working on a potential coronavirus vaccine..."

(U) Recommendations

(U) Cybersecurity

- Train & protect employees against phishing & email-based attacks
- Patch public-facing systems **quickly**
- Enforce Multi-factor authentication
 - Especially on remote access (VPN, etc.)
- (Off-box) Logging & monitoring access & usage logs of critical assets
- Reduce & monitor admins & admin privileges (granular access control)
- Enforce strong passwords & password rotation
- Ensure regular, robust, and offsite/offline backups of all critical decision data
- [Manufacturing] Logically or physically isolate Operational Technology (OT) from IT networks

(U) Supply Chain and Risk Management

- Understand & monitor relationships with contractors, supply chain, and other 3rd parties
- Prepare for additional activity if your organization is mentioned in the media regarding COVID-19 response – public messaging will result in increased targeting
 - Coordinate external messaging with internal IT security so that patching is up to date prior to release of external messaging related to COVID-19
- Ensure high-profile employees and those with access to critical information practice strong operational and communications security



Engage with your OWS Points of Contact for any questions or to request assistance.

Director of Security and Assurance

Brigadier General Michael McCurry

Email: Michael.mccurry@hhs.gov

Phone: (202) 260-7179

Operations/Information Security

MAJ Jeff West

Email: Jeffery.West@hhs.gov

SIPR: Jeffery.a.west2.mil@mail.smil.mil

Phone: 202-260-0098

Physical/Industrial Security

Ann Marie Smith

Email: Ann.Smith@HHS.gov

Phone: (202) 260-4449

Larissa A. Caton

Email: Larissa.Caton@hhs.gov

SIPR: Larissa.a.caton.civ@mail.smil.mil

Phone: (202) 691-2101

Cybersecurity and Infrastructure Security Agency

Natasha Cohen

Email: Natasha.Cohen@cisa.dhs.gov

Phone: 703-235-5703

Cyber Security

Daniel Bardenstein

Email: Daniel.Bardenstein@hhs.gov

Joshua Zaritsky

Email: Johnsua.Zaritsky@hhs.gov

Counterintelligence

Chris Tolbart

Email: christopher.m.tolbart.civ@mail.mil

Phone: (703) 695-2587

Lashonda Moore

Email: Lashonda.moore@hhs.gov

Phone: (202)-567-1168