LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

China's 14th Five-Year Plan and the Healthcare and Public Health Sector

05/06/2021

TLP: WHITE, ID# ***202105061300***

Agenda

- What Are China's Five-Year Plans (FYPs)?
- How Previous FYPs Guided China's Cyber Targeting
- History of Chinese Targeting of HPH Intellectual Property
- How the Current 14th FYP Relates to the HPH Sector
- Chinese Biological and Genomic Efforts
- Chinese APTs That Previously Targeted the HPH Sector
- Not Just Cyber: The Chinese Insider Threat
- Chinese Government-Connected Universities and Research Intuitions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What Are China's Five-Year Plans (FYPs)?

- The Communist Party of China's (CPC) FYPs are a method of governmental planning inherited from Soviet Russia.
- The CPC's first FYP was from 1953 to 1957
  - Agricultural production → Industrialization
- Second FYP: "Great Leap Forward"
- Early FYP was rigid and metric-oriented → 1980's guidance, not strictly implemented
- Applies to big companies—state-owned or not—and local government leaders
  - Expected to adjust as needed to support the current FYP
- Modern FYPs can focus on various areas of national development to include defense, energy, finance, and healthcare.

Five-Year Plan
2 : "A national governmental program of planned, coordinated, and cumulative economic and social development over a period of five years."
– Merriam-Webster

China's 13th FYP "Made in China" (2016-2020)

- Information technology
  - 2020: Seven Taiwanese semi-conductor companies targeted by suspected Chinese state actors
- Robotics (including AI and machine learning)
- Green energy and green vehicles
  - 2019-2020, APT10 targeted Japanese automotive company
  - 2006-2014, APT41 targeted U.S.-based SolarWorld
- Aerospace equipment
  - 2006-2018, APT10 targeted NASA's Jet Propulsion Laboratory
    - Date range for large APT10 campaign that resulted in a Department of Justice indictment in 2018
- Ocean engineering and high-tech ships
- Power equipment
  - 2006-2014: APT41 targeted Westinghouse Electric Co.
  - 2020: Chinese espionage group Bronze Butler, aka Tick, targeted Japanese electric company

China's 13th FYP "Made in China" (2016-2020)

- New materials
  - 2006-2014: APT41 targeted Allegheny Technologies Inc., United States Steel Corp., Alcoa Inc.
- Medicine and medical devices
  - 2019-2020: APT10 targeted Japanese pharmaceutical company
- Agriculture machinery
- Railway infrastructure

Other Targeting

- NSA warning from 2020: "NSA is aware that national security systems, defense industrial base, and Department of Defense networks are consistently scanned, targeted, and exploited by Chinese state-sponsored cyber actors"
- 2020: APT 41 targeted multiple German industrial firms

History of Chinese Targeting of HPH Intellectual Property

- July 2020
  - FBI Director Christopher A. Wray warned that “at this very moment, China is working to compromise American health-care organizations, pharmaceutical companies and academic institutions conducting essential [COVID] research.”
- May 2020
  - A joint statement by the FBI and the Department of Homeland Security stated that the FBI was investigating "the targeting and compromise of U.S. organizations conducting COVID-19-related research" by the Chinese military and other Chinese hackers.
- December 2019
  - Dr. Ross McKinney Jr., Chief Scientific Officer of the Association of American Medical Colleges: “Among the 6,000 Chinese scientists who have received grants from the National Institutes of Health, around 180 are under investigation for possible violation of intellectual property law.”
- December 2019
  - Zaosong Zheng “acknowledged that he had stolen eight of the samples [cancer cells] and had replicated 11 more based on a colleague’s research. Two other Chinese scientists who worked in the same lab as Mr. Zheng had successfully smuggled stolen biological material out of the country, prosecutors say.”
- As of November 2019
  - “71 institutions, including many of the most prestigious medical schools in the United States” were investigating potential theft of intellectual property, the majority of the investigations being related to biomedical research.

Overall → Self-Sustainment

HPH Specific Areas for Development

- Healthcare
- Elder care
- Clinical medicine
- Strategic industries → **Biotechnology**

A February 2021 report by the National Counterintelligence and Security Center stated that U.S. healthcare data may be particularly attractive and valuable to China due to the ethnic diversity of the U.S. population.

U.S. has fewer safeguards on HPH data:

- Medical
- Healthcare
- Research

Used in the development of artificial intelligence

14th FYP: 2021-2025

Additional information can be found in the March 19, 2021 Federal Bureau of Investigation (FBI) and the Office of Private Sector (OPS) report, *TLP:GREEN Liaison Information Report (LIR) 210319-007*

"The intelligence is clear: Beijing intends to dominate the U.S. and the rest of the planet economically, militarily and technologically."
- Former Director of National Intelligence, John Ratcliffe

What We Have Seen

- Chinese People's Liberation Army (PLA) has stated concerns about "national biological security (and) defense"
  - Infectious diseases
  - Military potential
  - Offensive applications of biotechnology
    - "Specific ethnic genetic attacks"
    - New synthetic pathogens that are "more toxic, more contagious, and more resistant"
- Human testing to biologically enhance Chinese soldiers
  - Clusters of regularly interspaced short palindromic repeats (CRISPR)

What We Could See

- Personally identifiable information (PII) + personal health information (PHI) + large genomic data sets =
  - Blackmail
  - Targeting of health conditions
  - Surveillance
  - Manipulation
  - Extortion

Chinese APTs That Previously Targeted the HPH Sector

- Chinese Advance Persistent Threats (APTs) identified by HC3 that targeted entities within the HPH Sector dealing with healthcare, medical devices, pharmaceuticals, biotechnology, and scientific research, and consulting:

  - APT1
  - APT10
  - APT18
  - APT41
  - APT24
  - Deep Panda
  - APT22
  - APT20
  - APT9

HC3 Chinese APT Focused Products:

- HC3 Brief November 19, 2020 - Chinese State-Sponsored Cyber Activity
- HC3 Brief June 9, 2020 - APT and Cybercriminal Targeting of HCS
- HC3 White Paper March 26, 2020 - APT41 Citrix and Zoho Attacks on Healthcare
- HC3 Brief October 24, 2019 – APT41

2019 Senate Investigation on the Thousand Skills/Talents Program

- Chinese state-sponsored program for theft of American research
- 2,000 high-quality overseas talents, including scientists, engineers, entrepreneurs, and finance experts
- Those that participated are rewarded with “salaries, research funding, lab space and other incentives”
- Can involve theft of files, physical research, and electronic files/research
- Those working on behalf of the Chinese government submit false information in applications for U.S. grants
- Starting in 2018, China began removing all references to the program online, in addition to a disapproved use of its name

Song Chen

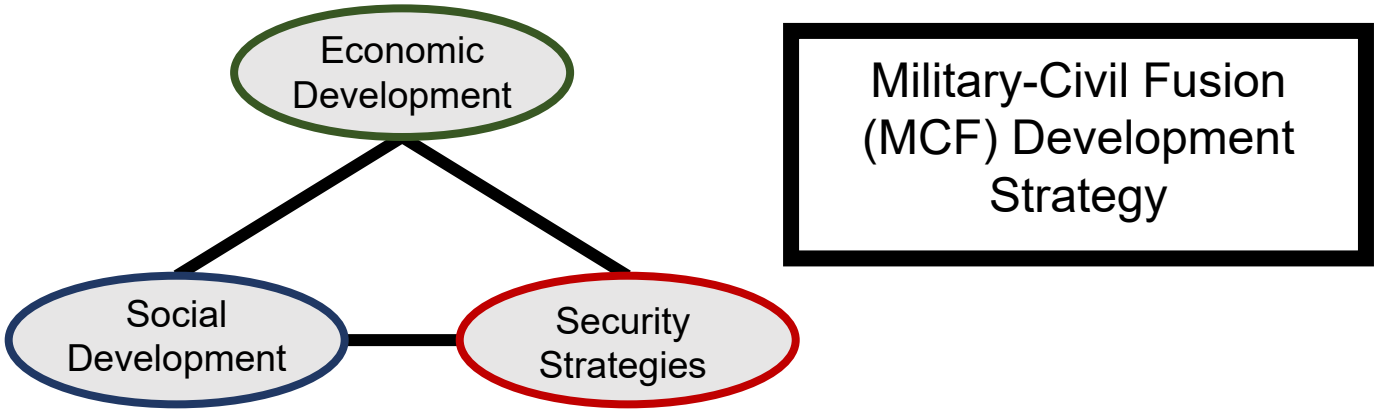
Juan Tang

Zaosong Zheng

- The “Seven Sons of National Defense”:

  1. Harbin Institute of Technology
  2. Nanjing University of Science and Technology
  3. Northwestern Polytechnical Institute
  4. Beijing Institute of Technology
  5. Harbin Engineering University
  6. Beihang University
  7. Nanjing University of Aeronautics and Astronautics

- People’s Liberation Army-affiliated laboratories: Tsinghua University, Beijing University, and Shanghai Jiaotong University, North University of China
- Defense industry, other state-owned enterprises (SOEs), and quasi-private companies



Reference Materials

References

- “five-year plan noun, often capitalized,” Merriam-Webster. Accessed on April 28, 2021. https://www.merriam-webster.com/dictionary/five-year%20plan
- "What is China’s five-year plan?," The Exonomist. Accessed on April 28, 2021. https://www.economist.com/the-economist-explains/2021/03/04/what-is-chinas-five-year-plan
- “Five-Year Plans,” Britannica. Accessed on April 28, 2021. https://www.britannica.com/topic/Five-Year-Plans
- “Chinese hacking groups to ramp up cyber attacks on some industries, experts say,” CSO. Accessed on April 28, 2021. https://www.csoonline.com/article/3384927/chinese-hacking-groups-to-ramp-up-cyber-attacks-on-some-industries-experts-say.html
- “Year in review,” Verizon. Accessed on April 28, 2021. https://enterprise.verizon.com/resources/reports/dbir/2020/year-in-review-2019/
- “Significant Cyber Incidents,” CSIS. Accessed on April 28, 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- “Chinese Hackers Target Japanese Organizations in Large-Scale Campaign,” SecurityWeek. Accessed on April 28, 2021. https://www.securityweek.com/chinese-hackers-target-japanese-organizations-large-scale-campaign
- “APT 10 GROUP,” FBI. Accessed on April 28, 2021. https://www.fbi.gov/wanted/cyber/apt-10-group
- “Chinese hacker group targets Japanese and South Korean businesses,” Nikkei. Accessed on April 28, 2021. https://asia.nikkei.com/Business/Technology/Chinese-hacker-group-targets-Japanese-and-South-Korean-businesses
- “Vast Dragnet Targets Theft of Biomedical…,” The New York Times. Accessed on April 28, 2021. https://www.nytimes.com/2019/11/04/health/china-nih-scientists.html

References

- “DOJ says five Chinese nationals hacked into 100 U.S. companies,” NBC News. Accessed on April 28, 2021. https://www.nbcnews.com/politics/justice-department/doj-says-five-chinese-nationals-hacked-100-u-s-companies-n1240215
- “FBI director says China seeks to compromise U.S. firms researching coronavirus,” The Washington Post. Accessed on April 28, 2021. https://www.washingtonpost.com/national-security/fbi-china-coronavirus/2020/07/07/40961c2e-c073-11ea-b4f6-cb39cd8940fb_story.html
- “Feds warn that Chinese attempts to hack health care, drug firms threaten U.S. COVID-19 response,” NBC News. Accessed on April 28, 2021. https://www.nbcnews.com/politics/national-security/feds-warn-chinese-attempts-hack-health-care-drug-firms-threaten-n1206151
- "Stolen Research: Chinese Scientist Is Accused of Smuggling Lab Samples,“ The New York Times. Accessed on April 28, 2021. https://www.nytimes.com/2019/12/31/us/chinese-scientist-cancer-research-investigation.html
- “China has done human testing to create biologically enhanced super soldiers, says top U.S. official,” NBC News. https://www.nbcnews.com/politics/national-security/china-has-done-human-testing-create-biologically-enhanced-super-soldiers-n1249914
- "China’s five-year plan focuses on scientific self-reliance,“ Nature. Accessed on April 28, 2021. https://www.nature.com/articles/d41586-021-00638-3
- “"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,“ The United States Department of Justice. Accessed on April 28, 2021. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

References

- “China’s Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security,” The National Counterintelligence and Security Center. Accessed on April 28, 2021. https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf
- “Government Report Finds China Could Use Medical Data for Blackmail,” Health IT Security. Accessed on April 28, 2021. https://healthitsecurity.com/news/government-report-finds-china-could-use-medical-data-for-blackmail
- “China’s Military Biotech Frontier: CRISPR, Military-Civil Fusion, and the New Revolution in Military Affairs,” The Jamestown Foundation. Accessed on April 28, 2021. https://jamestown.org/program/chinas-military-biotech-frontier-crispr-military-civil-fusion-and-the-new-revolution-in-military-affairs/
- “APT and Cybercriminal Targeting of HCS,” Health Sector Cybersecurity Coordination Center. Accessed on April 28, 2021. https://www.hhs.gov/sites/default/files/apt-and-cybercriminal-targeting-of-hcs.pdf
- “Threats to the U.S. Research Enterprise:China’s Talent Recruitment Plans,” Permanent Subcommittee on Investigations. Accessed on April 28, 2021. https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf
- “Military and Security Developments Involving the People’s Republic of China,” Office of the Secretary of Defense. Accessed on April 28, 2021. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF
- “UPDATED: FBI arresting visiting researchers, including one at Stanford, claiming they were working for China’s military,” Daily Post. Accessed on April 28, 2021. https://padailypost.com/2020/07/24/researcher-at-stanford-accused-of-working-for-chinese-military/

Questions

Upcoming Briefs

- “API Security for HPH” – 5/20

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV