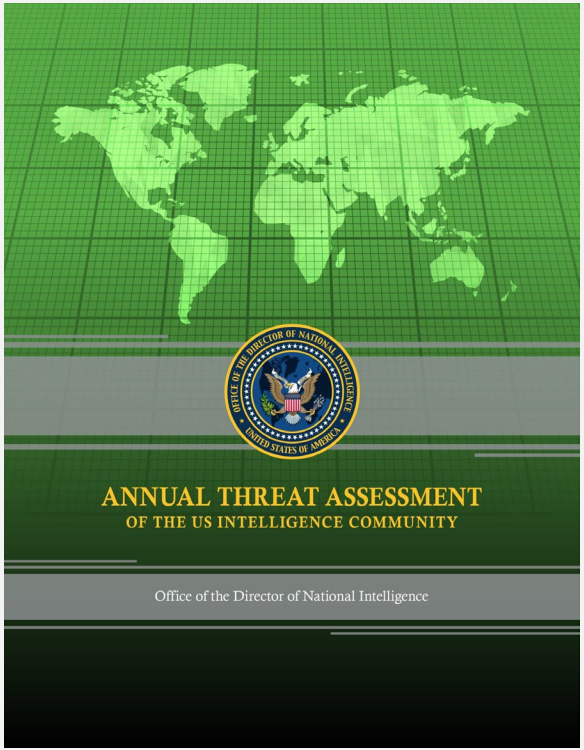
CHINA CYBER CAPABILITIES



https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

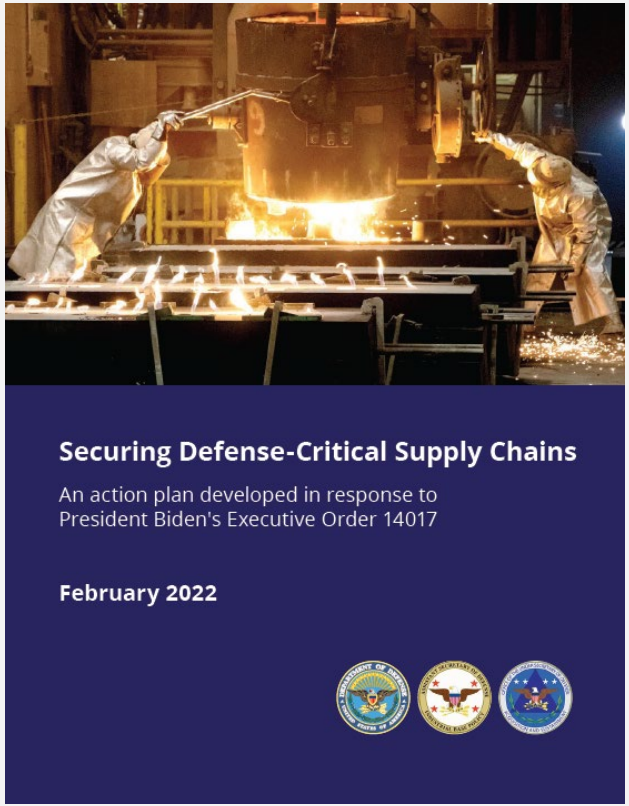
"We assess that China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat. China's cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US homeland, suppression of US web content that Beijing views as threatening to its internal ideological control, and the expansion of technology-driven authoritarianism around the world." (p. 8)

CHINA IN THE SUPPLY CHAIN

"DoD has several specific areas of risk resulting from the scale of China's investments and its technology transfer:

- Supply chains for U.S. military equipment and services are increasingly owned by Chinese firms.
- China's targeted investments to close the gap in capabilities between its military and the U.S. military.
- Industrial espionage and cyber theft mean key defense designs and plans are in Chinese hands.
- There is no agreed upon list of technologies to protect for the future though an effort exists today to delineate technologies critical to current acquisition programs (JAPEC7)." (p. 4)

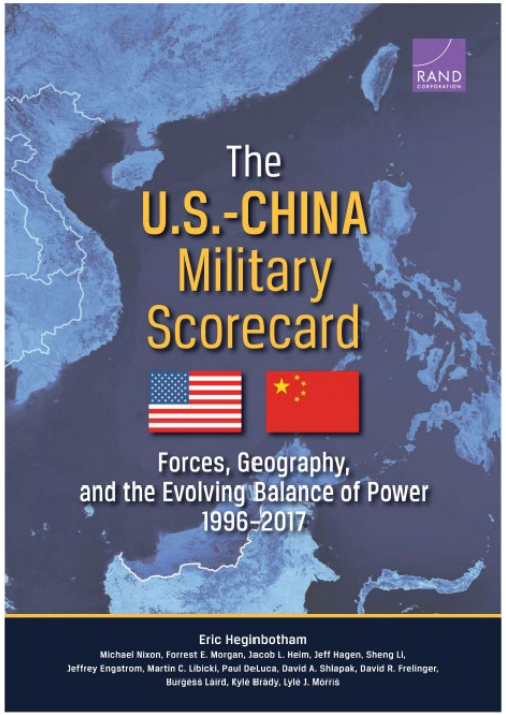
CYBERSECURITY - SCRM



"A focus on Cybersecurity-Supply Chain Risk Management (C-SCRM) should be an overarching priority for supply chain cyber resilience. C-SCRM efforts manage supply chain risk by identifying susceptibilities and vulnerabilities to cyber-threats throughout the supply chain and developing mitigation strategies to counter those threats whether presented by the supplier, the supplier's products and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal)" (p. 54 - 55)

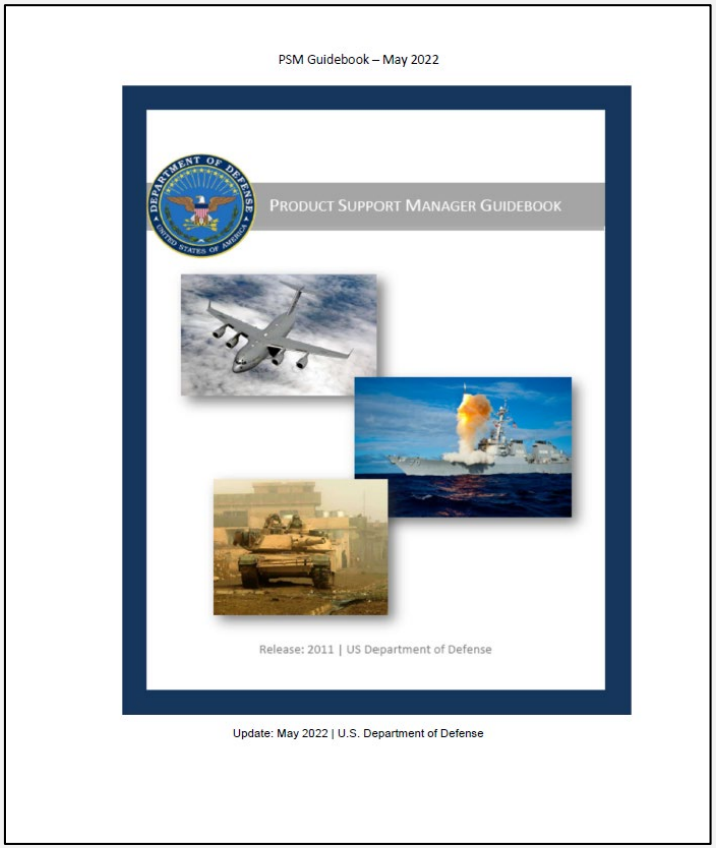
https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

LOGISTICS THREATS



"U.S. logistics systems are more vulnerable to cyber attack than are many other parts of the military establishment. Nevertheless, to affect U.S. operations, Chinese cyber operators have to execute a three-bank shot: penetrating systems, translating penetrated systems into undetected (and, hence, uncorrected) logistical system errors, and inducing a significant, negative effect on operations." (p. 261)

PRODUCT SUPPORT MANAGER



Cybersecurity is mentioned 16 times. These mentions require the following PSM skills:

- How to understand cybersecurity risks and supply chain risk impacts?
- Use a cybersecurity and intelligence threat assessment?
- Understand a Program Protection Plan (PPP) and its attachment in the Cybersecurity Strategy (CSS)?
- Understand a DIB contractor for their cybersecurity assessments - NIST 800-171 self-assessment, POA&M, SPRS entry, DCMA assessment, CMMC certification (future requirement), Protection of FCI, etc..
- Work effectively with Cybersecurity SMEs
- Understand a cybersecurity vulnerability assessment, cybersecurity scans, and cybersecurity test results (penetration test, Cyber Table Top, CVPA, adversarial assessment, etc.)
- Understand/perform elements of a cybersecurity operational mission risk assessment
- Understand/perform elements of a supply chain risk assessment