Bryce S. Pedicini

- Age 27
- Former Chief Fire Controlman
- Arrested May 19, 2023

  Found guilty at a general court-martial of Attempted Espionage and Attempted Violation of Lawful General Order.

CDSE

Center for Development of Security Excellence

CASE STUDY

Conspiracy to intentionally cause damage

WHAT HAPPENED

Bryce Steven Pedicini was a former Chief Fire Controlman (Aegis) previously assigned to the USS Higgins (DDG 76), who wrongfully transported classified information while stationed at Yokosuka Naval Base, Japan. Pedicini was found guilty at a general court-martial of UCMJ Article 103a (Attempted Espionage), Article 92 (Failure to Obey a Lawful Order), and Article 80 (Attempted Violation of a Lawful General Order).

According to the Navy Criminal Investigative Service (NCIS), beginning as early as October 2022, Pedicini was contacted by, and began sharing national defense and classified information with, an unknown representative from a foreign government. Pedicini had reason to believe this information could be damaging to the U.S. and beneficial to the foreign nation.

Pedicini engaged with the foreign government representative under the guise of writing research papers, a tactic increasingly used by foreign adversaries to obtain classified and unclassified national defense information.

Beginning in October 2022, an unknown foreign national contacted Pedicini via Facebook Messager under the guise of being a defense researcher and requested information about United States military capabilities and strategies in the INDO-PACOM area of responsibility. This foreign agent offered Pedicini money in exchange for writing research papers and providing information. The foreign agent provided incentives for classified information, increasing the payout based on the value and sensitivity of the information.

Pedicini sent multiple documents to the agent from November 2022 to May 2023, according to court records, and he sent the agent photographs of material accessed on the military's secure internet protocol router (SIPR) on May 8, 2023.

Pedicini was detained by NCIS on May 19, 2023, and placed into pre-trial confinement by his command.

INDICATORS

Access Attributes – Pedicini used his access to classified spaces to collect military information and wrote research papers based on classified and sensitive information for the foreign agent.

Technical Activity – Pedicini sent multiple military documents and photographs of material accessed from the military's SIPR.

Social Engineering – An unidentified foreign agent first contacted Pedicini on Facebook in October 2022, claiming to be a "defense researcher" from Japan. According to court filings, the foreign agent offered Pedicini "money in exchange for information about the United States military capabilities and strategies." The agent also told Pedicini he could receive "more money based on the value and sensitivity of the information [Pedicini] could provide and specifically asked for classified information."

IMPACT

- Chief Pedicini was charged with, inter alia, seven specifications of violating Article 103a for alleged espionage and seven specifications of violating Article 134 as crimes not capital, with the alleged crimes being violations of the Espionage Act.
- A military judge in San Diego sentenced Pedicini, of attempted espionage and other charges, to 18 years in military prison. The judge also reduced his rank to E-1 and issued a dishonorable discharge.
- Pedicini was initially charged with espionage. However, the appointed judge opted to convict Pedicini of the lesser offense of attempted espionage, citing the classified nature of the event.

ADDITIONAL INFO

- The NCIS investigation revealed that Pedicini delivered classified and national defense information to a representative of a foreign government as early as November 2022 and had reason to believe the information would be harmful to the U.S. or advantageous to the foreign nation.
- The foreign agent operated under the guise of writing research papers, a tactic increasingly used by foreign adversaries to obtain classified and unclassified national defense information.
- Pedicini attempted to share photos of a SIPR Network while back in Japan, just prior to his arrest. Organizations, supervisors, and co-workers should report violations of security protocols as well as personnel acting outside of their norm. Living in a digital world, it is important to get ahead of the threats and be both proactive and predictive in the ways we approach cybersecurity.

Questions to consider:

- What efforts could be implemented in your organization to enhance awareness of the real dangers associated with social engineering attempts?
- What steps can organizations take to reduce the risk of employees and coworkers becoming an insider threat?

Resources for further exploration:

- Phishing and Social Engineering: Virtual Communication Awareness Training DS-IA103.06
  (https://www.cdse.edu/Training/eLearning/DS-IA103/)
- Insider Threat Indicators Job Aid
  (https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf)
- Insider Threat Mitigation Guide – CISA
  Insider Threat Mitigation Guide (cisa.gov)

Supporting Through Reporting!

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager