21st Annual National Defense Industrial Association
Systems and Mission Engineering Conference

Enhancing DoD Technological Advantage





Mr. Brian D. Hughes

Office of the Under Secretary of Defense for
Research and Engineering

October 25, 2018

These Are Not Cooperative R&D Efforts

XIAN Y-20

C-17

Hongjian-12 Red Arrow

Javelin

HUMVEE

Dongfeng EQ2050

LIJAN SHARP SWORD

X-47B

Agenda

- The threat starts early
- Engaging research protection at the earliest stages
- Techniques to prioritize controlled technical information for protection efforts
- Use of critical intelligence parameters to monitor operational threats
- Development of counterintelligence parameters to alert programs of strategic adversary attempts to acquire program technology through use of joint ventures, etc.
- Working with Counterintelligence and Law Enforcement entities
- Inclusion of regulatory clauses to strengthen government and industry options
- Industry's role in strengthening the defense industrial base in support of the DoD's effort to maintain military and technology advantage

Threat Starts Early: *Duke University Graduate Student Transfers Intellectual Property to China*

Background

- In 2006, a Duke lab created a prototype "invisibility cloak" to conceal objects from microwave detection for an AFOSR project.
- Ruopeg Liu, a Chinese PhD student working on the project, initiated collaboration with a Chinese research lab, with agreement from Duke faculty.
- In 2009, Liu published new research in collaboration with the Chinese lab for a new invisibility cloak, which could work at a broad spectrum of frequencies from 10 megahertz to 18 gigahertz, and can be produced in significantly less time.
- Unknown to his faculty, Liu allegedly began sending intellectual property and research to the Chinese lab.
- According to an FBI report, "A Chinese national targeted the lab and created a mirror institute in China."
- The episode cost Duke significantly in licensing, patents, and royalties and kept the Duke faculty from being the first to publish groundbreaking research.
- The FBI never charged Liu with a crime.

Who is Ruopeng Liu

- Liu is selected at age 29 as top-level "863 specialist" in metamaterials, a national honor rarely granted to someone so young.
  - "863" is a code name for top-level government-sponsored research project.
- His net worth is $1.3B, and serves as President of Kuang-Chi Institute of Advanced Technology. Dr. Liu is the Founder of Kuang-Chi Innovative Technology Limited.
- Chinese President Xi Jinping toured a few technology companies in Shenzhen after taking office in 2012, – Kuang-Chi Institute was first stop his delegation visited.

Impact

- **March 2018: Local media reports China is mass producing metamaterials in a state-run lab that reportedly functions as 'invisibility cloaks' and could be used to make fighter jets impossible to detect.**
- **Chinese news platform Sina reported the assembly line is directly related to the military and the materials will likely be used to camouflage J-20 fighter jets.**

SOURCE: https://www.dukechronicle.com/article/2017/10/how-one-graduate-student-allegedly-stole-duke-research-to-create-a-billion-dollar-chinese-company

Strategic competitors are reaping the benefits of U.S. research

Engaging Research Protection at the Earliest Stages

- **Tailored Technology Control Plans for Controlled Research (Proprietary and Dissemination controls)**
  - Authorized personnel
  - Dissemination and publication rules
  - Physical security
  - Information technology security
  - Export Control and Data Security Training
  - Conduct Background Check (Criminal, Credit) of Project Personnel
  - U.S. Government Restricted Party List Screening
    - Persons and Entities convicted of export control violations
- **Hosting International Visitors**
- **Foreign Travel Notification**
  - Limit unpublished research
  - Export License for data taken overseas
- **Dedicated Security Staff**
  - Export Controls
  - Basic Security
  - IT Security

Source: See notes

Robin Rasor, Executive Director of Duke Office of Licensing and Ventures:

"It's kind of like when you get married. You don't want to have a prenup but sometimes it makes sense to have a prenup. So, we do collaboration agreements when we have faculty collaborating with another university, and often those agreements do provide for what happens if there are inventions."

SOURCE: https://www.dukechronicle.com/article/2017/10/how-one-graduate-student-allegedly-stole-duke-research-to-create-a-billion-dollar-chinese-company

Prioritizing Technology Protection Efforts for Increased Effectiveness

Problem: **Amount of technology exceeds analysis and protection capability**

- Further refinement bounds the problem while still maintaining a baseline of protection

Technology prioritization criteria:

- Focus on DoD's Critical Programs & Technologies
  - Determine consequence if technology is cloned or countered by an adversary
  - Determine exclusivity of production by U.S. controlled production entities
  - Determine the likelihood of strategic competitors need to obtain the technology or technical information about use of technology

Bounding technical information enables DoD to focus technology protection assets

Use of Critical Intelligence Parameters (CIPs) to Monitor Threats

- **CIPs identify thresholds that, if breached, indicate an adversary's potential to substantially reduce the performance or even defeat the capability of the weapon system undergoing development.**
  - Developed by the Acquisition and Requirements Communities and monitored by the Intelligence Community
  - Provide indications and warning to enable changes to requirements and acquisition programs to outpace the threat

Source: GAO-17-10 Report on Defense Intelligence Nov 2016

- **CIPs can be used to monitor technology transfer threats**
  - Provide warning to protect key programs and research
  - Continuous monitoring by Intelligence organizations

CIPs provide another tool for technology protection

Develop Critical Intelligence Parameters

- **Establish a Critical Intelligence Parameter (CIP)**
  - Acquisition and Requirements communities determine what items require monitoring
  - CIP needs to clearly articulate what aspect of technology protection needs to be monitored
  - Formally communicate to the Intelligence Community (IC) to review and monitor
- **Monitor Reporting**
  - IC performs constant evaluation of intelligence reporting for CIP breaches
- **Communicate**
  - IC report breaches to Acquisition and Requirements communities for action
  - CIP breach triggers a review process to resolve or mitigate breach
- **Revalidate**
  - Acquisition and Requirements communities should revalidate CIP periodically to ensure the parameters still reflect program priorities

IC brings multiple capabilities to the fight. Leveraging them in unique ways is essential to bring them to the fight

Working with Intelligence, Law Enforcement & Security Entities

- **Counterintelligence/Law Enforcement**
  - Collect against adversary activity
  - Field presence, facility security analysis, investigations
  - Assess CI threat
- **Intelligence**
  - Identify adversary technology needs
  - Collect against adversary
- **Security**
  - Integrate Counterintelligence/Security posture
  - Coordinated Security Classification Guides
  - Proactive Classification Guide Development by Defense Industrial Base
  - Contractor facility reports and vulnerability assessments tailored to individual Critical Programs and Technologies
  - Contractor threat education

Team effort: Better integration enables more effective protection

Regulatory Clauses to Strengthen Government and Industry Options

- **32 CFR Part 236.4 DoD launched the Defense Industrial Base Cybersecurity (DIB CS) program in 2007**
  - Voluntary program enables Government-Industry threat information sharing, industry cyber incident reporting, and damage assessment of information losses
  - Currently 350 partners and ~210,000 threat information products shared
  - DIB Enhanced Cybersecurity Services (DECS) provides additional engagement with commercial service providers
- **DFARS 252.204-7012 published Nov 18, 2013 requires mandatory reporting of compromised Unclassified Controlled Technical Information**
  - Required reporting within 72 hours of discovery of any reportable cyber incident
  - Reportable cyber incidents include:
    - A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.
- **DFARS 252.204-7012 updated with interim rules Aug 26, 2015/Dec 30, 2015 and finalized Oct 21, 2016 to address safeguarding**
  - Covered Defense Information
  - Operationally Critical Support
  - Enables submission of the malicious software associated with the cyber incident to DoD (if the contractor discovers and is able to isolate)
  - Does NOT enable Government - Industry threat information sharing
  - Requires submission of media for cyber incident damage assessments

Successful cyber defense requires effective government–industry information sharing

Industry's Role

Strengthening the DIB/National Security Innovation Base (NSIB) to Maintain DoD Technology Advantage:

- **Identify crucial elements for protection up front**
  - **Requires coupling technical know how with CI/LE/Security expertise**
- **Identify illegal and unethical practices**
- **Examine Joint Ventures for inadvertent technology transfer**
- **Identify collaborative actions**
- **Engage international partners**
- **Identify U.S. Industry needs**
- **Identify other means to enhance the competitiveness of U.S. Industry**
- **Report (e.g., cyber incidents, media theft and loss, suspicious contacts, and insider threats)**
- **Consider joining the DIB CS program:**
  - Enables information sharing
  - Join and contribute to the DIB CS program at http://dibnet.dod.mil/
- **Maintain an open dialogue with all protection stakeholders**
  - Counterintelligence, Law Enforcement, Network Security, etc.

DIB is a critical partner in preventing unauthorized access to precious U.S. intellectual property and manufacturing capability by adversaries

Conclusion

- **DoD must enhance our technological advantage in a complex and multifaceted space**
  - Strategic competitors leverage not only illegal means to steal our technology, but also legal yet unethical means to transfer technology at every opportunity
  - Government employs a multi-pronged approach such as monitoring CIPs and planned joint ventures, working with law enforcement and counterintelligence entities, regulations, and enhanced protections applied to U.S. critical programs and technologies
  - DIB role is crucial to strengthening and maintaining U.S. military and technological advantage

"[Strategic Competitors] have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals." 2018 National Defense Strategy of the United States of America

DoD Research and Engineering Enterprise
Solving Problems Today – Designing Solutions for Tomorrow










Questions

Mr. Brian D. Hughes

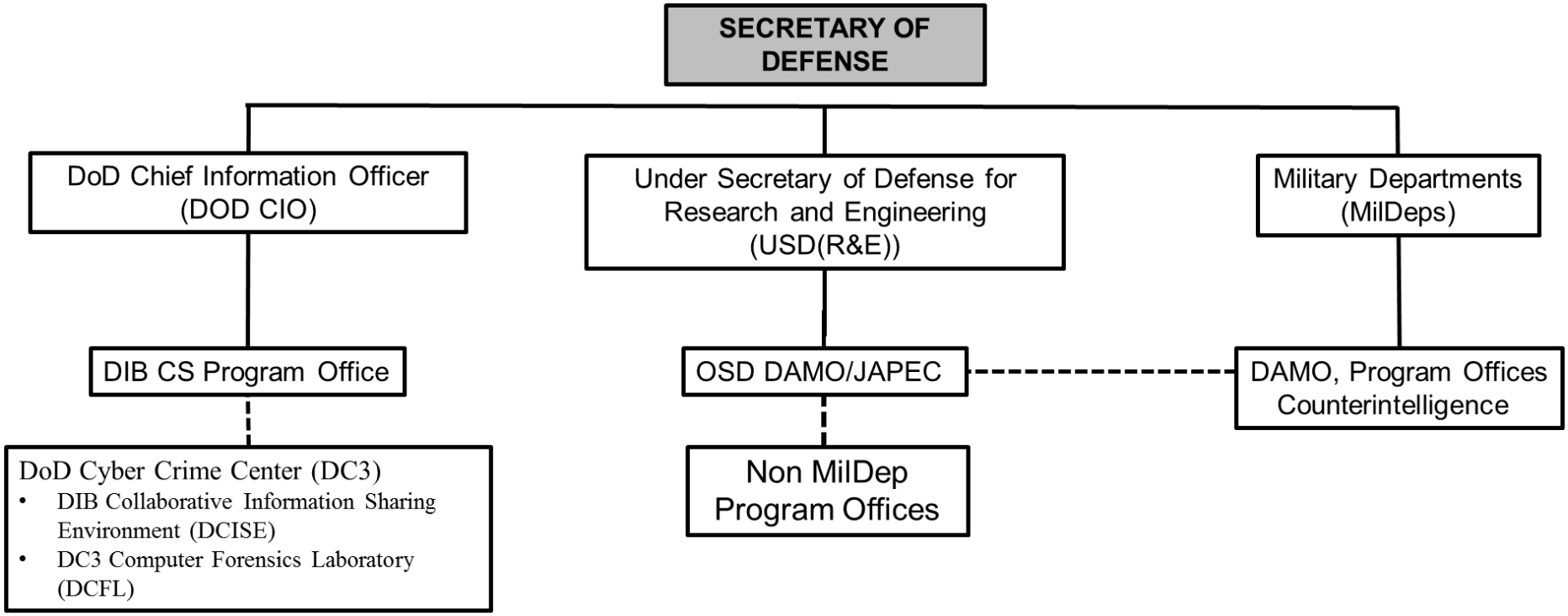
Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)

brian.d.hughes3.civ@mail.mil

571-372-6451

Organizational Chart

Damage Assessment Management Office (DAMO)



DAMO MISSION: Determine impact of cyber compromise to DoD Scientific and Research Projects, Programs, Platforms, & Warfighting Capabilities.

Addressing the Loss of CTI

Risk = f (threat, vulnerabilities, consequences)

Goals:

- **Enable information-sharing, collaboration, analysis, and risk management between acquisition, LE, CI, and IC**
  - Connect the dots in the risk function (map blue priorities, overlay red threat activities, warn of consequences)
- **Integrate existing acquisition, LE, CI, and IC information to connect the dots in the risk function - linking blue priorities with adversary targeting and activity**
  - Many sources and methods are relevant (e.g., HUMINT, joint ventures)
  - Cyber is only one data source
    - Focus precious resources
    - Speed discovery and improve reaction time
    - Ultimately, evolve to a more proactive posture

JAPEC Mission: Integrated Analysis

The Joint Acquisition and Protection and Exploitation Cell (JAPEC) integrates and coordinates analysis to enable Controlled Technology Information (CTI) protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten US military advantage.