OPA | PERSEREC

OFFICE OF PEOPLE ANALYTICS | DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

From Indicators to Differentiators: Moving Espionage Research Forward

Stephanie L. Jaros, Project Director

2018 IEEE Workshop on Research for Insider Threats (WRIT)

May 24, 2018

THE CHALLENGE

THE CHALLENGE: "Loss of our secrets whether through espionage, theft or unauthorized disclosure for other reason – will never be eliminated, but the opportunities therefor can be diminished and attempts at compromise made more different at acceptable – indeed modest – cost."

RECOMMENDATION: Establish a policy that all persons entering or leaving defense activities, including, to the extent practical, its contractors, are subject to inspection of their briefcases and personal effects, to determine if classified material is being removed without authority.

- The Stilwell Commission Report (1985)

Time Magazine cover from http://content.time.com/time/covers/0,16641,19850617,00.html

THE CHALLENGE PERSISTS

"'If you have a bag full of stuff, you're probably going to get stopped.' . . . But, in general . . . 'Disneyland has more physical security checks than we had.'"

- NSA Employee, In response to Harold Martin III exfiltration (2016)

Photo from Indiana Daily Student, http://www.idsnews.com/article/2016/10/prosecution-of-whistleblower-demonstrates-govt-overreach

Quotation from The Washington Post, https://www.washingtonpost.com/world/national-security/nsa-contractor-thought-to-have-taken-classified-material-the-old-fashioned-way/2016/10/12/ffc25e22-8cb1-11e6-875e-2c1bfe943b66_story.html?utm_term=.ea914e2d853b

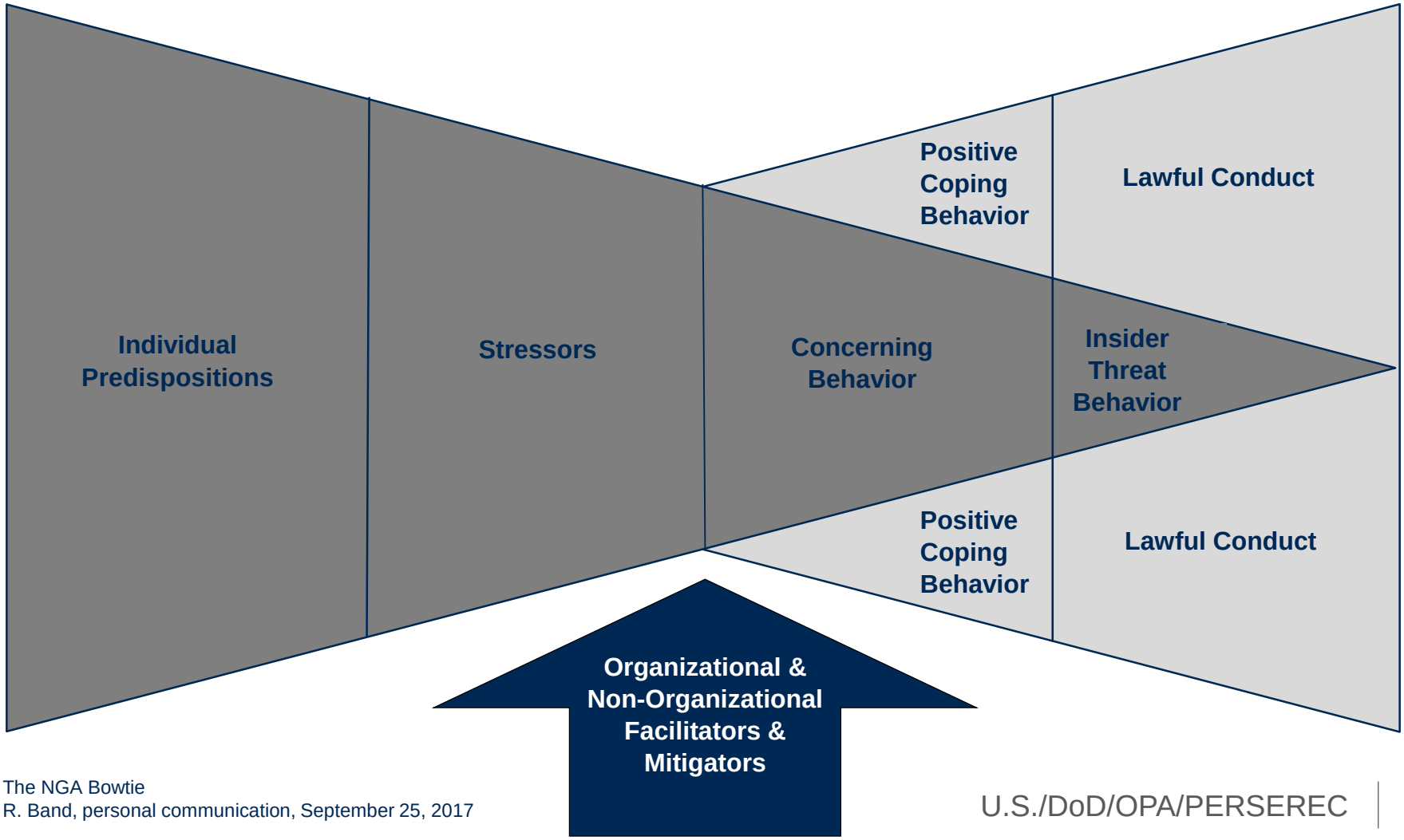
THE HUMAN PROBLEM

"Where we're missing the boat, oftentimes, is on the human resource side. . . . At the end of the day, what we have to realize is, we'll never stop the insider threat. The goal is to stop them before he or she decides to. We have to find a way to identify, mark them ahead of time and say, 'hey listen, I know things are rough, you're having problems, but there's other options.'"

- Bill Evanina, Director, National Counterintelligence and Security Center (2017)

- Quotation from Meritalk.com, https://www.meritalk.com/articles/insider-threat-programs-miss-human-side-problem-bill-evanina-odni-cybersecurity/

THE NGA BOWTIE



The NGA Bowtie
R. Band, personal communication, September 25, 2017

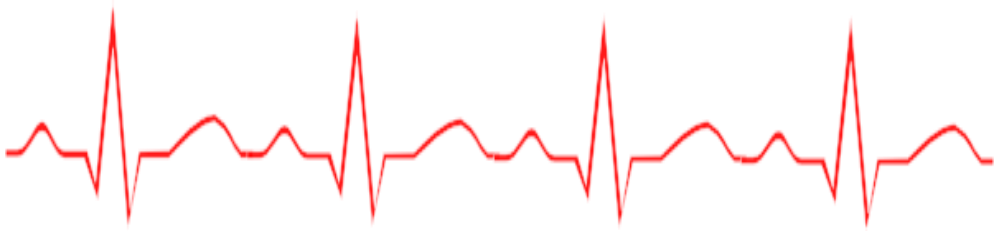
SOCIAL AND BEHAVIORAL SCIENCE INSIDER THREAT RESEARCH

- A person's transformation from a trusted employee to an insider threat is a process rather than an event.
- The risk of becoming an insider threat is not randomly distributed throughout the workforce – certain people are more likely to pose threats.
- Insider threats occur in a social context – certain environments are more likely to facilitate insider threat behavior.
- High-impact, low frequency insider threat behavior is correlated with and preceded by far more common indicators that can be observed, modeled, and mitigated.

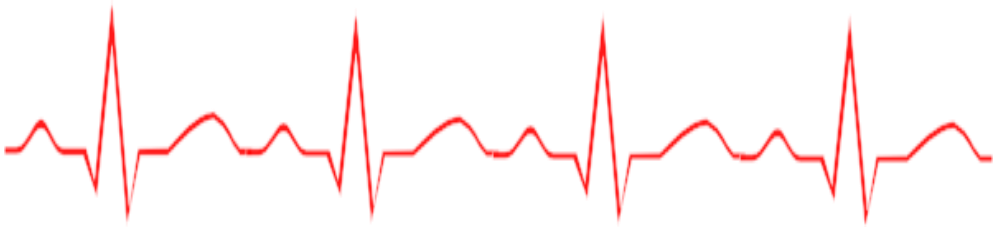
BEHAVIORAL INDICATORS

Gambling problems Adultery Unexplained absenteeism Unusual interest in weapons Threatening communications Requesting information without a need-to-know Criminal behavior Extensive use of equipment to reproduce or transmit material Installing unauthorized software Asking for a colleague's password Leaving a safe open Discussing classified information in a public setting Removing classification markings from documents Anti-U.S. comments Decline in work performance Working outside usual hours Decline in mental health Hostile behavior Unreported foreign travel and/or foreign contacts Drug and/or alcohol abuse Divorce Physical illness Bankruptcy Financial affluence Bizarre behavior

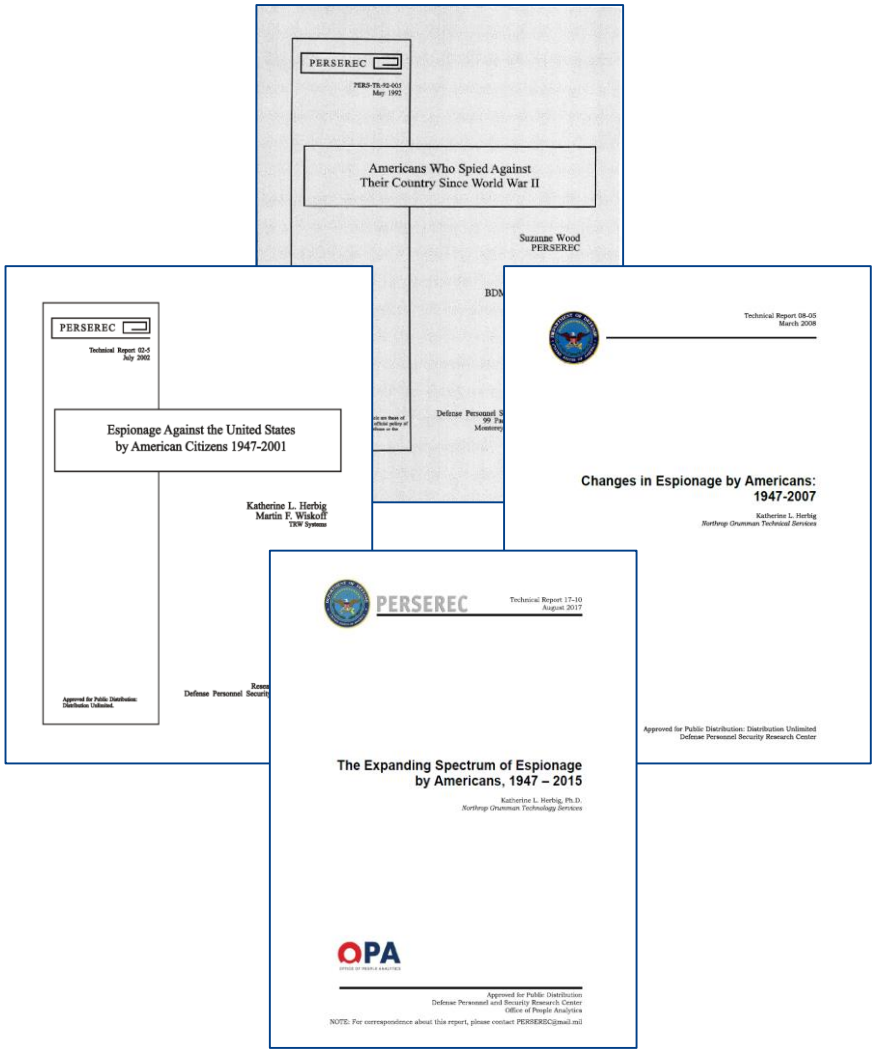
BEHAVIORAL INDICATORS



Report any behavior that deviates from an individual or peer group baseline



MOVING ESPIONAGE RESEARCH FORWARD



THE RESOURCE EXFILTRATION PROJECT

- Revised eligibility criteria to focus on the incident rather than the prosecutorial outcome
  - Include spies, leakers, hoarders
  - Include classified and unclassified government resources

- Revised codebook
  - Minimal training required to implement
  - Mutually exclusive and exhaustive categories
  - Differentiate among Yes, No, Unknown, N/A

THE RESOURCE EXFILTRATION PROJECT

- Adjudicative Guidelines
  - A: Allegiance to the U.S.
  - B: Foreign Influence
  - C: Foreign Preference
  - D: Sexual Behavior
  - E: Personal Conduct
  - F: Financial Considerations
  - G: Alcohol Consumption
  - H: Drug Involvement
  - I: Psychological Conditions
  - J: Criminal Conduct
  - K: Handling Protected Information
  - L: Outside Activities
  - M: Use of IT Systems

GUIDELINE I: PSYCHOLOGICAL CONDITIONS

A57. GUIDELINE I1 ***(Numeric)***

Person engaged in behavior that cast doubt on his/her judgment, reliability, or trustworthiness that was not covered under any other guideline, including, but not limited to, emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior.

0	No
1	Yes

A58. GUIDELINE I2 ***(Numeric)***

A duly qualified mental health professional opined that the individual had a condition not covered under any other guideline that may have impaired judgment, reliability, or trustworthiness.

0	No
1	Yes

A59. GUIDELINE I3 ***(Numeric)***

The individual failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition (*e.g.,* failure to take prescribed medication).

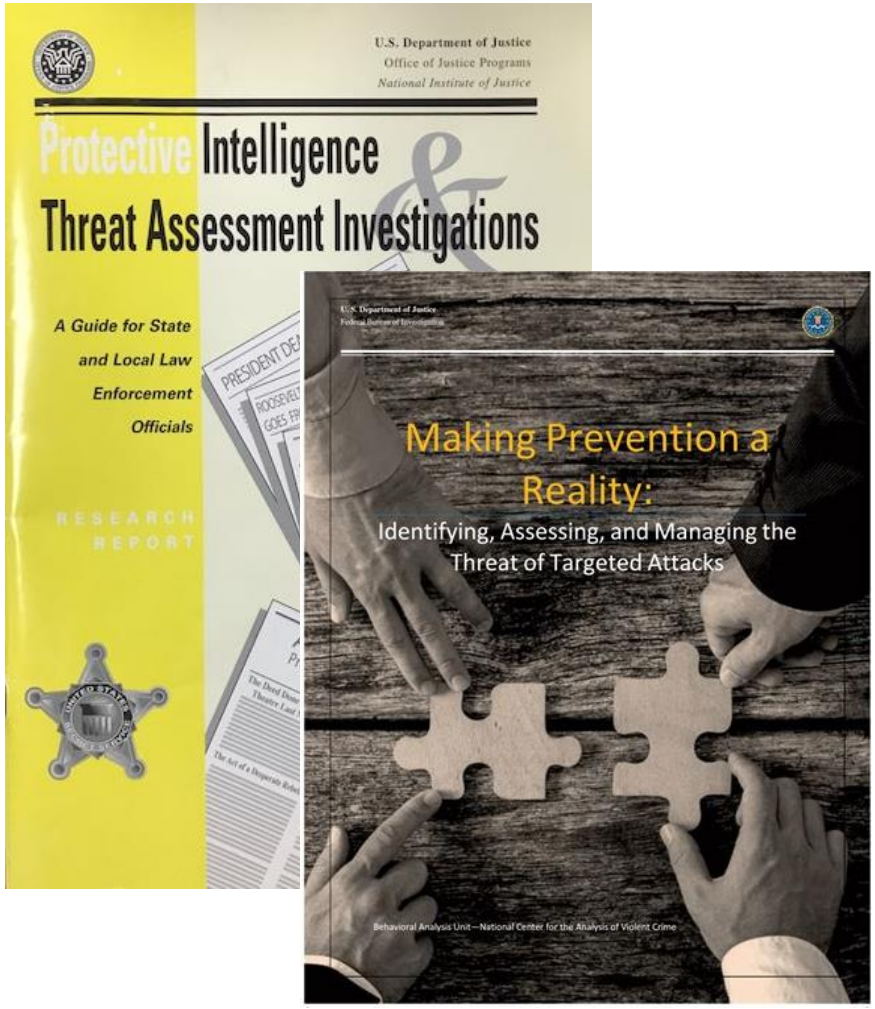
0	No
1	Yes

A60. GUIDELINE I COMMENTS ***(String)***

Description of Guideline I issues.

Examples: Person reported auditory hallucinations to his security manager in late 1978; Medical expert testified on person's behalf at trial that he was often non-compliant with doctor's prescribed medication plan prior to arrest

THE RESOURCE EXFILTRATION PROJECT



- Adapted Threat Assessment Categories
  - Motives
  - Concerning Communications
  - Concerning Interests
  - Planning Behavior
  - Significant Life Events
  - Concerned Others

THE RESOURCE EXFILTRATION PROJECT

H17. RELATIONSHIP ISSUE *(Numeric)*

According to open source intelligence, person experienced an issue/event related to marital/relationship status that facilitated his/her decision to commit resource exfiltration.

0	No (*Skip to H19*)
1	Yes

H18. RELATIONSHIP ISSUE DETAIL *(String)*

Describe information in open source intelligence about person's issue/event related to marital/relationship status.

Examples: Spouse died in 2000 and she had trouble paying bills; Began dating a Chinese national in June 1991 who requested classified material and turned out to be an unregistered foreign agent

THE RESOURCE EXFILTRATION PROJECT

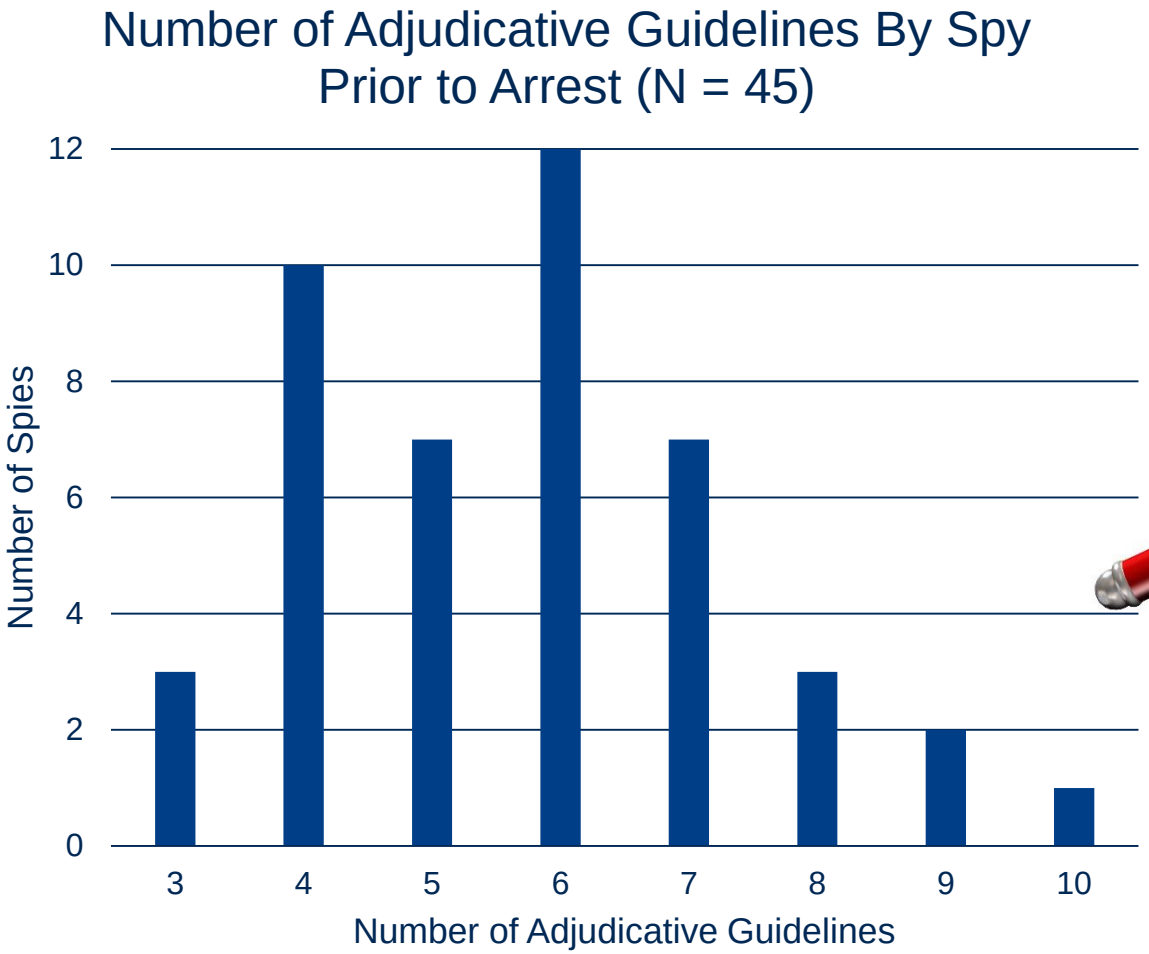
2018 Technical Report
Autumn 2018 Release Date

Jonathan Jay Pollard
Arrested 11/21/1985

Gregory Allen Justice
Arrested 7/7/2016

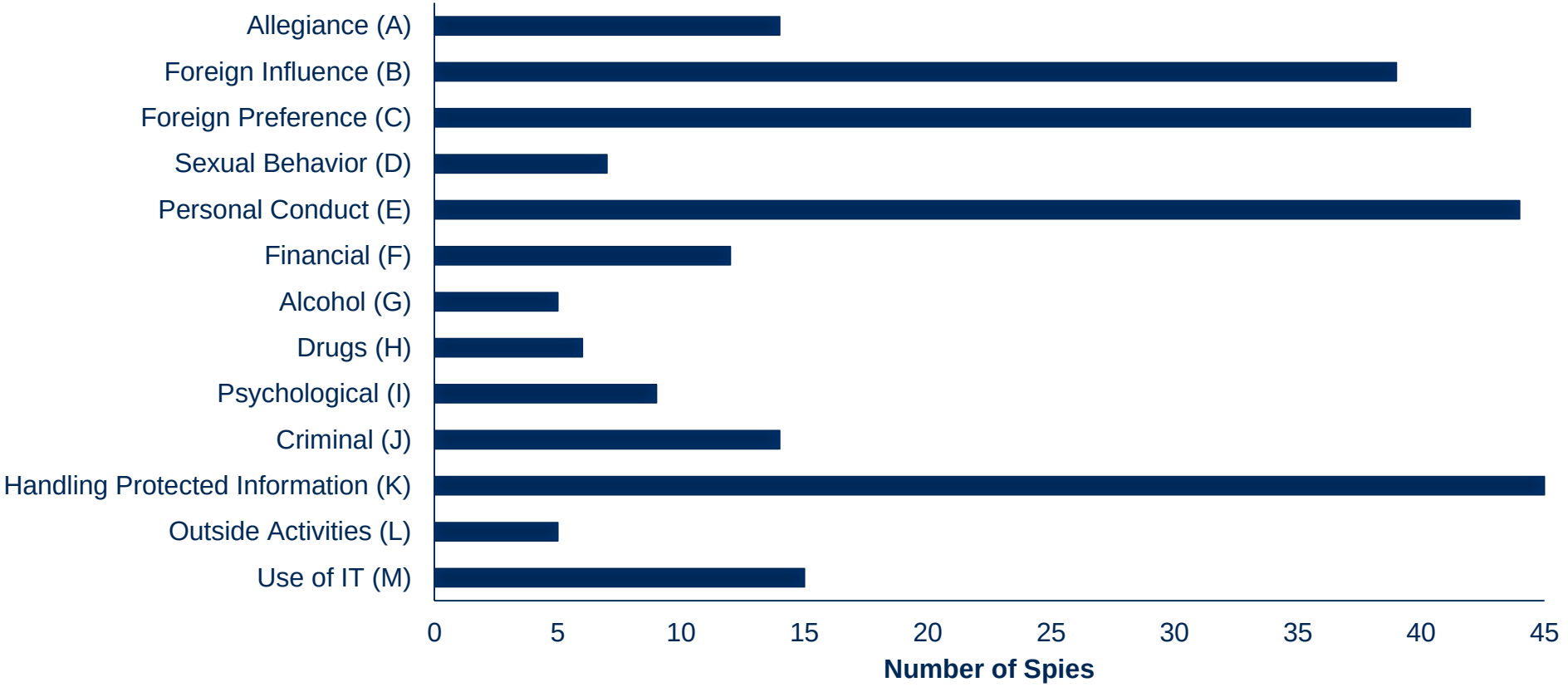
- Additional eligibility criteria
  - DoD personnel: Civilian, Military, Contractor
  - Exfiltrated a DoD resource
  - Arrested between November 20, 1985 and December 31, 2017
  - Convicted or pled guilty

PRELIMINARY FINDINGS

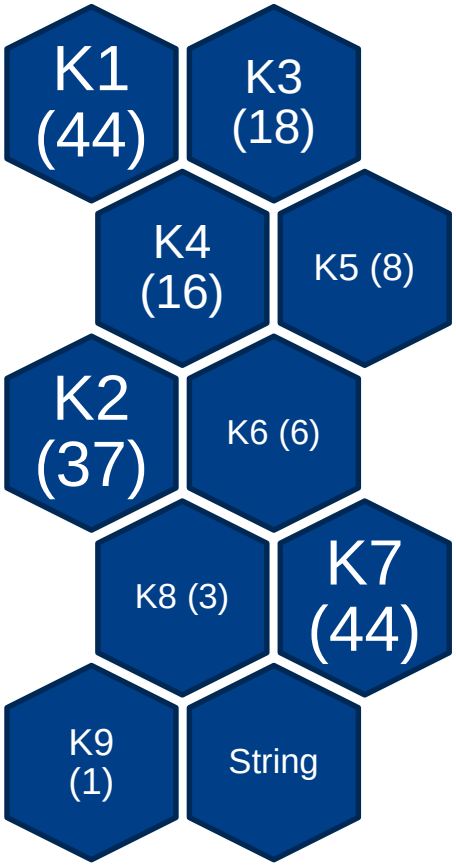


PRELIMINARY FINDINGS

Pre-Arrest Behavior Categorized by Adjudicative Guideline (N = 45)



PRELIMINARY FINDINGS



Guideline K:
Handling Protected Information

K1: “Person engaged in deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including, but not limited to, personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences.”

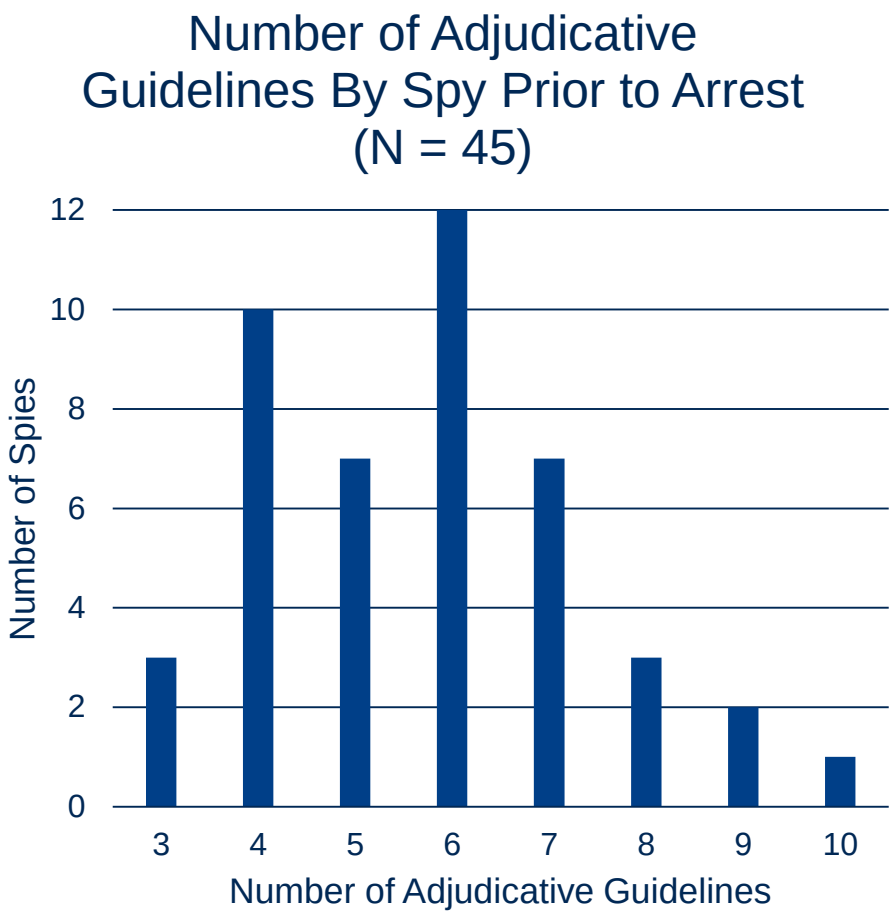
K7: “Person failed to comply with rules for the protection of classified or other protected information.”

K2: “Person collected or stored classified or other protected information at home or in any other unauthorized location.”

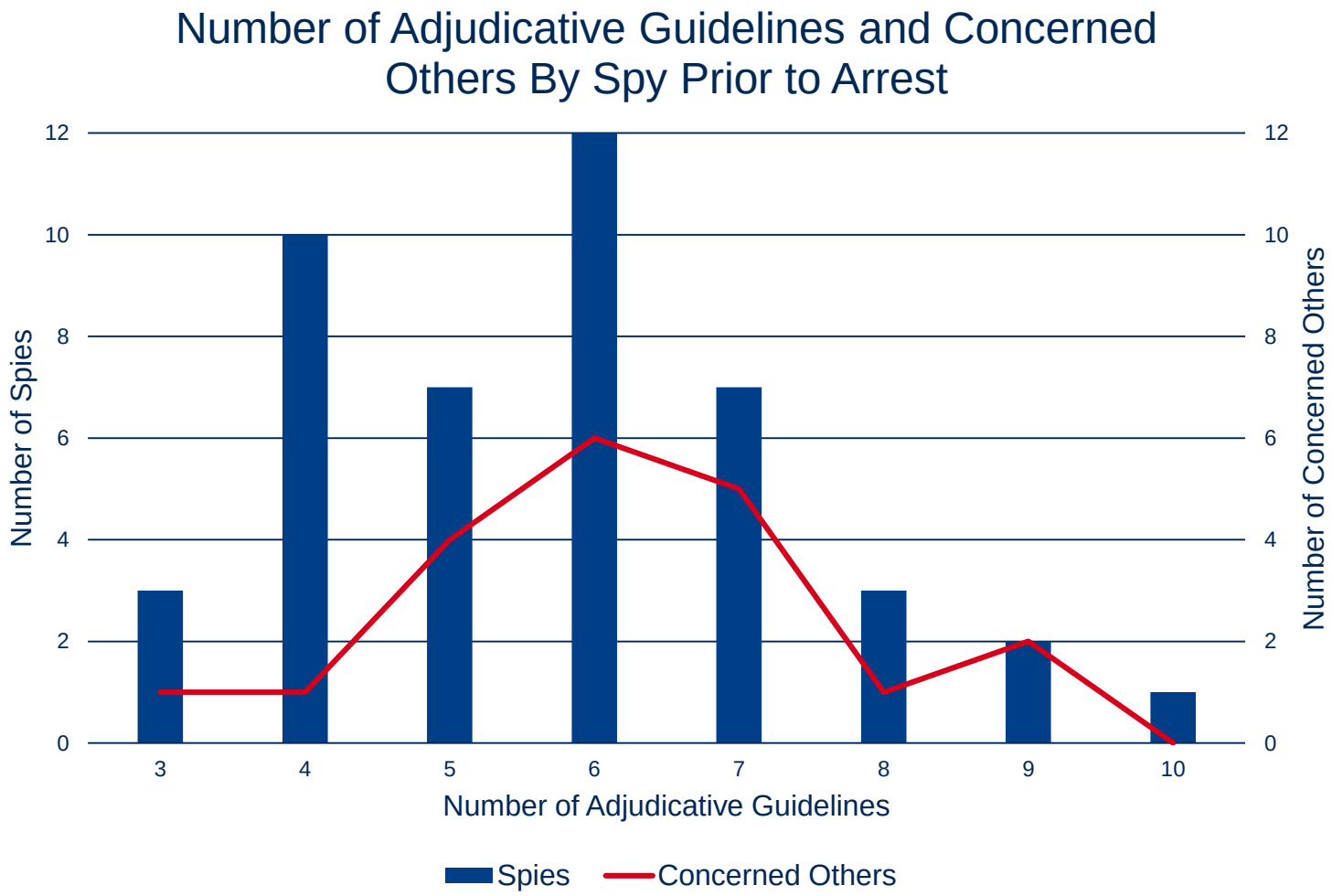
PRELIMINARY FINDINGS

- In 20 of the 45 cases, someone noticed the spy's concerning behavior or a change in behavior prior to arrest
  - In 15 of these 20 cases, someone went on to report the concerning behavior prior to arrest

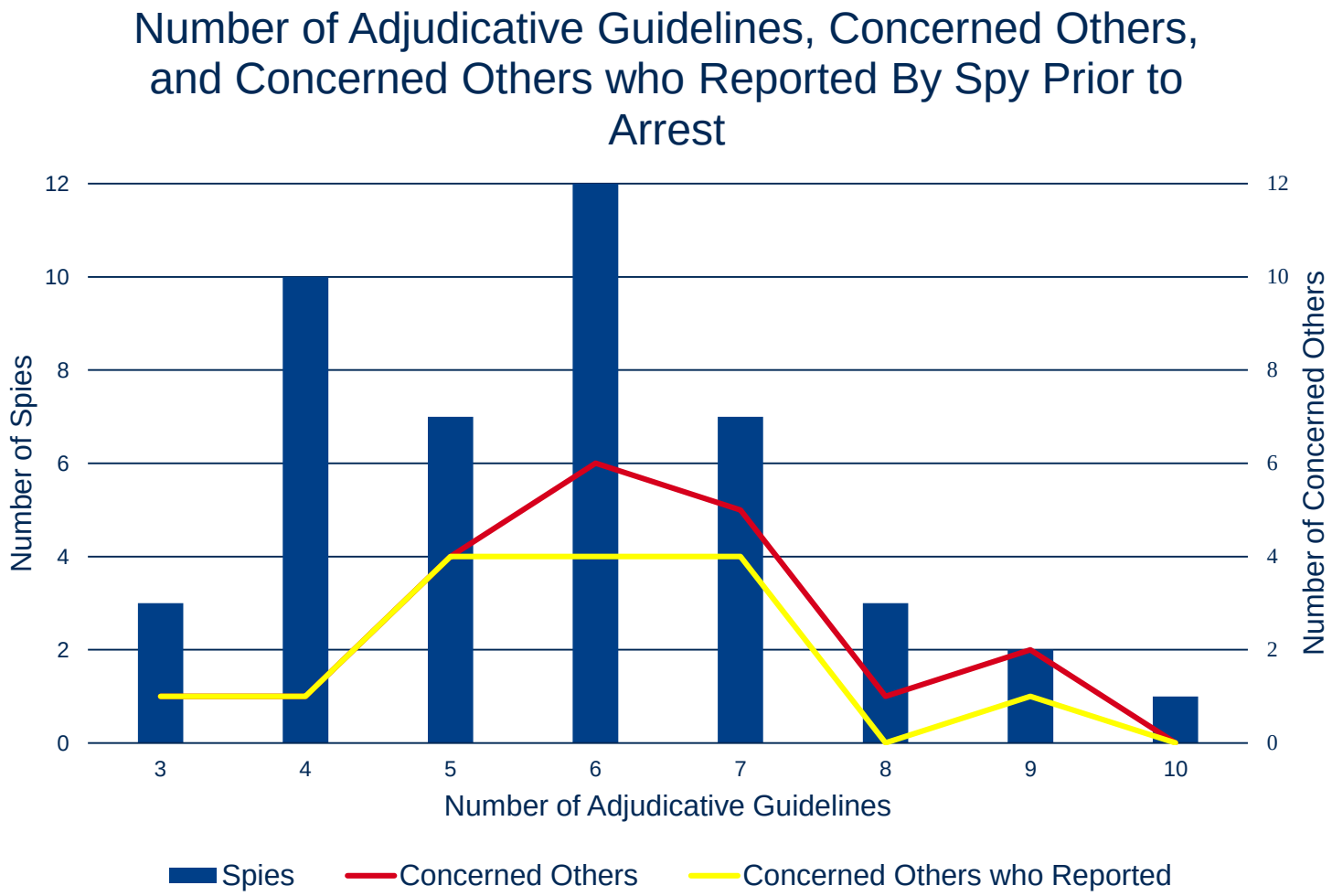
- Hypothesis: There is a direct relationship between the number of adjudicative guidelines and the number of concerned others



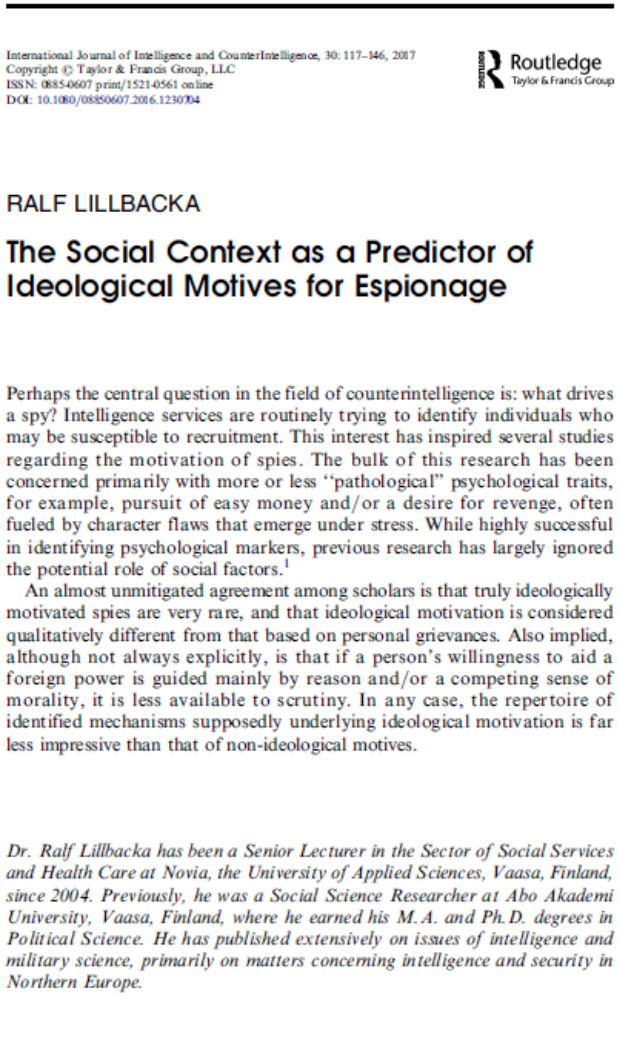
PRELIMINARY FINDINGS



PRELIMINARY FINDINGS



FINAL REPORT & FUTURE RESEARCH



International Journal of Intelligence and CounterIntelligence, 30: 117–146, 2017
Copyright © Taylor & Francis Group, LLC
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2016.1230704

Routledge
Taylor & Francis Group

RALF LILLBACKA

The Social Context as a Predictor of Ideological Motives for Espionage

Perhaps the central question in the field of counterintelligence is: what drives a spy? Intelligence services are routinely trying to identify individuals who may be susceptible to recruitment. This interest has inspired several studies regarding the motivation of spies. The bulk of this research has been concerned primarily with more or less "pathological" psychological traits, for example, pursuit of easy money and/or a desire for revenge, often fueled by character flaws that emerge under stress. While highly successful in identifying psychological markers, previous research has largely ignored the potential role of social factors.[1]

An almost unmitigated agreement among scholars is that truly ideologically motivated spies are very rare, and that ideological motivation is considered qualitatively different from that based on personal grievances. Also implied, although not always explicitly, is that if a person's willingness to aid a foreign power is guided mainly by reason and/or a competing sense of morality, it is less available to scrutiny. In any case, the repertoire of identified mechanisms supposedly underlying ideological motivation is far less impressive than that of non-ideological motives.

Dr. Ralf Lillbacka has been a Senior Lecturer in the Sector of Social Services and Health Care at Novia, the University of Applied Sciences, Vaasa, Finland, since 2004. Previously, he was a Social Science Researcher at Abo Akademi University, Vaasa, Finland, where he earned his M.A. and Ph.D. degrees in Political Science. He has published extensively on issues of intelligence and military science, primarily on matters concerning intelligence and security in Northern Europe.

- Final Report
  - Spies, Leakers, Hoarders
  - Exfiltration and Transmission Methods
  - Motives
  - Analyses of Adjudicative Guidelines and Threat Assessment Variables

- Future Research: Do indicators and methods vary by whether individual was motivated by ideological or non-ideological factors?

OPA
OFFICE OF PEOPLE ANALYTICS

PERSEREC
DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

For More Information or to Request a Copy of the Final Report

Stephanie L. Jaros
Project Director
Stephanie.L.Jaros.civ@mail.mil
www.dhra.mil/perserec/

May 24, 2018