Prevention
The Missing Link

Proposing a New, Comprehensive Strategy to Prevent, Not Detect, Insider Threat in the US Intelligence Community

Counterintelligence is the Stepchild of the Intelligence Community

Prevention is the Stepchild of Counterintelligence

Detection Gets All the Love

Dr. David L. Charney
Psychiatrist

NOIR4USA.ORG
PART ONE
Proposing a New, Comprehensive Strategy to Prevent—Not Detect—Insider Threat in the Intelligence Community (IC)

- The Problem: Insider Threat
- Analyzing Failed Links in Security Chains
- Missing Links in IC Security Chains: Off-Ramp Exits

PART TWO
Scope of the Problem

- Importance of Prevention Despite Neglect
- Overly Focusing on Detection at the Expense of Prevention
- Great Hopes of the Moment
- Dirty Little Secret of Counterintelligence

PART THREE
The NOIR White Paper Series on Insider Threat, Counterintelligence (CI) and Counterespionage (CE)

- WHITE PAPER PART 1: “True Psychology of the Insider Spy” This paper introduced the Core Psychology of the Insider Spy as well as the Ten Life Stages of the Insider Spy
- WHITE PAPER PART 2: “NOIR: Proposing A New Policy for Improving National Security by Fixing the Problem of Insider Spies”
- WHITE PAPER PART 3: This paper will examine in detail the most important missing link in IC security chains: Prevention
- The Vision: A Full Spectrum Solution for Managing Insider Threat

PART FOUR
Rethinking Insider Threat

Introducing two new complementary categories that advance a high-level conceptual overview of insider threat management:

- External Management of Insider Threat (EMIT)
- Internal Management of Insider Threat (IMIT)

Human Psychology is Central to IMIT-Based Prevention
- Situations of Concern
- Modern Sales Practices Are Key for Achieving “Left of Boom” Interventions
- At its root, the insider threat actor’s problem is self-disappointment and loss of self-respect
- Not New! IMIT-Based Approaches Already Practiced in Specialized IC Units
- Basic Strategy with Hostage Takers (“hostages” in IC = classified information)
- Behavioral Change Stairway Model
- Full Spectrum Solution for Managing IC Insider Threat Requires EMIT and IMIT
- EMIT-based detection is necessary but not sufficient
- IMIT-based prevention complements, does not replace EMIT-based detection
- Prevention addresses the situation before the decision gets made to cross the line—the most important missing link in the security chain
- Detection needs to be supplemented by adding off-ramp exit solutions

PART FIVE
Detection: Strengths and Weaknesses

- Detection: Core Mission of Traditional Law Enforcement
- Strengths of Detection
- Weakenesses of Detection
- Factors Contributing to Detection Weakness
  - Present Day Conditions
    - Exponentially Increased Risk Today
    - More Foreign Intelligence Entities on the Prowl
    - Generational Changes
  - Intrinsic Weaknesses
    - Detection is Subject to the Law of Diminishing Returns
  - Workplace Barriers That Thwart Detection
    - Coworkers find it hard to speak up; Moral reluctance; Privacy concerns; Legal risks; Functional blindness; Pervasive all-seeing surveillance regime can backfire
  - Workforce Hiring Paradoxes Within the IC
    - IC’s Claims About Its Ideal Hires
  - Net Result of Detection Weaknesses
    - Overly stringent detection surveillance regimes can cut two ways. Weighing security vs. competence, what is the right balance?

NOIR provides the back-end exit solution for after the decision gets made to cross the line

GOALS OF THIS PAPER: Change the current situation, which is the almost exclusive reliance by the IC on EMIT. Remedy the imbalance by adding IMIT tools to the arsenal.

COMMENT ON “WHISTLEBLOWERS”: Proposals explored in this paper are designed to be effective not only with conventional state-sponsored insider spies but also with whistleblowers and other categories of insider threat actors.

<table>
<thead>
<tr>
<th>FACTORS</th>
<th>EMIT</th>
<th>IMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Identity</td>
<td>Police</td>
<td>Sales</td>
</tr>
<tr>
<td>Spirit of Professionals</td>
<td>Hunters</td>
<td>Farmers</td>
</tr>
<tr>
<td>Actions</td>
<td>Catch</td>
<td>Persuade</td>
</tr>
<tr>
<td>Manner of Engagement</td>
<td>Doing TO</td>
<td>Doing WITH</td>
</tr>
<tr>
<td>Approach</td>
<td>Hard</td>
<td>Soft</td>
</tr>
<tr>
<td>Type of Cop</td>
<td>Bad Cop</td>
<td>Good Cop</td>
</tr>
<tr>
<td>Carrots and Sticks</td>
<td>Sticks Only</td>
<td>Carrots Too</td>
</tr>
<tr>
<td>Emotional Tone</td>
<td>Cold</td>
<td>Warm</td>
</tr>
<tr>
<td>Sensitive to Psychology</td>
<td>Minimal</td>
<td>Maximal</td>
</tr>
<tr>
<td>Concerns About Subject’s Family</td>
<td>None</td>
<td>Major</td>
</tr>
<tr>
<td>Change Subject’s Thinking?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Subject’s Decision</td>
<td>Involuntary</td>
<td>Voluntary</td>
</tr>
<tr>
<td>Identified How?</td>
<td>Detection</td>
<td>Self-Identified</td>
</tr>
<tr>
<td>Highest Aim</td>
<td>Punish</td>
<td>Save</td>
</tr>
<tr>
<td>Ideally, How it Ends?</td>
<td>Incarceration</td>
<td>Back to Work</td>
</tr>
<tr>
<td>Where?</td>
<td>Bureau of Prisons</td>
<td>Home Agency</td>
</tr>
<tr>
<td>Ancillary Professionals</td>
<td>Lawyers, Judges</td>
<td>Counselors</td>
</tr>
</tbody>
</table>

Government tends to throw big money at tough problems for solutions that will not necessarily work.
Prevention: Strengths and Weaknesses

Strengths of Current Practices
- Prevention elements that do work well, often combined with elements of detection

Weaknesses of Today
- Cultural: Prevention is the Stepchild of Counterintelligence
- Measuring Success: Prevention’s Biggest Problem
- Prevention Resources Today Need Strengthening
- Three Classes of Troubled Employees
- Stories Heard from the Corridor re EAPs

Result: Employees of greatest concern, with the most serious problems, are the very ones who will not dare make the call for help and will never show up at their home agency’s EAP.
- EAPs Today are like Urgent Care Centers

Weaknesses of Today
- Prevention Resources Today Need Strengthening
- Measuring Success: Prevention’s Biggest Problem
- Cultural: Prevention is the Stepchild of Counterintelligence
- Prevention elements that do work well, often combined
- Insider Threat
- Bedrock foundation for robust multilayered defenses against both before and after crossing the line. EMIT still remains the
- IMIT confers advantages over EMIT for managing insider threat
- Sadly, Not Every Troubled Employee Will Be Rescuable
- Easier Decisions • Cheaper • Faster
- Looking Ahead: Excessively Optimistic Claims for New High-Tech Advances
- Artificial Intelligence (AI), Big Data, Algorithms, and Machine Learning (ML)
- Algorithm Bias: A Newly Named Concept
- Paradigm of Home Security Systems
- Thresholds in the Context of the IC
  - If set too high or if set too low; no way to achieve a perfect threshold setting!
- Defining Suspects Based on an Algorithm
  - An Insider Threat Score?
  - Arbitrary Thresholds Tend to Get Turned into Concrete Categories
- Congratulations! You Identified a Suspect. Now What?
  - High-Tech Indicators: Helpful or Problematic?
  - Parallels the Problem of What to Do with Weather Forecasts
  - Bring in the Big Guns: The FBI Will Solve It!
  - Hassles Managing Suspects
- Despite the Hype, High Tech Offers Little Relief for Decision Makers
- Defeating Newest Detection Technology? Zero Days Are Every Day
  - Determined Insiders can and will defeat any security technology devised
  - Exceptions showing the best protections can be overcome
  - What everybody in the information technology (IT) world knows
  - Cycle Times and OODA Loops
  - Continuous Evaluation (CE)
  - Message to Designers of Detection Systems, Including CE

Big Picture Considerations: IMIT Advantages Over EMIT
- Easier Decisions • Cheaper • Faster
- Easier to manage • Rescue vs. Catch
- Sadly, Not Every Troubled Employee Will Be Rescuable

IMIT confers advantages over EMIT for managing insider threat both before and after crossing the line. EMIT still remains the bedrock foundation for robust multilayered defenses against insider threat.

PART SIX

Building A New Comprehensive Prevention Program

General Considerations
- IMIT Concepts Will Be Its Guiding Principles
  - Key Concern: Safety is Number One
  - “Lean on Me”
  - Initial Contact: Making It Safe
  - Off-Ramp Exits Needed Before Someone Crosses the Line
  - Rapid
  - Remove all Barriers
  - Comprehensive and Practical
- Useful Starting Fact: About 90% of Insider Threat Actors Are Male
- Males constitute about 90% of caught spies.
- Intervention Windows: When Open or Closed?
  - First Open Window: Stage 2 (Stress/Spiral Stage): Before Someone Crosses the Line
  - Intervening During Early and Mid-Stage 2
  - Closed Windows: Stages 3 and 4: The Blackout Periods
  - Open Windows: Stage 5 (Remorse, Morning After Stage); Stage 6 (Active Spy Career Stage); and Stage 7 (Dormancy Stage): The Stages After Someone Crosses the Line
- Two Tier Structure
  - First Tier: Existing EAPs Internal to Each IC Agency
  - Second Tier: Second Level EAP—Outside Home Agency
- Resources Must Be Real
  - To truly fulfill promises to help, the IC cannot make promises that are not kept! Resources offered need to go beyond psychological counseling.
  - An External EAP Has the Advantages of a Third Party
    - What is Needed and Why
    - Setting Up Resources Will Not Be Simple
      - Staffing Personnel Will Be Challenging
      - Specialized Training Will Be Needed
      - Authorities
        - Primary Aim: Rescue a basically good employee and get him back to work
    - Separation from service must remain an option
    - Case Manager Approach
    - Security Concerns
- Making New Prevention Program Work
  - Targeting the Correct Audience
  - Communicating the Right Way with the Target Audience
    - Adopt Proper Tone
    - Engage by Making Offers Instead of Threats
    - Packaging Offers
- New Prevention Program Should Be Rolled Out in Phases
  - Phase One: Redefining the Meaning of Spying
    - Can a Commonly Held Assumptions Be Changed? Yes, If Done Right
    - How Redefining the Meaning of Spying Helps Change Inner Calculations
  - Phase Two: Proving the Redefined Meaning of Spying
    - Consider the Power of Memes
  - Phase Three: Getting the Messages Out
    - Outreach to the General Public
    - New Security Training for the IC Workforce
      - Semi-Annual Computerized Training
      - New helping resources will be described

Part Seven

New Prevention Program Should Be Rolled Out in Phases

Phase One: Redefining the Meaning of Spying
- Can a Commonly Held Assumptions Be Changed? Yes, If Done Right
- How Redefining the Meaning of Spying Helps Change Inner Calculations

Phase Two: Proving the Redefined Meaning of Spying
- Consider the Power of Memes

Phase Three: Getting the Messages Out
- Outreach to the General Public
- New Security Training for the IC Workforce
  - Semi-Annual Computerized Training
  - New helping resources will be described

High-Tech Indicators: Helpful or Problematic?
- Congratulations! You Identified a Suspect. Now What?
  - High-Tech Indicators: Helpful or Problematic?
  - Parallels the Problem of What to Do with Weather Forecasts
  - Bring in the Big Guns: The FBI Will Solve It!
  - Hassles Managing Suspects
- Despite the Hype, High Tech Offers Little Relief for Decision Makers
- Defeating Newest Detection Technology? Zero Days Are Every Day
  - Determined Insiders can and will defeat any security technology devised
  - Exceptions showing the best protections can be overcome
  - What everybody in the information technology (IT) world knows
  - Cycle Times and OODA Loops
  - Continuous Evaluation (CE)
  - Message to Designers of Detection Systems, Including CE

Big Picture Considerations: IMIT Advantages Over EMIT
- Easier Decisions • Cheaper • Faster
- Easier to manage • Rescue vs. Catch
- Sadly, Not Every Troubled Employee Will Be Rescuable

IMIT confers advantages over EMIT for managing insider threat both before and after crossing the line. EMIT still remains the bedrock foundation for robust multilayered defenses against insider threat.

PART SIX

Prevention: Strengths and Weaknesses

Strengths of Current Practices
- Prevention elements that do work well, often combined with elements of detection

Weaknesses of Today
- Cultural: Prevention is the Stepchild of Counterintelligence
- Measuring Success: Prevention’s Biggest Problem
- Prevention Resources Today Need Strengthening
- Three Classes of Troubled Employees
- Stories Heard from the Corridor re EAPs

Result: Employees of greatest concern, with the most serious problems, are the very ones who will not dare make the call for help and will never show up at their home agency’s EAP.
- EAPs Today are like Urgent Care Centers
Dr. Charney is the Founder and Medical Director of Roundhouse Square Counseling Center, in Alexandria, Virginia. He specializes in Anxiety and Mood Disorders, Couples and Family Therapy, as well as Attention Deficit Disorder in adults.

In addition to his usual practice, he has also treated personnel from within the Intelligence Community. As a result of unusual circumstances, he had the opportunity to join the defense team of his first spy case, Earl Pitts. Subsequently, Plato Cacheris, the attorney of Robert Hanssen, invited Dr. Charney to join his defense team, which added a further dimension to his experience. With the addition of his third spy case, Brian Regan, Dr. Charney further deepened his knowledge of the psychological nuances of captured spies.

As a member of their defense teams, Dr. Charney was perceived by these insider spies as an understanding and supportive figure, which lowered their defensive mindsets, and provided a truer picture of their inner lives. Many common assumptions of spy motivation were brought into question by Dr. Charney’s work.

Dr. Charney elaborated his findings in Part One of his White Paper, entitled True Psychology of the Insider Spy. Part Two of his White Paper, entitled NOIR (proposing a National Office for Intelligence Reconciliation), lays out Dr. Charney’s innovative and perhaps controversial recommendations for making use of what he learned to better manage the problem of insider spies. To educate and promote these concepts and ideas, he founded NOIR for USA, a non-profit organization. Its website is: NOIR4USA.org.

---

**Ten Life Stages of the Insider Spy**

**THE TEN LIFE STAGES**

- 1. Sensitizing Stage
- 2. Stress/Spiral Stage
- 3. Crisis/Climax/Resolution Stage
- 4. Post-Recruitment Stage
- 5. Remorse (Morning After) Stage*
- 6. Active Spy Career Stage*
- 7. Dormancy Stage(s)*
- 8. Pre-Arrest Stage
- 9. Arrest and Post-Arrest Stage
- 10. Brooding in Jail Stage

*Windows = Windows of Opportunity  *Convergence = Convergence

---

**ABOUT THE AUTHOR**

**Dr. David L. Charney**

Dr. Charney is the Founder and Medical Director of Roundhouse Square Counseling Center, in Alexandria, Virginia. He specializes in Anxiety and Mood Disorders, Couples and Family Therapy, as well as Attention Deficit Disorder in adults.

In addition to his usual practice, he has also treated personnel from within the Intelligence Community. As a result of unusual circumstances, he had the opportunity to join the defense team of his first spy case, Earl Pitts. Subsequently, Plato Cacheris, the attorney of Robert Hanssen, invited Dr. Charney to join his defense team, which added a further dimension to his experience. With the addition of his third spy case, Brian Regan, Dr. Charney further deepened his knowledge of the psychological nuances of captured spies.

As a member of their defense teams, Dr. Charney was perceived by these insider spies as an understanding and supportive figure, which lowered their defensive mindsets, and provided a truer picture of their inner lives. Many common assumptions of spy motivation were brought into question by Dr. Charney’s work.

Dr. Charney elaborated his findings in Part One of his White Paper, entitled True Psychology of the Insider Spy. Part Two of his White Paper, entitled NOIR (proposing a National Office for Intelligence Reconciliation), lays out Dr. Charney’s innovative and perhaps controversial recommendations for making use of what he learned to better manage the problem of insider spies. To educate and promote these concepts and ideas, he founded NOIR for USA, a non-profit organization. Its website is: NOIR4USA.org.

---

For more information or further briefings, contact Dr. David Charney:

EMAIL David.Charney@NOIR4USA.org | PHONE 703-836-7130 | MOBILE 703-395-5454 | WEBSITE NOIR4USA.org