

INSIDER THREAT

AWARENESS & REPORTING



IN THE NEWS

WIKILEAKS

Army SGT Bradley Manning



- Accused of leaking 250,000 Classified documents



FORT HOOD

Army MAJ Nidal Malik Hasan



- Charged with 13 counts of premeditated murder and 32 counts of attempted murder

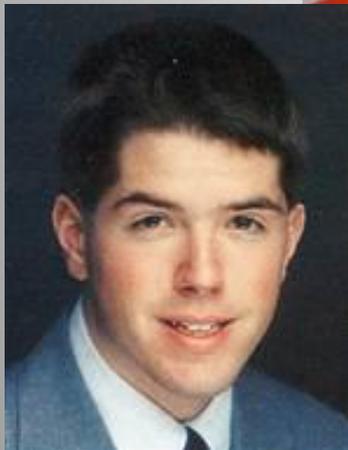
THE INSIDER THREAT – PERSISTENT AND CONTINUAL



**CONVICTED
1986
2 LIFE TERMS**



**CONVICTED 1994
LIFE W/O PAROLE**



**CONVICTED 2004
LIFE**



**CONVICTED 2003
LIFE W/O PAROLE**



**CONVICTED 2009
LIFE**



**CONVICTED 2002
LIFE**

ESPIONAGE

Espionage is the clandestine collection of information by people either in a **position of trust** for a targeted entity, or with access to people with such access. It includes the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. Espionage is punishable by **DEATH** under UCMJ & U.S. Code.

TERRORISM

Terrorism involves acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state law and appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

The various “dangerous acts” referred to above like murder are punishable by **DEATH** under UCMJ and federal and state law.

INSIDER

Anyone who has authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.

INSIDER THREAT

An insider who uses his or her access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism or kinetic actions resulting in loss or degradation of resources or capabilities.

“Perhaps the most imminent threats today come from insiders.”

–Louis J. Freeh, former FBI Director during Congressional testimony

WHY SHOULD YOU CARE?

- Potential **DEATHS** of military and civilian personnel.
- **LOSS** of U.S. military superiority and possible **COUNTERMEASURES** to U.S. weapons & tactics.
- Intelligence sources **COMPROMISED**.
- Billions of dollars & thousands of man-hours devoted to Research, Development and Acquisition **WASTED**.
- **DESTRUCTION** of families.

“I have opened the door for calumny [slander] against my totally innocent wife and our children. I hurt them deeply. I have hurt so many deeply.” –Robert Hanssen



THREATS

The intention and capability of any adversary to acquire and exploit critical information or cause harm to the U.S. and its resources to include personnel.

The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S. program, operation, or to promote an ideology.

Adversaries include “friendly” and “allied” countries.

**FOREIGN
INTELLIGENCE
ENTITIES**

TERRORIST

INADVERTENT

**WORKPLACE
VIOLENCE**

“It would not be normal for us to spy on the U.S. in political matters or military matters, but in economic and technical spheres we are competitors; we are not allies.” –Pierre Marion, Former Dir of France’s Eternal Intelligence Service

FOREIGN INTELLIGENCE ENTITIES (FIE)

Any known or suspected foreign organization, person or group (public, private or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, disrupt U.S. systems or programs or to gain a competitive edge in the research, development and acquisition of U.S. programs. Adversaries include foreign intelligence and security services, terrorist organizations, and organized crime groups.

Adversaries collect small pieces of information which combined can reveal the whole picture.

“Using public resources openly and without resorting to illegal means, it is possible to gather 80% of information needed about the enemy.”

–Al Qaeda Handbook

How they operate:

- **Public/Open Sources** - Social networking sites like Facebook and Twitter as well as blogs are often monitored and exploited.
- **Elicitation** - Get you talking & keep you talking.
 - **Flattery/Appeal to Ego:** They may ask your opinion and /or give value to your opinion.
 - **Quid Pro Quo:** They share information so you feel obligated to share information.
 - **Mutual Interest:** Real or feigned.
- **Eavesdropping & Electronic Surveillance**
- **Recruitment** - Build a personal relationship with an insider in order to exploit them to obtain critical information. Gain trust little by little.
 - Exploit personal characteristics, circumstances, or behaviors.
 - May use inducements to cooperate or coercion based on the insider's characteristics, circumstances, or behaviors.
 - Small request and then bigger demands.

TERRORIST GROUPS

Every successful terrorist attack has been preceded by at least one successful intelligence attack to gather information about the intended target.

In addition to stealing information, terrorists are engaged in planning, preparing, supporting or executing some violent action.

Support for terrorism is often indicated by whom an individual associates with, certain public actions or internet use, and/or expressed support for a terrorist ideology.

Any support or advocacy of terrorism, or association or sympathy with persons or organizations that are promoting or threatening the use of force or violence, is a concern even, if the individual is not directly involved in planning a terrorist attack.

Self-radicalization is a phenomenon in which individuals become terrorists without affiliating with a radical group, although they may be influenced by its ideology and message. It usually addresses radical Islam, but there certainly have been instances of "lone wolf" terrorism from all ideologies, such as Timothy McVeigh.

INADVERTENT

Did you know? A U.S. Government official on sensitive travel to Iraq created a security risk for himself and others by tweeting his location and activities every few hours.

- Loose lips sink ships.
- The person does not have to intend harm to create a threat.
- Adversaries exploit DoN personnel through social networking sites, elicitation and eavesdropping/electronic surveillance.

Remember!

- Think before you talk or post
- Never speak about classified or sensitive info in public or on unsecured lines
- Shred sensitive information including PII
- Create strong passwords for each account and change them often
- Update and use security software (anti-virus, anti-spyware, anti-phishing components and firewalls)
- Follow the need-to-know principle
- Follow all security and IA policies and procedures
- Don't take home classified material

WORKPLACE VIOLENCE

When an individual's behavior indicates movement towards using violence as a means to advance a set of beliefs (political, religious, or social change) or to solve a personal conflict or problem.

Did you know? In 2008, 526 people were killed in the U.S. due to workplace violence?

- Past behavior is the best indicator for future behavior (i.e. history and/or promotion of violence)
- Anti-establishment and/or anti-authority sentiment
- Movement from idea to action (planning, recruiting, surveillance, acquisition of weapons)

CYBERSPACE

Adversaries gain unauthorized access to DoN computer systems for the purpose of stealing or corrupting data by gaining access to a network user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites or areas of the network. Sometimes personnel unwittingly facilitate an adversary's efforts by using their organization's internet portal to visit freeware sites and download infected games, screen savers and apps which facilitate the covert entry of the adversary into DoN systems.

New playing field using old techniques

Adversaries also use the internet and social networking sites (SNS) to obtain information on DoN personnel in order to exploit them through elicitation, inducements and coercion. Frequently monitored and exploited SNS include:

- Online dating
- Virtual Gaming
- Twitter
- Facebook
- Google +
- YouTube
- Blogs



OVER SHARING ON SNS

The USMC are preparing to support a big drug bust. One of the members on the team is upset he has to miss a social event and tweets that “something big” is going down at work. The tweet gets posted on Facebook by a friend. The dealers were able to search Facebook for keywords of the drug shipment, saw that “something big was going down” posted by a military member referencing their location and decided to call off the transaction.

An adversary wants to obtain info on a DoD scientist in order to exploit him for info on the latest DoD technology. However, the scientist has a limited internet profile. The adversary is able to find a common friend and discover his love for muscle cars on Facebook. The adversary makes up a false Facebook profile using a photo of a beautiful woman. The adversary “friends” the scientist via their common friend and infiltrates the relationship. They then send the scientist a link loaded with a Trojan virus and download all of his files.

EXPLOITATION VIA FALSE PRETENSE

Two USN intel officers discuss sensitive information in their vehicle. Little do they know, an adversary is trailing them. Using a device that has the capability to turn on the Bluetooth device on a cell phone, the adversary is able to listen to their conversation.

BLUETOOTH DEVICE EXPLOITATION

WHY YOU ARE A TARGET ...

CIRCUMSTANCES

- Placemat
- Access
- Ethnic/Cultural Background



BEHAVIORS

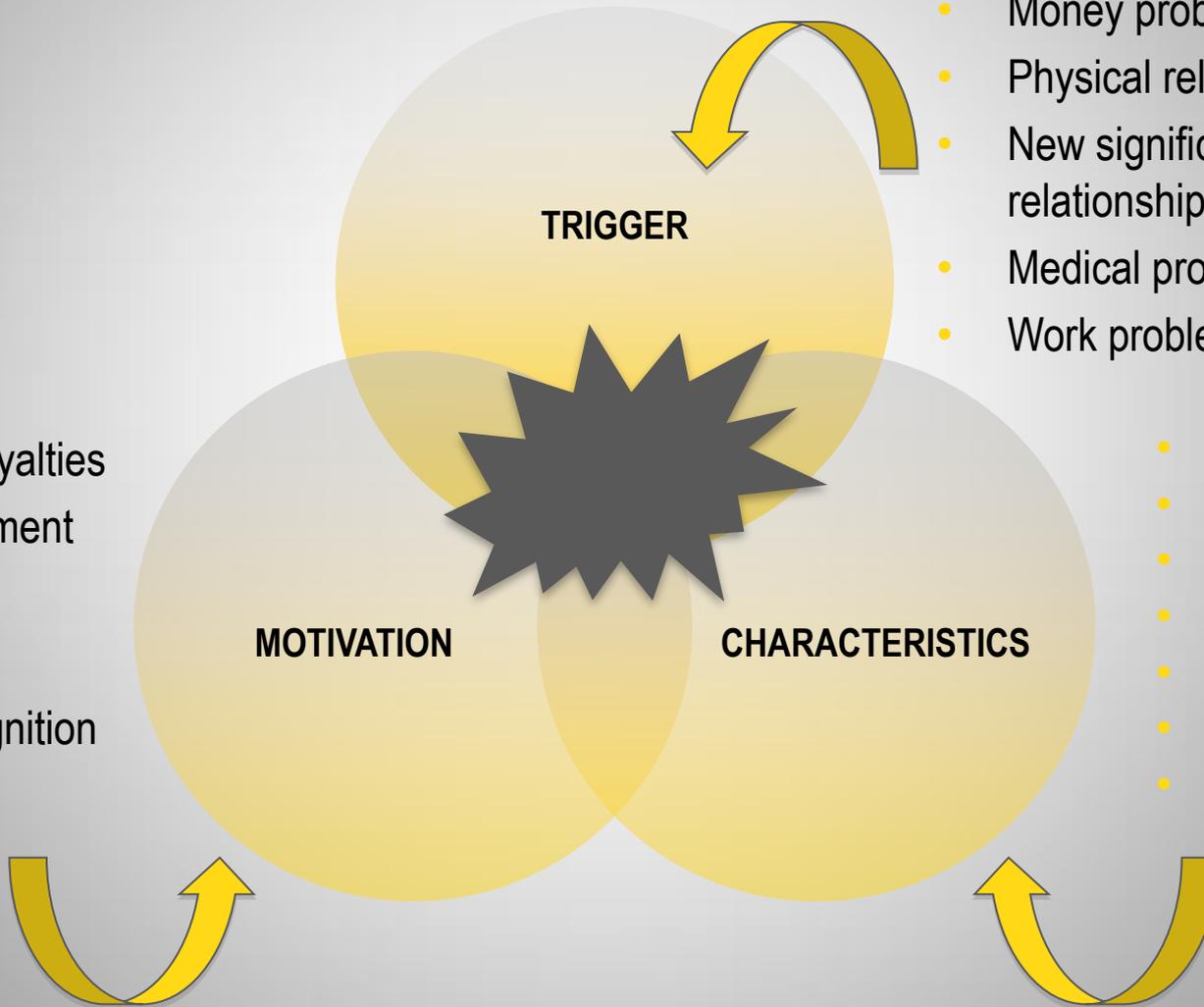
- Personal Relationships with Foreigners
- Illegal, Immoral or Embarrassing Behavior
- Strong Disagreement w/ US Policy
- Disgruntled
- Financial Problems
- Substance Abuse

CHARACTERISTICS

- Narcissistic
- Paranoid
- Entitled
- Antisocial
- Vindictive
- Impulsive/
Risk Seeking

WHAT ARE THE CAUSES

- Divided Loyalties
- Disgruntlement
- Money
- Thrills
- Ego/Recognition
- Coercion
- Ideology



- Divorce
- Death of a loved one
- Money problems/debt
- Physical relocation/PCS
- New significant relationship
- Medical problems
- Work problems

- Anti-social
- Narcissistic
- Entitled
- Vindictive
- Paranoid
- Impulsive
- Risk-seeking

GUESS WHO IS THE INSIDER THREAT



STATISTICS

- Most espionage is committed by men, 86%
- 83% are 30 years old or older
- 67% are civilians, however in the most recent cases the % of civilian and military members is about even
- 37% hold no clearance while 26% have a Secret clearance, 20% Top Secret and 17% Top Secret/SCI
- 67% volunteer
- Recent cases reflect a growing trend of spying for Al Qaeda or related groups
- Since 1990 more insiders were naturalized citizens, had foreign attachments (relatives or close friends), foreign business connections, or foreign cultural ties.
- #1 motive - divided loyalties, #2 - disgruntlement, #3 - money/debt
- Increased reliance on the Internet and sophisticated use of information retrieval and storage.

INDICATORS OF ESPIONAGE

- Divided loyalties
- Disgruntled
- Unexplained affluence
- Unreported foreign travel
- Unreported foreign contacts
- Working odd hours without authorization
- Taking classified material home without authorization
- Bringing unauthorized electronic devices into work areas
- Obtaining classified information without a need-to-know
- Inappropriately seeking classified information from others
- Unnecessary photocopying of classified material
- Bragging about what they know



INDICATORS OF TERRORISM

- Membership in any group which advocates the use of force or violence to achieve political goals or advocated loyalty to a foreign interest over loyalty to the U.S. government.
- Distributes publications prepared by group or organization of the type described above
- Makes pro-terrorist statements.
- Makes statements of support for the militant jihadist ideology of holy war against the West, and statements of support for suicide bombers even though they kill innocent bystanders, in e-mails or chat rooms, blogs, or elsewhere on the web.
- Frequent viewing of Web sites that promote extremist or violent activities that are not part of one's job.
- Makes statements about having a bomb, about having or getting materials to make such a device, or about learning how to make or use any such device, when unrelated to the person's job.
- Takes any action that advises, counsels, urges, or in any manner causes or attempts to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the armed forces of the U.S.

WHAT TO REPORT

Foreign Contact & Travel Reporting

- **ALL personnel** are to report to NCIS, contacts with any individual, regardless of nationality, whether within or outside the scope of the individual's official activities, in which:
 - Illegal or unauthorized access is sought to classified or otherwise sensitive information, or
 - The employee is concerned that he or she may be the target of exploitation by a foreign entity.
- In addition, personnel with a **security clearance (Confidential/Secret/Top Secret)** must also report to their security manager, foreign connections – an individual's immediate family, including cohabitants and other persons to whom the individual is bound by affection or obligation and are not citizens of the US and any financial interest in a foreign country. Those with a security clearance must also report all personal foreign travel as part of their required periodic reinvestigation.
- Those personnel with additional **accesses such as CPI, SCI and SAP** have additional reporting responsibilities to include reporting all projected official and unofficial travel and reporting of all foreign contacts that are close and continuing. Contact your SSO for your access program's specific reporting requirements.

WHAT TO REPORT

REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS per DODD 5240.06

Table 1. Reportable Foreign **Intelligence** Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report items 1-22 are subject to punitive action. The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action.

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through SNS that is not related to official duties.
2.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
3.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
4.	Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
5.	Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
6.	Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
7.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
8.	Discovery of suspected listening or surveillance devices in classified or secure areas.
9.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
10.	Discussions of classified information over a non-secure communication device.

WHAT TO REPORT

REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS per DODD 5240.06

Table 1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report items 1-22 are subject to punitive action. The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action.

11.	Reading or discussing classified or sensitive information in a location where such activity is not permitted.
12.	Transmitting or transporting classified information by unsecured or unauthorized means.
13.	Removing or sending classified or sensitive material out of secured areas without proper authorization.
14.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
15.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
16.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
17.	Unwarranted work outside of normal duty hours.
18.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
19.	Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.
20.	Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.
21.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
22.	Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or SNS.
23.	Trips to foreign countries that are: <ol style="list-style-type: none"> Short trips inconsistent with logical vacation travel or not part of official duties. Trips inconsistent with an individual's financial ability and official duties.
24.	Unexplained or undue affluence. <ol style="list-style-type: none"> Expensive purchases an individual's income does not logically support. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture. Sudden reversal of a bad financial situation or repayment of large debts.

WHAT TO REPORT

REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS per DODD 5240.06

Table 2. Reportable International **Terrorism** Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report items 1-9 are subject to punitive action. The activity in item 10 is reportable, but failure to report this activity may not alone serve as the basis for punitive action.

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

WHAT TO REPORT

REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS per DODD 5240.06

Table 3. Reportable FIE-Associated **Cyberspace** Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report items 1-10 are subject to punitive action. The activities in items 11-19 are reportable, but failure to report these activities may not alone serve as the basis for punitive action.

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of DoD account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data exfiltrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.



**HISTORY OF ALCOHOL ABUSE
REPEATED SECURITY VIOLATIONS**



GUN FANATIC

OVER \$270,000 IN DEBT



DISGRUNTLED



TOOK CLASSIFIED MATERIAL HOME

PAID CASH FOR \$540,000 HOUSE



DIVIDED LOYALTIES



AT OFFICE LATE AT NIGHT

FREQUENTED VIOLENT JIHADI WEBSITES & BLOGS

WHY REPORT

- Duty to report - first line of defense
- Subject to UCMJ, Article 92 or similar civilian statutes for not reporting
- Protects critical technologies/assets/infrastructure/personnel
- Limits potential battlefield vulnerabilities
- Helps determine foreign intelligence and terrorist activities
- Deflects unwarranted scrutiny and security suspicions
- Provides information for analysis

WHEN IN DOUBT REPORT!

Report any contact information or circumstances that could pose a threat to the security of U.S. personnel, resources, classified information, or controlled unclassified information to the Naval Criminal Investigative Service.

Phone 1-800-543-6289 | Web www.ncis.navy.mil | Text "NCIS" + your tip info to CRIMES (274637)

