Covert Action & Human Intelligence

"A good spy knows more about his informant than the man's own mother."
- Michael Collins

When we think of spying, we usually think of James Bond, Jason Bourne, Maxwell Smart or maybe Austin Powers. Spying is often called the second oldest profession in the world. Yet traditional cloak and dagger spies with their tradecraft seem more suited to the two world wars or the cold war between NATO and the Warsaw Pact in the last century.

Today's modern arsenal of technology allows us to capture secure communications via satellite 24/7, send up a "smart" drone to ascertain if it is friend or foe on a cell phone signal or unleash cyber hackers who will bring down a foe's computer firewalls like the walls of Jericho. It seems these technological advances make human spying obsolete.

Yet, traditional Human Intelligence (HUMINT) collection is more prolific than ever, and they are targeting our nation, our government, our businesses, our civic organizations, and our political freedoms. Today's threat is not just nation state enemy targeting U.S. interests regarding our military activities, economic needs, or geopolitical interests. Foreign business companies target our corporate knowledge and technology that drive our economy or worse collect our controlled technologies to build weapons designed to kill Americans or our allies.

Political, cultural, and social intelligence have become the latest trend with hostile elements, both foreign and domestic, utilizing "social engineering" techniques to manipulate social change and regulate the future development or behavior of a society. With data collected from Open Source Intelligence (OSINT), these hostile groups can formulate plans to penetrate groups and organizations using deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes while collecting valuable internal use only information.

This short presentation on the modern threat of HUMINT collection will:

a. Provide an Introduction to Espionage
b. Describe Intelligence Tradecraft Techniques
c. Discuss Alert Indicators to Tradecraft Techniques
d. Introduce Ways to Detect & Deter Tradecraft Techniques

Here in the Dallas-Fort Worth area we have corporations in several major industries like aerospace, energy, technology, finance, and medicine. We also have one of the largest foreign student populations attending our local universities along with hundreds of visiting foreign professors. We are located on a major crossroad of economic and corporate espionage operations and we need to pay attention to the threat.

"Never Attempt to Secure by Force What Can Be Won by Deception." – Niccolò Machiavelli

Elicitation Techniques

- **Assumed Knowledge** - Pretend To Have Some Knowledge On The Information Wanted
- **Bracketing** - Give A High Or Low Estimate Value To Entice A Specific Number
- **Confidential Bait** - Appear To Give Confidential Information To Get A Similar Response
- **Criticism** - Criticize People, Groups Or Plans The Target Has A Specific Interest In
- **False Statement** - Say Something That's Completely Incorrect To Induce A Correction
- **Feign Ignorance** - Be Ignorant & Exploit The Target's Desire To Inform & Educate
- **Use Flattery** - Use Praise To Coax A Person Into A Conversation About The Desired Data
- **Good Listener** - Just Listen & Exploit The Instinct To Tell A Story, Complain, Or Brag
- **Leading Question** – Ask A "Yes" Or "No " Question, But With A Buried Presumption

Deflecting Elicitation

- Refer The Person To Public Sources Or Official Websites
- Ignore Any Question Or Statement You Believe To Be Improper
- Change The Topic Or Deflect The Statement With A Question Of Your Own
- Give A Vague Answer Or Say You Simply Don't Know
- Say You Need To Clear The Topic With Management
- Simply Say You Can't Discuss The Matter

If You Believe Someone Has Tried To Elicit Information From You...

REPORT IT!

The Original Simple Sabotage Techniques

1. **Obedience** - Doing Everything By The Book, Use Proper Channels & No Short-cuts
2. **Speech** - Talk Frequently, Make Speeches & Cite “Personal Experience”
3. **Committee** - Put All Decisions To A Committee For “Extensive Consideration”
4. **Irrelevant Issues** - Bring Up Matters Not Related To The Specifics Of The Meeting
5. **Wording** - Haggle Over The Wording Of Communications, Minutes Or Resolutions
6. **Revisit Old Decisions** – Question Previous Meetings Decisions Or Solutions Selected
7. **Caution** - Excessive Warning, Suggest Prudence In Deciding & Caution In Solutions
8. **Authority** - Ask "Is This Really Our Decision Or Who Has The Authority To Decide?”
9. **Policy** - Ask If This Decision Will Conflict With Management Policy Or Procedures

Modern Simple Sabotage Techniques

1. **Email** - Carbon Copy Anyone Remotely Tied To A Project & Require A Response
2. **Matrix Management** - A Matrix Outline Tends To Make Nobody Feel Responsible
3. **Same Talent** - Using The Same Talented People To Work On Important Projects
4. **Success** - Assuming The Same Talented Person In One Vocation Can Do the Same in Another

What Is Your Best Defense

- To Have A Firm Security Posture About The Information You Have
- Maintain Good Situational Awareness With Whom You Are Interacting
- Develop A Counterintelligence Mindset That You May Be Targeted
- Be Aware Of Journalists That Use Leading Questions To Create Quotes Or Headlines
- Keep Your Opinions, Motivations, Habits, Ideology, Vices & Skeletons To Yourself

Protect Your Secrets

- Recognize The Intelligence Threat & Protect Important Information
- Limit Access To Sensitive Material & Use "Need To Know" Methods When Sharing It
- Develop An Insider Threat Assessment Based On Projects, Plans, People & Threats
- Be Aware Of Elicitation Attempts From People You Do Not Really Know
- Be Aware Of Simple Sabotage Habits Brought On By Ignorance Or By Intent

Report Suspicious Events

Who & What To Avoid

- Blabbermouths (Walking Billboards, Alligators, Opinioned Hotheads, etc.)
- Lobbyists Or Activist Groups (They Always Want Something)
- Elected Officials Or Staffers (Staffers Are The Worst)
- Journalists (Conservatives, Liberal & Middle of the Road)
- Social Media Platforms (Facebook, Twitter, Blogs, etc.)
- Meetings In Public Venues (Hotel Lobbies, Bars, Clubs Or Restaurants)