Subversion and Espionage Directed against You (SAEDY)
SAEDA -- Subversion and Espionage Directed Against the (US) Army

Background
Personal experience
Inspiration

‘Rouse him, and learn the principle of his activity or inactivity. Force him to reveal himself, so as to find out his vulnerable spots.’

‘All warfare is based on deception.’

― Sun Tzu, The Art of War
Behavioral Infosec

**Design For Behavior, Not Awareness**: by Ben Tomhave, Oct 31, 2017;
http://www.secureconsulting.net/2017/10/design-for-behavior-not-awareness.html

- Behavior happens when three things come together: **Motivation**, **Ability**, and a **Trigger** (a prompt or cue)

So if we need people to start following a better, preferred process that will help reduce risk to the organization, we must find a way to make it easy to do (**Ability**) or find ways to make them want to follow the new process (**Motivation**). Thus, when we tell them "follow this new process" (**Trigger**), they'll make the desired choice.
Social Engineering (SE) is a blend of science, psychology and art. “Any act that influences a person to take an action that may or may not be in their best interest.”

– Chris Hadnagy, @HumanHacker  https://www.social-engineer.org/

Based on **specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques.** (Wiki)
“Organizations hire me to evaluate their security, which I do by seeing if I can bypass it. i.e. lockpicking, climb over walls or hop barbed wire fences. I get to go dumpster diving and play with all sorts of cool gadgets”

“But usually, I…to pretend to be someone I am not. Most often I get to approach people in-person”

Sophie <Daniels> is a physical penetration tester and information security consultant. She specializes in social engineering security assessments including physical, voice (vishing) and text (phishing). Prior, Sophie was a journalist, photographer, and a mom. @HydeNS33K

Why Use Social Engineering

...because it consistently works.

There is no patch for an untrained user or even an experienced security professional who forgets, in the heat of the moment, to follow what they have been taught.

It is this naivety that creates a perfect atmosphere for a breach.
Espionage: "... gathering, transmitting, Or losing ... information related to the national defense".

US defines espionage: "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".
Spying — v. First known use: 13th Century

• To watch secretly usually for hostile purposes

• To try secretly to get information about a country, organization, etc.

US man may face execution, accused of sending secrets to Chinese spies with illicit communications device

Bumbling Ex-CIA Officer Charged With Selling Secrets to China

A prestigious Chinese think tank provided cover for the intelligence operation that ensnared Kevin Mallory.
A systematic attempt to overthrow or undermine a government or political system working secretly from within.

**Russian Hackers Stole NSA Tools From Contractor Who Used Kaspersky Software**

Suspected to be the main entity behind NSA-Kaspersky issue and is sentenced to 5.5 years.

The material included hacking tools he was helping to develop to replace others considered compromised following the breach of NSA material by former contractor Ed Snowden.
Traditional idea of espionage, where one country or company is spying on another or a target group. The stages are similar to traditional surveillance.

"We don't need to be following folks around in order to gain some competitive advantage. We're better than that. To be crystal clear, to the extent anyone is working on any kind of competitive intelligence project that involves the surveillance of individuals, stop it now."

—Uber's general counsel Tony West...no place at the company for surveillance practices
Industrial, economic espionage, or corporate espionage is a form of spying conducted for commercial purposes instead of purely national security.

U.S. charges Chinese-Canadian citizen with trade secret theft

**Medrobotics**. CEO Samuel Straface was leaving the office the evening of August 28 when he spotted a man he did not recognize working on a few laptops in a company conference room. After being confronted the uninvited guest explained he was there to meet a couple of executives of the company. Straface knew that one was out of the country and the other did not have such meetings scheduled. The intruder then claimed he was there to meet the CEO, Samuel Straface, himself.

**Dong Li**’s his lawyer argued that prosecutors lacked evidence that Liu accessed Medrobotics Corp’s computer systems.

His lawyer, Robert Goldstein, also said in court papers that Liu suffered a brain injury in an accident in 2012, when he was a partner at a Chinese patent law firm, and had been “struggling to accept the fact he was no longer brilliant.”
The legacy of Cold War espionage:
Following the end of the Cold War, the US Intelligence noted a redirection amongst the espionage community from military to *industrial targets*, making use of "underemployed" spies.

- Most Soviet spies were Americans
- There were legal and illegal agents
  - Legal agents would be a part of the Embassy, etc.
  - Illegal agents would be here to blend in with citizens
- Russia prefers illegals, who often serve as couriers
- It is very expensive to maintain spies
“…the old proven tradecraft is pretty much the same.”
Former GRU Officer, Boris Volodarsky
Why didn't you use this information to your advantage and attack the United States?

“There is an irony here, which you overlook. In a way, John Walker helped both countries avoid a nuclear disaster. How?

Because he enabled us to understand your true intentions. This helped us determine when you were willing to fight and when you were simply puffing up your cheeks.”

This is an aspect of spying that often is overlooked.
North Korea Cyberwarfare

After watching the American “shock and awe” campaign of the 2003 invasion of Iraq, Kim Jong-il issued a warning to his military:

“If warfare was about bullets and oil until now, warfare in the 21st century is about information.” – to top NK commanders

“Both the US & SK have placed digital “implants” in the Reconnaissance General Bureau, the NKorean equivalent of the CIA, according to documents Snowden released.”
Trust, But Verify (1986)
Don’t Trust, Verify (2017)

“Trust, but verify”

Pres. Reagan preparing for talks with Mikhail Gorbachev in 1986, learned a few Russian proverbs, and the one liked best was “Doveryai no proveryai” — trust, but verify.

Reagan liked it so much, Gorbachev expressed annoyance for his using it at every meeting.

The Blockchain community adopted it as a catchphrase, every node in a blockchain network verifies the data that it receives from others in order to ensure security.

“Don't Trust, Verify"
Social Engineering = Espionage / Spying / Subversion

“Any act that influences a person to take an action that may or may not be in their best interest”

Suspected Russian spy found working at US embassy in Moscow; Austrian colonel ‘spied for Russia since 1990’s;

Details Surface About Chinese Spy Who Worked For Sen. Feinstein

Mole for the government of China managed to stay by Senator Dianne Feinstein’s side for nearly 20 years as her driver.

Accused Russian spy Maria Butina
MICE - motives for spying

“Did you do it for love, did you do it for money, did you do it for spite, did you think ya had to, Honey?”

- **Money**

- **Ideology**

- **Compromise or Coercion**

- **Ego or Extortion**

Since real spies are so good, you never really know what actual spying is. But I do think spying is a lot more dangerous than we are led to believe.

---

Richard Armitage

---

*BEWARE OF SPIES!*

DON'T TALK. THE ENEMY HAS EARS EVERYWHERE.

DON'T imagine that every one who SPEAKS ENGLISH is to be trusted, and that every UNIFORM covers a FRIEND.
John Walker, Navy, spied 18 yrs

“They could have exposed Walker if they had learned about him. So the fact that Walker was never exposed by us (USSR) shows that we did our job well. In my opinion, there were actually perhaps no Mistakes with Walker. And he could have continued to make us happy up until today if it were not for his own mistakes – his lavish spending, his problems with his wife, etc.
Aldrich Ames, CIA employee, spied 9 yrs

Ames sold information to the Soviet Union and Russia exposing 12 American spies working undercover in Moscow. All of them were jailed, most of them were executed.

In 1985, broke, Ames made his first sale of names at the Soviet Embassy in Washington D.C. for $50,000 ($112,000 today). Marrying his second wife, Maria del Rosario Casas, a Columbian spy, also charged with espionage, the KGB gave them a $2 million wedding present. According to the Times, it was the most money that any American spy received from the Soviet Union. Ames pled guilty to espionage, on April 28, 1994, he was sentenced to life in prison without the possibility of parole.
• A person will become a spy simply because of their beliefs.

• These can include their political opinions, their national allegiances, their cultural or religious beliefs.

Ann Montes, Queen of Cuba, got a 25-year prison sentence, five years probation, and avoided the publicity of a trial.

Walter Myers, State Dept. analyst, spied for Cuba, gets life; wife 6 years
“Frequently, people who go along a treasonous path do not know they are on a treasonous path until it is too late.”
--Former CIA Director John Brennan testified in May 2017

So sure in their convictions they are acting in their own best interest or in the best interest of their country they have no idea they are being completely manipulated.

The Russians know all this, too.
Threats of injury or death are the most direct form of coercion.

Threats can also be made against family or friends of the target.

A more subtle form of coercion is blackmail, threatening to release embarrassing information about a person's activities unless that person provides them with secret information. Add: extramarital affairs, homosexuality, and undiscovered crimes.
MICE - Compromise or Coercion

“Any act that influences a person to take an action that may or may not be in their best interest”
Coercion — the reason for security screenings

Honeypots are as old as espionage itself.

Step 1: Have a “swallow” seduce a spy, government employee, or politician, take photographs.

Step 2: Threaten to release the photographs.

The result: A shake-and-bake spy at its finest.

In the world of espionage, the term “honeypot” refers to the use of sexual seduction to recruit agents, or perhaps trap an enemy agent.

For example, a scientist living in London, Mordechai Vanunu, who had disclosed Israeli nuclear secrets, began an affair with a Mossad (the Israeli intelligence service) agent, Cheryl Bentov, operating under the name "Cindy" and masquerading as an American tourist, on September 30, 1986. She persuaded him to fly to Rome, Italy, with her on a holiday. Once in Rome, other Mossad agents drugged him and smuggled him to Israel on a cargo ship.
MICE - Compromise or Coercion

“Any act that influences a person to take an action that may or may not be in their best interest”

How to set a honey trap

The best security and military training in the world is no match for the charms of a femme fatale. Using feminine wiles to access state secrets sounds like hackneyed fiction – surely anyone with a secret worth keeping would run at the sight of a beautiful lady in red lipstick? But the oldest trick in the book never stops working, and spy agencies continue to use seduction as an effective method of espionage.

Stefan Wolff, professor of international security at Birmingham University, says that few governments would consider seduction an off-limit technique. “If you’re in the spying business, any opportunity that you have to get information, you will use,” he says. “Especially given what we’ve learnt from Wikileaks and Snowden, not much is considered to be beyond the pale when it comes to key issues of national security. I would argue, maybe that’s the right approach. If you want to save lives then a honey trap is a much more palatable approach than waterboarding.”
MICE - Compromise or Coercion

- Sparrows (spies) were weapons in a global struggle for power.
- They were taught to intuit what was needed and become that.
- There were no limitations on what the state might ask of a sparrow.
Caught in a Honeypot – Marine Clayton Lonetree Betrays His Country

More Moments in U.S. Diplomatic History

Marine Security Guard Clayton Lonetree was seduced by a Russian woman, “Violetta Seina,” at the annual Marine Corps Ball in November 1985. She worked as a telephone operator and translator for Embassy Moscow but lived a double life as a KGB agent. Lonetree was so highly regarded that he was chosen to be part of the Marine unit assigned to provide security for the 1985 summit between Soviet premier Mikhail Gorbachev and President Ronald Reagan. However, despite the strict non-fraternization (“no frat”) policy imposed on all MSGs in such parts of the world, Lonetree and Seina began a relationship soon after they met. She introduced him to her “Uncle Sasha,” KGB operative Aleksey Yefimov, who asked Lonetree to become a “friend of the Soviet Union.”

Lonetree was soon convinced to turn over confidential information, including after he was transferred to Embassy Vienna in 1986, he passed on blueprints and burn bags with top secret cables, including on U.S. arms reduction. On December 10, Lonetree came forward to the CIA station chief in Vienna and confessed. He turned over to the Navy Intelligence Service (NIS) and placed under arrest, espionage.

Lonetree was convicted on multiple counts of turning over classified information in 1987 and sentenced to 30 years in prison. He was the first U.S. Marine ever convicted of espionage. Because of his cooperation with authorities, his sentence was reduced by 25 years of which he served nine before being released in February 1996.

Chaos ensued as this scandal began to unfold. Secretary of State George Shultz did little to address the issue. Brown was a former Marine who had served in Moscow in his oral history, when the Secretary of State “asks you to do something, you do it.”

Lonetree’s case was assumed to have been so infiltrated that staff pass messages back and forth, while the new embassy building was discovered. Lonetree's cooperation interviewed by Charles Stuart Kennedy beginning in November 1998.
MIA ASH FACEBOOK SCREENSHOTS AND PHOTO POSTINGS (Pleas of Mia’s friends on Facebook were men from ages 20 to 40 and they frequent commented on her newly added photos and kept up with her updates. The is for organizations and in positions which were targets of this Iranian Threat oil/gas, technology, construction, aerospace, financial and consulting organ Israel, Saudi Arabia, Iraq, India, U.S. and Bangladesh.

Mia Ash primarily lured middle-aged men who worked as technicians and engineers at oil and gas, aerospace and telecommunications firms in the Middle East. Those include Saudi Arabia and Israel in addition to India and the United States.

Dell SecureWorks observed Mia Ash sending specific malware, concealed as a “photography survey” with an attachment, to victims that matched malware sent by Iranian hacking group Cobalt Gypsy.
MICE - Compromise or Coercion

“Any act that influences a person to take an action that may or may not be in their best interest”

In the ’60s, a communist mole who had infiltrated the CIA gained his colleague’s trust through wife swapping. Free love helped Karl and Hana Koecher get to know important CIA officials, and they then passed information onto the KGB. Meanwhile a French diplomat, Bernard Boursicot, was seduced by Chinese secret agent Shei Pei Pu – whom Boursicot thought was a woman, but was in fact a man. The pair were together for 18 years, and Shei Pei Pu even convinced Boursicot that he was pregnant and had given birth to their son.

>> Shi Dudu

Shi was a man but told Boursicot that he had been born female

It’s not just about sex

The most successful acts of seduction aren’t quick flings but long-term emotional manipulations, where the target often believes that they’ve fallen in love. After World War Two, there were far more women than men in West Germany, and so the East German government sent “Romeo” spies to entrap lonely secretaries. In some instances, the spy married his target and admitted that he was a double agent – but working for a friendly country. “Romeo” would tell his wife that his government was worried that West Germany wasn’t being completely honest – could she provide a few details to keep his boss happy? These marriages could last for decades.
Ego and pride in motivating spies is observed, but is often hard to demonstrate.

Superiority over colleagues, whom they are outwitting. A person can be enticed by the sense of importance or significance which it gives them.

MICE - Ego or Extortion
MICE - Ego

WHISTLEBLOWER COMES CLEAN: 'I'VE DONE NOTHING WRONG'
Robert Hanssen is the alpha and omega of ego-driven spies. Hanssen felt unappreciated at the FBI and his self-esteem demanded satisfaction.

Money “was a way to keep score and a trigger, but not the driver.”
Subversion and Espionage Directed Against You

Just because you are paranoid,

doesn't mean they are not after you!
Spies Like Us
Spies Like Us

SOME STATISTICS:

100% of men didn’t notice King Kong in this picture
Calling these efforts SE instead of espionage, reduces the severity of the activities.

Information security training, as per compliance rules, however individuals go back to their work environments leaving this information behind as well.

Become enlightened, self-aware you are targets and it is personal, as you are facing centuries of proven espionage tradecraft successfully applied.

My 0-day exploits are your employees.

8:23 AM - 3 Oct 2016
Reporting & Questions

**Reminder:** While indicators do not always equate to an actual foreign collection threat, they can serve as a signal.

A number of indicators in a given situation might warrant further examination.

Reports of actual, probable, or possible espionage should be submitted to the FBI.

Do not talk or share with anyone else.

There is no patch for an untrained user or even an experienced security professional who forgets, in the heat of the moment, to follow what they have been taught.