INVESTIGATING CYBER TERRORISM - NOTES

CYBERCRIMES, TERRORISM, & WARFARE

CYBERCRIME - A crime that has been committed with the use of a network (intranet, Internet, Darkweb, etc.) and is a key element of a crime.

TYPES OF CYBERCRIMES

1. Hacking
2. Digital Child Pornography
3. Identity Theft
4. Intellectual Property Theft
5. Online Fraud
6. Cyber Stalking
7. Cyber Bullying
8. Malware

HIGH TECHNOLOGY - Highly developed electronic devices such as computers, networking components, cellular phones, point of sale components, telephony, global positioning systems (GPS), satellites, and other communication systems.

HACK - The manipulation of hardware or software to perform an act that was not originally intended by the developer.

HACKING - Is the theft, removal, alteration, deletion, encryption, or publishing of data by unauthorized means victimizing an individual, government, and/or business.

TYPES OF HACKERS

- Black-Hat – Personal gain or malicious attack which causes damage. This epitomizes the hacker image.
- White-Hat – These are the good guys in the hacking world. They provide security for networks and the Internet.
- Gray-Hat – Opportunistic and will hack for profit. Often, they will create a network breach and then extort money by offering to solve it.
- Script Kiddies – Most dangerous of all hackers, because they do not have the knowledge to create their own hack/worms. Instead, they rely on hacker programs created by others. Their lack of knowledge is what makes them dangerous.
- Hacktivists – These hackers attempt to spread a political or social message.
- Cyber Terrorists – Create fear of death and destruction in the general public based on ideology.

CYBER WARFARE

The use of high-technology by a nation-state to cause damage or disruption of another nation's communications, network, electronic systems, or any other military assets.

- Operation Orchard (2007) - a military operation conducted by Israel to destroy a nuclear enrichment plant located in Syria. Israeli hackers disabled the Syrian air defense system

to make their bombers invisible.

- Estonia (2007) – a Russian BOTNET DDOS attack conducted against Estonia's government and banking networks which shut down all of the country's networks

TERRORISM
The preparation for and/or the use of violence or threat of violence against non-combatants or property to intimidate or coerce a government, the civilian population, or any segment thereof in the furtherance of political, religious, or social objectives.

ELEMENTS OF TERRORISM

1. Threat or use of violence
2. Non-combatants (civilians)
3. Coerce or change public policy
4. Political, religious, or social objectives

CYBER TERRORISM
The use of high-technology breach the integrity, confidentiality, and/or availability of information which creates or threatens physical bodily harm, death, and/or the serious destruction of critical infrastructure in order to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political, religious, or social objectives.

ELEMENTS OF CYBER TERRORISM

1. Use of computer network or high-technology;
2. Breach of data (alter, delete, encrypt, etc.);
3. Threats to or creates serious harm to critical infrastructure; and
4. Political, religious, or social objectives

FUTURE CYBER THREATS

- Modern Living – smart everything
- Health – pacemakers, insulin pumps, etc.
- Fit Devices – Fitbit, iPhone, etc.
- Hospital Equipment – monitors and reporting
- Financial Sector – Near Field Communications (NFC) smart phones, Apple Pay, etc.
- Transportation – modern cars (fly by wire), GPS, Internet hub, Bluetooth, etc.
- Energy & Water – remote meters, remote on/off
- Public Services – smart grids, power, water, waste, etc.
- Robots – cleaning, home health care
- RFID Chips – will everybody and everything have one? IP v.6

CYBER CRIMES DEFINED

CYBER INTRUSION (Hacking)
The unlawful or unauthorized access of a computer network or system for any reason (read, write, delete, alter, etc.). This act is commonly known as "hacking."

CYBER ESPIONAGE
Knowingly benefit a foreign government by stealing trade secrets with the use of high-technology. Cyber Espionage may be conducted by a corporation, individual(s), or state actors.

MALWARE
Software designed to gain access, damage, and/or alter a computer or system without the knowledge of the owner. Examples of this software includes computer viruses, worms, Trojan horses, ransomware, spyware, and adware.

IDENTITY THEFT
Accessing personal identifiable information without the person's consent.

CYBER FRAUD
Using a person's personal identifiable information for illicit financial game.

CYBER BULLYING
Aggressive behavior involving a real or perceived power imbalance that is repeated, or has the potential to be repeated, over time using high-technology, such as cell phones, computers, social media, texting, chat programs, blogs, and Web sites.

CYBER THREATS
Threatening communications that are conveyed via high-technology to harm a person or property, to kidnap a person, or to damage a person's reputation (18 U.S.C. § 875).

CYBER STALKING
The use of high-technology to commit a pattern of repeated and unwanted attention, harassment, contact, or any other course of conduct directed at a specific person that would cause a reasonable person to feel fear for themselves or their immediate family.

SWATTING
Deceives emergency responders into dispatching a Special Weapons and Tactics (SWAT) team to the location of the victim. Swatting is extremely dangerous for the victim and law enforcement personnel.

CYBER EXTORTION
An attack or threat of attack against computer services or networks using DDoS or malware that encrypts data on an organization's computer system or network (Ransomware).

SEXTORTION
A form of cyber extortion that occurs when individuals demand that the victims provide them with sexual images, sexual favors, or other things of value. These demands are accompanied by threats to harm or embarrass the victims if they fail to comply (e.g., intimate photos). Victims of sextortion are often minors but can also be adults.

REVENGE PORN
The distribution of nude/sexually explicit images/videos taken consensually during an intimate relationship. The images/videos are posted online, often with personal identifiable information, motivated by revenge.

CYBER TERRORISM
The use of computer network or high-technology to breach data (alter, delete, encrypt, etc.) with the purposes of creating serious harm to critical infrastructure with to with political, religious, or social objectives.

OTHER DEFINITIONS

- **DOXING**
  Broadcasting personally identifiable information about an individual on the Internet. It can expose the victim to an anonymous harassers, phone calls, email, and appearing at the victim's home ("GamerGate").

- **PERSONAL IDENTIFIABLE INFORMATION (PII)**
  Information which can be used to distinguish or trace an individual's identity.

CRITICAL INFRASTRUCTURE

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 identifies 16 critical infrastructure sectors.

16 CRITICAL INFRASTRUCTURE SECTORS

1. Chemical - The Chemical Sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely.

2. Commercial Facilities - The Commercial Facilities Sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within the sector operate on the principle of open public access, meaning that the general public can move freely without the deterrent of highly visible security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities.

3. Communications - The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government using interconnected; satellite, wireless, and wireline providers which depend on each other to carry and terminate their traffic.

4. Critical Manufacturing - The Critical Manufacturing Sector has identified several industries to serve as the core of the sector including; primary metals manufacturing; machinery manufacturing; engine and turbine manufacturing; electrical equipment, appliance, and component manufacturing; and transportation equipment manufacturing.
5. Dams - The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

6. Defense Industrial Base - The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

7. Emergency Services - The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

8. Energy - The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

9. Financial Services - The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.

10. Food and Agriculture - The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity.

11. Government Facilities - The Government Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment.

12. Healthcare and Public Health - The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters.

13. Information Technology – This sector provides virtual and distributed functions which produce and provide hardware, software, and information technology systems and services.

14. Nuclear Reactors, Materials, and Waste - The Nuclear Reactors, Materials, and Waste Sector covers most aspects of America’s civilian nuclear infrastructure, from the power reactors that provide electricity to millions of Americans, to the medical isotopes used to treat cancer patients.

15. Transportation Systems - The Transportation Systems Sector consists of seven key subsectors, or modes: aviation; highway and motor carrier; maritime transportation system; mass transit and passenger rail; pipeline systems; freight rail; and postal and shipping.

16. Water and Wastewater Systems – This sector ensures that the supply of drinking water and wastewater treatment and service is maintained to sustain the Nation’s economy.

What does a cyber warrior look like?

Distributed Denial of Service (DDoS)

- Attempts to overwhelm it’s target(s) with requests.
- Prevents legitimate use of server.
- Web services, email, corporate operations, etc.
- Targeted attack.

Advanced persistent DoS (APDos)

Crime-as-a-Service (CaaS)
Hacking services purchased online/darknet to accomplish tasks or create malware.

Bot (robot) + Net (network) a/k/a "Zombie Army"

Botnet - A group of computers infected with malware that allows for the unauthorized control.

Command and Control Server – sends commands to zombie computers / botnet. There may be several C&C servers.

Botmaster – Creates and operates the C&C servers.

First Botnet emerged in 1999
"Sub7"
"Pretty Park"

2002 New Developments
"SDBot" – Developer made widely available.
"Agobot" – 3 prong attack, 1) Backdoor, 2) Disable AV; 3) Blocked AV sites.

2003 SPAM bots and data mining
"Spybot" keystroke and mining
"Bagle" & "Bobax" first SPAM bots

2005 Zeus
Developed by group called "UpLevel"
"Point-and-click" malware creation
Modular and customizable.

THE CYBER TERRORISM PROCESS

STEP 1 - GATHERING TARGET INTELLIGENCE
- Target selection
- Specific target group information (org chart, personnel, etc.)
- Physical presence (brick & mortar)
- Gathering system information (probing)
- Test runs & responses

STEP 2 - GATHERING TECHNOLOGY
- CRIME as a SERVICE (CaaS) - Hackers For Hire.
- Darkweb - Cyber flea market for cyber weapons and personnel.
- DDOS attack software (blunt object).
- Prices vary on kits.
- Development & testing difficult – systems not available for testing.

STEP 3 - OPERATIONAL
- Carry out the attack via attack vector (step-by-step chain).
- Each step must be completed before moving on.
- Create access to the target (spoofing, forging credentials, etc.).
- Access to air-gapped systems.
- Expensive if not lucky.

WHAT STARTS AN INVESTIGATION?

- Strategic Initiative(s)
- Event takes place.
- Ancillary to another crime.
- Tips (see something, say something)
- Informant(s)
- Suspicious Activity Reports.

4 STEPS OF HIGH-TECH FORENSICS

1. Collection – Preserve the data and preserve the evidence. Take pictures/video of the scene.

2. Examination – Maintain the integrity of the data/evidence. Document the methodology used to examine the evidence. Review the warrant .

3. Analysis – Understand what how the evidence relates to your case or other cases.

4. Reporting – The documentation must be complete and understandable to non-forensic experts.

COLLECTION

U.S. CONSTITUTION, 4TH AMENDMENT
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

REASONABLE SUSPICION
An officer may stop and briefly detain a person for investigative purposes if he has a reasonable suspicion supported by articulable facts that criminal activity may be afoot. Review of reasonable suspicion will be based on the totality of the circumstances that exist at the time and place of the stop. If, during the course of an investigation, reasonable suspicions are dispelled, the stop must end.

PROBABLE CAUSE
Probable cause exists where the facts and the totality of the circumstances within the officer's knowledge and of which they had reasonably trustworthy information are sufficient in themselves to cause a man of reasonable caution to believe that an offense has been or is being committed

EXCEPTIONS TO THE WARRANT REQUIREMENT

- Consent
- Exigent Circumstances
- Incident to an Arrest
- Plain View
- Inventory Searches
- Probation and Parole

CONSENT TO SEARCH

Elements of consent:

- Must have the authority to give consent
- Must be of mature age to give consent
- Must have the mental capacity to give consent
- Cannot be under duress

Consent document should contain:

- The area to be searched
- What is being searched for
- Investigators intention to search within the computer
- The potential need to make a copy
- The potential need to remove the computer or electronic device from the premises

The ways consent can be withdrawn:

- Verbally.
- Obvious Gesture.
- The natural end to the consensual search.

EVIDENCE & INFORMATION COLLECTION

- #1 RULE - SAFETY FIRST.
- Research (OSINT, HUMINT, records, subpoenas, court documents, etc.).
- Create investigative plan (people, locations, equipment, and the technology).
- Plan for the scenes (warrant, devices, storage, live data capture, dead data capture, etc.).
- Control the scene and suspects (keep away from input devices).
- Videos, photographs, and sketches of the scene.
- Collecting the evidence. Maintain the "chain of custody" (bags, access logs, SOP).
- Maintain the integrity of the evidence and data.
- Write-Blockers (work with copies only).
- Log and document every step.

OBTAINING A WARRANT

Application is based on "probable cause."

- Ancillary to another case/charges
- Informant(s)
- SAR (Suspicious Activity Report)
- IP address from Internet provider
- IDS – Intrusion Detection Systems (firewalls, honeypots, logs)
- PROFILE – online profile/IRL profile information

Supported by signed affidavit(s) under oath.
Signed by a judge or magistrate.

HARDWARE ACQUISITION

- SAFETY FIRST!
- Check the Search Warrant (location, scope, date, signature, etc.)
- Make sure the search team understands digital preservation rules.
    - DO NOT turn on or off computers or other electronics.
    - DO NOT allow suspect(s) to touch keyboards or other equipment.
    - DO NOT unplug or move equipment before photographs, video, printing & sketches.
- Photograph and video front/back/monitor of computer and network equipment.
- In most cases, remove power cord from power source (UPS) and remove battery.
- CELL PHONE CONSIDERATIONS: screen locks, passwords, remote wipe, plain view.

- Label and use evidence markers before placing in paper containers.
- Log all evidence contemporaneously.
- Use "Faraday" bags or containers when possible.

EXAMINATION

FORENSIC ACQUISITION

- Forensic Examination of Digital Evidence: A Guide for Law Enforcement
- Review the warrant
- IMAGE COPY – "sector-by-sector replica," Work with copy only
- WRITE BLOCKERS - HASH VALUES - Verify the data
- RAM - Volatile data
    - Memory dump leaves a footprint
    - Decide what is more important
    - Programs/processes running
    - What files opened
    - Network connections
    - Passwords
    - Malware running

COUNTER FORENSICS

- **ENCRYPTION** sha256 encryption VERY tough to break
- **MEDIA WIPING** Using wiping software to add 1s and 0s to delete evidence.
- **STEGANOGRAPHY** Legitimate files are gutted to hide evidence.
- **ROOTKITS** Programs hidden in flash memory which will hi-jack the way the operating system acts. Logic bombs can be hidden in these rootkits/booby-traps.
- **HOMOGRAPHIC** Using specialized text to hide the name of a real file
- **FILE SIGNATURE MODIFICATION** Changing the file extensions
- **METADATA** Programs used to change metadata of files to hide illegal activity.
- **SLACK SPACE** The space on a hard drive that is not used by the operating system but can be used to hide illegal activity
- **RESOURCE WASTE** The cost to process the media far exceeds the benefits.
- **FORENSIC TOOLS VULNERABILITIES & EXPLOITS**
  Programs inserted on the hard drive so that when forensic tool kits (EnCase, FTK, etc.) are used, they activate software designed to attack the investigator's computer.
- **ANTI-FORENSIC – FLUSHABLE DEVICES**
  Running operations strictly on flash memory so that information will be flushed upon

turning the computer off.

- **COMPRESSION BOMBS** Zip files with "0s" going multiple levels freezes system.

- **MISLEADING EVIDENCE**
  Evidence left on the hard drive to send investigators down a rabbit hole.

ANALYSIS

- Create dictionaries
- Establish search parameters, terms, and hash sets
- Signature Analysis (file extension match)
- Filter Evidence (known good, hash sets, OS)
- Keyword searches (registry, files, slack files, temp files)
- LNK Files – Link files provide path to original file
- PREFETCH – indicates what programs have run (C:\Windows\Prefetch)
- EVENT LOGS – Everything the computer has done
- REGISTRY – programs, configurations, boot process
- RESTORE POINTS – previous logs, registry, and temp files

REPORTING

Most forensic software will have a built-in report generator.

The report will be used for:

- Helping the prosecutor decide whether to go forward with an indictment.

- Assisting the prosecutor in convincing the defendant to plea bargain.

- Helping the prosecutor during the trial phase.

Investigators should remember that their reports and actions will be scrutinized by both sides and the careful attention to detail in forensic reports are as important as any other police report.

MIDTERM ----------

USCYBERCOM

- Component of US Strategic Command (USSTRATCOM)
- Plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

Three Focus Areas

1. Defend the Department of Defense Information Network (DoDIN)
2. Provide support to combat commanders
3. Strengthen our nation's ability to withstand and respond to cyber attack

United States Computer Emergency Readiness Team (US-CERT)

- The National Cyber Incident Response Plan (NCIRP)
- The Critical Infrastructure Cyber Community C³ (pronounced "C Cubed") Voluntary Program
-

The National Institute of Standards and Technology (NIST)

- Founded in 1901 & part of the U.S. Department of Commerce.
- One of the nation's oldest physical science laboratories**.**
- Maintains the "Cyber Security Framework"

Cyber Security Framework (CSF)

The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk.

Cyber Security Framework 5 Core Functions

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Cyber Security Framework Core Functions

1. **Identify** – Understand the cybersecurity risk to systems, assets, data, and capabilities of the critical infrastructure.
2. **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Develop a plan to mitigate the impact of a potential cybersecurity event.
3. **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.
4. **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. This includes the ability to contain the impact of a potential cybersecurity event.
5. **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The National Cyber Incident Response Plan (NCIRP)

The Federal Government uses a coordination structure known the Cyber Unified Coordination Group (UCG) to organize its activities into concurrent lines of effort:

1. **Asset Response –** DHS through the National Cybersecurity and Communications Integration Center (NCCIC).

2. **Threat Response –** The Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF).

3. **Intelligence Support –** The Office of the Director of National Intelligence (ODNI) through the Cyber Threat Intelligence and Integration Center (CTIIC).

4. **Public Entities –** The affected public or private entity's response efforts, which may include managing the effects of the cyber incident on its operations, customers, and workforce.

Federal Bureau of Investigations
Computer intrusion cases, counterterrorism, and counterintelligence, are the paramount priorities of the FBI's cyber program because of their potential relationship to national security.

Presidential Policy Directive/PPD-41 -- July 26, 2016

- FBI and the National Cyber Investigative Joint Task Force (NCIJTF) are the lead.
- Collecting & gathering evidence
- Identifying disruption activities
- Facilitating information sharing interagency coordination

FBI Programs

- **Internet Crime Complaint Center (IC3)** – online public reporting mechanism
- **Cyber Action Team (CAT)** - rapid deployment group of cyber experts - 48 hours
- **National Cyber Forensics & Training Alliance** - Combines law enforcement, private industry, and academia to identify and stop emerging cyber threats and mitigate existing ones.

Terrorists Using Cyberspace

WHAT
Propaganda
Indoctrination
Recruitment
Communication
Financing

HOW
Video Sharing
Online Forums & Blogs
Social Media
Online Gaming

Types of Social Media
Collaborative projects (Wiki)
Online blogs and micro-blogs (Twitter)
Content communities (YouTube)
Social networks (Facebook, Twitter)
Virtual gaming (World of Warcraft)
Virtual social worlds (Second Life)
Employment (LinkedIn)

Self-Indoctrinated
Self-taught Terrorism
Training documents & Videos
How to communicate with other terrorists
General Support

LONE RATS, NOT LONE WOLVES
"Yeah, people who use that term, it's not one I like because it conveys a sense of dignity I don't think they deserve. These homegrown violent extremists are troubled souls who are seeking meaning in some misguided way. And so they come across the propaganda and they become radicalized on their own, sort of independent study, and they're also able to equip themselves with training again through the Internet, and then engage in jihad after emerging from their basement. I prefer (the term) lone rat to capture the kind of person we're talking about…"
FBI Director James Comey
"60 Minutes" (2014)

Individuals Response to Cybercrimes & Cyber Terrorism
CSF for Individuals

Basic Disaster Cycle
Preparedness
Response
Recovery
Mitigation

CSF for Individuals

Identify
Individuals, families, and small units should identify important critical systems, assets, and data. Examples include, but are not limited to:

- Workstations
- Laptops
- Servers
- Home Security
- Home Automation
- Home Medical Equipment
- Intellectual Property
- Databases
- Banking & Finance Records
- Records of Ownership
- Cryptocurrency
- Photographs
- Cloud
- Backup
- Miscellaneous Documents

Protect
Individuals, families, and small units should take steps to protect the critical systems, assets, and data. Examples of these steps include, but are not limited to:

- Antivirus Software
- Firewall
- Computer / Appliance Updates
- Encryption
- Password Vault / Manager / Practices
- Social Media Presence
- Anonymizer / VPN / Proxy
- Education of Family Members
- Auto update or update reminders
- Backup, backup, backup…

Detect
Individuals, families, and small units should take steps to employ various methods of detection of threats to their critical systems, assets, and data. Examples of these detection methods include, but are not limited to:

- Antivirus (active and passive)
- IDS notifications and logs
- Network scans
- Credit monitoring
- Credit card usage notifications
- Unusual activities
- Preserved evidence
- Backup copies

Respond
Individuals, families, and small units should be ready to respond to a threat to their critical systems, assets, and data. Examples of a response include, but are not limited to:

- Log the threat
- Stop the threat
- Report the threat
- FBI Internet Crime Complaints Center(IC3) https://www.ic3.gov/default.aspx
- Change passwords and authentication
- Update firmware
- Update IDS / antivirus software
- Plug the leaks

Recover
Individuals, families, and small units should be ready to respond to a threat to their critical systems, assets, and data. Examples of a response include, but are not limited to:

- Restore backups
- After action report (what went wrong? what went right?)
- Create a mitigation plan
- Communication

Cyber Threat Hunting vs. Incident Responses

Incident Response

- Response to a cyber threat
- Reactionary

- Location & teams may vary

Cyber Threat Hunting
- Looking for the threat before it happens
- Pervasive
- Location & teams more consistent

PREPARATION
- Risk Assessment
- Personnel / Teams
- Tools
- Plans
- Tactics
- Communication
- Logistics
- Training

Military Framework to Cyber Threat Intelligence (F3EAD)
- **Find** - bad actor/malware
- **Fix** – location of bad actor/malware
- **Finish** - contain or eradicate threat
- **Exploit** – Acquire intelligence and data
- **Analyze** – trends, bad actors, tactics, after-action reports, etc.
- **Disseminate** – Communicate with team, C-suite, & stakeholders

OUTCOMES
- Contain and/or Eradicate Threat
- What are the gaps (security, response, equipment, Deploy and decay etc.)
- What are the strengths (personnel, equipment, tools, etc.)
- Where to hunt or search for
- What to hunt or search for
- What is the threat landscape

Cyber Threat Landscape

Uses of Ransomware
1. Disruption
2. Revenue
3. Decoy

Supply chain cyber threats
Software or firmware updates that are altered or replaced by malware.

Top malicious email themes
1. Bills or Invoices
2. Email Delivery Failure
3. Legal/Law Enforcement
4. Scanned Documents
5. Package Delivery Notifications

CASE STUDIES

STUXNET

BOWMAN DAM (Fall 2013)

- Rye, New York
- Hacked into SCADA system for the dam to repeatedly obtain information regarding the status and operation of the dam, including, water levels, temperature, and the the sluice gates (water levels and flow rates).
- HAMID FIROOZII and TSec Team (Iranian Nationals)

DREAD PIRATE ROBERTS (2011-2013)

- Ross Ulbricht
- Created an underground illegal marketplace on the Dark Web known as "Silk Road."
- Use of the Dark Web and Bit Coins (cryptocurrency)

OPERATION ORCHARD (September 2007)

- Israeli hackers disabled the Syrian air-defense systems network.
- Israeli hackers disabled the air-defense system to allow their bombers to infiltrate the Syrian airspace to destroy a nuclear power plant.
- Using stolen or bought codes, hacked air-defense system.

THE MIRAI BOTNET (October 2016)

- A complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53 (APDoS) from over 100,000 devices (IOT) at a magnitude in the 1.2 Tbps range.
- The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify, CNN, and Netflix.
- Cameras, DVRs, Home Routers & Switches, and other unprotected IOT devices using default admin passwords.

IOT TROOP OR REAPER (October 2017)

- Mirai evolved strategy that uses software-hacking techniques to break into IOT devices.
- The army has acquired a million networks and counting.
- Wireless IP Cameras (GoAhead), D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys, Synology and other devices.
- The attack is being spread by the IoT devices themselves.
- Has yet to be used on large scale

US V. MIGUEL ANGEL ESCAMILLA (2017)

- To justify a vehicle stop, officers must have a reasonable suspicion - that is, specific and articulable facts . . . taken together with rational inferences from those facts -that criminal activity is afoot.

- There can be implied consent from silence or failure to object and Escamilla voluntarily consented to Agent Garcia's search of the phone.

- There was a natural end to the consensual search.

- Escamilla expressly disclaimed ownership of the phone and left it in the possession of DEA agents. By doing so, Escamilla abandoned the phone and has no standing to challenge Agent Antonelli's "Cellebrite" search.