Cybersecurity Issues for Security Managers: 2019

Rick Aldrich, JD, LL.M, CISSP, CIPT, GLEG
Aldrich_Richard@bah.com, 703-545-2329
Excellence in Security Management, 1 Oct 2019

CSIAC (https://www.csiac.org)

- **Cyber Security and Information Systems Information Analysis Center (CSIAC)**
  - A Department of Defense (DoD) **Information Analysis Center (IAC)** sponsored by the Defense Technical Information Center (**DTIC**).
  - Consolidation of three predecessor IACs: the **Data and Analysis Center for Software (DACS)**, the **Information Assurance Technology IAC (IATAC)** and the **Modeling & Simulation IAC (MSIAC)**, with the addition of the **Knowledge Management and Information Sharing** technical area.
- **Basic Center of Operations (BCO)** collects and disseminates Scientific & Technical Information
  - Also performs up to four hours of support (free of charge) in response to **Technical Inquiries**.
  - Can also provide services as **Core Analysis Tasks (CATs)** procured and funded through the issuance of Delivery Orders (DO).
- CSIAC is chartered to leverage the best practices and expertise from government, industry, and academia in order to promote technology domain awareness and solve the most critically challenging scientific and technical problems in the following areas: Cybersecurity and Information Assurance, Software Engineering, Modeling and Simulation, and Knowledge Management/Information Sharing.

Legal Caveat

- Presentation is not legal advice*
- Designed to raise awareness of general legal principles applicable to information assurance and cyber security

*The information contained in this briefing is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, there may be omissions or inaccuracies in information contained in this presentation. Accordingly, the information in this presentation is provided with the understanding that the author is not herein engaged in rendering legal advice and services. As such, it should not be used as a substitute for consultation with professional legal advisers.

Objectives

At the end of this module you should be able to:

- Explain Cybersecurity and its National Focus
- Discuss Threats and Trends
  - APT, hacktivists, botherders
  - Insider threat
  - Social media
  - Cloud & virtual computing
  - Mobile computing
- Cybersecurity and the law
  - Search and seizure issues
  - Encryption

Cyberspace & Security

Cyberspace - A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CNSSI 4009)

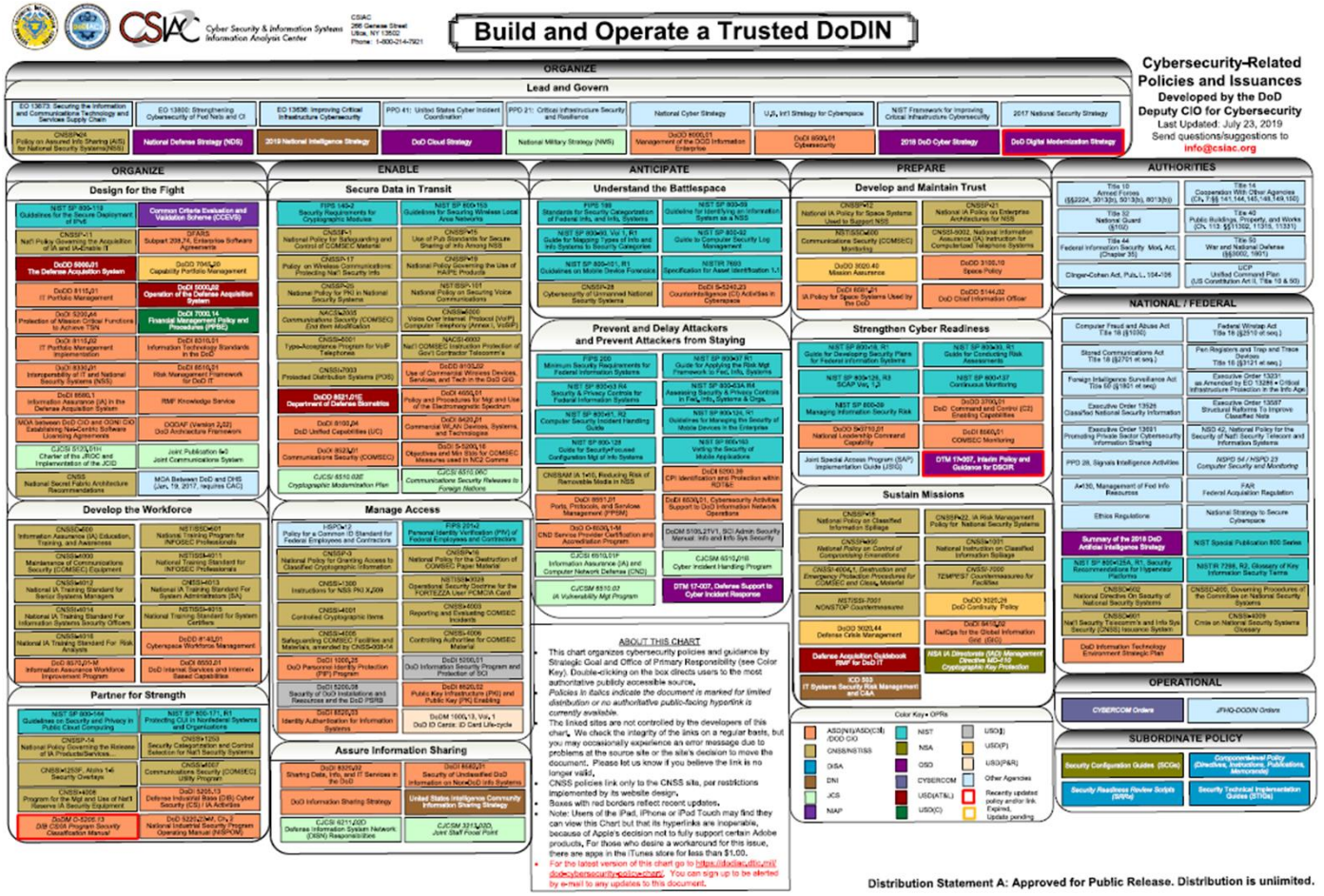
- Cyberspace allows the interdependent network of information technology infrastructures (ITI), telecommunications networks—such as the internet, computer systems, integrated sensors, system control networks and embedded processors and controllers common to global control and communications.

Cybersecurity - The ability to protect or defend the use of cyberspace from cyber attacks. (CNSSI 4009)

- Cyber Security involves protecting communications, transportation, shopping, medicine, and other information within the Internet by preventing, detecting, and responding to attacks.

DoD Cybersecurity Policy Chart

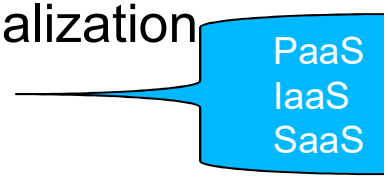
- Last updated 23 July 2019
- Covered in multiple publications including Wired.com
- This individual webpage has ranked 6th among all IA websites worldwide
- Feedback via website over-whelmingly positive
- Site provides alerts to followers



https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

Applying Risk Management

- Advanced Persistent Threats, Botherders, Hactivists
- Supply chain risk management
- Virtual Worlds and virtualization
- Cloud Computing
- Social Networks
- Mobile devices, removable media
- Cybercrime, cyberterrorism, cyberwar
- Cyber investigations: What are the lanes and who is in charge?



Advanced Persistent Threat

An adversary (generally a nation-state) that —

- Possesses significant levels of expertise/resources
- Creates opportunities to achieve its objectives by using multiple attack vectors over persistent period of time
- Establishes footholds within IT infrastructure of targeted organizations:
  - To exfiltrate information;
  - Undermine / impede critical aspects of a mission, program, or organization; or
  - Position itself to carry out these objectives in the future.

Where does the threat originate?

Botnets

What is a botnet?

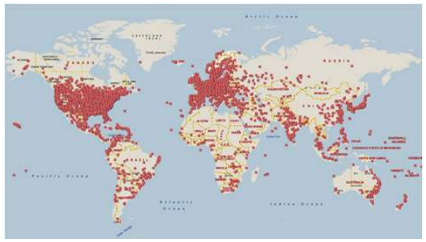
- A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Palo Alto Networks

How are botnets used?

- Denial of Service attacks, Send spam, Credential theft, Remote Access Tools (RATs), Ransomware, CoinMiners

Why are they a growing threat?

- Hijacking Internet of Things (IoT) devices has enabled them to grow larger and faster by leveraging relatively unprotected IoT



Legal Action to Take Down Botnets

Rustock (Operation b107): March 2011 Microsoft took civil action

- In Rustock case, Microsoft worked with US Marshals Service to seize equipment and 50,000 domain names

Zeus (Operation b71) and Kelihos (Operation b79)

- Ct allows Microsoft to control Zeus until late 2014 to prevent bank fraud

Citadel (Operation b54)

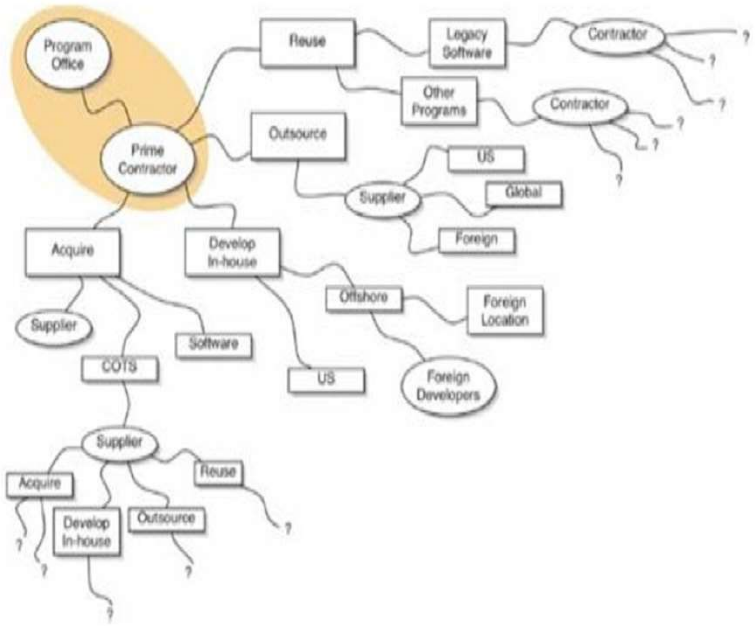
- 1.9 million computers sinkholed to MS servers.
- MS “fixes” infected computers.

Mariposa (First use 2008, 800,000 IDs stolen, ~12 M machines infected)

- Slovenian malware author: $38K, 58 months
- Spanish gang that ran it arrested but Spain has no criminal laws covering it
- June 2019 FBI filed new charges and arrest warrants

The SCRM Challenge in a Nutshell

- ICT products are assembled, built, and transported by multiple tiers of suppliers, brokers, and intermediaries around the world, most of whom are unknown to the buyer…and, in some cases, to the primary supplier.
- The supply chain is way beyond complex. Abundant opportunities exist for malicious insiders to tamper with, substitute, and sabotage products, flows, processes, data, and other insiders.
- The supply chain is vulnerable to external *and internal* compromise due to poor acquisition practices, profit-driven supplier priorities, and lack of supply chain transparency.



Think you know where your PC was built? *Think again.*

Component		Supplier or Potential Suppliers
Intel Microprocessor		US-owned factory in the Philippines, Costa Rica, Malaysia, or China *(Intel)*
Memory		South Korea *(Samsung)*, Taiwan *(Nanya)*, Germany *(Infineon)*, or Japan *(Elpida)*
Graphics Card		China *(Foxconn)*, or Taiwanese-owned factory in China *(MSI)*
Cooling fan		Taiwan *(CCI and Auras)*
Motherboard		Taiwan *(Compal and Wistron)*, Taiwanese-owned factory in China *(Quanta)*, or South Korean-owned factory in China *(Samsung)*
Keyboard		Japanese company in China *(Alps)*, or Taiwanese-owned factory in China *(Sunrex and Darfon)*
LCD		South Korea *(Samsung, LG.Philips LCD)*, Japan *(Toshiba or Sharp)*, or Taiwan *(Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)*
Wireless Card		Taiwan *(Askey or Gemtek)*, American-owned factory in China *(Agere)* or Malaysia *(Arrow)*, or Taiwanese-owned factory in China *(USI)*
Modem		China *(Foxconn)*, or Taiwanese company in China *(Asustek or Liteon)*
Battery		American-owned factory in Malaysia *(Motorola)*, Japanese company in Mexico, Malaysia, or China *(Sanyo)*, or South Korean or Taiwanese factory *(SDI and Simplo)*
Hard Disk Drive		American-owned factory in Singapore *(Seagate)*, Japanese-owned company in Thailand *(Hitachi or Fujitsu)*, or Japanese-owned company in the Philippines *(Toshiba)*
CD/DVD		South Korean company with factories in Indonesia and Philippines *(Samsung)*, Japanese-owned factory in China or Malaysia *(NEC)*, Japanese-owned factory in Indonesia, China, or Malaysia *(Teac)*, or Japanese-owned factory in China *(Sony)*
Notebook Carrying Bag		Irish company in China *(Tenba)*, or American company in China *(Targus, Samsonite, and Pacific Design)*
Power Adapter		Thailand *(Delta)*, or Taiwanese-, South Korean-, or American-owned factory in China *(Liteon, Samsung, and Mobility)*
Power Cord		British company with factories in China, Malaysia, and India *(Volex)*
Removable Memory Stick		Israel *(M-System)*, or American company with factory in Malaysia *(Smart Modular)*

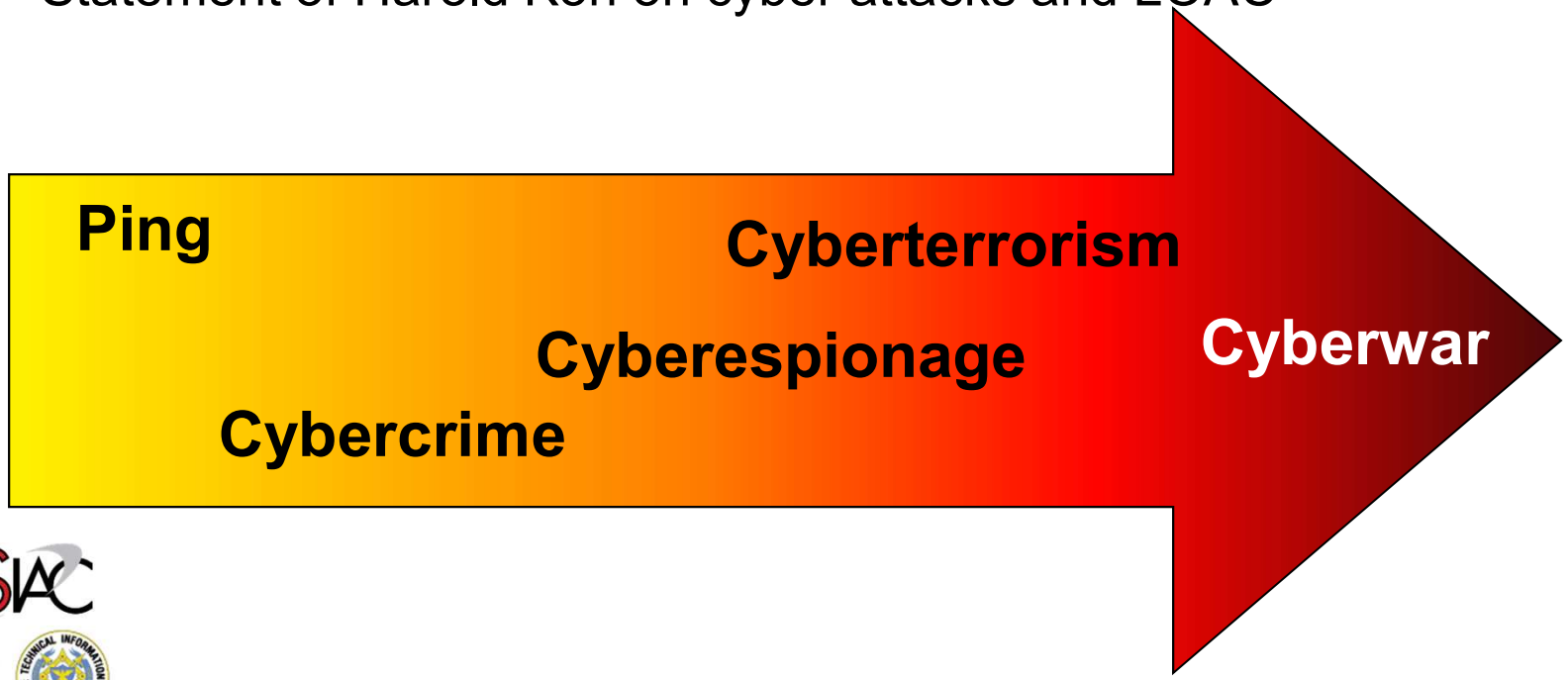
SOURCE: Thomas Friedman, *The World is Flat*

Virtualization and Cloud Computing

- Virtualization – virtual creations of hardware, software, networks, etc. Can save space, time, money, but…
- Cloud Computing – "the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer." Lexico
- General Alexander, Commander US Cyber Command: "*We can argue over merits of cloud structure but we have found it is easier to secure the cloud. Thinking about the cyber issues that face us, coming up with a defensible system is important and cloud computing is one way to help make that possible*." *(Cyber Colloquium, Nov 2011)*
- Reduce security risks by moving information away from desktops to centralized arrangement that allows for tighter control over access and more rapid response to cyber incidents, but …

Classes of Cyber Attacks

- Spectrum of Activity and Responses
- Rigid Lanes in the Road
  - System Provider, LE, CI, Warfighter
  - But USA PATRIOT Act lowered LE/CI “wall”
- Statement of Harold Koh on cyber attacks and LOAC



Classes of Hackers

White Hat Hackers: the good guys, computer security experts who specialize in penetration testing and other methodologies to ensure that a company's information systems are secure.

Black Hat Hackers: the bad guys, who are typically referred to as just plain hackers. Traditionally break into networks or computers, or create computer viruses. Motivated by money.

Grey Hat Hackers: hackers who fit between white and black hat hackers. They generally don't hack for personal gain, but may be willing to break the law to prove a security point or may disclose exploits broadly instead of just to the companies with the vulnerabilities.

Script Kiddies: black hat hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for themselves.

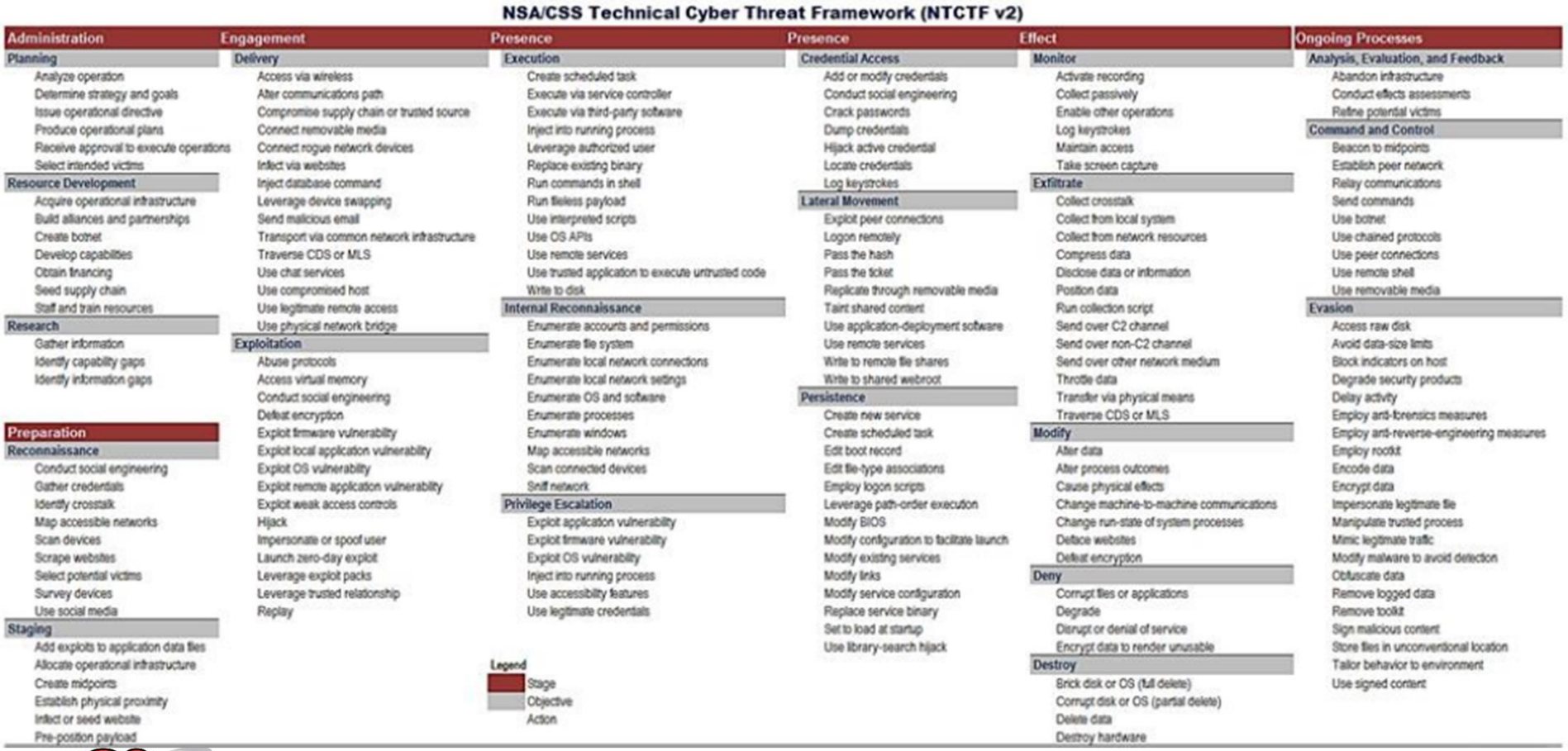
Classes of Hackers

State Sponsored Hackers: serves military objectives. “He who controls the seas controls the world,”, “He who controls the air controls the world.” Now it’s all about controlling cyberspace. State sponsored hackers have limitless time and funding to target civilians, corporations, and governments.

Cyber Terrorists: hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Cyber terrorists are by far the most dangerous, with a wide range of skills and goals. Cyber Terrorists ultimate motivation is to spread fear, terror and commit murder.

Hacktivists: hacker activists are motivated by politics or religion, while others may wish to expose wrongdoing, or exact revenge, or simply harass their target for their own entertainment. E.g., Anonymous, LulzSec.

Adversary Attack Lifecycle Framework



Using a common technical lexicon that is operating system independent and closely aligned with industry definitions supports sharing, product development, operational planning, and knowledge driven operations across the Intelligence Community.

Stuxnet

- Electronic “warhead” or “precision-guided cyber-munition” used to physically damage 1000+ centrifuges at Iran’s Natanz nuclear enrichment facility
- Natanz’s protection against bunker-buster bombs were of no help against a cyber attack
- Sophistication level led many to surmise the attacker was a nation-state
- No entity has claimed credit for the attack
- Even after over nine years, no definitive attribution
- Is this cyberwar?

What is “Phishing”?

- Use of apparently legitimate e-communication to obtain sensitive information (account name, password, etc.)
- Variants
  - Vishing (VOIP phishing, using fake caller-ID)
  - Smishing (Short Message Service (SMS) phishing)
  - Spear phishing (phishing targeted at an individual)
  - Whale phishing (spear phishing for senior executives)
  - Whaling (harvesting other’s phishing results from drop sites)
- Compare with
  - Typo-squatting
  - Doppleganger domains (same name but missing a dot)
  - Man-in-the-mailbox attacks (misspelled emails)

Cyberlaw Issues

Banners

Notice & Consent Banners

United States v. Long, 64 M.J. 57 (2006)

- LCpl Long charged w/illegal drug use
- Evidence: eyewitness testimony and e-mails Long sent to friends discussing her fear of urinalysis testing and efforts to mask her drug use
- Investigators requested sysad retrieve Long's e-mails from government server
- Long moved to suppress e-mails as an unreasonable search and seizure.
- M.J. denied motion; Long convicted, appeals
- NMCCA overturned MJ, but upheld conviction. Gov't appealed.
- Issue: Does a military member using a military computer over a military network have a reasonable expectation of privacy in that use?

Holding

- USCAAF: expectation of privacy was reasonable; error was not harmless
  - 1. Password
  - 2. SA thought private
  - 3. Banner weak
- DoD modified its banner and user agreement language
- Concerns over attorney-client privilege, other privileges
- DoD CIO Policy Memo issued 8 May 08
- New banner largely comports with USG model, with minor modifications to accommodate this decision and a privileged communication carve-out
- US Attys mixed on DoD banner
- DoD has not lost any court challenges on this banner
- US v. Al-Nashiri challenged
- IC seeking standardized banner (ICS 500-17)

New DoD Notice & Consent Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

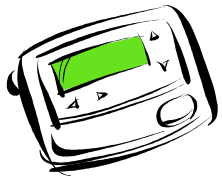
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

Banners

Banners/UAs and Expectation of Privacy



Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008)

- Quon signed e-mail policy acknowledging no reasonable expectation of privacy (REOP)
- Text messages considered to be w/in scope of policy
- Lt Duke: No audit if overage (>25K chars) paid
- Police chief ordered review of all overages for contractual reasons
- Quon's messages found to be personal and sexual
- DC: Q has REOP, but Chief's intent was reasonable so no liability
- Issue: Does Quon have a REOP in his text messages? Does the Chief's intent matter?

Holding

- 9th Cir. Ct of Appeals
  - Yes, Quon has REOP based on Duke's modification of the Department policy
  - No, Chief's intent doesn't matter
  - Rationale could have broader impact--potential that a low-level employee could effectively trump Agency policy
  - DoD Policy, banner, user agreement, annual training all seek to prevent low-level trumping
  - Appealed to Supreme Court

Quon (cont.)

- City of Ontario v. Quon, 560 US 746 (2010)
- S/C reversed 9th Cir on 17 Jun 2010
  - Vote was 9-0
  - Avoided ruling on REOP, but assumed it arguendo
  - Chief's intent did matter
  - Justified under workplace exception
  - "Noninvestigatory, work-related purpos[e]" or for the "investigatio[n] of work-related misconduct,"
  - Government employer's warrantless search is reasonable if it is
    - "'justified at its inception'" and
    - "'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of'"
- Search was within scope of that exception
  - Noninvestigatory purpose
  - Justified at inception
  - Measures were reasonably related to objectives
- Fact that less intrusive means may have been available is irrelevant as long as search was reasonable
- Suit by wife, mistress, friend also dismissed because litigated position was "if unreasonable as to Quon, unreasonable as to correspondents"
- Didn't cover if search was reasonable as to Quon could still be unreasonable as to correspondents

GPS Tracking Devices

United States v. Jones, 565 U.S. 400 (2012)

- Jones was a drug suspect. To tie him to drug deals LE obtained a search warrant to install and track GPS device.
- GPS tracked Jones for 28 days.
- Violation of warrant required government to argue no search or seizure. Asserted Jones had no reasonable expectation of privacy on public roads.
- Issue: Was the LE installation of GPS device and subsequent tracking over 28 days on public roads a violation of the 4th Amendment?

Holding

- Supreme Ct: Yes. Court departed from traditional Katz analysis, and returned to an earlier line of cases tied to common law trespass.
- Held that attachment of the GPS device to Jones' vehicle constituted a search because it was a trespass on his private property "conjoined with … an attempt to find something or obtain information." (Like a "tiny constable" "concealing himself in the target's coach in order to track its movements.")
- Majority recognized that individuals "have a reasonable expectation of privacy in the whole of their physical movements."
- When did the tracking become a search? Court side-stepped the issue. Concurrence: "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."
- What if LE had applied GPS to state plates which remain property of state?

Cell Phones

Riley v. California, 134 S. Ct. 2483 (2014)

- Riley was a gang member. When a rival gang member drove near his Olds, 3 people shot at the rival. Riley was a suspect, but was stopped by police in his Lexus for expired tags. He was arrested when police learned his driver's license was suspended.
- Police searched him incident to his arrest; seized his smartphone from his pants and later found contacts, pictures and videos all of which tied him to his gang membership. Cell records tied usage to scene of crime.
- Issue: Was the police search of Riley's smartphone in violation of the 4th Amendment?

Holding

- CA Supreme Ct: No. Per pretrial hearing, the phone was "immediately on his person" permitting a search on site and later.
- Separate case of *Wurie*: Yes. Search incident to arrest must be based on
  1. Protection of officers
  2. Preservation of destructible evidence

Under 1, Wurie conceded phone could be looked at to ensure it wasn't a weapon. This went much further. Gov't did not argue search was necessary for protection.

Under 2, Gov't claimed "arguably" necessary to preserve evidence. Ct said they could have

1. Turned off phone/removed battery.
2. Put phone in Faraday box.
3. Mirrored phone without viewing contents.

No case-by-case analysis—rather cell phone would be categorically excluded from the search incident to arrest exception.

- Both cases appealed to US Supreme Court.
- Issue: Does police search for digital evidence on phone under search incident to arrest exception violate 4th Amendment?

Cell Phones

Supreme Court Holding

- Yes-unanimous decision. Generally police may NOT search digital evidence on cell phone under search incident to arrest without a warrant.
- *Chimel*: limited to area w/in arrestees reach based on protection/preservation issues
- *Robinson*: search of cigarette pack upheld, extending Chimel to all cases of search incident to arrest
- *AZ v. Gant*: automobile exception
- Protection: Data not generally at issue, but exigent circumstances may justify in rare cases
- Preservation: Not prevalent, but police generally have other means to protect
- Cell phones differ from other property both qualitatively and quantitatively.
- What about an inventory search? Some courts have denied such, but what about Bitcoins stored on one's smartphone?

3rd Party Consent

Carpenter v. United States, 138 S. Ct. 2206 (2018)

- Several participate in armed robberies of Radio Shack and T-Mobile stores over 4 months
- 4 robbers later arrested. One confessed and provided his cell phone to FBI.
- FBI identified 16 phone numbers of interest and sought historic cell-site location info (CSLI) for each for 127 days from carriers under SCA (requiring only a showing of relevance to an ongoing criminal investigation, not the higher probable cause standard for warrants).
- Magistrate grants order. Carpenter identified in cell-site data, tried, convicted, sentenced to 116 years.
  - Issue: Is the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days permitted by the Fourth Amendment.

Holding

- 6th Cir: Yes, because
  1. The current law protects "content" but not "transactional" information.
  2. Records were carrier's business records, subject to 3rd party doctrine
  3. *Jones* does not apply because government didn't do extended GPS monitoring, carriers collected the data, and GPS monitoring is 12,500 times more accurate than cell-site locations.
  4. *Riley* doesn't apply because amount of data stored on a cell phone is not applicable to cell-site location.
- S/C: No. Facts fit intersection of *Jones*, *Miller/Smith* (3rd party) cases, and *Riley* ("privacies of life"). Equilibrium adjustment.
- Declines to extend 3rd party doctrine to CSLI as it is qualitatively different: "near perfect surveillance" akin to ankle monitor. Ct anticipated tech developments.
- "Narrow" holding doesn't address sting rays, tower dumps, conventional techniques such as security cameras, nor FISA techniques.
- Takeaway: For companies that collect sensitive data, this case may provide a basis to resist warrantless requests from the government. Review customer privacy agreements for impact on REOP.

Divulging Smartphone Passcode

***SEC v. Huang* (No. 15-269, E.D. Penn. Sep. 23, 2015)**

- Bonan and Nan Huang worked for Capital One as data analysts. They had access to non-public information in their job and used it to score big in the stock market.
- Capital One issued smartphones to employees and let them set passcode. Huangs left bank and returned phones. Capital One gave phones to SEC.
- SEC sought passcode to permit them to search for evidence on phones.
- Huangs refuse.
- Issue:

Can SEC force Huangs to divulge smartphone passcode?

Holding

- DC: No.
- SEC claimed business records are on phones and under "collective entity" doctrine, Huangs can't invoke 5th Amendment.
- Court counters that SEC is not seeking business records, but smartphone passcode, which is not a business record because Capital One let each employee set their own and not record it.
- SEC then argued "foregone conclusion" doctrine. But under 11th Cir. precedent, Gov't must show with "reasonable particularity" what "if anything, was hidden behind the encrypted wall."
- Court held SEC failed this test.
- "Producing" vs. "saying"
- May be very important in light of increasing use of smartphones with passcodes

Encryption


- Apple's encryption decision for iOS 8 and later
- Google's decision to do the same
- Reactions:
  - FBI Director Wray: Apple and Google Are Putting Their Customers 'Beyond The Law' (60 Minutes)
    - Like selling cars with trunks that couldn't be opened by law enforcement with a court order.
    - Like selling an apartment that couldn't be entered by law enforcement
    - [What about safes? Encryption software?]
  - Washington Post: Apple and Google should retain a "Golden Key"
  - A/G Barr: US needs encryption backdoors
- Questions:
  - Can police order you to divulge your password? A court?
  - Can they make you provide a fingerprint?
  - Can they legally get the data on your phone via other means?

Government Employer Related Issues

- How does the First Amendment impact social media issues?
- Can employers require employees reveal social media account names?
  - Some cities require job applicants provide account names and passwords (but CA, IL, MD prohibit employers from requiring such while AZ, CO, DE, GA, HI, IA, KS, MA, MI, MN, MO, MT, ND, NE, NH, NJ, NM, NY, OH, OR, PA, RI, SC, TX, UT, VT, WA have bills pending to do the same)
  - Some states now addressing restrictions in re school applications
  - Commanders in Iraq have required such of soldiers--some soldiers got punished for findings
- Friend Requests
  - Can employers require employees to accept their “friend” request?
  - What if employee only made employer a “limited friend”?
  - Clearance-related issues about accepting friend requests from Foreign Nat’ls?

Government Employer Related Issues (cont.)

- Does “unfriending” by a superior constitute an adverse personnel action?
  - NASA developed Spacebook (analog to Facebook) to avoid this
- What about embassy visits in Second Life?
  - Reportable for those with SCI/SAP clearances?
- Can law enforcement collect evidence from your privacy-protected Facebook page via your “friend’s” consent? (See *United States v. Meregildo*, No. 11 Cr. 576 (S.D.N.Y. 2012).)
- What about “official” use of commercial webmail accounts?
  - EPA Administrator Lisa Jackson used a secret alias Gmail-type account under the name “Richard Windsor”—allegedly this practice extends to other agencies
  - Hack of Gmail by Chinese in 2011 included many senior US government officials
  - Raises federal records management issues (44 USC 3101 et al)
  - Such accounts generally also circumvent Agency e-mail filtering and protection programs

Insurance

Mondelez Int'l v. Zurich American Insurance, 2018 WL 4941760 (Ill. Cir. Ct.)

- Mondelez Int'l is one of the largest snack food companies in the world (Nabisco, Oreo, belVita, others) marketing its products in 165 countries worldwide
- Mondelez was hit broadly by NotPetya, suffering ~$100M in damages, including the bricking of 1700 servers and 24,000 laptops.
- Files claim with insurer, Zurich, under "all risks" provision, which specifically includes "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction ...." Zurich required voluminous supporting evidence, which Mondelez provided.
- During this time Zurich ran ads citing NotPetya as a reason companies should purchase their cyber insurance.
- Zurich later denied coverage based on an exclusion for losses from "hostile or warlike actions" by any government (de jure or de facto) or their agents.
- Issue: Who wins and why?

Holding

Pending case, so no ruling yet but …

- Ultimate decision could dramatically rattle the cyber insurance industry.
- The US, the UK, Denmark, Lithuania, Estonia, Canada, and Australia all attributed NotPetya to Russia, based on intelligence, but unclear basis could be used in court or would meet legal standard.
- Other attacks: WannaCry attributed to North Korea, 12-year cyberespionage campaign attributed to China, Aramco attributed to Iran
- Takeaway: Companies should carefully review cyber insurance contracts to determine to what extent the insurer may be able to deny coverage if any linkage to a government sponsor can be shown or alleged.

Summary

- Trends
  - Fourth Amendment continues to evolve with technology
    - *Carpenter, Jones,* and *Riley* all suggest equilibrium adjustment
  - Circuit splits still in need of resolution
    - CFAA "without" or "exceeds" authorization interpretation
    - Encryption: 4th and 5th Amendment, forcing passphrases vs. forcing decryption, foregone conclusion, biometrics
    - Border searches: Do forensic searches require reasonable suspicion?
  - Cyber insurance and "war" exclusions raise new concerns
- Understand implications; cyberlaw is still immature/evolving
- Use briefing to help identify potential issues
  - Seek legal counsel when uncertain

Backup

3rd Party Consent

United States v. Rettenmaier, No. 8:14-cr-00188 (2017)

- Dr. Rettenmaier couldn't boot his computer so brought it to his local Best Buy in CA. Told he had a faulty HD. To recover data needed to send to BB's KY office.
- A child porn image found "accidentally" by Geek Squad Tech JW in unallocated space. JW was a paid FBI informant. He reported it to two other Geek Squad FBI informants then to the FBI. FBI allegedly made two additional searches w/o warrants, then sought a search warrant from a fed magistrate.
- Best Buy service order signed by Δ read: "I am on notice that any product containing child pornography will be turned over to the authorities."
- Issues: Did any of the searches violate 4th Amendment? Is data found in unallocated space sufficient for "knowing possession"?

Holding

- Case dismissed after T/C judge suppressed most of the evidence.
- Does 4th Amendment apply against GS?
  - Normally not—Only applies to Government
  - Did FBI payments make GS agents of Gov't?
    - Additional information indicates FBI appears able to access data to BB's KY facility at will.
  - Does "accidental" find make a difference?
  - Does it matter that data was in unallocated space?
  - Did "consent" form waive 4th Amend?
  - Did subsequent search warrant cure?
- If exclusionary rule not applied to data found in searches, does it matter that the data was found in unallocated space?

Searches – Consent

- Can a wife consent for her husband?
  - What if one consents and the others refuses to consent?
  - What if the consent involves search of the home?
  - What if the consent involves search of family hard drives?
- Can a parent consent for his/her child?
- Can a child consent for his/her parent?
- Can an employer consent for his employee?
- What is the effect of consent given to search a hard drive that is revoked?
  - Does it matter if a data duplicate was made?
- Can a cloud storage provider consent for the subscriber?

Does use of NIT violate 4th Amendment?

"Playpen" cases

- FBI's Operation Pacifier, based on a foreign government's tip that large child porn site (Playpen) operating in US.
- Site operated on the Dark Web and so was only accessible via Tor. FBI found site and was able to gain control of it, but couldn't ID users.
- FBI used a NIT (network investigative technique), with a warrant from a magistrate in the E.D. of Virginia.
- Exploit pulled back to user's actual computer and then ran code to search the computer for the computer's MAC address, the username of the current user, the computer's name and possibly other info.
- Data then transmitted back to an FBI computer that would log all that data and also the source IP address which was no visible because it was not being transmitted via Tor. FBI charged 137 individuals.
- Issues: Was warrant valid as to those outside magistrate's jurisdiction? Was warrant necessary? Can defendants move to disclose or dismiss? How does CIPA square with 6th Amend right to fair trial?

Holdings

- Courts mixed on validity of search warrant outside of Virginia, but majority so far holding invalid.
- Courts mixed on need for warrant, but majority seem to hold it is required. One holds users have no expectation of privacy in IP address. Like police looking through "broken blinds."
- FBI claims it cannot disclose technique and all source code because it would undermine criminal, terrorist and national security cases.
- Was it ethical for FBI to run Playpen for 2 weeks, with 9000 child porn images available for download and over 215,000 registered users in order to perfect cases against 137?

Border Searches

United States v. Touset, 890 F.3d 1227 (11th Cir., 2018)

- T identified as a child porn suspect due to pattern of low dollar transfers to persons in countries associated with sex tourism. Xoom alerted Yahoo based on email and messenger accounts.
- Yahoo found child porn in an associated email, sent alerts to NCMEC, DHS.
- When T arrived in Atlanta on int'l flight, CBP inspected electronic devices, did forensic searches on 4 of them. Found child porn on all four. Later Gov't obtained search warrants for home and found more evidence of child porn.
- T challenges forensic search, alleging no reasonable suspicion because Western Union money transfers were 1.5 years old, so stale.
- How should court rule?
  1. Does forensic border search of computers require reasonable suspicion?
  2. If so, was it present or stale?

Holding

- Magistrate: Reasonable suspicion is proper standard and was present.
- District court: Reasonable suspicion is proper standard and was present.
- 11th Cir.: Reasonable suspicion not required for search of computers and like devices at the border.
  - Reasonable suspicion only required for invasive searches of the body (strip searches or x-rays)
  - Refuses to extend rationale of Riley (search incident to lawful arrest not applicable to cell phones—requires a warrant) to border searches ("trailer loaded with boxes of documents")
- Extends split among circuits:
  - 4th and 9th have held computer searches at the border require reasonable suspicion
- Alternately, if reasonable suspicion is required, it was present here
  - Pedophiles rarely if ever delete files of child porn, so the basis for the reasonable suspicion was not stale
- Takeaway: Corporate IT moved outside of the US is subject to search and seizure. To protect proprietary data, ensure appropriate policies for IT going abroad.

Consent

United States v. Cruz-Zamora, No. 17-40100-CM (D. Kan., Jun. 4, 2018)

- CZ was stopped in Kansas by a trooper based on a suspended registration. CZ asked if the trooper spoke Spanish, but the trooper did not.
- Unaware the department had a live translator, the trooper used Google Translate to ask if he could search the car. Google translated it as "¿Puedo buscar el auto?" After some confusing interactions between the trooper and CZ, CZ said "yeah, yeah, go." The trooper found 14 pounds of meth and cocaine.
- At trial, CZ moved to suppress the drugs claiming he did not understand the question, so his alleged consent was not free and voluntary. Placed into Google translate in reverse order the above translates to "Can I find the car?"
- How should court rule?
  1. Did CZ's response constitute consent to search?
  2. Should "good faith" exception apply?

Holding

- No valid consent, as question was improperly translated so response could not be deemed to be clearly free and voluntary.
- Fruits of search should be suppressed.
- Government urged the court to apply the good faith exception based on prior case law that indicated a police officer's reliance on an erroneous entry in a government database justified application of the good faith exception.
- Court ruled that reliance on Google Translate was legally differentiable from reliance on a government database, so applying good faith was not appropriate.

Biometrics

In the Matter of Search of a Residence in Oakland, California, No. 4-1970053 (N.D. Calif., Jan. 10, 2019)

- US Gov't seeks a warrant relating to two individuals believed to be involved in extortion. Suspects alleged to have used Facebook Messenger to communicate with victim, threatening to distribute embarrassing video of him if he didn't provide money.
- Gov't also seeks the authority to compel any individual present at the time of the search to press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant.
- Issue: Should Magistrate issue warrant?

Holding

- Magistrate denies warrant application
- The Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices [under 4th & 5th Amends.]
- 4th Amend.
  - Kerr: Warrants should only deal with where and what is to be searched or seized, not how
  - How should be an ex post issue, not ex ante
  - Fingerprinting generally only requires reasonable suspicion
- 5th Amend.
  - Kerr: 5th Amend. requires "express invocation"
  - A biometric doesn't constitute "testimonial" self-incrimination
  - Foregone conclusion hinges only on testimonial act
- Furthermore, the Government may only seize those digital devices that law enforcement reasonably believes are owned and/or possessed by the two suspects named in the affidavit.
  - Contra 4th Amend law. Only issue is whether the things to be searched or seized are at the place listed in the warrant.

Additional Cases and Issues to Watch

- Kaspersky Lab v. United States
  - Kaspersky contested DHS's Binding Operational Directive and the NDAA of 2018 which required removal of K's AV on government computers. US prevailed.
- Solid Oak Sketches LLC v. Visual Concepts LLC et al, U.S. District Court, Southern District of New York, No. 16-00724
  - Copyright infringement in video games for displaying tattoos of NBA players
- Algorithmic warfare and the law of armed conflict
  - Especially algorithms that are difficult or impossible for humans to unpack
- Liability for self-driving cars

Additional Cases and Issues to Watch

- Arrest of Phantom Secure CEO
  - For selling super secure repurposed Blackberries and Androids to criminals with apparent knowledge of how they would be used
  - Servers placed in Hong Kong and Panama apparently because they were perceived as likely to be uncooperative with police
  - Charged as conspirator
- Data breach suits
  - Equifax (147M personal accounts with significant PII)
    - 350 class action suits being consolidated
  - Yahoo! (3B user accounts affected—punitive damages)

Virtual Worlds and Crime

- Japanese woman “kills” virtual ex-husband after messy online divorce in “Maple Story,” a virtual world

- Can she be charged with a crime?

- Yes, a computer crime for illegally accessing his account. Max penalty if charged and convicted is $5000 and 2 years confinement.
- What about virtual worlds?
  - Can some “illegal” things be done within the “game” without fear of prosecution?
  - How should the line be drawn?

Theft of Virtual Goods

LJN, no. BQ9251 (Dutch Supreme Court, Feb 2012)

- Two Dutch teens coerce a third teen at knifepoint to "drop" a virtual amulet and mask in Runescape for them to recover.
- Clearly committed a crime, but …
- Can they be convicted of theft of "goods"?
- Is it a defense that a point of the Runescape game is to steal virtual goods?

Holding: Yes

- Defense argued goods do not legally exist, but …
- Judge held they have value and can be sold for real money (even though in violation of Runescape rules).
- Acknowledged that an objective of the Runescape game was to take possessions from others, but this theft was out of the context of the game.
- The two were sentenced to 144 hours community service.
- Dutch Supreme Court upheld (Feb 2012)

Questions?

Rick Aldrich, JD, LL.M, CISSP, CIPT, GLEG
Aldrich_Richard@bah.com, 703-545-2329
Excellence in Security Management, 1 Oct 2019