Cybersecurity for the Confused

I.e., All of Us

- Sheldon Greaves, Ph.D.

Introduction: The Problem

Most security questions come down to striking a balance between convenience and safety.

Convenience

- The greater the amount of convenience, the larger the “attack surface.”
- The Internet’s primary contribution is to make things feasible that were too much trouble or too expensive to do before.
- The Internet is an accelerant. It is convenience amplified to unprecedented levels.
- What is convenient for you is usually also convenient for the bad guys.

Safety

- Security involves placing constraints in place to reduce the attack surface, or make it harder to access.
- Most security measures demand at least a little extra time and trouble, i.e., locking your front door.

The Internet Battlefield

Most of the traffic on the web is hostile.

- A study of “grey noise” on the Internet found that only 5% of the traffic at any given time is benign.
- 95% of traffic is ultimately hostile: automated “bots” searching for targets, illicit attempts to log into systems, self-replicating computer viruses, etc.

Costs of Cybercrime

The cost of criminal activity on the Internet is notoriously difficult to guage

- Internet Security Corporation McAfee puts the cost of cybercrime in 2017 at $600 billion.
- Another estimate puts losses for 2015 at $3 trillion, estimated to reach $6 trillion by 2021.
- Estimated costs of a cyberattack do not often include loss of reputation, shareholder confidence, degraded brand identity, and other intangibles that nonetheless translate into real losses.

Costs of Cybercrime

Other effects and costs:

- It takes the average company around 270 days just to discover that they've been hacked.
- Every 40 seconds a business falls victim to a ransomware attack. Cybersecurity Ventures predicts that will rise to every 14 seconds by 2019.
- In 2017, one estimate places 85% of business assets in digital form, so it should come as no surprise that market perception is directly linked to how company manages their cybersecurity.

Cybercrime’s “Greatest Hits”

Some instructive cases of data breaches.

Equifax

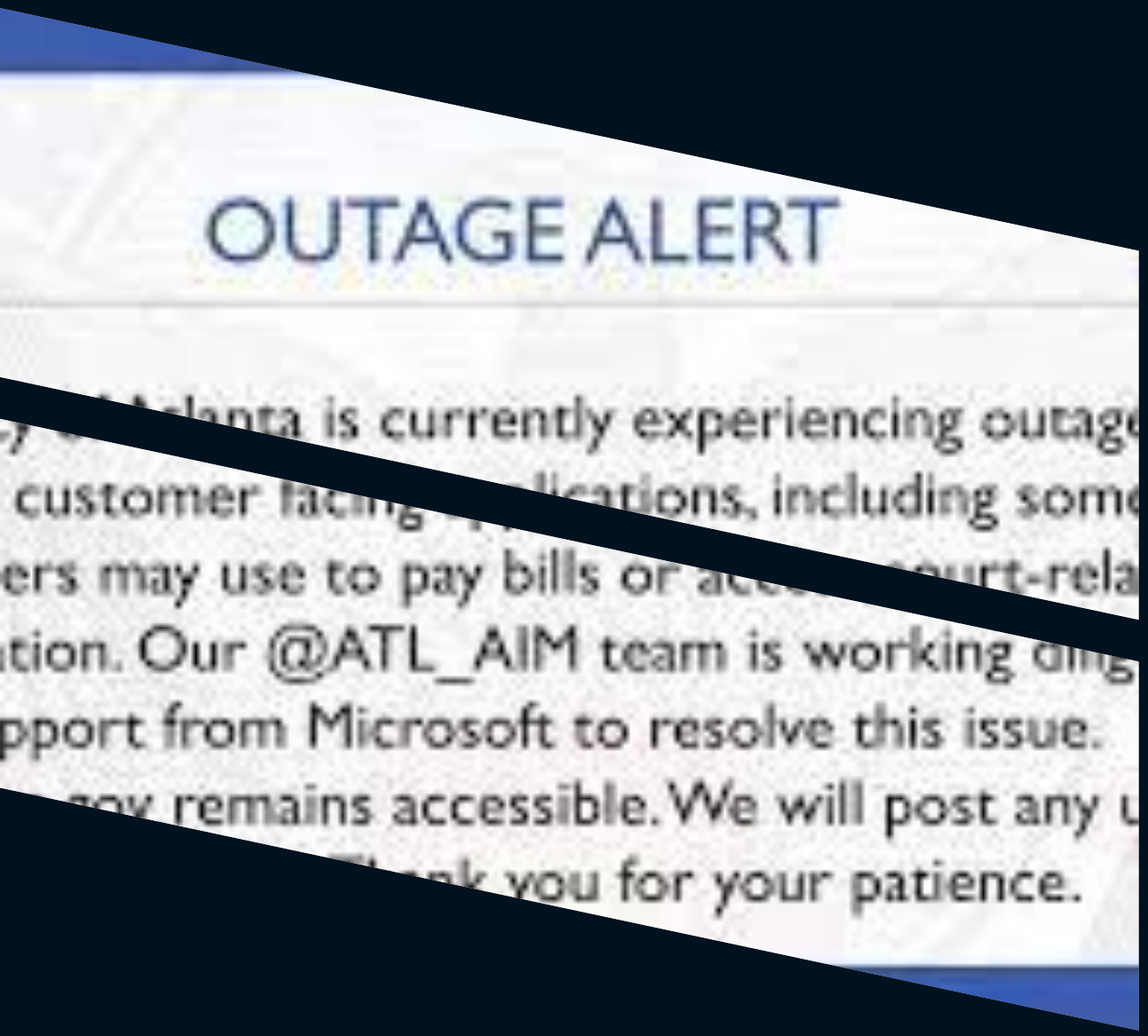
Negligence and poor security practices.

- 143 million records compromised
- Stolen data included Social Security numbers, driver's licenses, addresses, birthdates, and credit card information
- Equifax waited six weeks to report the breach.
- Response was sloppy, including additional security lapses.
- Data from this breach has disappeared; it never turned up on the Dark Web.

Target/Home Depot

When 3rd party vendors get careless.

- Stolen 3rd party credentials allowed hackers to penetrate the network using custom-built software.
- Credit card data for 53 million Home Depot customers stolen.
- 40 million credit cards stolen from Target customers.
- Additional damages from settlement of a class-action lawsuit.



City of Atlanta

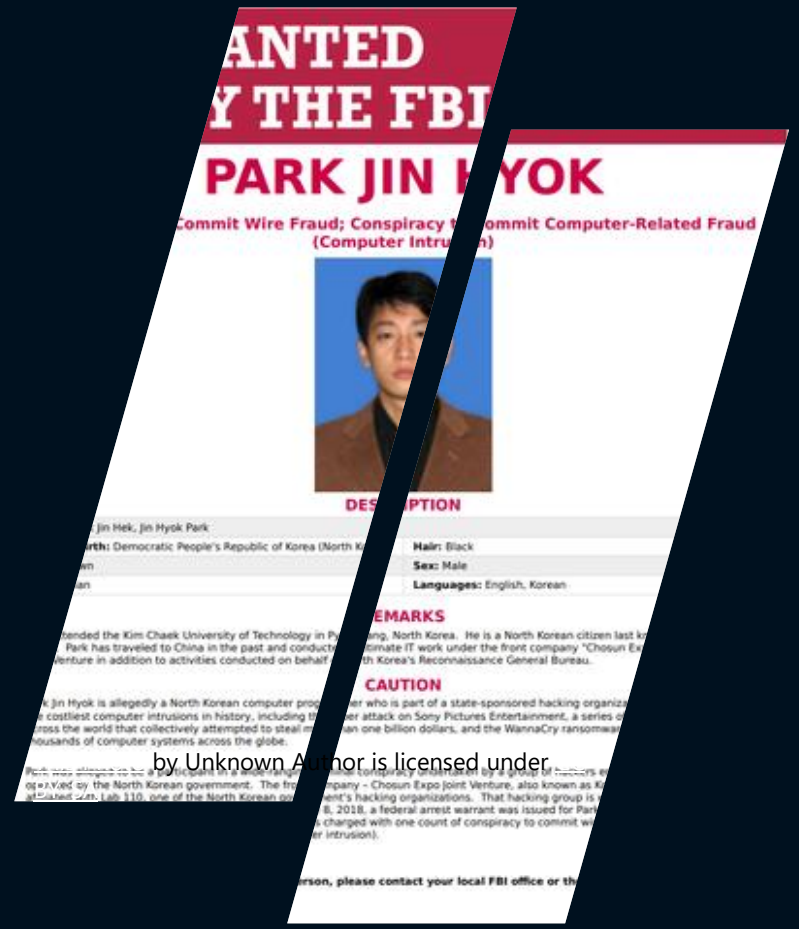
A City Threatened by Ransomware

- Municipal computers taken down and held for a ransom of $52,000 in bitcoin currency. The ransom was not paid.
- A team of at least two Iranian nationals among the suspects.
- For over a week, municipal court computers could not pull up cases.
- Residents could not pay bills online.
- Police reverted to writing reports and booking suspects by hand.

Sony Pictures

A carefully planned, brilliantly executed cyber attack.

- Launched by North Korea in retribution for movie “The Interview”
- Sensitive information, company records, emails, and four to-be-released films were exposed and made public.
- 70% of Sony’s company hard drives were destroyed.
- Workers had to resort to writing notes by hand and faxing them.
- An example of a single hacker, Park Jin Hyok working with significant backing by a nation state actor.

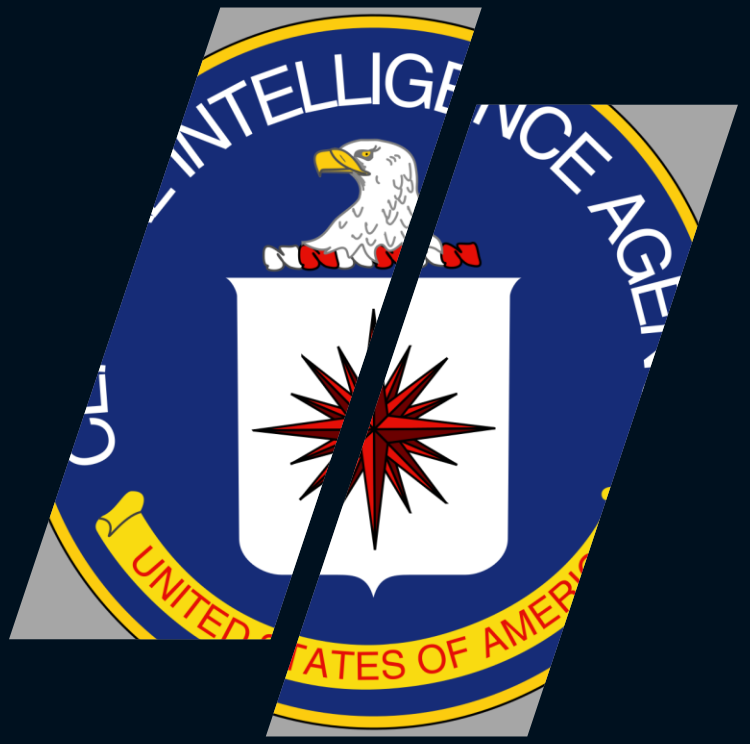


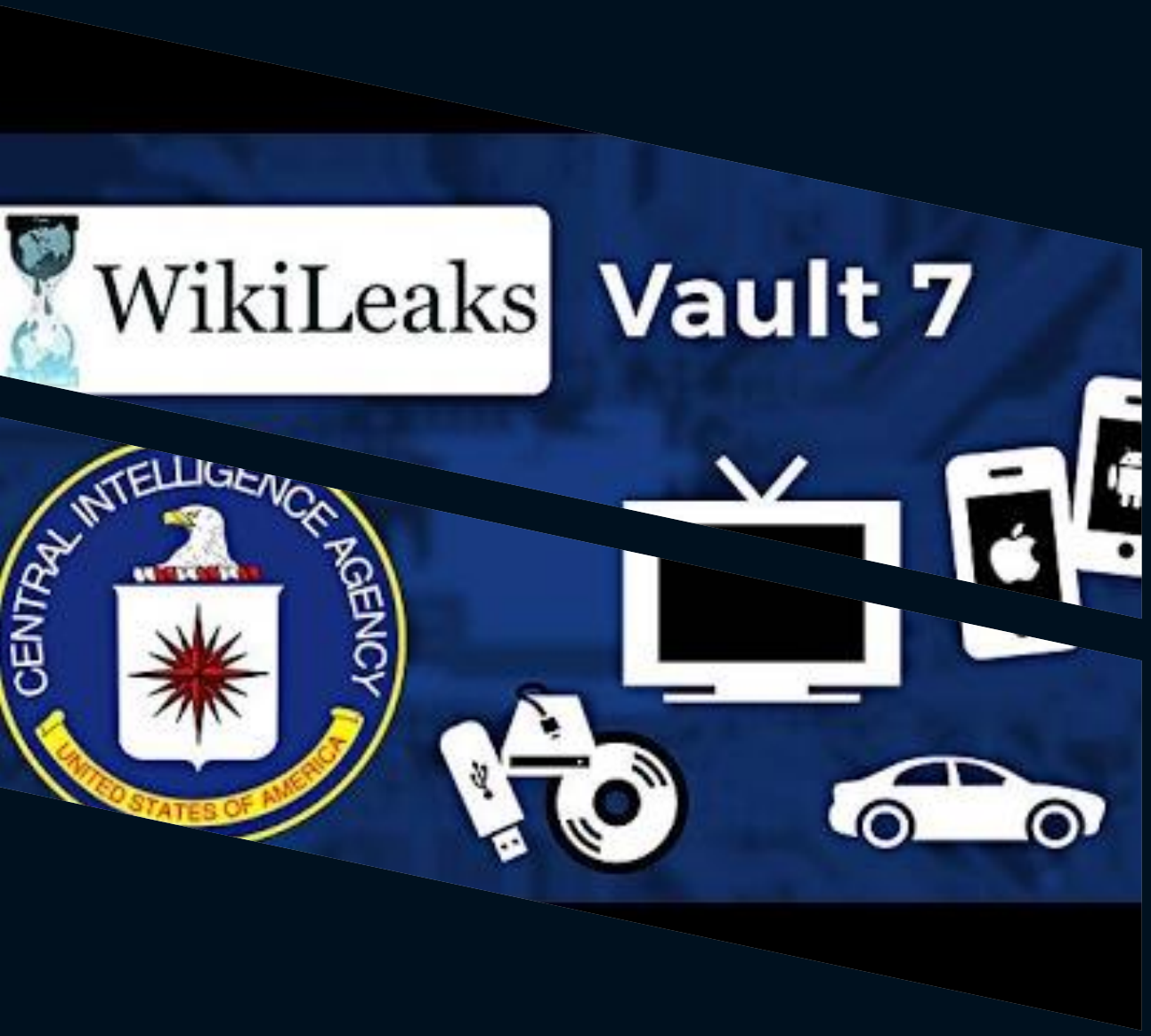
by Unknown Author is licensed under

CIA Communications Network Compromise

"This is one of the most catastrophic intelligence failures since September 11."

- A temporary global system for clandestine communications using secret web sites.
- The system was used far longer than it was designed or intended for.
- Iranian hackers uncovered the hidden sites using ordinary Google searches, and sold this information to other countries.
- In China alone, at least 30 Agency sources were exposed and killed.





Vault 7 Release

Leak of a secret trove to CIA hacking tools

- A former CIA worker sent Wikileaks a set of documents detailing CIA cyber efforts.
- Information disclosed Agency capabilities, targets, methods, and even actual software used to hack and monitor systems.
- Since this breach, there has been a significant increase in the sophistication of malware, viruses, and penetration techniques.
- The leaker, Adam Schulte, was caught by the FBI because he used the same password on his phone and computer.

OPM/Anthem

An attempt to identify possible targets for recruitment?

- Generally believed to be carried out by the Chinese government.
- Early infiltrations were expunged, but not before hackers installed a secret back door to re-enter the system.
- Administrators failed to take appropriate measures after the initial penetration
- Millions of SF-86 forms used in background checks and security clearances stolen.
- Anthem data thought to be cross-referenced with OPM data to find personnel with clearances but susceptible to blackmail.

Internet Research Agency

Propaganda and Influence Operation

- An extended propaganda campaign intended to influence the 2016 election and weaken US democracy.
- The campaign is based on a modified version of the old KGB Cold War playbook.
- Between 2015 and 2017, over 30 million users shared IRA memes via Facebook, Instagram, and other social media platforms.
- The current administration has made no effort to curtail these campaigns.

Ukraine Power Grid

First confirmed instance of a successful cyber attack on critical infrastructure.

- Russian hacker group BlackEnergy disabled a portion of Ukraine's power grid.
- 225,000 residents in and around Kiev were without power for several hours.
- The U.S. power grid is regularly probed and attacked by Russian, Chinese, and other parties.
- In 2014 Admiral Mike Rogers told a Congressional committee hearing that China and other unnamed countries were capable of taking down the U.S. power grid.

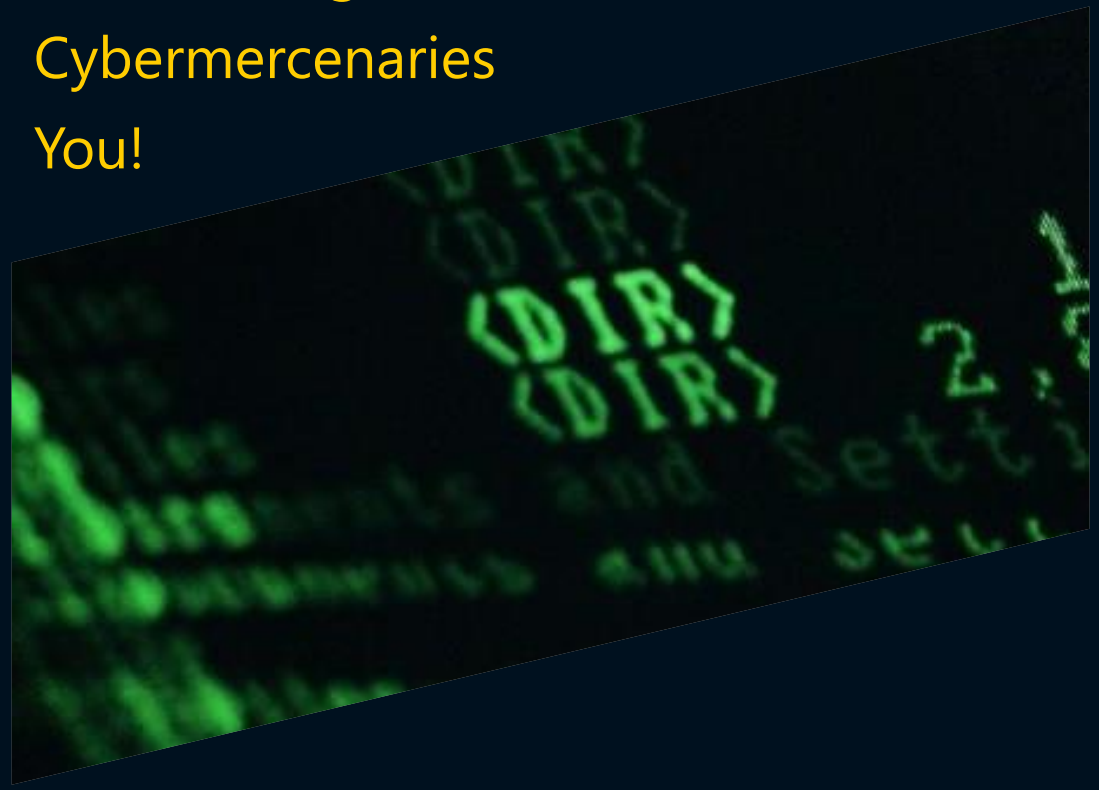
A Look at the Bad Guys

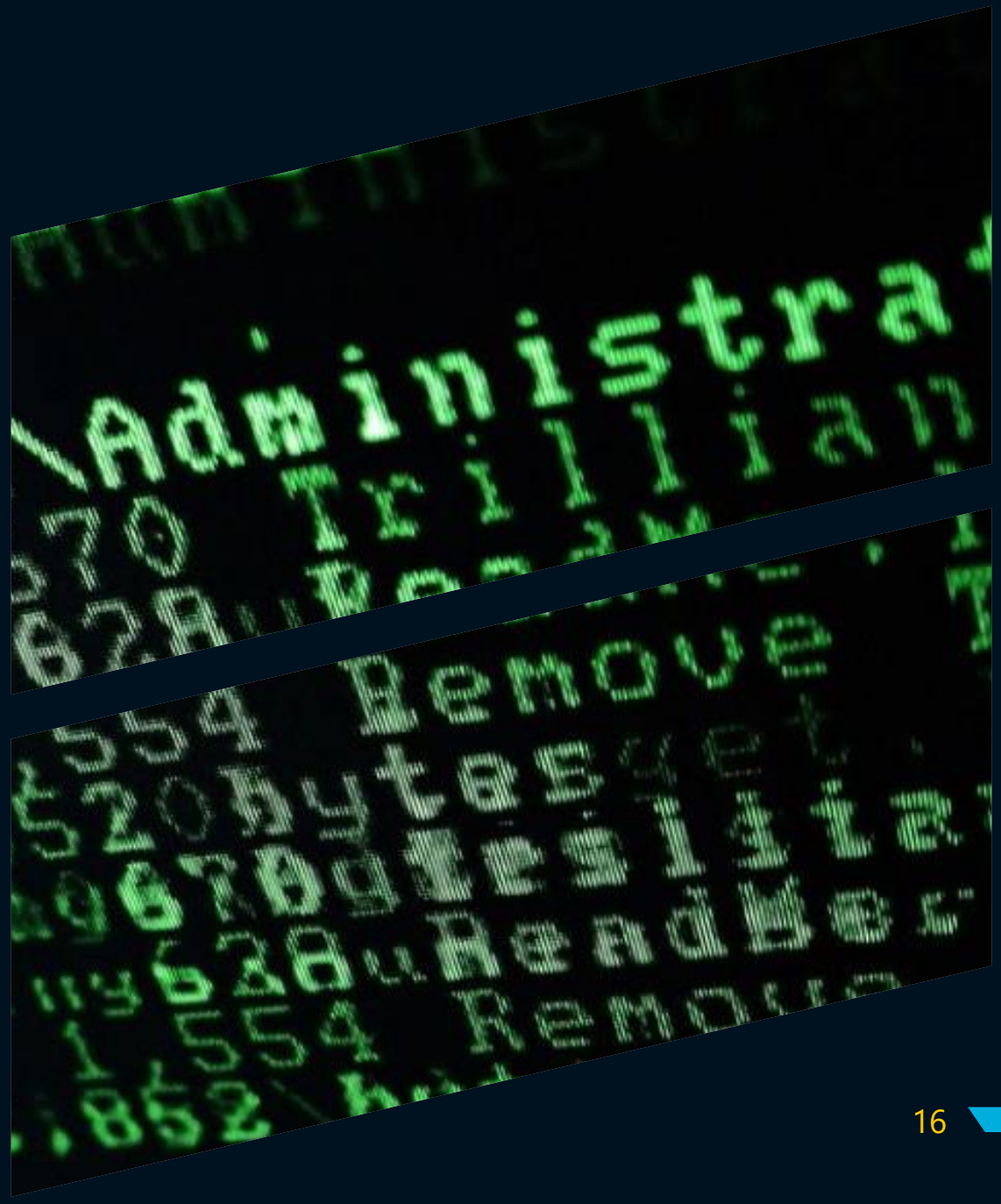
Nation States

Criminal Organizations

Cybermercenaries

You!





Nation State Actors

Capabilities and Priorities

Russia

- Seeking to expand influence despite a weak military
- Strong on propaganda, influence, meddling with elections
- High interest in suppressing dissent or reputational damage.

China

- Prolific; very robust cyber infrastructure
- More emphasis on industrial espionage
- Retains many “obsolete” technologies to be pressed into service if standard tech is compromised

Nation State Actors

Capabilities and Priorities

Iran

- Some of the most capable cyberwarriors in the world.
- Most of their efforts are directed to targets in the Middle East and Europe.
- An attack on Saudi Aramco destroyed over 40,000 computers.
- Iran has experimented with teaching aspects of hacking as part of its high school curriculum.

North Korea

- Cybercrime is now a significant fraction of the GDP with several robberies, including the hack of the Bank of Bengladesh.
- North Korea itself has extremely limited Internet access. Most NoKo hacking is done from inside China.
- Budget dedicated to cyber is roughly equivalent to that of NoKo's nuclear weapons program.
- Primary targets are the U.S. and South Korea.

Terrorists and Organized Crime

Sometimes working in concert or with support of nation states

Terrorist

- United Cyber Caliphate
- Syrian Cyber Army
- Most terrorist groups have in the past funded or hired hackers on a contract basis.

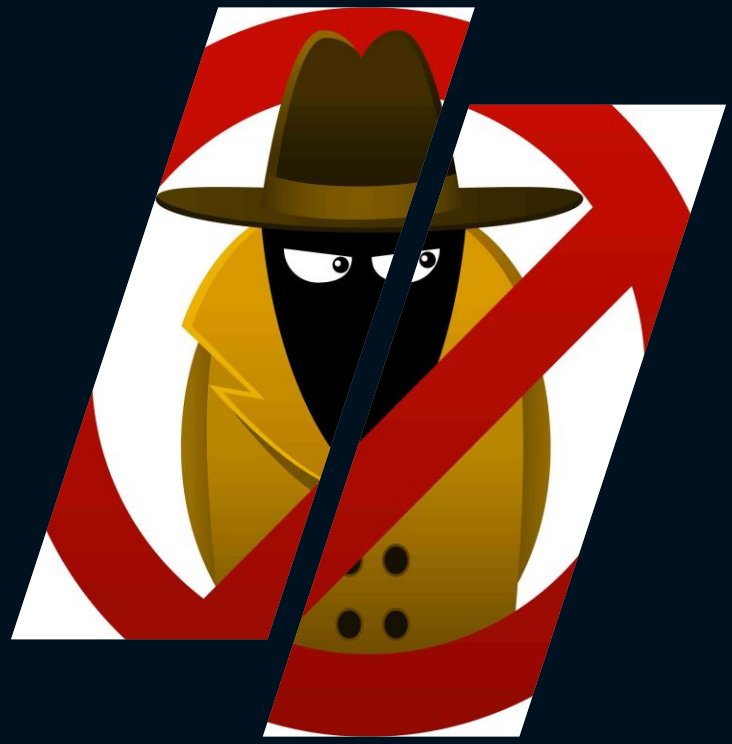
Criminals

- Lordfenix
- Carbanak Gang
- Besad Mesri, held HBO ransom
- FBI has a separate “Most Wanted” list for cyber criminals.

You Too, Can Become a Cybercriminal!

Adopting regular business practices has lowered the barrier to entry.

- Malware developers are applying Silicon Valley business practices to make better, cheaper malware.
- Cybercrime now has specialists, consultants, planners for hire.
- Some malware features customer service and money-back guarantees.
- Malware-as-a-service

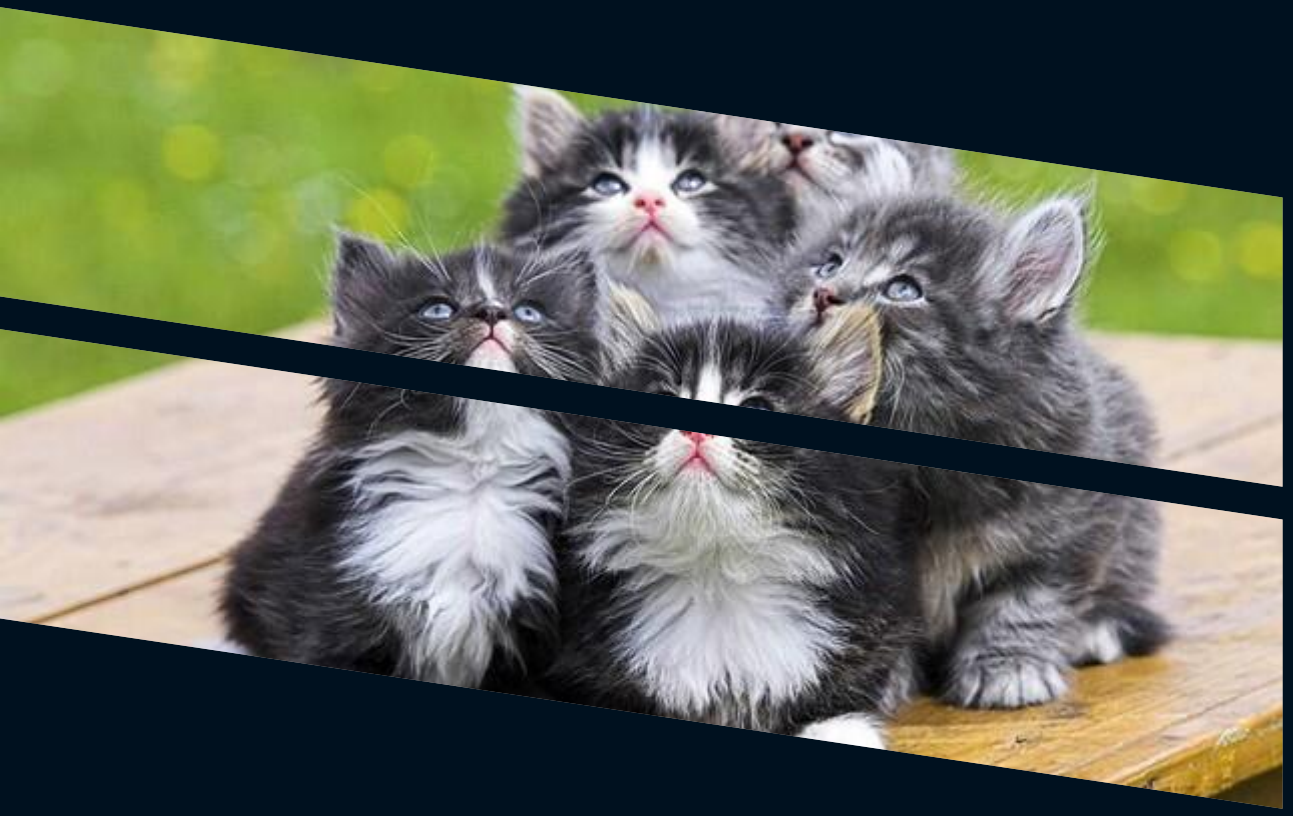


Where it Happens: The Dark Web

The Dark Web is about 96% of the entire Internet.

- Huge market for drugs, including shipping illegal drugs right to your door.
- Hackers for hire can break into university computers to change grades. One can also buy fake degrees and other forged documents.
- A famous scam lures people who want to hire hitmen.
- Stolen data usually is offered for sale on the Dark Web

Dark Web: Continued



More fun facts:

- The international arms trade is very active on the Dark Web, as well as sales of illegal antiquities, human trafficking, and endangered species.
- The Dark Web is only accessible by using special web browsers and other software designed to hide your identity.
- However, high-end parties such as the NSA have the tools needed to identify you anyway, even if you don't slip up somehow.
- Most serious criminal sectors of the Dark Web are "by invitation only."

Current Trends

Some of the more common threats:

- Identity theft
- Financial crimes
- Ransomware
- Healthcare theft
- Zombie computers and botnets
- Cryptocurrency mining

Cyberstupidity

The Internet of Things

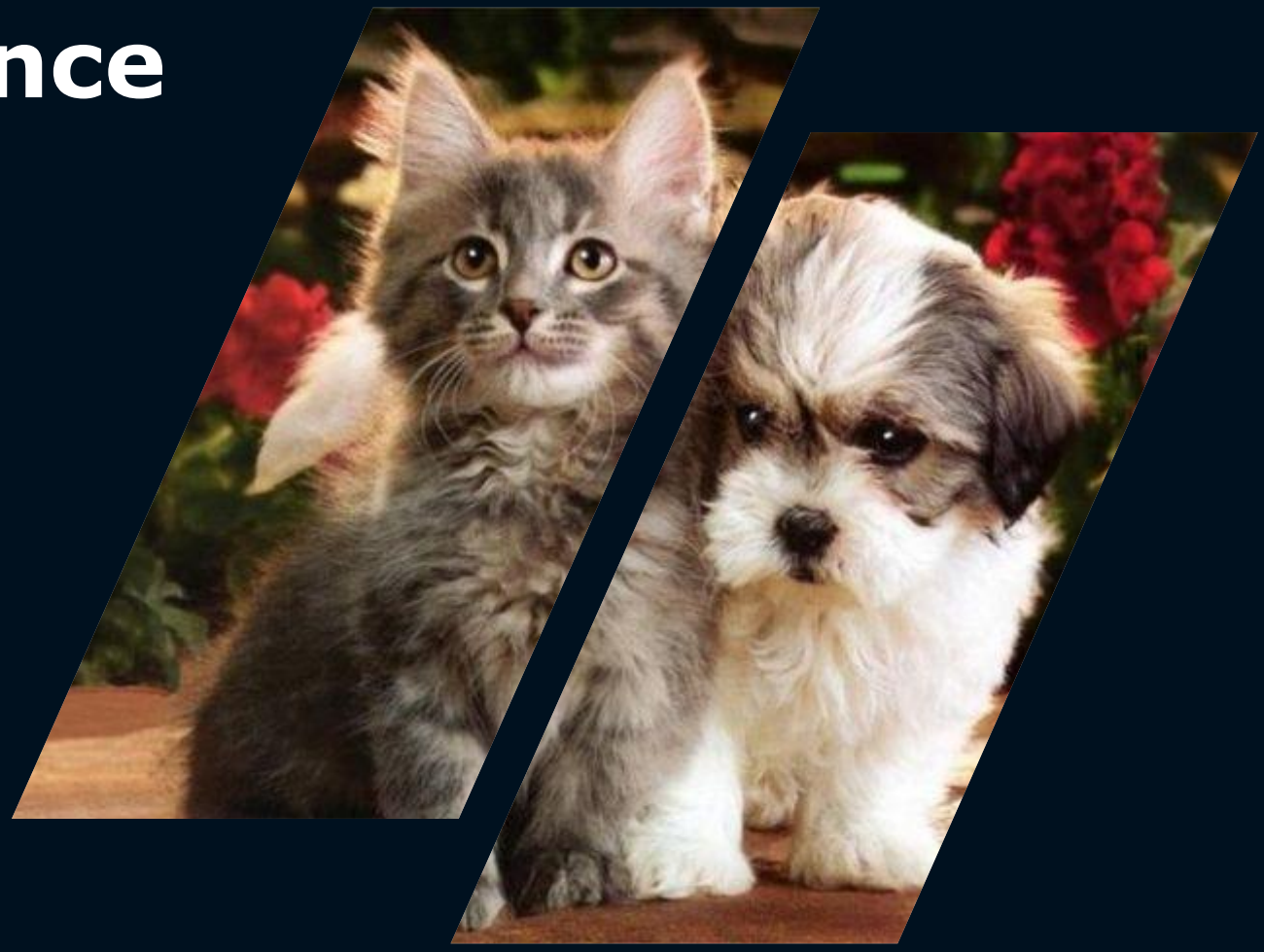
- The trend to connect everything to the Internet
- The purpose is to collect as much information about you as possible.
- Most devices have little or no security.

> “Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

Artificial Intelligence

A massively mixed blessing.

- Playing an increasing role in cyber attack and defense.
- "Literalism" creates a problem with solutions from Ais
- The extra speed and sensitivity of AI systems can make create dangerous systemic instabilities.
- Pressure to incorporate kinetic responses to catastrophic cyber attacks demands humans in the decision loop.

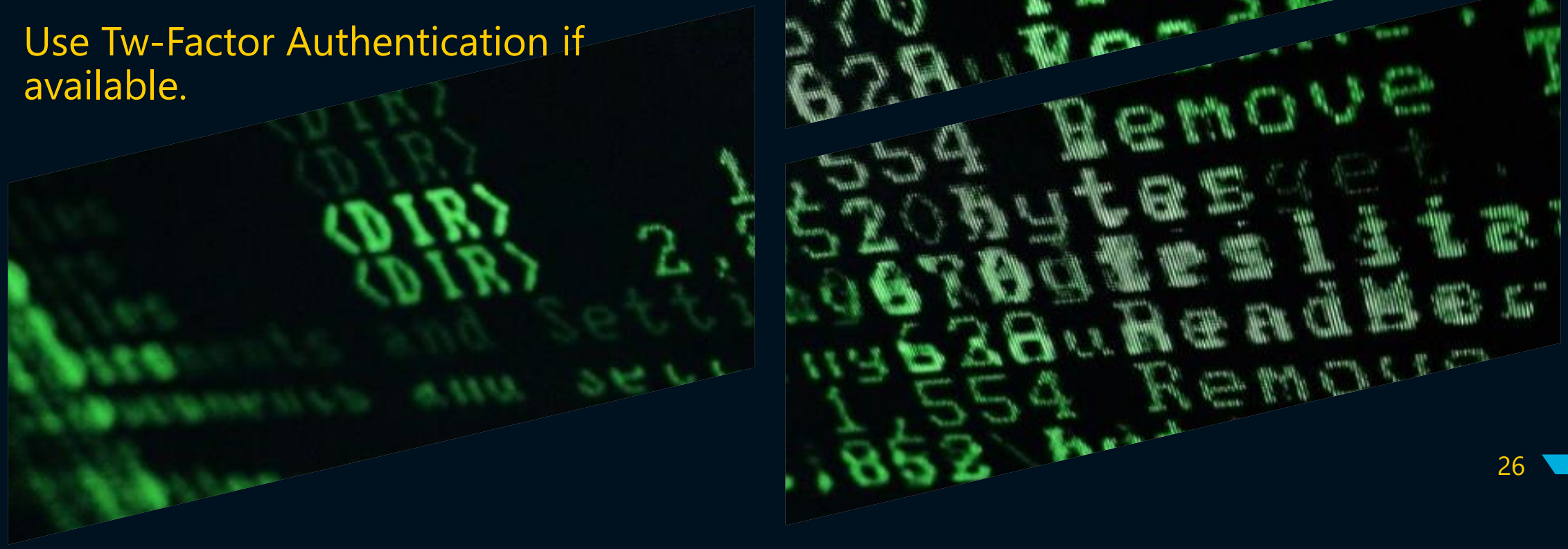


Check Your Password

How Secure Is My Password?

Have I Been Pwned?

Use Tw-Factor Authentication if available.



Secure Your Network

Talk to your ISP or go online to learn how to change your network settings.

- Change the passwords on your home internet router and any other routers and repeaters.
- Change default passwords on all IoT devices. Erase those passwords from any IoT devices you decide to retire.
- Set up a guest login for visitors that does not tie in to your regular home network.

System Updates

Irritating, but necessary

- Whenever a system update becomes available, install it. Don't wait.
- Install and maintain good anti-virus software. Don't use more than one system.
- Put a good backup system in place, preferably with both cloud and local backups.
- Create an emergency boot disk or flash drive.

Social Media, Browsing, and Searching

Protect your privacy

- Use browsers with a Virtual Private Network (VPN)
- Review and update your privacy settings
- Avoid using public WiFi to send or receive personal information
- When using SMS, use apps with end-to-end encryption
- Find out if your mobile device can be tracked and/or deactivated remotely if it's lost
- Only use apps from legitimate app stores.

The Other Problem: Big Data

The business models of Big Data are fundamentally at odds with your privacy.

Protecting Your Data

- As should be clear by now, data companies are not consistently good at protecting your data
- The purpose of data collection is to sales, marketing, and influencing your buying patterns, habits, and more.
- Even well-meaning measures to protect privacy can—and frequently do—backfire.

What's at Stake

- Technology by its very nature always creates unintended consequences.
- As consumers of technology, we need to be careful, thoughtful, and deliberate about what we really need.
- "An alert and knowledgeable citizenry…"

THANK YOU!

Sheldon Greaves

Blog

www.guerrillascholar.com/cogito/

Email

drshel02816@gmail.com