

Cyber Warfare

Cyber Security Seminar Series

January 2022

Part 1

John Jenkinson

To View an audio recording of this seminar
Use this link:

- No need to create nor use a Vimeo account.
- <https://vimeo.com/665386937>

Why this seminar?

- Twitter attack
- Vault 7 and Shadowbrokers
- Life, Liberty, the Pursuit of Happiness
- Information gives no indication of being stolen
- Identity theft is misleading
- Anonymous published transcript of conference call NSA <-> GCHQ
- Cyber security, Cyber crime, Cyber activism, Cyber hacktivism, Cyber bullying, Cyber war, etc.
- SolarWinds

Who is this guy?

- John Jenkinson
- 1962 first computing job first hack
- 1964 ARPA contracts
- 1966 US Army
- 1971 BS Physics 1975 BS Math 1978 MS Computer Science
- 1974 Mostek
- 1983 -> 2016 Big oil
- Cyber security focus, training, certifications, consulting
- FBI InfraGard DHS Critical Infrastructure US-CERT
- Mensa

Fifth Domain

- Land, Sea, Air, Space Cyber
- Before cyber, all required large resources
- Before symmetric
- Before attribution was easy
- Before there was greater than microsecond warning

Phases Cyber Conflict

- Realization

USA, UK,

Morris worm, Cuckoo's Egg, Citibank,

- Takeoff

USA, UK, Russia,

Eligible Receiver, Solar Sunrise, Moonlight Maze,

- Militarization

USA, UK, Russia, China,

Titan Rain, Estonia, Georgia, Buckshot Yankee

Cyber Warfare: a history

- Civil war Telegraph stations captured – false information
- Zimmermann telegram factor US entry WWII
- WW II Factor to develop computer for code breaking
- East German spy IBM German subsidiary

Cyber Warfare: a history

- Civil war Telegraph stations captured – false information
- Zimmermann telegram factor US entry WWII
- WW II Factor to develop computer for code breaking
- East German spy IBM German subsidiary 1968
- First *Reported* case?

CBNR

- Chemical, Biological, Nuclear, Radiological
- 1995 sarin gas Tokyo subway
- 2015 mustard gas Syria
- 2018 Novichok poisoning UK and Russia

- Fake news alert Georgetown lake poisoned

Twitter

- July 2020

- Accounts

Bill Gates, Barack Obama, Kanye West, Michael Bloomberg, Joe Biden, Apple, Elon Musk

- Bitcoin scam \$120,000

- Donald Trump – special Protections deactivation 2017



Elon Musk 

@elonmusk



Feeling grateful, doubling all payments sent to my BTC address!

You send \$1,000, I send back \$2,000!
Only doing this for the next 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

1:27 PM · Jul 15, 2020 · [Twitter Web App](#)

Ransomware

- Global economy impact
- Where is the money?

- Mass disruption
- Subtle influence
- New domain
land, sea, air, space, cyber
in front, to the side(s), behind, above, below, *inside*
- “Olympic Games” Stuxnet

Cyber War

- Ronald Reagan 1983 “War Games”
- Obama cyber spending soared
- Listen -> Alter
- Atomic weapons Resources
- Cyber weapons once used, avail to any/everyone
- Every aspect of daily life
- Access from any/everywhere
- Internet unregulatable
- Commutative

Olympic Games - Stuxnet

- Offensive cyber weapon
- Presidential authorization
- U.S. and Israel
- Slow Iran's nuclear program w/o armed conflict
- Duplicate facilities built US and Israel

Internet infrastructure is not secure

- DNS hijacking
- Autogenerated certificates
- BGP
- Internet is fragile Microsoft, Google,

NotPetya

- Stuxnet, Haiti invasion, Sony & response
- June 2017 A.P. Møller-Maersk
- Kiev, Ukraine Linkos Group M.E.Doc
- Update -> backdoor -> EternalBlue (NSA)
- Island hopping unpatched -> patched
- Encryption with random key
- \$10Billion
- Infection worldwide including Russia
- Nation-state weapon of cyber war

Saudi refinery

- September 2019
- Drones can be launched and have affect from close range
- Before an air force needed to bomb, now a \$100 drone
- Attribution almost impossible
- Air force thousands involved
- Drone cruise missile few involved

U.S.
CYBERSECURITY

STOP



Lisa ©2015 6-9 Dist by Wash. Post/Hitlers Group

- Scared?
- Awareness, Preparedness, Understanding
- Life, Liberty, Pursuit of happiness
- Helpful < > Harmful

Cyber War

- Social Media
- Malware as a Service
- Nationalism can be an individual thing

Helpful < > Harmful

- DNA testing

Information belongs to the testing agency Law enforcement

- HIPPA

Civil penalty Health care advance potential

Identity

- Uniquely distinguish you from the rest of mankind
- Chain of trust

Passwords

- PassPhrase
- *We* know how to use them
 - unlike biometrics we can change passwords
- A portion of credentials
- Multi Factor authentication SMS or Phone call Biometrics

passwords

- Credential stuffing
- Password Spraying
- Office of Personnel Management
 - Manning & Snowden Aging system OPM
 - Background check info Standard Form 86

MyLife

- Classmates & others
- RemovalRequest@MyLife.com
- Someone just pulled Your Reputation profile
- eMail then link

- Thank you for contacting MyLife™ to request removal of your Public Background Report & Reputation Score.

Unfortunately the information on your Public Background page cannot be removed as it is gathered from public records, government, and other public sources for the purpose of helping people learn more about others for business, dating and other reasons.

As MyLife is also here to help you monitor what's public about you, and help you improve your Reputation, **we offer several services that we recommend you use to:**

- Editing your public information
- See and delete your information on other sites you can't control
- Verify and correct your Background Report

Next Steps:

Please contact a Customer Care Representative to upgrade to Premium Membership by calling 888-704-1900 or sign up online at www.MyLife.com

About & Contact Info

Photos & Social Posts

Reviews & Ratings

Criminal & Court Records

Friends & Family



Bob Seger, 55

AKA: *Info Pending...*

Work: *Info Pending...*

School: *Info Pending...*

[Edit Photos](#)

Edit

Photos

Share

Reputation Score

4.00 (1 Review)

[Improve my Rating](#) | [Ask others to Rate](#)



Bob Seger is 55 years old and was born on 1/1/1963.

See, edit & monitor your Background Report

About Bob Seger - [Edit Info](#)

Birthday: 1/1/1963

Income: *Info Pending...*

Current Net Worth: *Info Pending...*

Political Affiliation: *Info Pending...*

Contact Information

Phone: [View Phone Number](#)

Email: *****@yahoo.com*

Address: [View Address](#)

MyLife

- About & Contact Info
- Photos and Social Posts
- Reviews & Ratings
- Criminal and Court Records
- Friends and Family

(and neighbors!)

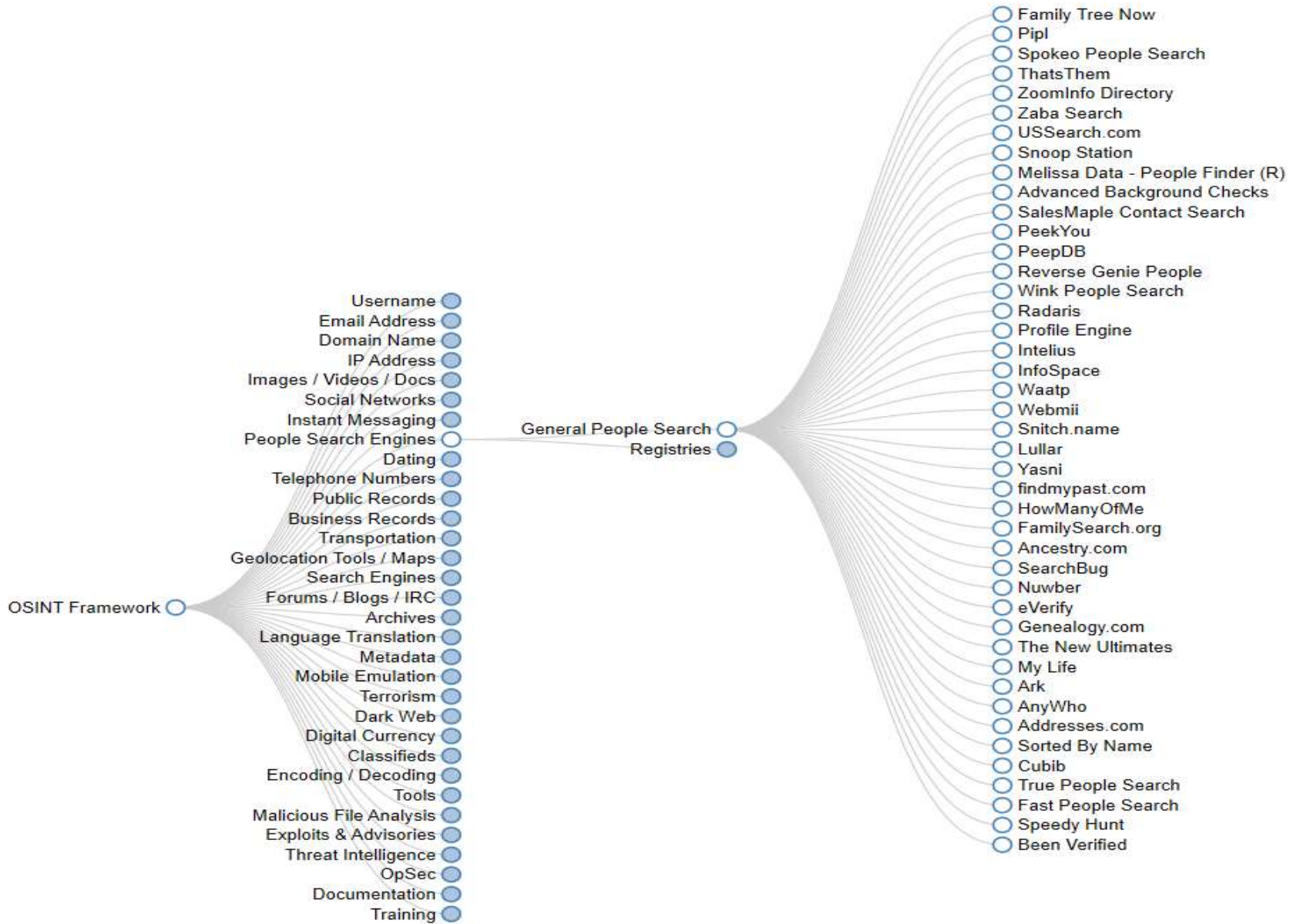
MyLife

and Neighbors

MyLife

- Political party
- Income
- Net Worth
- Reputation
- Religion
- Automobile
- Past physical addresses
- Aliases
- Evictions
- Work History

- <https://osintframework.com/>
- <https://www.cyberbackgroundchecks.com>



- Postal mail “Get out the vote”
- Identity theft
- Account takeover
- Theft misnomer

CBNR

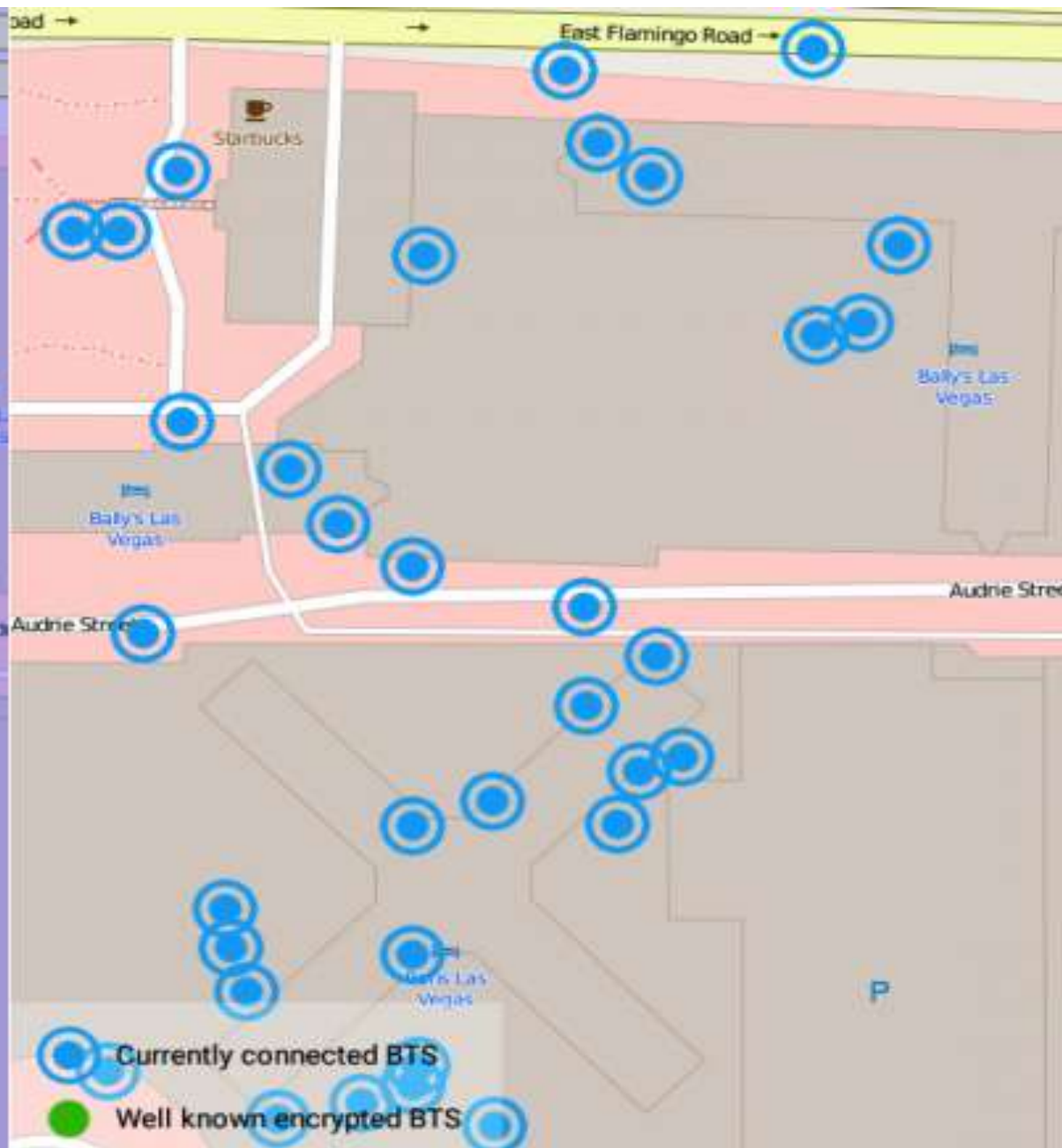
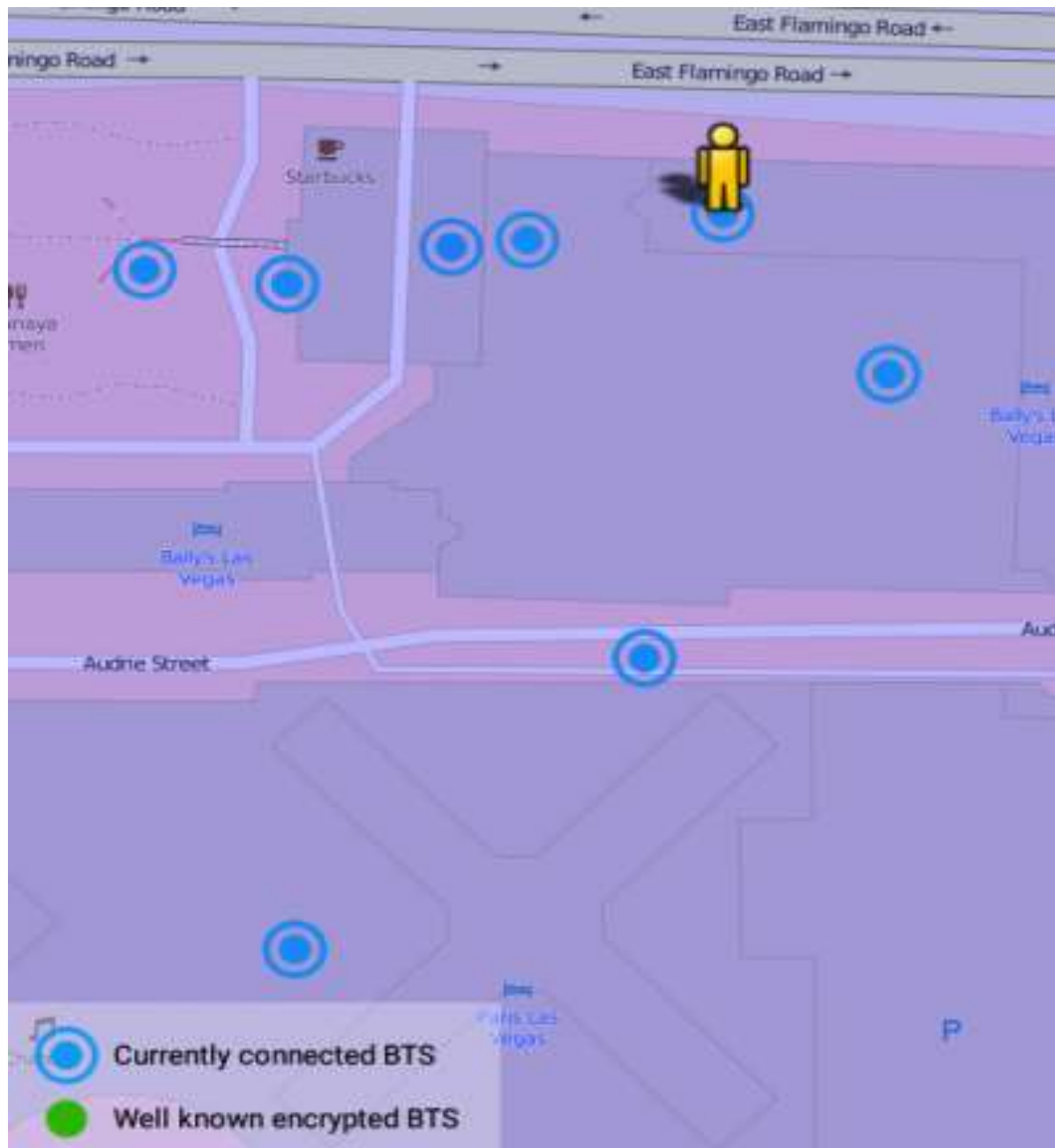
- Chemical, Biological, Nuclear, Radiological
- 1995 sarin gas Tokyo subway
- 2015 mustard gas Syria
- 2018 Novichok poisoning UK and Russia

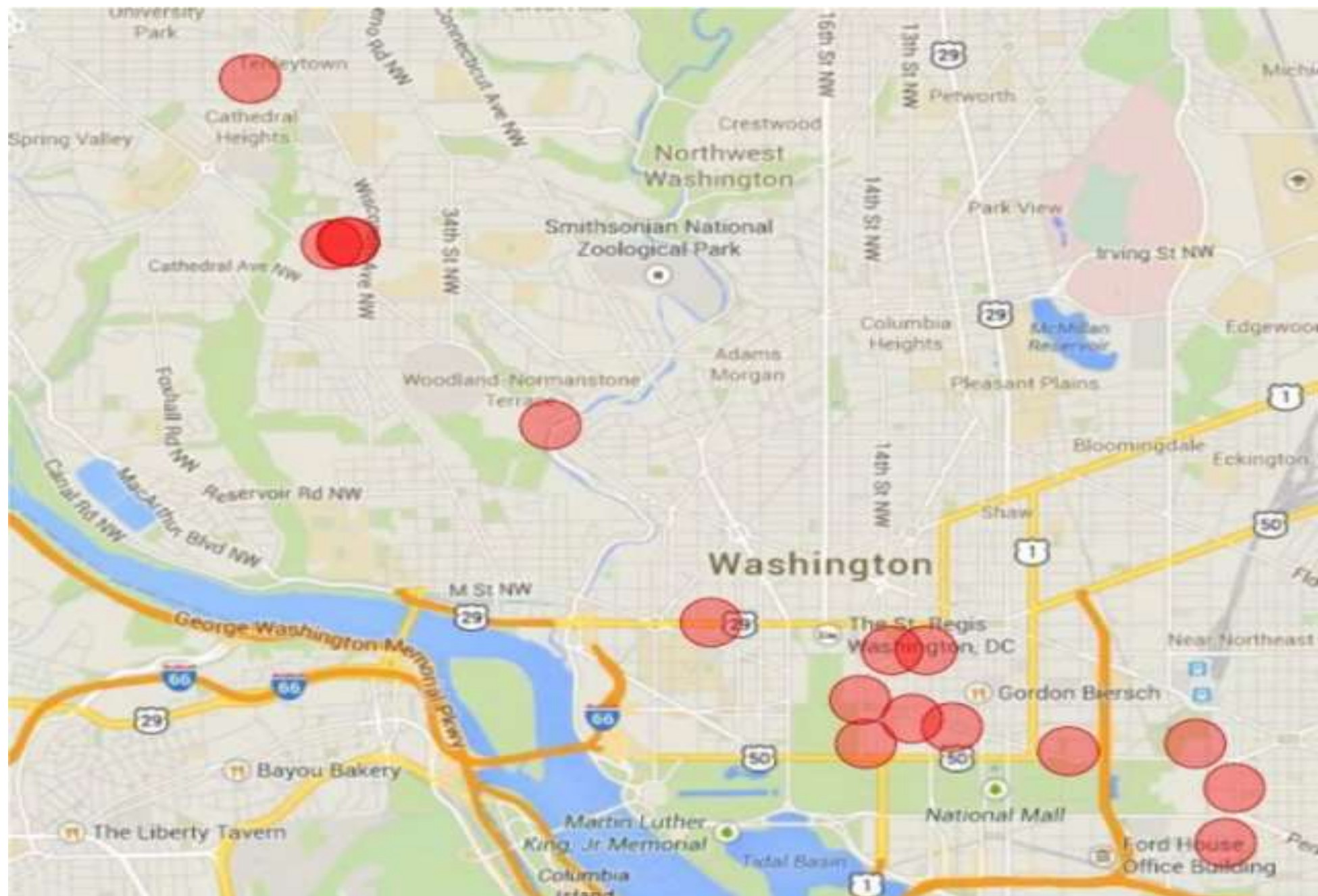
- Fake news alert Georgetown lake poisoned
- 2011 Bush, Rice, Powell counter-terrorism summit China
botulinum toxin White House “feet down, not feet up”
smallpox & radioactive scares

- AI Fake news generator author
- Sound byte editor
- GPS
spoofed

Cyber War

- Military IDS *quote*
- DoD Contractors
- BGP & DNS
- L0pht
- DOS Amazon, eBay, Yahoo
- 1994 Haiti invasion
- Mis-information warfare
- Firewalls facing wrong way
- Title 10 use of force Military
- Title 50 Intelligence





- Hack-a-satellite Hack-a-F35
- Hack the pentagon
- Hack DHS \$50 - \$500

- Internet ARPA DARPA
- Electronic Fence
- ICBM nuclear shield
- Cuban Missile crisis

Cyber War

- Operation Orchard 2007 Israeli Syria *false sky picture*
- Estonia attacks
- Idaho National Lab
- Aurora generator 2007
- 2008 Buckshot Yankee flash drive
- FISA
- National Security Letters
- Stuxnet
- North Korea ICBM failures
- 80% of Internet traffic thru US 2 locations
- 0-day vulnerabilities



BRUCE SCHNEIER

BEST-SELLING AUTHOR OF *DATA AND GOLIATH*



CLICK HERE TO KILL EVERYBODY

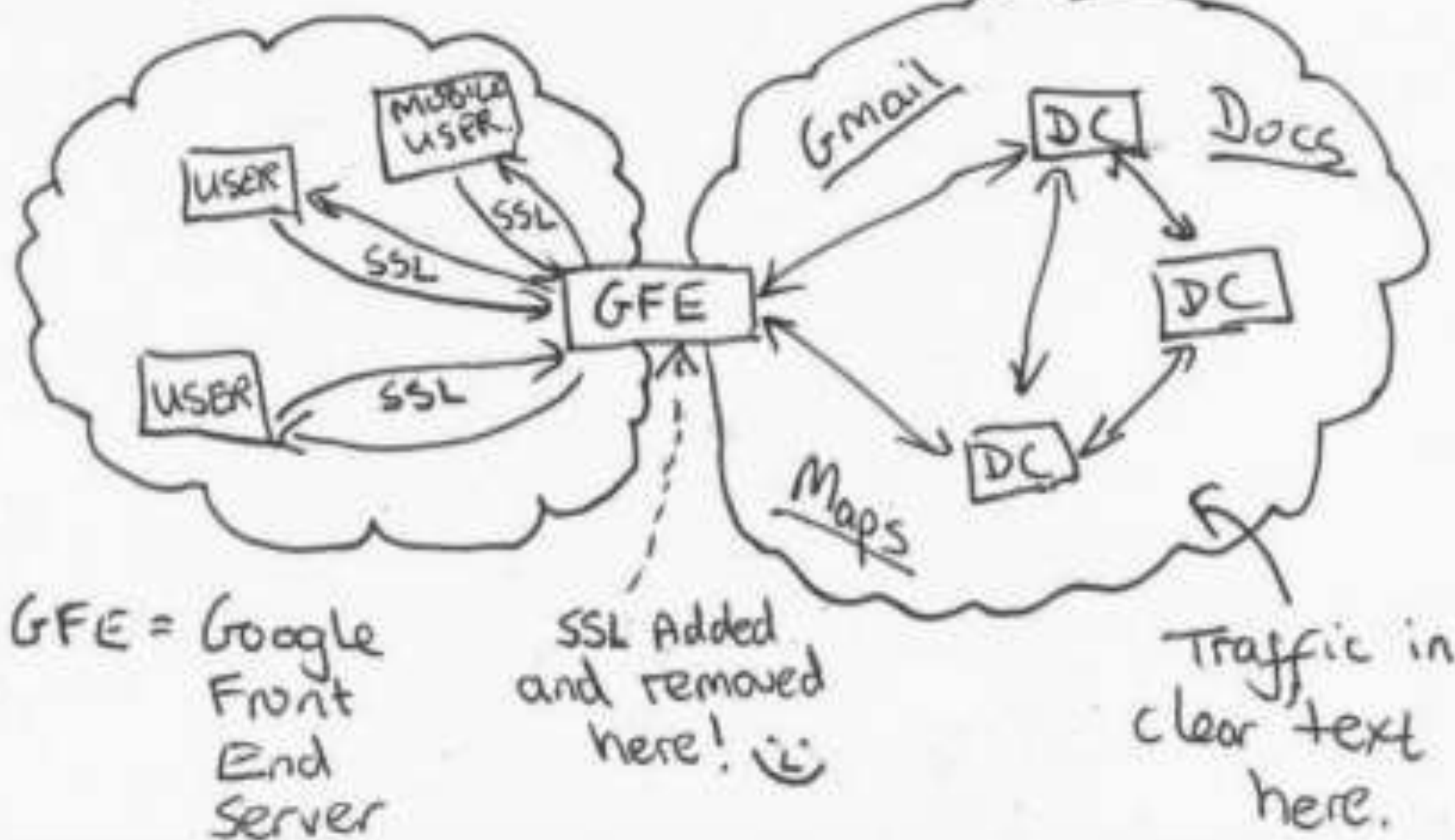
Security and Survival in
a Hyper-connected World

OK



PUBLIC INTERNET.

GOOGLE CLOUD.



It just takes One

- Manning Snowden (??)
- Buckshot yankee flash drive
- Black hat 1 vulnerability White hat every vulnerability
- Ivy Bells
 - 1970 – 1980 NSA submarine and divers tap Soviet Navy's cable
 - NSA communications specialist with bankruptcy issue
 - Soviet embassy
- Any cyber tool Once used Reverse engineering

A timeline

- 1943 Colossus enigma Bombe
- 1969 ARPA ARPAnet
- 1970 Electronic fence
- 1982 CIA altered Canadian software for Soviet pipeline explosion
- 1986 Cuckoo's egg
- 1988 Morris worm Computer fraud and abuse act
- 1994 Griffiss AFB “sniffer”
- 1997 Eligible Receiver exercise

A timeline

- 1998 3 teenagers detected in Air Force systems
Cyber security plan DoD Joint Taskforce Computer network defense
- 2001 Code Red White House web site
- 2003 Anonymous WikiLeaks Media and Credit card companies
Chinese military Titan Rain
- 2007 Estonia DDOS 22 days
US Secretary of Defense email hacked
British Foreign office

A timeline

- 2008 Russia & Georgia war, DDOS Georgia's government
Flash drive in Middle East US VERY significant data breach
- 2009 Israel's government cites 15 million junk mails/second
US drone's live feeds hijacked by insurgents
- 2010 Stuxnet Cyberspace new warfare "domain"
Anonymous attack WikiLeaks "enemies"
- 2014 US indicts members of Chinese Peoples Liberation Army
Office of Personnel Management

A Timeline

- 2014 Sony

Very Few of the incidents known

The unknown and/or unreported

Stuxnet

- It “got away”
- Iran – financial institutions
 - GREAT increase in cyber prevention efforts
 - Not GREAT efforts to disclose
 - Washington summit of financial executives
- Iran Bowman Avenue dam
- Iran’s attacking infrastructure not in Iran

And then

- Saudi Aramco
 - Ramadan
 - 30,000
 - Hard disk drive shortage
 - Many global entry points
-
- Financial, oil supply, infrastructure

Cyber War

- China USA summit June 7,8, 2013
- June 6, 2013, Snowden leaks reported

- Feb 2014 Sands Corp. assault
- Nov 2014 Sony attack

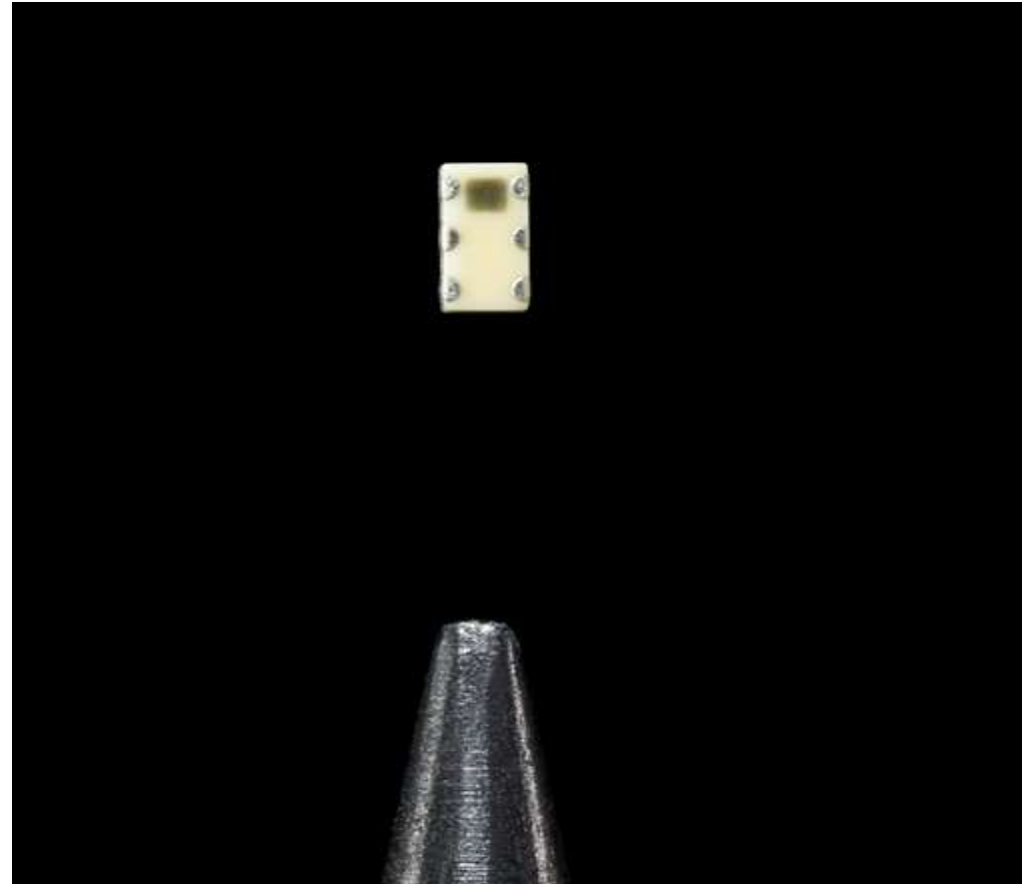
- Proportional response

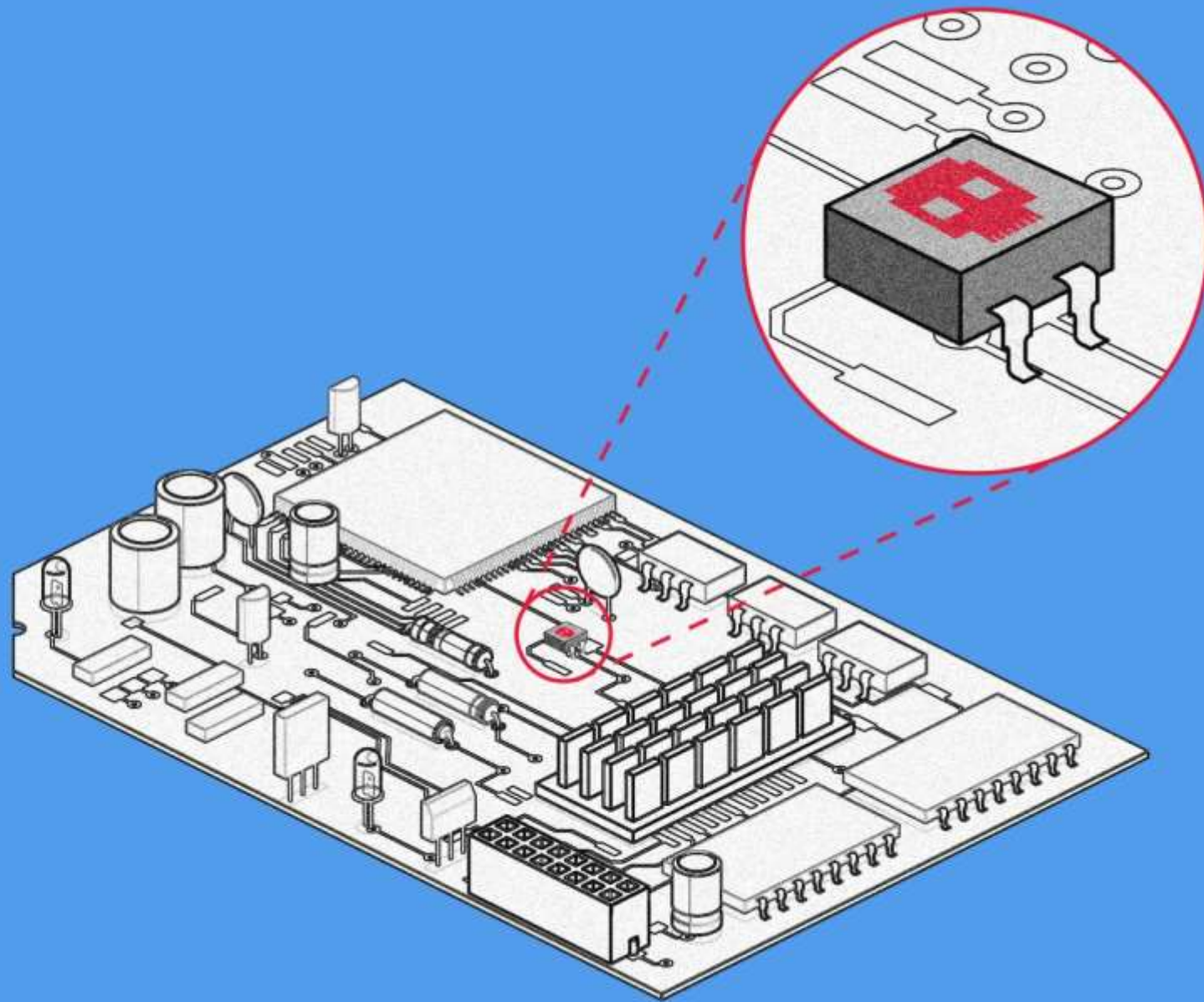
Surveillance

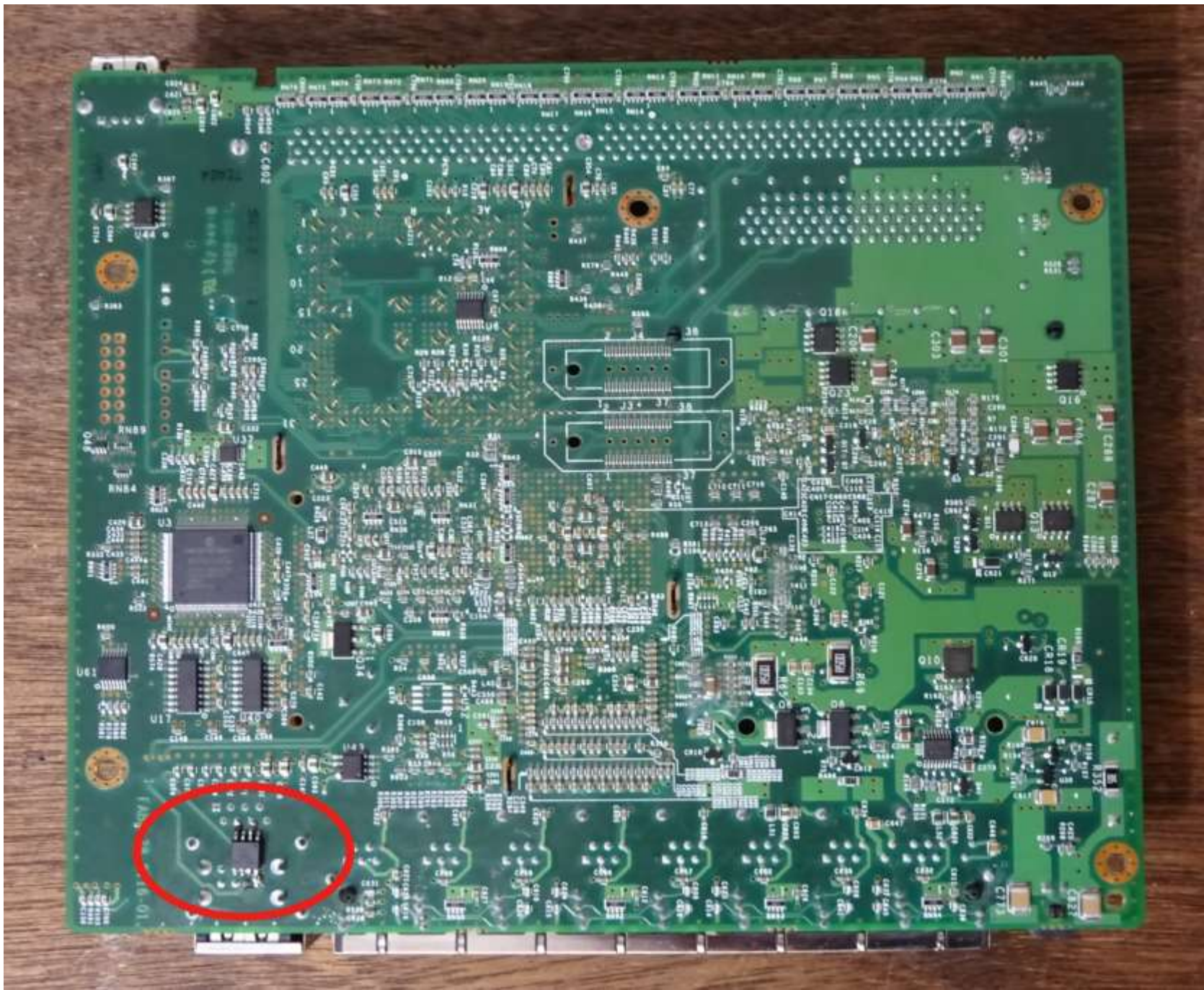
- Old as war itself
- Supply chain

FACET

- Supply chain
- No one does anything alone
 - NSA has semiconductor foundry
- Alyeska Pipeline
 - Disk drives with malware
 - Conference room
 - Cisco







KCC - REM - STX - BarraCuda
Seagate singapore int'l HQ Pte,Ltd
Koolhovenlaan 1,
Product of Thailand
HDD Mfg by
Seagate Technology LLC



2TB
BarraCuda
ST2000DM006
S/N: ZWE3EX5X
P/N: 2DM14C - 302
F/W: CC46
WWN: 5000C5008FFA26T1
P8ID: YJ4H90B0UFXQ6JZ
05GYHTQV36HTZBUNR



019952370443
verify.seagate.com



+5V 0.75A
+12V 0.75A

Site: TK
DOM: 02JUN2018

KCC - REM - STX - BarraCuda
Seagate singapore int'l HQ Pte,Ltd
Koolhovenlaan 1,
1119 NB Schiphol - Rijk,
The Netherlands
Product of Thailand
HDD Mfg by
Seagate Technology LLC

2019/10/1 16:51

RUG - REM - STA - BarraCuda

Seagate Singapore Int'l HQ Pte,Ltd
Koolhovenlaan 1,
Singapore

Product of Thailand

UMR Mfg Co



Earth satellites

- 730
- 2220

Ransomware

- Attribution is hard
- Tracing digital currency is easy, determining the exit point is hard
- Attacker might be an employee or half a world away
- If no clear evidence exists data was stolen as well – no requirement to report to law enforcement
- Ransomware as a service
- Ransomware being outsourced Victims being sold Data being sold
- Ransomware can take time past backup cycle
- US Treasury Advisory payments to sanctioned parties
- Ransomware insurance Ransomware Specialist
- It just takes 1 Daily occurrence Fatality reports

Ransomware

- Trickbot botnet 1 million hijacked PCs
- US Cyber command Persistent engagement
- Troll farms
- Potential election disruption

Election Disruption

- Apolitical
- Venezuela trip early 1990s
- The truth A truth
- Persona

- Trump & Russia
- 2011 Putin troubles - Cause Hillary Clinton

- News Journalism -> Publisher
- Rise of persona Social media Trolls
- Person Organization Media
- Internet Research Agency IRA 2013 St Petersburg
- Putin's chef (Prigozhin) Few amateurs Organized professionals
NETWORKED
- Wagner "little green men"

Ukraine

- Oct 2013 President Yanukovich East West division
- Violence fanned by IRA and others
- Feb 2014 Yanukovich flees interim government
- Carousel of lies Ukraine 1 Ukraine 2
- Victoria Nuland Assistant Sec of State Phone call to Ukrainian ambassador EU vs UN “recording better than mine”
- BOTH sides

Ah ha

- English speaking IRA hires Trips to USA
- VKontakte -> Facebook, Instagram, YouTube, Pinterest, Reddit, ...
- BOTH sides Heart of Texas BlackMattersUS
- The message “Don’t Vote”
- 100 scribblers with comments, cartoons, stories cause

And Then

- DNC *hack* X-agent Gmail credentials compromised
- *Gather, exfiltrate, analyze*
- GRU Intelligence military SVR
- Dec 2015 Western Ukraine power grid Playground/test bed
- Dec 2014 Hack into election server Corrected days later
- Fancy Bear Cozy Bear
- FBI detect Call DNC
- DCLeaks.com for document dump
- Guccifer 2.0
- Wikileaks 20,000 eMails just before convention

And then

- Wikileaks source?
- Putin denial
- Ukraine, Syria, ... Urgent vs important
- Brennan Bortnikov warning
- Attack on US person at US embassy in Moscow
- Sanctions, indictments, cyber cyber escalations

- Fusion GPS
- Magnitsky act
- Election “hacking”
- *Thousands of probes*
- Defcon Black hat voting machines
- Voter data online “we’re the government, we’re here to help”
- State of Georgia DHS “hack” sources & methods
- Oct 7 Hurricane, DHS statement, Access Hollywood tape, Podesta eMails
- Comey voter fraud TEN_GOP raise doubt ???
- Mueller Report *Social Media* *Hacking and Information release*

- Little cooperation/coordination in Russian Intelligence agencies
- Russian internal internet
- Lack of heavy activity recently
- NSA & UK National Cyber Security Centre warn
Turla group activity Iranian APT group takeover

And now?

- ABC news Large increase mis-information less effective?
- FOMO
- US Cyber command Trickbot
- Microsoft CVE-2020-1472 Zerologon VPN flaws Election support

Cyber Hygiene

- A LOT of material
- Helpful <-> Harmful
- <https://sctxcompclub.org>

Tickets | Business Directory | Sun Rays Magazine | Contact Us | RESIDENT LOGIN

About Us | Lifestyle & Activities | Clubs & Groups | Fitness | Golf | Communications




Computer Club

Computer Club / Photography Club Cooperation

Transitional Guidelines for Reopening

[Click here to take a virtual tour of our facilities.](#)

Be One of Us in 2020

Welcome to the website of the Sun City Texas Computer Club.

Sun City meeting space availability diminishes every year. In the spirit of neighborly cooperation, and to maximize the use of the facilities allocated to the Computer Club, the Board has welcomed the Photography Club for periodic classes and meetings in our facilities.

Contact: clubofficial@scctxcompclub.org for more information.

Phone ~ Cyber Center: 512-868-9780

Lab Hours: Monday through Friday ~ 9 a.m. - noon

WHERE CAN I FIND THE COMPUTER CLUB?

CYBERCENTER CLOSURE DATES

VOLUNTEER INTEREST FORM

ALL CLUBS

COMPUTER CLUB

ARCHIVES

CLUB ADMINISTRATION

EDUCATION

LAB INFORMATION

LAB MONITORS

MALWARE HELP

MEETINGS

MEDIA CONVERSION



MEMBERSHIP

SPECIAL INTEREST GROUPS (SIGS)

OUR WIKI FOR ONLINE HELP

Tickets | Business Directory | Sun Rays Magazine | Contact Us | RESIDENT LOGIN

About Us | Lifestyle & Activities | Clubs & Groups | Fitness | Golf | Communications

Computer Club

Computer Club / Photography Club Cooperation

Transitional Guidelines for Reopening

[Click here to take a virtual tour of our facilities.](#)

Be One of Us in 2020

Welcome to the website of the Sun City Texas Computer Club.

Sun City meeting space availability diminishes every year. In the spirit of neighborly cooperation, and to maximize the use of the facilities allocated to the Computer Club, the Board has welcomed the Photography Club for periodic classes and meetings in our facilities.

Contact: clubofficial@scctxcompclub.org for more information.

Phone ~ Cyber Center: 512-868-9780

Lab Hours: Monday through Friday ~ 9 a.m. - noon

WHERE CAN I FIND THE COMPUTER CLUB?

CYBERCENTER CLOSURE DATES

VOLUNTEER INTEREST FORM

ALL CLUBS

COMPUTER CLUB

ARCHIVES

CLUB ADMINISTRATION

EDUCATION

LAB INFORMATION

LAB MONITORS

MALWARE HELP

MEETINGS

MEDIA CONVERSION

MEMBERSHIP

SPECIAL INTEREST GROUPS (SIGS)

OUR WIKI FOR ONLINE HELP

Computer Club Special Interest Groups (SIGs)

The Computer Club has many groups that meet each month to discuss topics of interest. Computer Club members, click on the SIG name below for description, and meeting schedule.

CyberSecurity

This special interest group deals with CyberSecurity in all forms. Check out the news feed from the CyberSecurity SIG, which is an entry on the SIG menu.

First Time

The First Time SIG is for members seeking answers to their questions about how to use computers. Its volunteers assist beginning computer users to become more knowledgeable about their computers and to use them more effectively. For more information click on the name *First Time* just above.

Genealogy

The Genealogy SIG provides a forum for the exchange of information and experience about the use of computer programs and the many resources found on the web for genealogical research.

Hearing Solutions

The HEARING SOLUTIONS SIG is comprised of those who seek knowledge regarding hearing loss, searching for solutions & related professional information. The SIG meets most months on the 2nd Thursday at 10:00 am in the Activity Building Atrium.

iDevices

The iDEVICES SIG provides opportunity for sharing of experiences and knowledge about iPhones, iPads, Apple watches, iTunes & Applications. It meets most months on the 2nd Friday at 1:30 pm in the Activity Center Atrium.

Internet of Things (IoT)

A forum for the informal exchange of information and to educate and guide one another on how to experiment, design, and implement the microprocessors, micro-controllers, sensors, and activators associated with the Internet of Things.

VectorVest

The VectorVest & Beyond (VVB) Special Interest Group (SIG) provides a forum for the exchange of information and experience about investing software for curious members at beginning and intermediate levels. The goal is to learn more about using tools found within VectorVest.com and other software such as AAll.com, FinViz.com, Morningstar.com, and StockCharts.com.

Windows

The WINDOWS SIG is dedicated to the understanding and proficiency of the Microsoft Windows operating systems. It meets the 2nd and 4th Tuesday at 9:00 AM.

Sun City Texas
Community Association

Tickets | Business Directory | Sun Rays Magazine | Contact Us | RESIDENT LOGIN

About Us | Lifestyle & Activities | Clubs & Groups | Fitness | Golf | Communication

CYBER SECURITY

ALL CLUBS

MEETING NOTES

CyberSecurity

Current news articles are given in the *Cyber Security News Archive* link.

Tutorials on computer topics are given in the *Seminars* link.

Life, Liberty and the Pursuit of Happiness Any or all of these basic human rights can be taken by our current cyber environment, our home network, and/or our Internet connected devices.

Life *low risk* implanted medical devices, health records.

Liberty *medium risk* use of your network or device by criminals to attack others. Unwarranted surveillance.

Pursuit of happiness *high risk* fraud via your network or devices.

The Cyber Security SIG mission: To help preserve these rights by raising awareness, preparedness, and understanding of the threats and techniques that attack these rights.

The SIG is scheduled to meet on the first and third Thursday of each month at 3 p.m. in the Annex.

Topics for the SIG meetings are chosen by the SIG membership.

To join the Cyber Security SIG contact the SIG at SCCCCyber@gmail.com

MEETINGS

Note: All meetings are now audio recorded

Next Presentation with audio

November 5, 2020

On Line with audio

Zoom Meeting



» ALL CLUBS

MEETING NOTES

- [Meeting Notes Archive 2019](#)
- [Cyber Security News Archive](#)
- [Meeting Notes Archive 2018](#)
- [Seminars](#)

Cyber Security SIG Meeting Notes

2020

- [July 21 Safer Browsing Class \[Download | View \]](#) | 100,000
- [January 2 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [January 16 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [February 6 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [February 20 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [March 5 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [March 19 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [April 2 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [April 16 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [May 5 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [May 21 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [June 4 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [June 18 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [July 2 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [July 16 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [August 6 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [August 20 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [September 3 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [September 17 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [October 1 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [October 15 Cyber Security SIG Presentation with audio \[Download | View \]](#) | 100,000
- [February 20 MUG re-Presentation \[Download | View \]](#) | 100,000

» ALL CLUBS

MEETING NOTES

[Meeting Notes Archive 2019](#)

[Cyber Security News Archive](#)

[Meeting Notes Archive 2018](#)

[Seminars](#)



More ▾

Create Blog

SCCCCyber

Wednesday, September 23, 2020

Firefox on Android platforms

VERY important. Firefox on Android platforms had a SERIOUS Local Are Network flaw that allowed attackers to force the Firefox browser to visit sites that held malicious content and/or take over the Android device.

IMPORTANT to update Firefox. I show version 81.1.1 as the current release.

Posted by John Jenkinson at [10:56 AM](#)

No comments:



Sunday, August 30, 2020

Internet down/slow 30-Aug-2020

Some sites unresponsive. If you experience slowness, outage, be aware.

Posted by John Jenkinson at [9:10 AM](#)

No comments:



Saturday, August 29, 2020

Adobe Lightroom version 5.4 for iOS devices DELETES customer photos!!

Adobe has announced that users who updated Lightroom to version 5.4 may have lost all photos, presets, edits, watermarks, etc.

Adobe apologizes, says there is no way to recover unless costumers had backup in Adobe cloud or other backup.

Blog Archive

- ▼ 2020 (49)
 - ▼ September (1)
 - Firefox on Android platforms
 - ▶ August (7)
 - ▶ July (4)
 - ▶ June (3)
 - ▶ May (5)
 - ▶ April (14)
 - ▶ March (8)
 - ▶ February (3)
 - ▶ January (4)
- ▶ 2019 (28)
- ▶ 2018 (57)
- ▶ 2017 (62)
- ▶ 2016 (16)

« ALL CLUBS

MEETING NOTES

Meeting Notes Archive 2019

Cyber Security News Archive

Meeting Notes Archive 2018

Seminars

Cyber Security SIG Meeting Notes

-  Sun City Computer Club WEB site navigation and information [[Download](#) | [View](#)] | 2,602.35kb
-  First Time SIG Safer Computing [[Download](#) | [View](#)] | 126.09kb
-  Safer WEB Browsing Class [[Download](#) | [View](#)] | 800.65kb
-  Safer WEB Browsing Part one [[Download](#) | [View](#)] | 1,585.12kb
-  Safer WEB Browsing Part two [[Download](#) | [View](#)] | 407.06kb
-  Sun City MAC Users Group MUG Securing your MAC [[Download](#) | [View](#)] | 786.08kb

Cyber Security

- Awareness, Preparedness, Understanding
- Helpful <-> Harmful
- Information gives no indication of being stolen
- IDentity theft is misnomer
- Information is cumulative
- As each of us are safer, we ALL are safer
- Mis-Information is Information

Cyber first responders

- Similar to pilot training before WWII
- Cyber Patriot
- SANS Cyber Camp

- South Korean Senior University?

Current Events

- NYT 10/22/2020
- Iran eMail Proud Boys
- Hack into Russia to determine Russia moves
- Zerologon & VPN vulnerabilities
- Fear, Uncertainty, Doubt FUD
- yourefired -> maga2020!
- 6 Russian hackers indicted car registrations



PROUD BOYS



Vote for Trump or else!



o Proud Boys <info@officialproudboys.com>

Today at 10:44 AM

To: [REDACTED]

[REDACTED] We are in possession of all your information (email, address, telephone... everything). You are currently registered as a Democrat and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on Election Day or we will come after you. Change your party affiliation to Republican to let us know you received our message and will comply. We will know which candidate you voted for. I would take this seriously if I were you.

Vote for Trump or else!

Attribution is hard

- Third party can start conflict between two parties
- Proxy
 - Delegation
 - Orchestration
 - Sanction
- Military – legitimate use of physical force

- Rohna disaster
- HMT Rohna

Cyber Warfare

Cyber Security Seminar Series

Part 2

January 2022

Realization Phase

- MILNET split from ARPANET 1983
- FAREWELL dossier KGB French intelligence
Request for USA software Canadian software
Soviet pipeline explosion October 1982
CIA test of French?
- *The Cuckoo's Egg* Cliff Stoll 1986
German hackers Lawrence Berkeley Lab Star Wars 75¢
Who pays for Germany trip? What damages? Creditable
evidence

Realization Phase

- Morris worm November 1988
Rapid spread Widespread Private sector contained
- Computer Emergency Response Team (CERT)
- Computer Fraud and Abuse Act 1986
- Zippies DOS UK ban on outdoor raves
- Vladimir Levin – Russian - \$10M from Citibank extradited
- First Gulf War 1991 Information warfare Cyber elements
- Information has mass, motion, topography
- Air Force Information Warfare Center and others
- Defense & Offense (Offense classified SCIF)
Sensitive Compartmented Information Facility

Realization Phase

- Holland teenagers -> 34 military installations 1990
Gulf war leadup NOT sophisticated NOT classified NOT noticed
- If teenage hackers can... what could professionals with money do?

Takeoff Phase (1998 – 2003)

- Presidential Decision Directive 63 1998
Military & economy reliant on critical infrastructure and cyber
- National Infrastructure Protection Center (NIPC)
Warn industry Industry warns
- ELIGIBLE RECEIVER 1997 no notice interoperability exercise NSA
- INFOCON like DEFCON
- SOLAR SUNRISE first thought to be Iraq
California teenagers mentored by Israeli
“who’s in charge?”

Well, who is in charge? And in charge of what?

- Cyber defense Cyber offense
- Stealth entry into country's systems to alter information
Offense/Defense?

Microsecond response

- Can be “over” before it “starts”
- Thus, response is automated
- What could possibly go wrong?

Recent Events

- Iran Stuxnet
- Iran Saudi Aramco
- Iran US Financial institutions

- Iran GPS lure oil tankers into Iran waters Gulf of Hormuz
- US Cyber command publish cyber attack on Iran's shipping database
- Iran shot down US drone \$182M
- Iran (?) missile attack Saudi refinery
- Gas prices

Recent Events

- Cyber tools can “escape”
- Cyber lacks “precision”
- Cyber war lacks any rules

Hide in plain sight

- The \$200 chip in circuit board
- Reverse engineering semiconductor chip circuit
- ~2B transistors on CPU chip
- Previous reverse engineering use Copying
- Current reverse engineering use Altering
- FACET
- Code sprinkles
- Self Modifying Code

Not Petya

- MEDoc 27 June 2017
- Update compromised
- Similar to earlier attack using same vector
- EternalBlue
- WannaCry “kill switch”

Printer hack

- WSJ web site

"Wall Street Journal would like to apologize to pewdiepie. Due to misrepresentation by our journalists, those of whom have now been fired, we are sponsoring pewdiepie to reach maximum subscribers and beat Tseries to 80 million."

```
--- WHAT TO DO ---  
1. Unsubscribe from T-Series  
2. Subscribe to PewDiePie  
3. Share awarness to this issue  
#SavePewDiePie #PrinterHack2  
4. Tell everyone you know. Seriously.  
5. Fix your printer. It can be abused!  
6. BROFIST!
```



Facial Recognition

- AI
- China millions of AI enabled surveillance cameras
 - Social Credit Score
- UK surveillance cameras
- Grocery store shelves
- Dragon flies don't swarm

Information warfare Mis Information warfare

- Israel air strike Syrian nuclear facility “false sky picture”
- 6 day war Egyptian air defense radar
- GPS

Jamming kits

Spoofing Putin location NATO North Sea exercise

1st Calvary Ft. Hood presentation cyber battlefield

Critical Infrastructure

- Electrical power
 - Brazil - cyber but who?
 - Ukraine - twice
 - Russia June 2019 issues warning
 - DoE Boise Idaho Generator 2006
- Waste water & water supply
- MAD
- Mutually Assured Disruption

Critical Infrastructure

- Financial
- 92% currency is electronic
- Coronal Mass Ejection 1859

Political

- Snowden 2013
- 2nd Snowden
- Pentagon Papers, Chelsea Manning, Benjamin Franklin
- 1777 first whistleblower protection law
- 2014 Nuland phone call “green men”
- Internet Research Agency Glavset
- NYT June 2019 US Russia power grid



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft



Yuriy Sergeyevich Andrienko



Sergey Vladimirovich Detstov



Pavel Valeryevich Frolov



Anatoliy Sergeyevich Kovalev



Artem Valeryevich Ochichenko



Petr Nikolayevich Pliskin

- October 19, 2020
- Ukraine
- French elections
- NotPetya
- Olympic Destroyer
- Novichok
- Georgian Government

Breaking News

- Energetic Bear NYT
- State & Local government probing/prowling
- US west coast airports Wi-Fi portals
- Thousands could be targets about 10 were
- Malware downloaded then looks for energy sector employees
- Possible election outcome confidence outcome steer

Breaking news

- US stepping up Russia power grid incursions
- New authorities under Trump Cyber offence US Cyber Command
- Classified National Security Presidential Memoranda 13
- Military Authorization Bill
- “Message-sending” operations
- Safety systems attacks
- Russia Internet isolation tests Deadman switch

- The leap NotPetya
- June 27, 2017
- Cadbury factory Tasmania Merck stopped vaccines production
- Maersk Largest shipping company paralyzed
- Ukraine No ATMs, no mass transit, no Chernobyl monitoring, computers wiped
- Cassandras predictions coming true?
- 2007 Russia hackers Estonia geopolitical

- Ukraine Power grid test lab?

- Dec 23, 2015

BlackEnergy malware

SCADA remote substations off

Infrastructure UPS, modems, RTUs, commutators

KillDisk

DOS against call-centers

Watching the mouse move the mouse was not moving

- Dec 2016 again a “tune-up” 00:00 exactly
- Aurora 140 KB

0-day

- Unpatched vulnerability
- eMail, WEB sites, Office suites, drive-by, security suites, etc.
- Great power e.g. PowerPoint
- Scripting ex. Java
- Port knocking
- SCADA summit Idaho National Labs
- Vulnerability scanners Virtual Machines C&C obfuscation
- Signature based defenses
- Sandworm signature

SCADA

- Air-gapped until it isn't constant scan
- PLCs ladder logic 24x7 Safety focus not easily isolated
- Reconnaissance
- Industrial Control Systems Cyber Emergency Response Team ISC-CERT
- They are in place Travelling SCADA technicians?
- SCADA technicians need access emergency access
- “we see you” methods and resources kept secret

Ukraine

- Slavic “borderland” long history of conquest, occupation, war
- 1918 grain 1932 starvation increased genocide to high degree
- 1980’s independence April 25, 1986 Chernobyl news suppression
- Feb 2014 Invasion July 2014 Malaysian passenger jet
- May 2014 CyberBerkut Central Election Commission Fancy Bear
- IRA
- Power pylons to Crimea
- Nov 2015 Pentagon meeting – warning “turn out the lights”
- SANS analysis placed on hold NERC

Moonlight Maze

- Hacking from Russia \neq Hacking for Russia
- Russian general “those intelligence so-and-sos”
- No more Russian general less hacking then better hacking
- Joint Task Force-Computer Network Defense JTF-CND
- If power grid is at risk, everything is at risk

Estonia

- VERY Internet connected
- April 2007
- Statue relocated → Riots President moved
- Domestic network crippled
- Hackers enlist help from any/everyone “here it comes”
- Fight for days Cut off from outside
- Victory Day May 9 00:00
- NATO Article 5
- WEB War I

Georgia

- Aug 2008 Kinetic 25,000 troops 200 planes naval blockade
- Hybrid War I

North Korea

- North Korea develop cyber hackers
- North Korea steals large amounts of funds
- North Korea not part of IMF
- Dec 2014 Sony attacks
- We will respond proportionally, in a place & time we choose
- Nationwide internet outage days later
- Blame of misconfiguration
- North Korea has 1 class C network routed through China

Ukraine again

- Ukraine pension system
- Ukrzaliznytsia railway system holiday travel
- Historians do not need to talk to PLCs
- DHS DOE “road show”
- Taking US down harder Keeping it down easier

CRASHOVERRIDE

The background of the slide features a dark blue sky with a network of black power lines and lattice towers, creating a technical and industrial aesthetic.

**Analysis of the Threat
to Electric Grid Operations**

What about U.S.

- Crashoverride report to congress
- Perfect storm timing
- “we’re fine, go away”
- Protective relays
- Sun City transformer fire
- Protection relays

0-day

- ShadowBrokers summer 2016 NSA Eternalblue
- Vault 7 2017 CIA
- How security suites work
- 0-days hoard or alert?



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Macedonia, Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Ooops, your important files are

you see this text, but don't see the "Wana"
your antivirus removed the decrypt soft
from your computer.

you need your files you have to run the d
we find an application file named "@Wana"
older or restore from the antivirus qua

BOARDWAY

In memory of the nation
In remembrance of His Majesty
King Bhumibol Adulyadej



ก. วิทย
Witthayu Rd

Wannacry

- Island hopping Just takes one
- Any/everywhere
- Uncontrolled NSA-zero-day worm
- Iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea
- North Korea
- Kaspersky Moscow based
- How security suites work
- How virtual machines work

THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Northern District of California under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:

The United States Attorney's Office for the Northern District of California

Federal Bureau of Investigation



For additional information, see <https://www.justice.gov>

Work From Home WFH

- Twitter hack Trump twitter passphrase
- Certificate Authority
- Mimikatz Pass the hash
- Credential stuffing
- Financial legacy theft MFA
- US Cyber command “hunt forward”

Other Russia ??

- France 2015 TV5Monde
- France 2017 20,000 emails Presidential campaign
- Germany 2015-2017 Election interference
- Kyrgyzstan 2009 ISPs offline US air base
- Poland Facebook dis-information campaign
- South Korea Olympic Destroyer 2018 Winter Games
- UK Brexit
- Tokyo Olympics

NotPetya

- Week 1
- WannaCry on steroids Administrator rights & privilege
- No kill switch no decryption keys
- Eternal Blue + Mimikatz
- Escaped from Ukraine
- Ukraine hard hit
- Maersk 1 terminal 3000 trucks per day

Well, patch

- Critical
- Patch Large Infrastructures
- Apps were written decades ago
- Pirated copies - not easily patched
- Perfect storm
- Today Zerologon VPN

- Feb 2018 WH & GCHQ public statement
- Sanctions & indictments
- Indictments require evidence
- Bad Rabbit smokescreen?
- Olympic Destroyer forged metadata
- ISIS
- IRA disabled for 2018 Mid-terms
- Iowa caucus
- Perception attack?

- US not calling out actions so those actions are available to US
- Geneva civilian protections in time of war
civilian attacks in time of peace

Other Actors

- USA
- Syrian Electronic Army
- 5 Eyes
- North Korea
- China
- EVERY ONE

China

- Titan Rain 2003 –
- Sensitive
- Espionage unreported unknown unnerved
- 2011 Google
- 2011 RSA stepping stone F-35 cost overruns
- BYZANTINE HADES Mandiant APT persistent
- Nortel ↓ Huawei ↑
- Greatest transfer of wealth in history
- Government & Industry
- OPM data breach

Power Grid

- USA 3 grids
- Nov. , 2018 DARPA Plumb Island grid

Estonia revisit

- Statue relocated still
- Tactical & strategic defeat for attackers
- Estonian government not coerced
- Economy and reputation improved
- NATO Cooperative Cyber Centre of Excellence Tallinn, Estonia
- Estonia aware of impending attacks NATO and world leaders not
- Estonia control IXP (Internet Exchange Point)
- Georgia not Georgia transferred some sites to US
International consequences?

Buckshot Yankee

- 2008 US Central Command classified network
- Agent.btz
- SIPRNET operational commands
- JWICS highest classification intelligence material
- It just takes 1 USB drive infection?

Hackers are cyber immune systems

- Cuckoo's Egg Morris Worm
- Encryption of military drone
- Hack a F-35 Hack the Pentagon Hack a satellite
- Cyber warfare is **very different**
- As each of us are safer we are ALL safer

Cyber Warfare

- Increased sophistication
- Increased magnitude
- Increased intensity
- Increased volume
- Increased velocity
- One hits 155 countries in ONE DAY It just takes one
- Perfect weapon Perfect storm Pandemic, riots, division, election + cyber
- Dis-informationdemic
- Hacking-as-a-service

China

- OPM 25 Million security clearance files
- F-35
- RSA
- Google
- Anthem
- Huawei
- Covid-19 research
- China government & Industry strongly linked
- Economic inroads

Voter registration

- You can see yours, mine, and others
- Those databases can be purchased
- Those databases have been left with no or little protections in cloud

Voter Lists | 50 State Political Voter Database

Why Voter Lists?

Gravis Marketing believes that **accurate voter lists** are essential to any campaign. As the new currency in politics, voter lists can make or break elections by determining whom your campaign is reaching.

Having access to a detailed voter database is the most effective way to streamline your campaign, sending your message to specific voters from any region, affiliation, or demographic.

Why Our Voter Database?

Gravis Marketing can adapt your voter lists to the changing trends of your voters, helping you with your specific goals in the specific ways you need.

We know that making the most of your budget is a priority. You need something flexible, customizable, and dependable. That's why our comprehensive database includes:

- **Voter files** from all states, kept up-to-date with 24-hour turnaround.
- **Phone numbers**, including updated landlines and cell phones.
- **Email addresses**, trimmed of inactive and unresponsive inboxes.
- **Detailed demographic information**, including age, race, ethnicity, religion, and income.
- **National changes of address**.
- **Party and interest group affiliations**, with voter histories.
- **Social memberships**.

Lessons Learned & Unlearned



QUESTIONS?

