Interesting Times

WHAT IS OLD IS NEW AGAIN

2022.03.24 | MATTIAS ALMEFLO

Mattias Almeflo

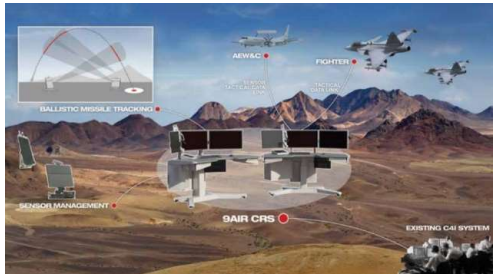
2022	Týr CYBER Defense	• **Principal Security Consultant & CEO**
2018	NIXU cybersecurity.	• **Principal Security Consultant**
2017	COMBITECH	• **Senior Information Security Architect**
2016	SAAB	• **Team Leader | Information Security Architect** • **Systems Integrator | Information Security Architect | Team Leader**
2009	SAAB Defence and Security	• **Thesis Worker | Software Developer**

Mattias Almeflo

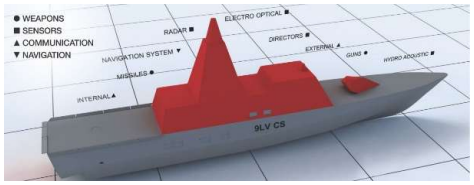
And the domains of conflict

2017 –
Development Environments & Infrastructure

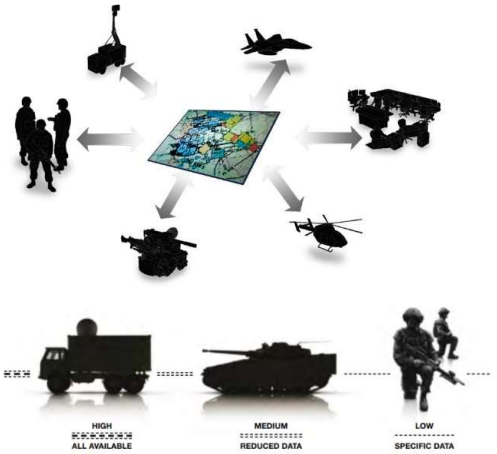
2016 – 2017
R&D Defensive Cyber Warfare



2013 – 2015
Windows Security in Air Control Backbone



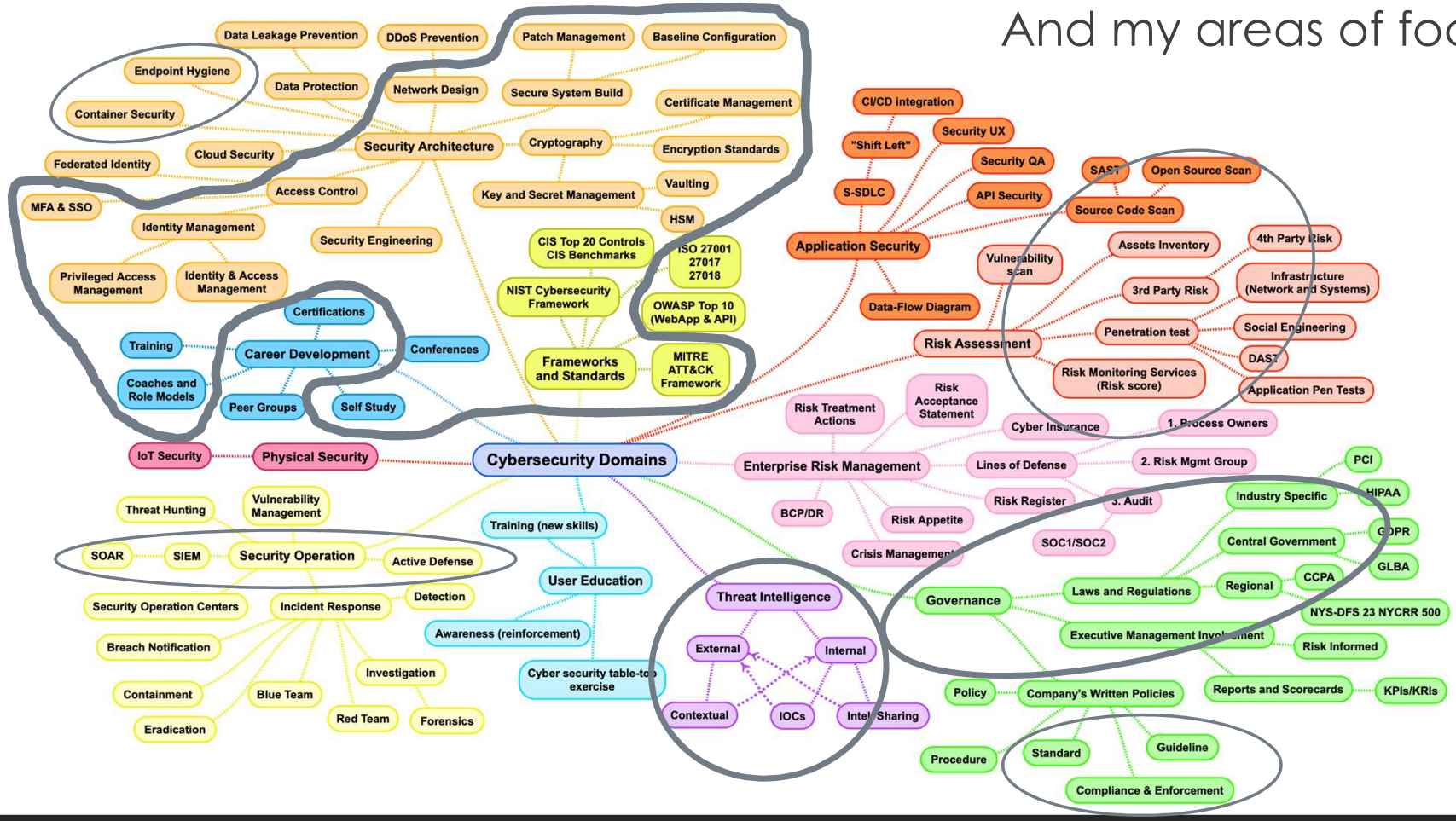
2015 – 2016
Docker Security in Naval Systems



2010 - 2013
Created the Secure Operating Environment (SOE) for the Swedish Armed Forces

The complexity of the domain is staggering

And my areas of focus




Ask Cybergibbons!
@cybergibbons
Follow
"There is no security without a threat model, only paranoia"
I quite like that.
1:23 PM - 24 Jun 2018
57 Retweets 170 Likes
4
57
170
Ask Cybergibbons! @cybergibbons · 24 Jun 2018
From here
What's your threat model? What are you trying to ...
How can I prevent my home security system from ...
What's your threat model? What are you trying to protect against? There is no security without a threat model, only paranoïa.
reddit.com

Three types of attack scenarios

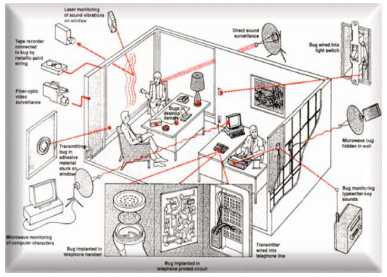
The 3 categories

1. Espionage (corporate / state sponsored)
2. Collateral Damage
3. Organised Crime / Ransomware

Three Types of Security / Attack Vector Scenario

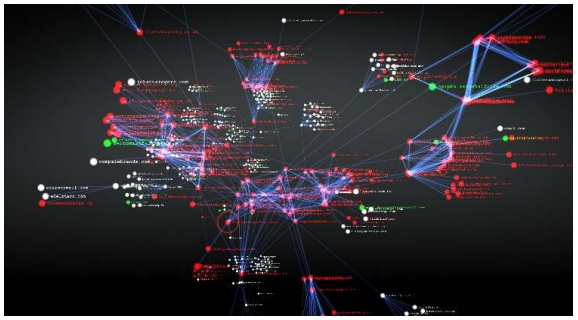
Site Security

Home | Office



Information Security

Home | Office



Travel Security

Home | Office

Two types of threats

Non actor driven (not antagonistic) threat

- Possible, unwanted event with a negative outcome for operations, which isn't caused by a human actors deliberate actions.
- Generally speaking non-antagonistic threats can be divided into three (3) categories:
  - **Natural phenomena** (natural disasters, disease)
    - Site security related threats (Fire, locks, alarms accidents etc)
  - **Errors in technical systems** (bugs, malfunction)
  - **Non-intentional actions by human actors** (accidents, negligence)
    - Loss of device, Incorrect or careless handling of info

Two types of threats

Actor driven (antagonistic) threat

- Threat driven by an actor in the form of an individual, group, network, organisation, state etc.
- Actor driven threats are normally intentional.

A general threat assessment for public sector or private parties, that falls under the Protective Security Act

"Hotbild mot säkerhetskänslig verksamhet, juni 2019"

A public threat report by the Swedish Security Service (SÄPO), 8 pages

- Two nation states: Russia & China
  - Capability: Very High
  - Intent: Very High

- Two non state actors in the category "ideological motivated":
  Islamic fundamentalists & Right wing extremists
  - Capability: Low (event driven)
  - Intent: High

The Threat Landscape

How do you know what you don't know?

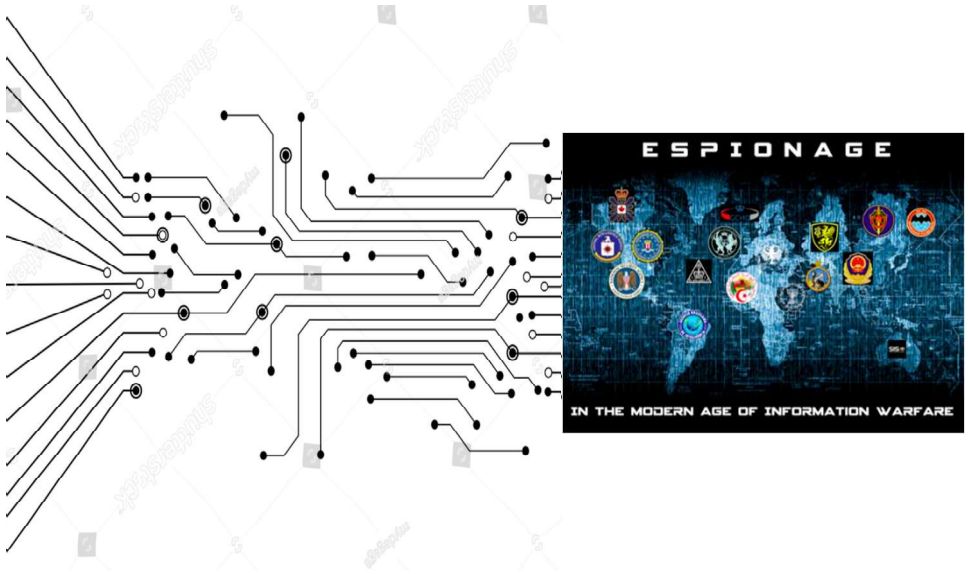
Intelligence

Known Knowns

Known Unknowns

Unknown Knowns

Unknown Unknowns

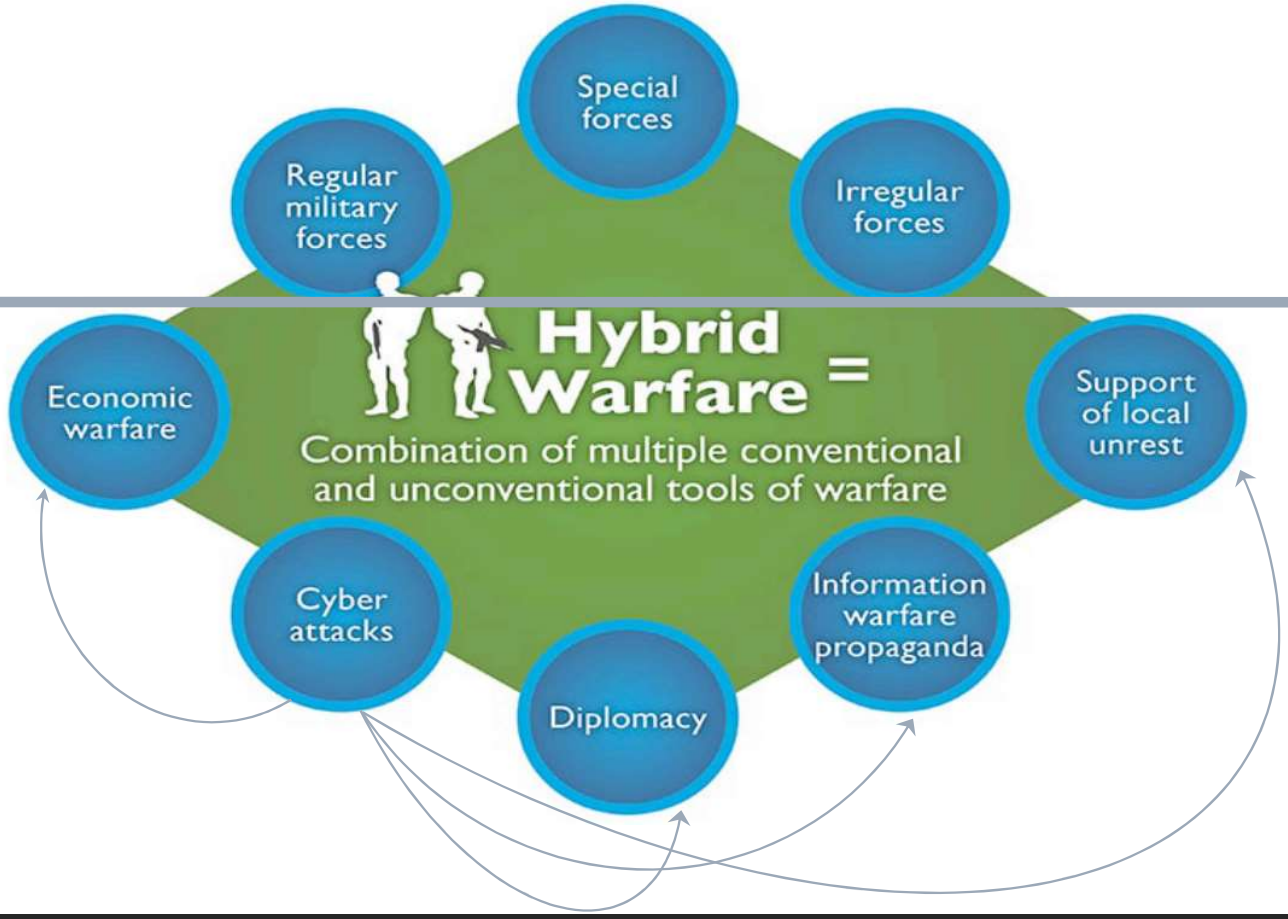


A comic on cyber threats and clearances

The evolution of state sponsored conflict (war)

Asymmetric warfare
"below this line…"

The evolution of state sponsored conflict (war)



Asymmetric warfare
"below this line…"

China – USA: Cold War

The accession of China to the rank of second world power is a fait accompli.

World Power & the Silk Roads project

Starting from nothing, China's international military system is progressing rapidly. Its naval capacity is growing steadily. The establishment of 18 military bases on the international level is planned

China – USA: Cold War

Industrial Espionage

Twenty (20) leading sectors have been declared strategic, starting with artificial intelligence and semiconductors, but also including robotics, advanced materials and pharmaceuticals.

Made in China 2025 has aimed to transform China into a "manufacturing superpower." In particular, the plan highlighted 10 priority sectors, which include **new-generation information technology**; advanced numerical control machine tools and robotics; **aerospace technology**, including aircraft engines and airborne equipment; and biopharmaceuticals and high-performance medical equipment.

Examples of incidents/threats

- Surveillance of employees
- Mapping
- Contacts (Humint)
- Intrusions (hotel rooms, safety deposit, conference rooms)
- Entrapment (Honey Trap)
- Phone tapping
- Technical intrusions
- Transportation accidents
- Incidents related to high risk countries

Category 1 - Cloud Hopper

"thought to be one of the largest ever sustained global cyber espionage campaigns in an operation."

- **The mother of all Upstream Attacks**, 2014-2016
  - The Target breach in 2013 affected 41 million customer payment card accounts along with contact information for more than 60 million Target customers

- 2017, PwC UK states that CH impacted multiple organizations in North America, Europe, South America, and Asia
- It targets Service Providers (cloud infrastrucutre)
  - Managed Service Providers (MSP)
    - United Kingdom (U.K.), United States (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, **Sweden**, South Africa, India, Thailand, South Korea, and Australia
  - Service Providers

Cloud Hopper

- **The targets were not the MSP but their clients**
  - Industries affected include those in engineering, industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies
  - Massive exfiltration of data
- over 70 variants of backdoor families and Trojans were involved in the cloud hopper campaign.
  - Spearfishing…
- Anti-virus is not enough and network detection lacking
  - Out of 300 defined IOCs there where still 69 that no single anti-virus software detected after a year post-breach
  - Data was moved upstream with valid (stolen) credentials

Lessons Cloud Hopper

- **Attacked ”everyone” not just Defence Contractors…**
  - Used for further infiltration
- Outsourcing is very risky
- Effeciency is NOT balanced with security when facing nation state actors

- The lessons are ongoing but if you are swedish a good start is to read the unprecedented FRA report: ”Åtgärdsförslag - Angrepp via tjänsteleverantörer”

Zero Day exploits (Technical Intrusions)

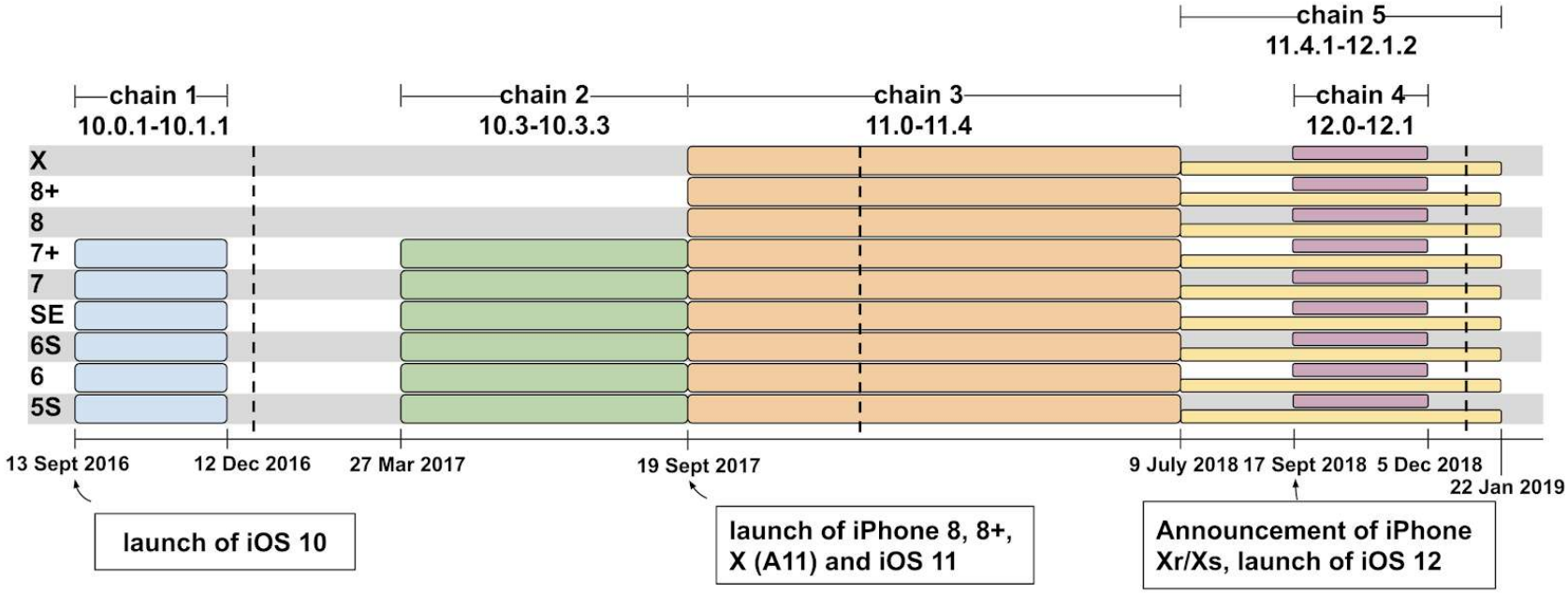
A booming multi-million dollar international business

- Stuxnet (2010) used 4 zero days and from there on the zero day market exploded (pun intended)
- Trident (2016) used 3 zero days to spy on a human rights defender, based in the United Arab Emirates
- 30% of malware attacks utilises (1) zero day BUT almost 93% of malware gets in through email…

iOS Exploit chains found in the wild

"monitor the private activities of entire populations in real time"

5 separate, complete and unique iPhone exploit chains, covering almost every version from iOS 10 through to the latest version of iOS 12.



Zero Day exploits

Apple no longer top dog in mobile security

Zerodium
@Zerodium

We will NOT be acquiring any new Apple iOS LPE, Safari RCE, or sandbox escapes for the next 2 to 3 months due to a high number of submissions related to these vectors.
Prices for iOS one-click chains (e.g. via Safari) without persistence will likely drop in the near future.

2:05 PM · May 13, 2020 · Twitter Web App

622 Retweets **392** Quote Tweets **1.1K** Likes

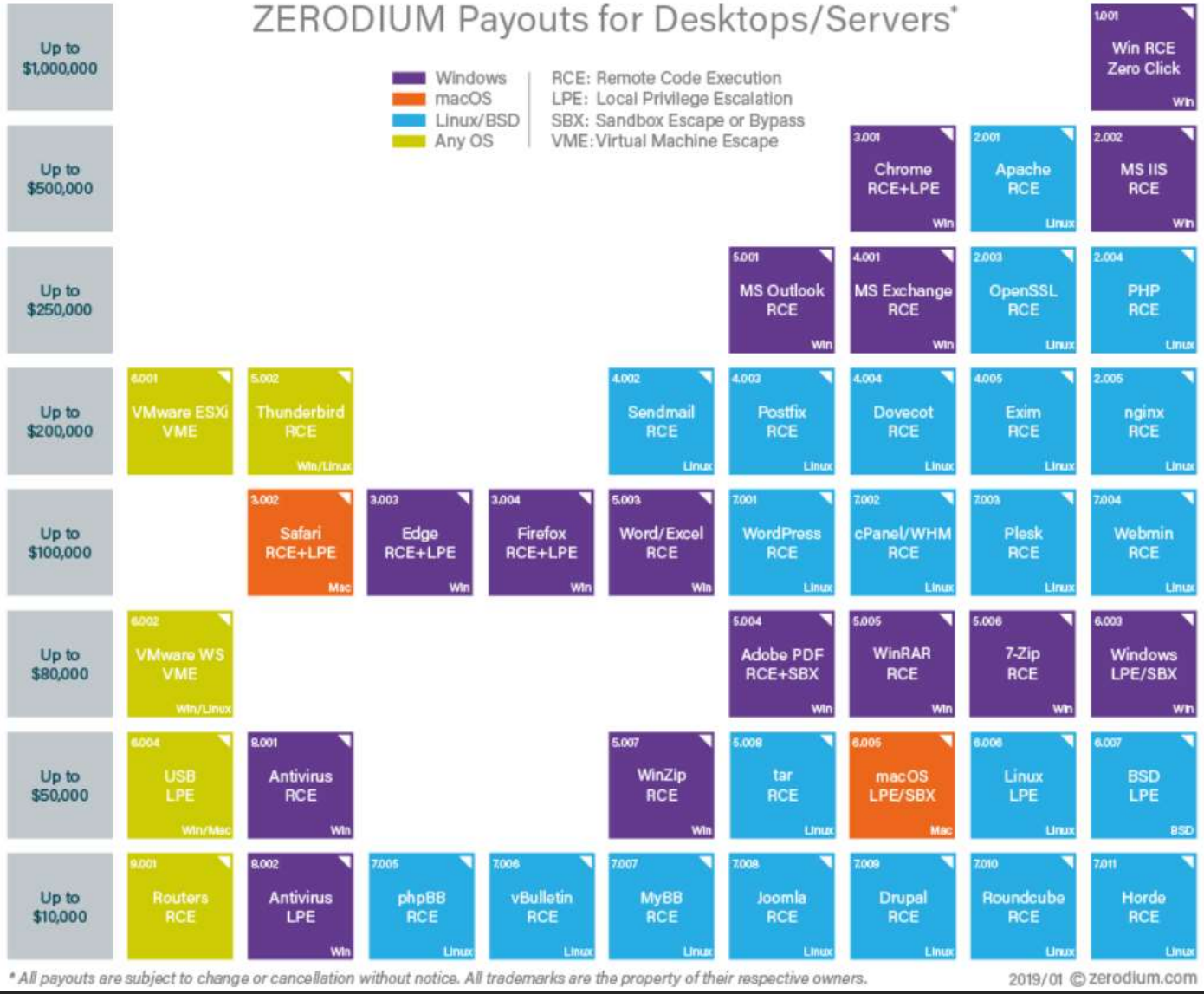
Zerodium Retweeted

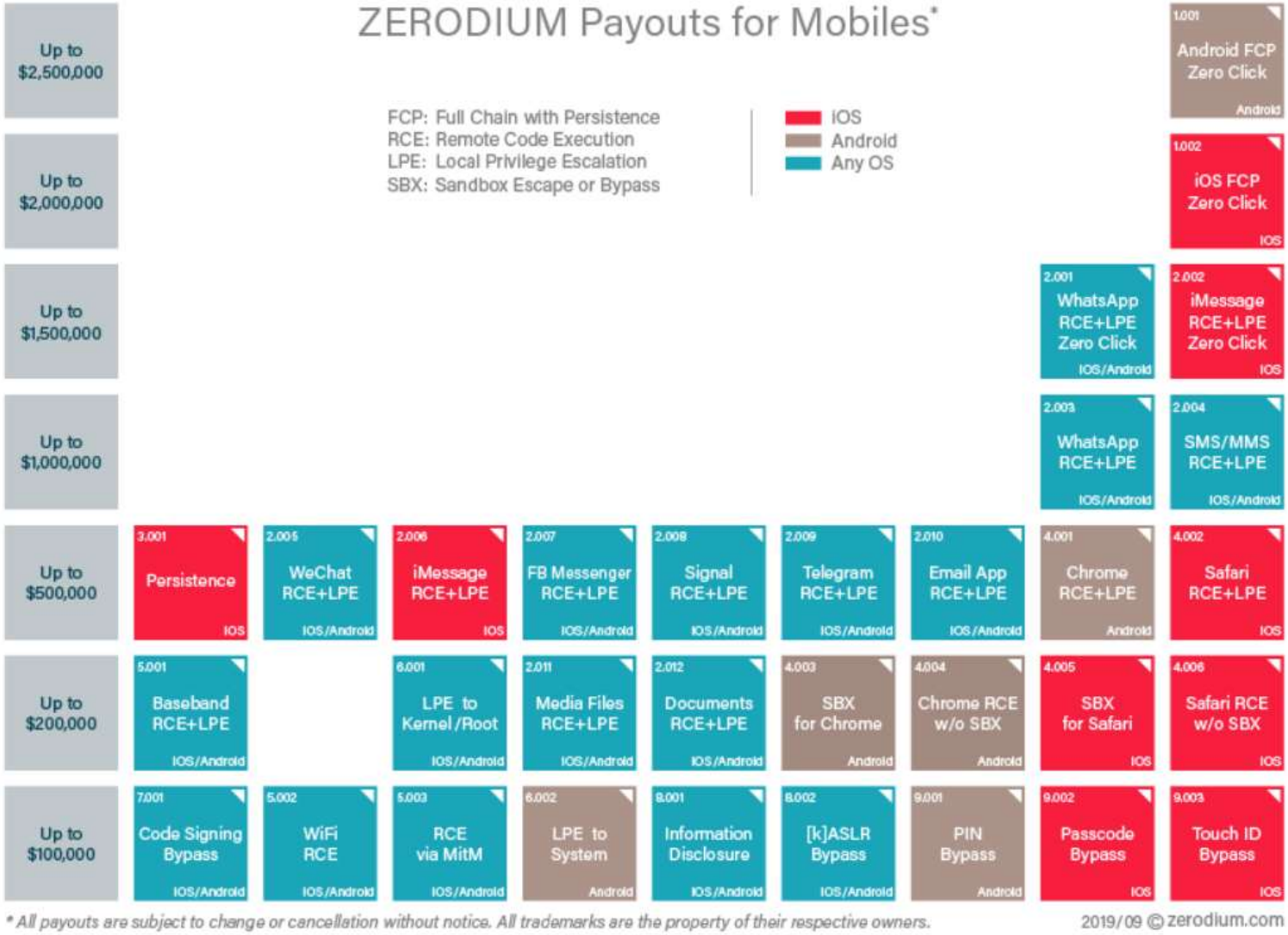
Chaouki Bekrar @cBekrar · Sep 22

Fun fact: Apple iOS 14.x has more persistence 0days than iOS 12.x. As always: more features, more zero-days, more tears.

Apple should just buy @Zerodium and finally make iOS as secure as it should be. Our current valuation is 1 billion dollars. PS: I accept cash or Apple shares.

9 101 348


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com


ZERODIUM Payouts for Mobiles*
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $2,500,000
Up to $2,000,000
Up to $1,500,000
Up to $1,000,000
Up to $500,000
Up to $200,000
Up to $100,000
1.001 Android FCP Zero Click Android
1.002 iOS FCP Zero Click iOS
2.001 WhatsApp RCE+LPE Zero Click iOS/Android
2.002 iMessage RCE+LPE Zero Click iOS
2.003 WhatsApp RCE+LPE iOS/Android
2.004 SMS/MMS RCE+LPE iOS/Android
3.001 Persistence iOS
2.005 WeChat RCE+LPE iOS/Android
2.006 iMessage RCE+LPE iOS
2.007 FB Messenger RCE+LPE iOS/Android
2.008 Signal RCE+LPE iOS/Android
2.009 Telegram RCE+LPE iOS/Android
2.010 Email App RCE+LPE iOS/Android
4.001 Chrome RCE+LPE Android
4.002 Safari RCE+LPE iOS
5.001 Baseband RCE+LPE iOS/Android
6.001 LPE to Kernel/Root iOS/Android
2.011 Media Files RCE+LPE iOS/Android
2.012 Documents RCE+LPE iOS/Android
4.003 SBX for Chrome Android
4.004 Chrome RCE w/o SBX Android
4.005 SBX for Safari iOS
4.006 Safari RCE w/o SBX iOS
7.001 Code Signing Bypass iOS/Android
5.002 WiFi RCE iOS/Android
5.003 RCE via MitM iOS/Android
6.002 LPE to System Android
8.001 Information Disclosure iOS/Android
8.002 [k]ASLR Bypass iOS/Android
9.001 PIN Bypass Android
9.002 Passcode Bypass iOS
9.003 Touch ID Bypass iOS
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/09 © zerodium.com

APT groups aka advanced threat actors

Advanced Persistent Threat groups came to light in 2013

The ATT&CK framework has +120 different threat groups in its catalogue. Some belong to the same Threat Actor

Roughly 60% of the threat actors are attributed to countries:

- +35 are presumed to be Chinese-based
- +10 are presumed to be Iranian-based
- +10 are presumed to be Russia-based
- 5 are presumed to be North Korea-based
- 2 are presumed to be South Korea-based
- +50 are presumed to be unknown

Hacking as Service

Israel's NSO Group – Pegasus Spyware, 2016-2021

Pegasus by the numbers

- 36 likely operators
- 45 Countries with likely infections
- 10 Operators with infections in another country
- 6 Operators linked to countries with a history of abusing spyware to target civil society

"Zero click remote code execution, full chain persistence"

Hacking as Service

Israel's NSO Group – Pegasus Spyware, 2016-2021

Pegaus infected Khashoggis friend Abdulaziz's phone.

It gave hackers access to virtually his entire phone, including his daily conversations with Khashoggi.


CNN World

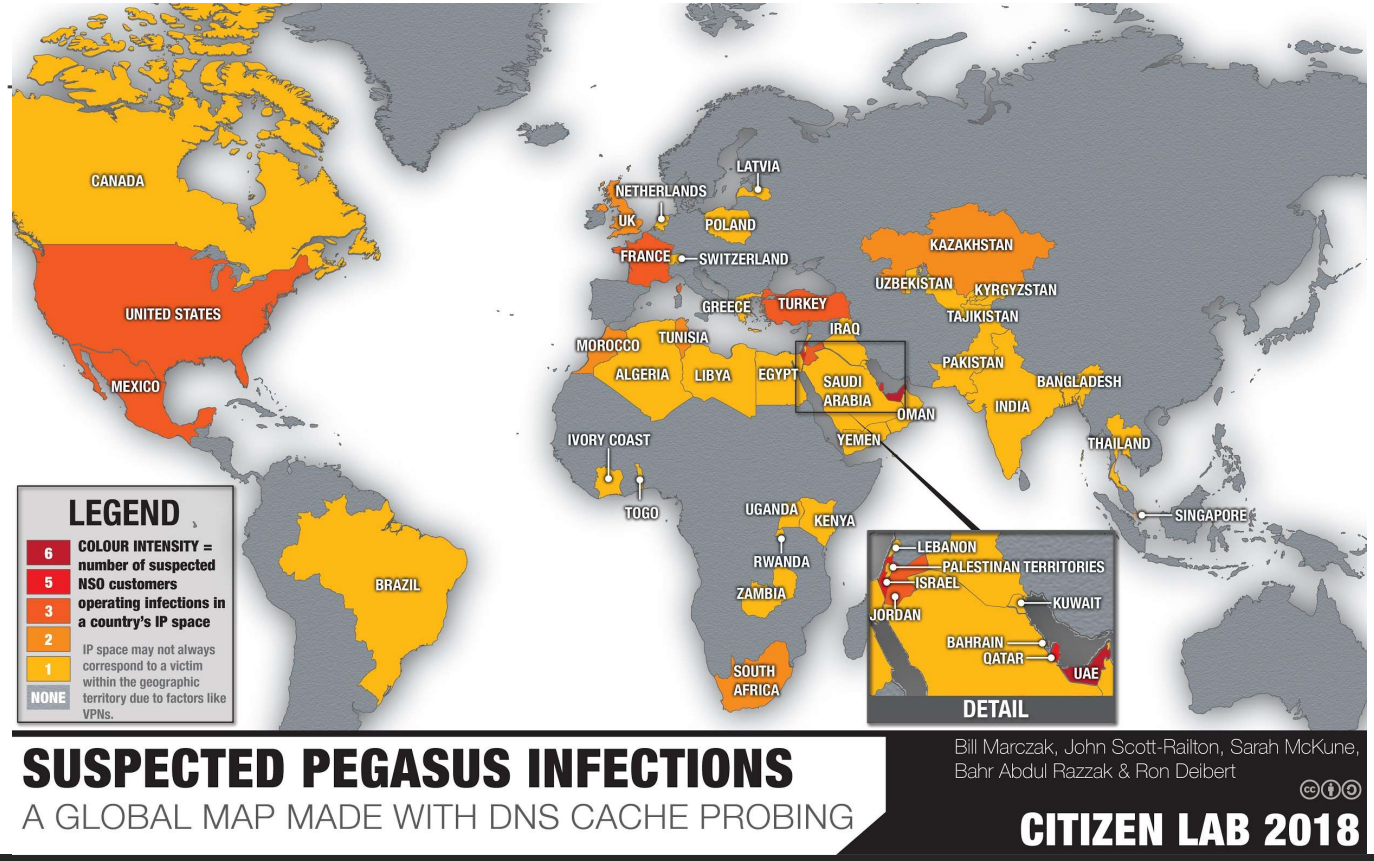
How a hacked phone may have led killers to Khashoggi

By Oren Liebermann, CNN

Updated 1415 GMT (2215 HKT) January 20, 2019

Hacking as Service

Israel's NSO Group – Pegasus Spyware, 2016-2021

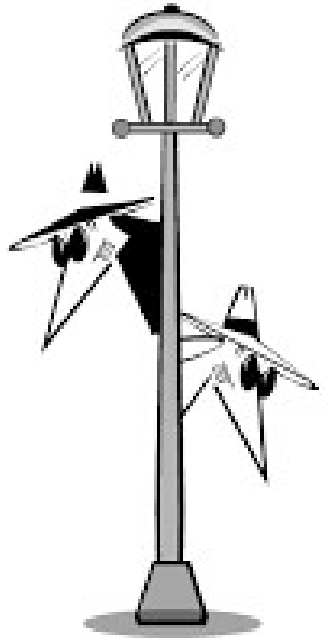


France vs Germany

France leads over China and Russia in regards to industrial spying

"French IPR (intellectual property rights) espionage is so widespread that the damages (it causes) the German economy is greater than that inflicted by China or Russia,"

- U.S. embassy cable, dated November 20, 2009,
  quoting Berry Smutny, the head of German satellite company OHB Technology



U.S. National Intelligence Estimate 2013

France, Russia, Israel vs China vs USA

Most aggressive intelligence service against the U.S

1. **China**
2. Russia
3. Israel

Using cyberespionage against the U.S for economic gain

1. **China**
2. France

Human Intelligence (HUMINT)

Changing but still extremely relevant in todays complex reality

Requires boots on the ground. All countries that are strong in traditional espionage have very high capability in regards to HUMINT operations.

In the cyber arena Social Engineering is the synonym for HUMINT and can be contracted as any other cyber security service.

“I see all these CIO that spend all this money on firewalls and stuff, and they spend zero dollars on awareness.”

- Shane MacDougall (2x winner of the Defcon SE competition)

Bulk telecom intercepts

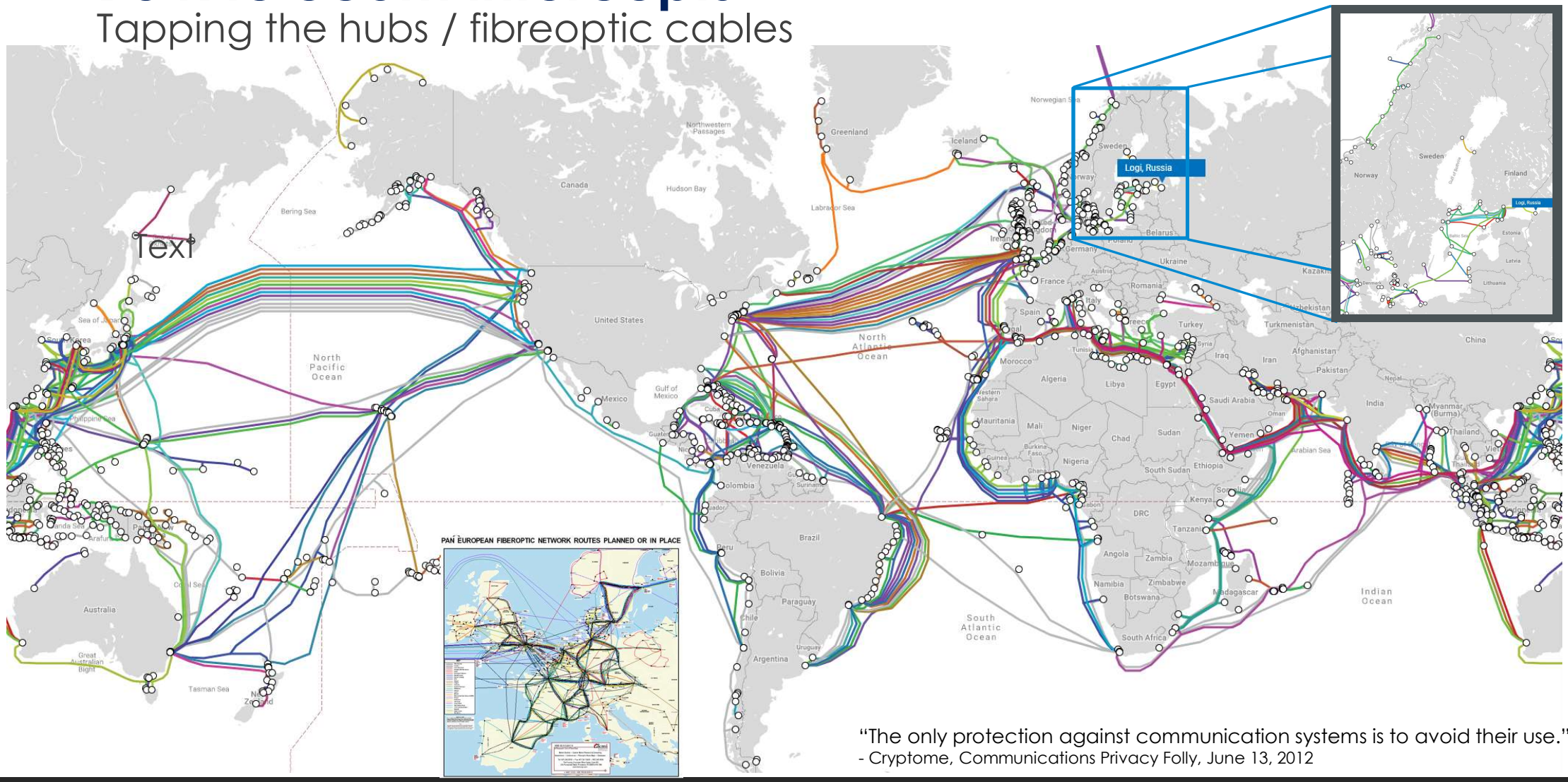
Lawful interception: Passive and active systems for the interception of traditional telephony services as well as the more sophisticated internet applications

All countries have interception capabilities, within their borders.

Countries with highly developed signal intelligence have very high capability for bulk communication interception and analytics.

Bulk telecom intercepts

Tapping the hubs / fibreoptic cables



"The only protection against communication systems is to avoid their use."
- Cryptome, Communications Privacy Folly, June 13, 2012

Category 3 - Ransomware is modern organised crime

- They organize themselves and commit crimes online very differently from your local offline gang.
- Launched from anywhere in the world, so it's very difficult to prosecute these criminals.
- Several parties coordinate across borders, which makes legal matters even more complicated.

Interpol:

Holding the world to ransom: The top 5 most dangerous criminal organizations online right now

BY ROBERTO MUSOTTO, BRIANNA O'SHEA, PAUL HASKELL-DOWLAND | JUL 07, 2021

- **DarkSide** (Russia)
  - Colonial Pipeline
  - Ransomware as a service
- **Revil** (Russia)
  - Kaseya (COOP)
  - JBS (meat industry)
  - Quanta Computer (Apple)
- **Clop** (Russia)
  - Double extortion
- **Syrian Electronic Army** (Syria)
  - Crime/terror group
  - Fake news wiping billions in stock market
- **FIN7** (Russia)
  - The "super villain" of ransomware

FINCEN Report

The US Department of the Treasury's Financial Crimes Enforcement Network

- Total value was $590 million
  - January 1 - June 30, there were 635 ransomware-related SARs filed by financial institutions, including 458 transactions
- Monthly payment amounts ranging from $3,095 to $43.06 million.
  - The top 10 ransomware variants identified during the review period were responsible for $217.56 million in suspicious activity

Ransomware Variant	Start/End Date	Accept XMR (Y/N)	Accept BTC (Y/N)	Sent BTC (USD)				
				Exchange	DNM	Mixer	Other [46]	Total
Variant 1	April 2019 - July 2021	Y	Y	~$6.3 million	~$826,000	~$6.5 million	~$32.3 million	~$46 million
Variant 2	December 2019 - present	N	Y	~$66.1 million	~$7.3 million	~$4 million	~$161 million	~$238.5 million
Variant 3	August 2020 - May 2021	Y	Y	~$14.3 million	~$609,000	~$6.5 million	~$76.8 million	~$98.2 million
Variant 4	June 2020 - June 2021	N	Y	~$4.9 million	~$660,000	~$1.6 million	~$6.3 million	~$13.5 million
Variant 5	September 2019 - present	N	Y	~$1.7 billion	~$241.6 million	~$9.7 million	~$1.7 billion	$3.6 billion
Variant 6	July 2018 - present	N	Y	~$604.4 million	~$622,700	~$2.2 million	~$184.5 million	~$791.7 million
Variant 7	October 2019 - present	N	Y	~$3 million	~$3,600	~$2.3 million	~$3.5 million	~$8.8 million
Variant 8	December 2019 - present	N	Y	~$240 million	~$740,000	~$1 million	~$64.3 million	~$305.8 million
Variant 9	November 2019 - present	N	Y	~$519,000	~$79,000	~$9,900	~$6.9 million	~$7.5 million
Variant 10	September 2019 - present	N	Y	~$8.4 million	~$76,300	~$1.3 million	~$11 million	~$20.7 million
Total				**~$2.6 billion**	**~$252.5 million**	**~$35.2 million**	**~$2.3 billion**	**~$5.2 billion**

2021 State of Ransomware Survey & Report

Preventing and Mitigating the Skyrocketing Costs and Impacts of Ransomware Attacks

- 72% have seen cybersecurity budgets increase due to ransomware threats
- 93% are allocating special budget to fight ransomware threats
- 50% said they experienced loss of revenue and reputational damage from an attack
- 42% indicated they had lost customers as a result of an attack

Budget “$3,095 to $43.06 million per month”

Bugging physical locations

Five categories of "Bugs": Acoustic, Ultrasonic, RF, Optical, and Hybrid

Russia bugged the Swedish embassy in Moscow for 14 years (1972- 1986), without discovery.

"Installationerna av avlyssningsutrustning var mycket skickligt utförda och innebar bl.a. att ledningar hade "frästs" in i armeringsjärn inne i prefabricerade byggelement.

Installationerna kunde inte upptäckas med den teknik som fram till slutet 1980-talet stod till buds för att söka efter avlyssningsutrustning."

Bugging physical locations

All the usual nation state suspects have very high capability

2017, Since it's construction in **2012** the African Union's building in Brussels have sent all it's data to China every night.

2010, NSA bugged offices and spied on EU internal computer networks in Washington and at the United Nations, according to documents stolen by Snowden.

Bugging physical locations

All the usual nation state suspects have very high capability

2003, Brussels, EU building, bugging devices on the phonelines were discovered in the rooms of the delegations of Britain, France, Germany, Spain, Italy and Austria.

- the devices were likely installed during the construction of the building in **1995**.
- Unclear which state actor is responsible (U.S. is a prime suspect according to Der Spiegel, based on documents stolen by Snowden).

Information Operations (IO)

Russia is top dog, China and USA close behind

> *Information can disorganise governance, delude adversaries and reduce an opponent's will to resist.*

"What stands clear today is that information technology has reached critical mass.

Information systems are so vital to the military and civilian society that they can be the main targets in war, and they can also serve as the main means for conducting offensive operations. In effect, **Information Warfare is really the dark side of the Information Age**."

Information Operations (IO)

Or how to win a political election through the abuse of social media

2015-2018, Facebook–Cambridge Analytica data scandal

- Harvested data on 87 million Facebook profiles
  - Aided Ted Cruz and Donald Trumps political campaigns
  - targeted users, friends and lookalikes directly with digital ads

Information Operations (IO)

Or how to win a political election through the abuse of social media

"The parallels between the US and the Philippines are striking."

"Once Duterte won, that machinery of opinion formation went from a campaign strategy to a state-sponsored one."

- 2015-2019, Philippines, Duterte administration IO
  - Duterte utterly dominated Facebook during the country's presidential election
  - Fake news to fuel and support "the drug war"
  - Facebook has been used as a key amplifier of pro-administration narratives and sentiment.
  - Duterte has repeatedly called local news outlets "fake news."
- 2013, Facebook launched "Free Facebook" (Free internet)
  - 97% of Filipinos use Facebook and spend most time online, on social media worldwide

Category 2 - ~~WannaCry, Petya~~, NotPetya

"To date, it was simply the fastest-propagating piece of malware we've ever seen"

- A month after the debute of WannaCry, NotPetya hit the world
  - using the same EternalBlue weakness (+ Mimikatz) to spread within corporate networks, but without being able to jump from one network to another.
  - NotPetya was seeded to victims through a hacked version of a major accounting program widely used in Ukraine.

Notpetya - Wiperware

"In June 2017, the Russian military launched the most destructive and costly cyberattack in history"

- **More than $10 billion in total damages**

- **Notable examples:**
- **Maersk (shipping industry)**
  - Every 15 minutes a Maersk ship docks somewhere in the world
  - 250-300 million USD in losses
  - 10 days blitz: 4000 servers, 45000 PCs & 2500 apps all rebuilt
    - 20% drop in productivity
    - 2 months 24/7 to rebuild Maersk's software setup

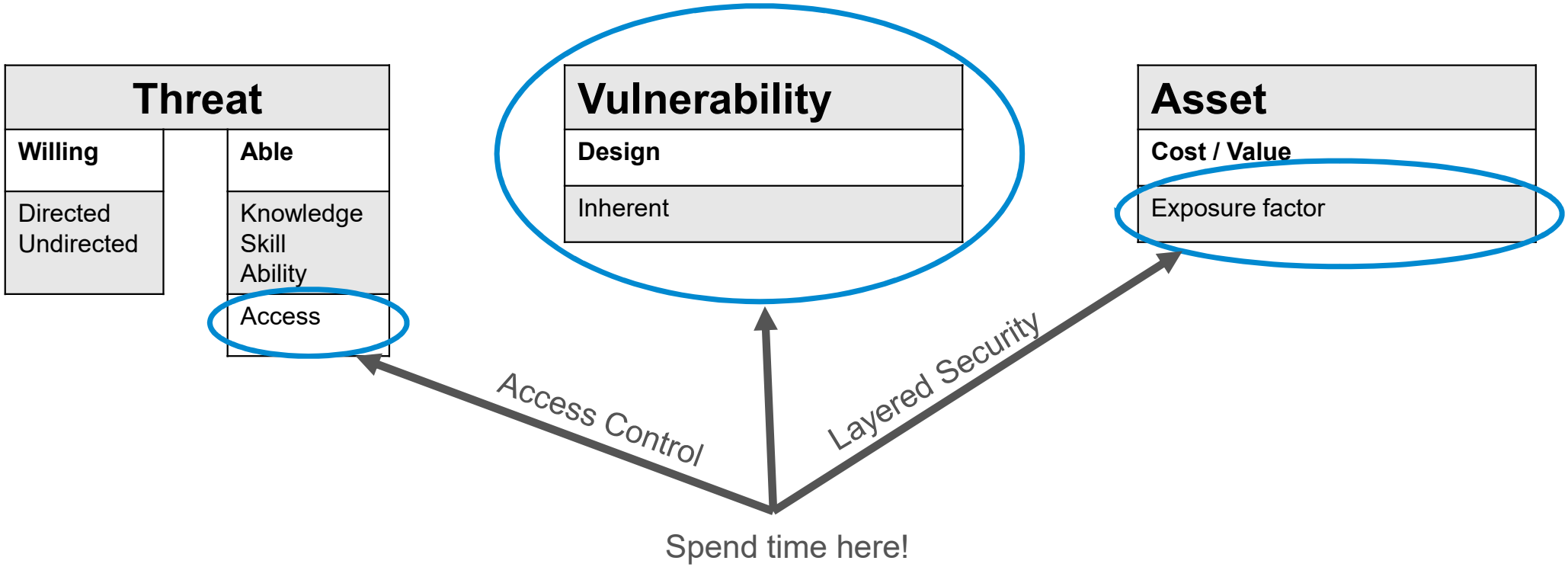
- **Merck (pharmaceutical company)**
  - 870 million USD in losses
  - Staff not allowed to work

- **FedEX/TNT Express (postal/shipping industry)**
  - 400 million USD in losses

Lessons NotPetya

- Be wary of doing business in war zones, even if they're not "hot"
  - Do you know where all parts of your network is geographically located?
- Patch your systems
- Use 2FA (at least for critical systems)
- Separate email from critical systems
- network segmentation is a good thing
- Have manual routines that work
- Offline, Off-site backup is a good thing

Focus Areas


Threat
Willing
Able
Directed
Undirected
Knowledge
Skill
Ability
Access
Vulnerability
Design
Inherent
Asset
Cost / Value
Exposure factor
Access Control
Layered Security
Spend time here!

A Security Design Principle

A declarative **statement**
made with the intention of
guiding security design decisions
in order to meet the security goals of a system

Security Design principles

There are many sets of security design principles

They share a lot of similarities between them at a fundamental level

To tackle todays reality I recommend to start with these
ten (10) security design principles

10 security design principles

For defensible architectures

1. Assign the **least privilege** possible
2. Separate **responsibilities**
3. **Trust cautiously**
4. **Simplest** solution possible
5. **Audit** sensitive events
6. **Fail securely** & use **secure defaults**
7. **Never** rely upon **obscurity**
8. Implement **defence in depth**
9. **Never invent security** technology
10. Find the **weakest link**

10 security design principles

For defensible architectures

# 01	LEAST PRIVILEGE
Why?	Broad privileges allow malicious or accidental access to protected resources
Principle	Limit privileges to the minimum for the context
Tradeoff	Less convenient, less effecient, more complexity
Example	- Run server processes as their own users with exactly the set of privileges they require - No root or super-admin access, ever

10 security design principles

For defensible architectures

# 02	SEPARATE RESPONSIBILITIES AND SYSTEM FUNCTIONS
Why?	Achieve control and accountability, limit the impact of successful attacks, make attacks less attractive
Principle	Separate and compartmentalised responsibilities, privilegies and admin/user systems
Tradeoff	Development and testing costs, operational complexity, troubleshooting more difficult
Example	- System admin are separate from security log admin - admin interfaces are not allowed to run in the same domain as user interfaces

10 security design principles

For defensible architectures

# 03	TRUST CAUTIOUSLY
Why?	Many security problems caused by inserting malicious inntermediaries in communication paths
Principle	Assume unknown entities are untrusted, have a clear process to establish trust, validate who is connecting
Tradeoff	Operational complexity (particularly failure recovery), reliability, some developement overhead. Not a trivial problem…
Example	- Two-way-authentication (client – server) - Two-factor authentication for user auth - Only use trusted PKI that you control - Never share underlying HW for VMs in different sec. domains

10 security design principles

For defensible architectures

”The price of reliability is the pursuit of the utmost simplicity”

– C.A.R. Hoare

# 04	SIMPLEST SOLUTION POSSIBLE
Why?	Security requires understanding of the design – complex design is rarely understood – simplicity allows analysis.
Principle	Actively design for simplicity – avoid complex failure modes, implicit behaviour, unnecesary features…
Tradeoff	Hard decisions on features and sophistication. Needs serious design effort to be simple.
Example	- Fixed configuration (defined configuration as in CIS Benchmarks) - Hardening (minimize attack surface) in terms of no unused services

10 security design principles

For defensible architectures

# 05	AUDIT & ANALYZE SENSITIVE EVENTS
Why?	Provide record of activity, deter wrong doing, provide a log to reconstruct the past, provide a monitoring point
Principle	Record all security significant events in a tamper-resistant store
Tradeoff	Performance, operational complexity, development cost
Example	- Record all unsuccessful login attempts, IPS/IDS events of relevance - Use a data-diod in order to safe guard the security logs

10 security design principles

For defensible architectures

# 06	FAIL SECURELY & USE SECURE DEFAULTS
Why?	Default passwords, ports & rules are ”open doors” Failure and restart states often default to ”insecure”
Principle	Force changes to security sensitive parameters Think through failures – must be secure but recoverable
Tradeoff	Convenience
Example	- On failure don’t disable or reset security controls - Don’t allow default accounts with default passwords

10 security design principles

For defensible architectures

# 07	NEVER RELY ON OBSCURITY
Why?	Hiding things is difficult – someone is going to find them, accidental if not on purpose
Principle	Assume attacker with perfect knowledge, this forces secure system design
Tradeoff	Designing a truly secure system takes time and effort
Example	- Use reputable crypto - Assume that an attacker will be able to guess password encodings, port knocking etc

10 security design principles

For defensible architectures

# 08	DEFENCE IN DEPTH
Why?	System do get attacked, breaches do happen, mistakes are made – need to minimise the impact
Principle	Don't rely on a single point of security, secure every level, vary mechanisms, stop failures at one level propagating
Tradeoff	Redundancy of policy, complex permissioning and troubleshooting, can make recovery harder
Example	- Access control in UI, services, database, OS - Multiple layers of authentication (HW, SW, Users)

10 security design principles

For defensible architectures

# 09	NEVER INVENT SECURITY TECHNOLOGY
Why?	Security technology is difficult to create – specialist job, avoiding vulnerabilities is dificult
Principle	Don't create your own security technology Always use a proven component
Tradeoff	Time to assess security technology, effort to learning it, complexity
Example	- Don't invent your own SSO mechanism, secret storage or crypto libraries. Use industry standards!

10 security design principles

For defensible architectures

# 10	SECURE THE WEAKEST LINK
Why?	”Paper Wall” problem – common when focus is on technologies not threats
Principle	Find the weakest link in the security chain and strengthen it – repeat! (Threat modelling)
Tradeoff	Significant effort required, often reveals problems at the least convenient moment
Example	- Data privacy threat met with encrypted communication but with unencrypted database storage and backups

The Force Multipliers

or "how to fight the war"

Technical Controls

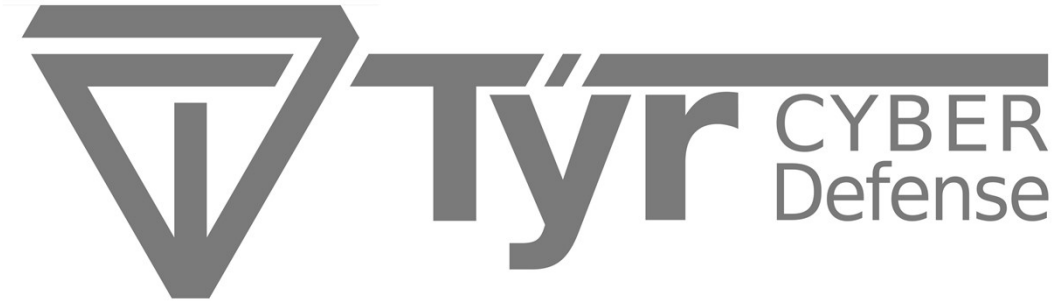
- Strong authentication (Multifactor: smart cards, yubikey, sms etc)
- Separation (physical and logical)
- Security logging
- White listening
- SANS Critical Security Controls / CIS 20
- Regular backups
- Timely Patching

Engineering

- Know your network
  - Documentation vs Implementation
- Threat modeling
  - Crown Jewels
- Think in graphs
  - Not everything is equal

People

- Relationships matter



Mattias Almeflo

Principal Security Consultant & CEO

mattias.almeflo@tyrgroup.se

https://twitter.com/tyrgroup

https://www.linkedin.com/company/tyrgroup/about/

https://tyrgroup.se

Credits and prior art

"discovering truth by building on previous discoveries“

Me, Myself & I
S02-04: Saab, the corporation video (6 min) - https://www.youtube.com/watch?v=2KsdPHsgR9Q
S02-04: The domains of war - https://saab.com/land/, https://saab.com/air/, https://saab.com/naval/, https://en.wikipedia.org/wiki/Cyberwarfare
S02-04: LinkedIn Cyber Security Domain Map - https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/

Initial Quotes
S05: Cybergibbons on threat models - https://twitter.com/cybergibbons/status/1010981698593591296

Three types of security
S07: Picture Site Security: https://reolink.com/how-to-secure-single-family-home-construction-sites/
S07: Picture Site Security: https://krypt3ia.files.wordpress.com/2018/06/espionge-in-the-modern-age-of-information-warfare.pdf
S07: Picture Information Security: http://www.opengraphiti.com/gallery/cryptolocker-bfs4.png
S07: Picture Travel Security: https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban

Two types of threat
Actor driven vs non-actor driven threat
S08-09: H SÄK Grunder, 2013 - https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/h-sak-grunder.pdf
S08-09: IT-Säkerhetsarkitektur, 2015 - https://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/vagledning-it-sakerhetsarkitektur-final.pdf
S08-09: Picture: https://krypt3ia.files.wordpress.com/2018/06/espionge-in-the-modern-age-of-information-warfare.pdf

Credits and prior art

"discovering truth by building on previous discoveries“

SÄPO Hotbild mot säkerhetskänslig verksamhet, juni 2019
S10: https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64a/1560776860929/Hotbild-mot-sakerhetskanslig-verksamhet-juni-2019.pdf
S10: Kompletteringar till den nya säkerhetsskyddslagen, Sammanfattning på svenska och engelska
https://www.regeringen.se/48d97d/contentassets/b1524299913334d788c59a12d8d10d0f3/sammanfattning-pa-svenska-och-engelska-av-sou-2018-82.pdf

The Threat Landscape
S11: There are known knowns: https://en.wikipedia.org/wiki/There_are_known_knowns
S11: Picture inspiration: https://www.eccouncil.org/programs/certified-threat-intelligence-analyst-ctia/
S11: Picture: https://krypt3ia.wordpress.com/2018/06/02/espionage-in-the-age-of-modern-information-warfare/
S11: Security Intelligence: Introduction (pt 2): https://digital-forensics.sans.org/blog/2009/07/23/security-intelligence-introduction-pt-2/

A comic on cyber threats and clearances
S12: Littke Bobby on Cyber threats - http://www.littlebobbycomic.com/projects/week-229/

The evolution of state sponsored conflict (war)
S13-14: Picture: https://krypt3ia.files.wordpress.com/2018/06/espionge-in-the-modern-age-of-information-warfare.pdf

China – USA: The New Cold War
S15-16: Made in China 2025, Explained: https://thediplomat.com/2019/02/made-in-china-2025-explained/
S15-16: Chinese geopolitics: continuities, inflections, uncertainties: http://www.cadtm.org/Chinese-geopolitics-continuities-inflections-uncertainties
S15-16: When the China dream and the European dream collide: https://warontherocks.com/2019/01/when-the-china-dream-and-the-european-dream-collide/
S15-16: FBI, Made in Beijing: The Plan for Global Market Domination: https://youtu.be/GdapE82GceA

Examples of incidents/threats
S17: Picture, Anna Chapman (Russian spy, caught in USA):
https://www.dailymail.co.uk/news/article-3652547/Glamorous-Russian-spy-launches-fierce-attack-England-supporters-country-s-hooligans-head-home-Euro-2016.html
S17: Picture, Surveillance Hotel Lobby: https://www.euroweeklynews.com/2017/10/29/man-arrested-for-breaking-into-fifty-spanish-hotel-rooms-in-brit-holiday-hotspots/
S17: Social media icons made by Freepik from https://www.flaticon.com/
S17: Picture, Tracking individuals in crowd: https://promarket.org/road-to-digital-serfdom-surveillance-capitalism-visible-hand/
S17: Picture, Guy with camera in car: https://www.eldoradoinsurance.com/private-investigator-industry-news/mobile-surveillance-dangers-pitfalls-liabilities/

Credits and prior art

"discovering truth by building on previous discoveries“

Cloud hopper
S18-20: Operation Cloud Hopper: https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html/
S18-20: The Weakest Link: https://newsfromthelab.files.wordpress.com/2017/04/the-weakest-link-f-secure-state-of-cyber-security-2017.pdf
S18-20: FRA:s åtgärdsförslag med anledning av angrepp mot tjänsteleverantörer: http://www.fra.se/snabblankar/nyheterochpress/nyhetsarkiv/nyheter/frasatgardsforslagmedanledningavangreppmottjansteleverantorer.411.html
S18-20: https://kryptera.se/sa-identifierars-cloud-hopper-apt10/
S18-20: APT10 - Operation Cloud Hopper: https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html
S18-20: Global targeting of enterprises via managed service providers: https://www.ncsc.gov.uk/information/global-targeting-enterprises-managed-service-providers

Zero Day Exploits
S21-25: A very deep dive into iOS Exploit chains found in the wild: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
S21-25: Inside Endgame: A Second Act For The Blackwater Of Hacking: https://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/
S21-25: L3 Technologies acquires two hacking companies: https://www.cyberscoop.com/l3-acquires-azimuth-and-linchpin/
S21-25: Startup Offers $3 Million to Anyone Who Can Hack the iPhone: https://www.vice.com/en_us/article/pax987/crowdfense-offers-3-million-for-iphone-android-hacks
S21-25: Cellebrite Battlefield Recovery/SSE: https://theintercept.com/surveillance-catalogue/cellbrite/
S21-25: US State Police Have Spent Millions on Israeli Phone Cracking Tech: https://www.vice.com/en_us/article/aekqkj/us-state-police-have-spent-millions-on-israeli-phone-cracking-tech-cellebrite
S21-25: Zerodium Raises Zero-Day Payout Ceiling to $2M: https://threatpost.com/zerodium-raises-zero-day-payout-ceiling-to-2m/140624/
S21-25: Stuxnet: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf
S21-25: Trident: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
S21-25: Zerodium Payout program: https://zerodium.com/program.html
S21-25: 33% zerodays: https://www.computerweekly.com/news/450415866/Nearly-a-third-of-malware-attacks-are-zero-day-exploits
S21-25: Zerodium twitter: https://twitter.com/Zerodium/status/1260541578747064326
S21-25: Zerodium CEO twitter: https://twitter.com/cBekrar/status/1308406389379923969

APT groups aka advance threat actors
S26: MITRE ATT&CK Group pages: https://attack.mitre.org/groups/
S26: Mandiant/Fireeye report about APT1 to US Congress which outed China (2013, Nov): https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
S26: 2013 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION: https://www.uscc.gov/sites/default/files/annual_reports/Complete%202013%20Annual%20Report.PDF

Credits and prior art

"discovering truth by building on previous discoveries“

Hacking as a service
S27-29: HIDE AND SEEK - Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
S27-29: Pegasus: The ultimate spyware for iOS and Android: https://www.kaspersky.com/blog/pegasus-spyware/14604/
S27-29: The Spy in Your Phone | Al Jazeera World: https://www.youtube.com/watch?v=IfOgm1IcBd0&ab_channel=AlJazeeraEnglish
S27-29: How a hacked phone may have led killers to Khashoggi: https://edition.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html

France vs Germany
S30: Enlightened Secrets: Silk, Intelligent Travel, and Industrial Espionage in Eighteenth-Century France: https://pdfs.semanticscholar.org/3d1c/694388eedb3940fff607b8aacaed84382523.pdf
S30: Cold War espionage paid off—until it backfired, East German spy records reveal: https://www.sciencemag.org/news/2017/07/cold-war-espionage-paid-until-it-backfired-east-german-spy-records-reveal
S30: France is top industrial espionage offender: https://www.france24.com/en/20110104-france-industrial-espionage-economy-germany-russia-china-business
S30: Espionage? Moi?: https://foreignpolicy.com/2013/07/02/espionage-moi/

U.S. National Intelligence Estimate 2013
S31: Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation: https://www.amazon.co.uk/Partly-Cloudy-Interrogation-Professional-Intelligence-ebook/
S31: Chapter 7 - The China Factor: https://www.sciencedirect.com/science/article/pii/B9781597497404000071
S31: Gates: French cyber spies target U.S.: https://www.politico.com/story/2014/05/france-intellectual-property-theft-107020
S31: Fair Play: The Moral Dilemmas of Spying: https://www.amazon.co.uk/Fair-Play-Moral-Dilemmas-Spying/dp/1574889494/
S31: U.S. said to be target of massive cyber-espionage campaign:
https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html
S31: Spy vs. Spy, America and Israel Edition: https://foreignpolicy.com/2015/03/24/spy_vs_spy_america_and_israel_edition/

Human Intelligence (HUMINT)
S32: The Ultimate Guide to Human Intelligence (HUMINT): https://www.intelligence101.com/the-ultimate-guide-to-human-intelligence-humint/
S32: Myths and Realities: Social Engineering vs. Traditional Hacking: https://economiccrimeintelligence.wordpress.com/2013/01/24/myths-and-realities-social-engineering-vs-traditional-hacking/

Credits and prior art

"discovering truth by building on previous discoveries“

Bulk telecom intercepts

S33-34: Picture: https://www.scenicsolutionsgroup.com/telecommunication-services/
S33-34: Lawful Interception - Historical context and future challenges for Internet Service Providers: http://caia.swin.edu.au/talks/CAIA-TALK-030514A.pdf
S33-34: Backbone maps: Mapping the Internet: https://www.itgsnews.com/mapping-internet-maps/
S33-34: The Territoriality of Pan-European Telecommunications Backbone Networks: https://www.lboro.ac.uk/gawc/rb/rb136.html
S33-34: An Honest Conversation About Evading Spies: https://www.counterpunch.org/2015/02/27/an-honest-conversation-about-evading-spies/
S33-34: Hijacking the Internet Is Far Too Easy: https://slate.com/technology/2018/11/bgp-hijacking-russia-china-protocols-redirect-internet-traffic.html
S33-34: You won't guess where European mobile data was rerouted for two hours. Oh. You can. Yes, it was China Telecom: https://www.theregister.co.uk/2019/06/10/bgp_route_hijack_china_telecom/
S33-34: China hijacking internet traffic using BGP, claim researchers: https://nakedsecurity.sophos.com/2018/10/30/china-hijacking-internet-traffic-using-bgp-claim-researchers/
S33-34: If China Isn't Hijacking Internet Traffic, There's No Reason Why Not: https://www.forbes.com/sites/emmawoollacott/2018/11/13/if-china-isnt-hijacking-internet-traffic-theres-no-reason-why-not/#512fed905ed5
S33-34: Grey is the new black: covert action and implausible deniability: https://academic.oup.com/ia/article/94/3/477/4992414

Ransomware

S35-38: Holding the world to ransom: The top 5 most dangerous criminal organizations online right now: https://gcn.com/articles/2021/07/07/top-ransomware-gangs.aspx
S35-38: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021: https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
S35-38: 83% of ransomware victims paid to get data restored: https://www.securitymagazine.com/articles/96333-83-of-ransomware-victims-paid-to-get-data-restored

Bugging physical locations

S39-41: Handläggningen av vissa säkerhetsfrågor: https://data.kb.se/datasets/2015/02/sou/1993/1993_26%28librisid_17112410%29.pdf
S39-41: Nya Avslöjanden om avlyssning på Sveriges ambassad I Moskva: https://cdnc.ucr.edu/?a=d&d=VEST19870312.2.5&e=-------en--20--1--txt-txIN--------1
S39-41: Granite Island Group, Types of bugs: http://www.tscm.com/typebug.html
S39-41: Bugging devices found in EU offices: https://www.theguardian.com/world/2003/mar/20/eu.politics
S39-41: China “gifted” the African Union a headquarters building and then allegedly bugged it for state secrets: https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years
S39-41: U.S. bugged EU offices, computer networks: German magazine: https://www.reuters.com/article/us-usa-eu-spying/u-s-bugged-eu-offices-computer-networks-german-magazine-idUSBRE95S0AQ20130629
S39-41: UK embassy 'bug' angers Pakistan: http://news.bbc.co.uk/2/hi/south_asia/3257265.stm
S39-41: Picture: http://www.bugsweeps.com/info/bugsweepers.html

Credits and prior art

"discovering truth by building on previous discoveries“

Information Operations (IO)
S42-44: Warfare in the Information Age, ch. 7: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch7.pdf
S42-44: Cyber war in perspective: Russian aggression against Ukraine: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf
S42-44: Pursuing a Strategy for Yesterday's War: https://smallwarsjournal.com/jrnl/art/pursuing-strategy-yesterdays-war
S42-44: The Cambridge Analytica scandal changed the world – but it didn't change Facebook: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
S42-44: Facebook–Cambridge Analytica data scandal: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
S42-44: How Duterte Used Facebook To Fuel the Philippine Drug War: https://www.buzzfeednews.com/article/daveyalba/facebook-philippines-dutertes-drug-war
S42-44: Facebook Removes Accounts Linked to Duterte's Former Social-Media Manager: https://www.wsj.com/articles/facebook-removes-accounts-linked-to-dutertes-former-social-media-manager-11553861357
S42-44: A Journalist Trolled by Her Own Government: https://www.nytimes.com/2019/02/22/opinion/maria-ressa-facebook-philippines-.html

~~WannaCry, Petya~~, NotPetya & Lessons
S45-47: The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History' - https://www.wired.com/story/white-house-russia-notpetya-attribution/
S45-47: WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 - https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware
S45-47: The Untold Story of NotPetya, the Most Devastating Cyberattack in History - https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
S45-47: NotPetya Ushered In a New Era of Malware - https://www.vice.com/en_us/article/7x5vnz/notpetya-ushered-in-a-new-era-of-malware

Security Design Principles
S49-61: GOTO 2016, Secure by Design – the Architect's Guide to Security Design Principles - https://www.youtube.com/watch?v=4qN3JBGd1g8

Credits and prior art

"discovering truth by building on previous discoveries“

The force multipliers - or “how to fight the war from the trenches”
S62: Strong authentication: https://en.wikipedia.org/wiki/Strong_authentication
S62: YubiKey: https://en.wikipedia.org/wiki/YubiKey
S62: Smart Cards: https://en.wikipedia.org/wiki/Smart_card
S62: Google Authenticator: https://en.wikipedia.org/wiki/Google_Authenticator
S62: Google: Security Keys Neutralized Employee Phishing - https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
S62: Microsoft: Using multi-factor authentication blocks 99.9% of account hacks - https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/
S62: Separation (physical and logical). Unfortunately I have not found any good public resources describing this.
- The basis of the separation concept is the idea of a security domain - https://en.wikipedia.org/wiki/Security_domain
- which is based on the concept of domain based security - https://en.wikipedia.org/wiki/Domain_Based_Security
Examples of Network separation
- Logical separation, VLAN som separationsmetod för industriella styrsystemsnät - https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4070--SE
- Unidirectional network (a common separation mechanism within military networks) - https://en.wikipedia.org/wiki/Unidirectional_network
S62: Security logging - https://en.wikipedia.org/wiki/Security_information_and_event_management
S62: White/Black listening - https://en.wikipedia.org/wiki/Whitelisting#Program_whitelists & https://en.wikipedia.org/wiki/Blacklist_(computing)#Information_systems
S62: SANS Critical Security Controls - https://www.cisecurity.org/controls/ & https://www.sans.org/critical-security-controls
S62: (Know your network) NSA TAO Chief on Disrupting Nation State Hackers video (38 min) - https://www.youtube.com/watch?v=bDJb8WOJYdA
S62: (Know your network) Improving the Security of Your Site by Breaking Into it (20 pages) - http://www.dcs.ed.ac.uk/home/rah/Resources/Security/admin_guide_to_cracking.pdf
S62: (Threat modelling) “Think Like an Attacker” is an opt-in mistake - http://emergentchaos.com/archives/2016/04/think-like-an-attacker-is-an-opt-in-mistake.html
S62: Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win - https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/

Read the books:

- The Cyber Security Body Of Knowledge: https://www.cybok.org/
- Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition (1232 pages): https://www.cl.cam.ac.uk/~rja14/book.html (HIGHLY RECOMMENDED)
- Site Reliability Engineering, How Google Runs Production Systems (552 pages) - http://shop.oreilly.com/product/0636920041528.do
- Vem kan man lita på?: den globala övervakningens framväxt (304 pages) - http://www.adlibris.com/se/bok/vem-kan-man-lita-pa-den-globala-overvakningens-framvaxt-9789175453958
- Konsten att gissa rätt - Underrättelsevetenskapens grunder (218 pages) - https://www.adlibris.com/se/bok/konsten-att-gissa-ratt---underrattelsevetenskapens-grunder-9789144004389
- The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age (384 pages) - https://www.amazon.com/Perfect-Weapon-Sabotage-Fear-Cyber/dp/0451497899