



Please note, all microphones and the video option are disabled for this webinar. This webinar will be recorded.

If you wish to ask a question during the webinar, please write in the Q&A chat. The trainer will answer the most representative questions before the end of his module session.

Many thanks for your cooperation



Level 1 training

Cyber Preparedness Training for a holistic approach in the MARitime logistics supply chain

Cristiano C, Cyberoo

24 November 2020, Zoom webinar

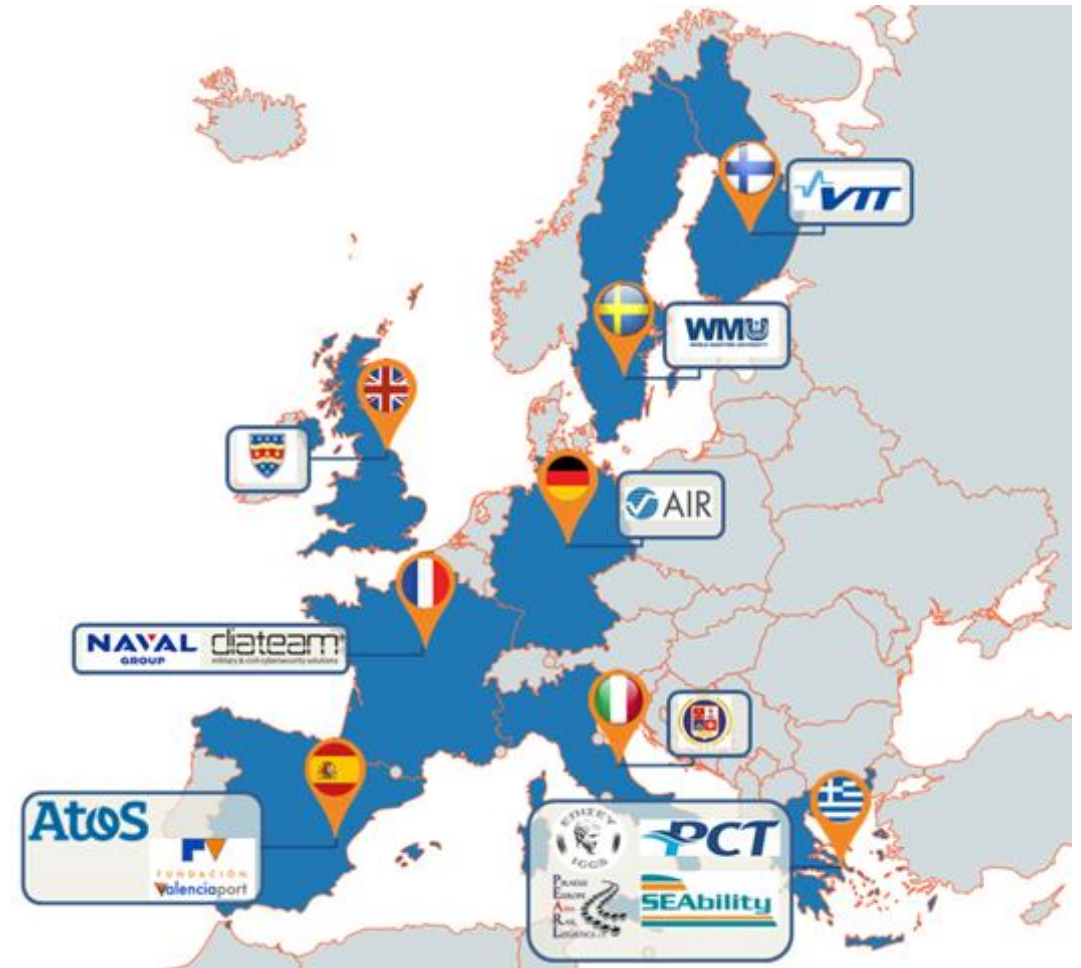
Cyber-MAR Consortium

The selection of partners of **different nationalities, social-cultural backgrounds** and complementing **multidisciplinary expertise** secure a high-quality actor participation from each intervention domain.

Comprises of **13 partners** from **8 European Countries**:

- **3 SMEs** (DIATEAM, SEAbility, PEARL)
- **3 Industries** (ATOS, AIR, Naval Group)
- **2 Research Organizations** (ICCS, VTT)
- **3 Universities/Foundations** (FAIMM, UoP, WMU)
- **2 End-users** (PCT, VPF)

It is well balanced between Research & Academia and Industry & SMEs. The consortium covers almost all different actors across the maritime logistics value chain ensuring the complete coverage of the sector.



Cyber-MAR Partners - WP Training and awareness raising (WMU – WP Leader)



Comprises of 7 **partners** from:

- **3 SMEs** (DIATEAM, SEAbility, PEARL)
- **3 Universities/Foundations** (FAIMM, UoP, WMU)
- **1 End-users** (VPF)

It is well balanced between Research & Academia and SMEs & End Users.





Please note, all microphones and the video option are disabled for this webinar. This webinar will be recorded.

If you wish to ask a question during the webinar, please write in the Q&A chat. The trainer will answer the most representative questions before the end of his module session.

Many thanks for your cooperation

Day 1

1. Intro and Scenarios
2. Regulatory Framework
3. Attacks in deep

Day 2

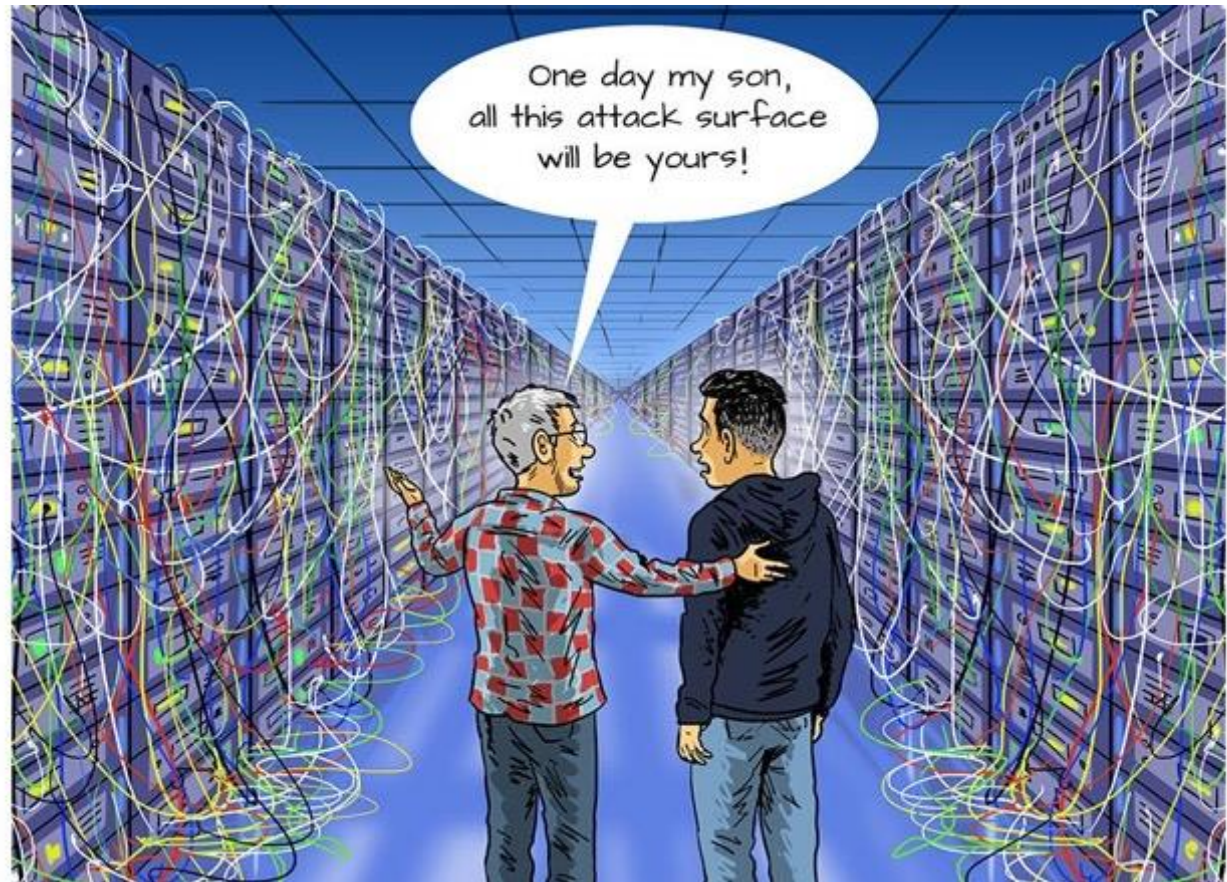
1. Mitigation and remediation
2. Cybersecurity in real life
3. Real cases

Day 3

1. Knowledge check
2. Final evaluation
3. Reasons of Cyber Range

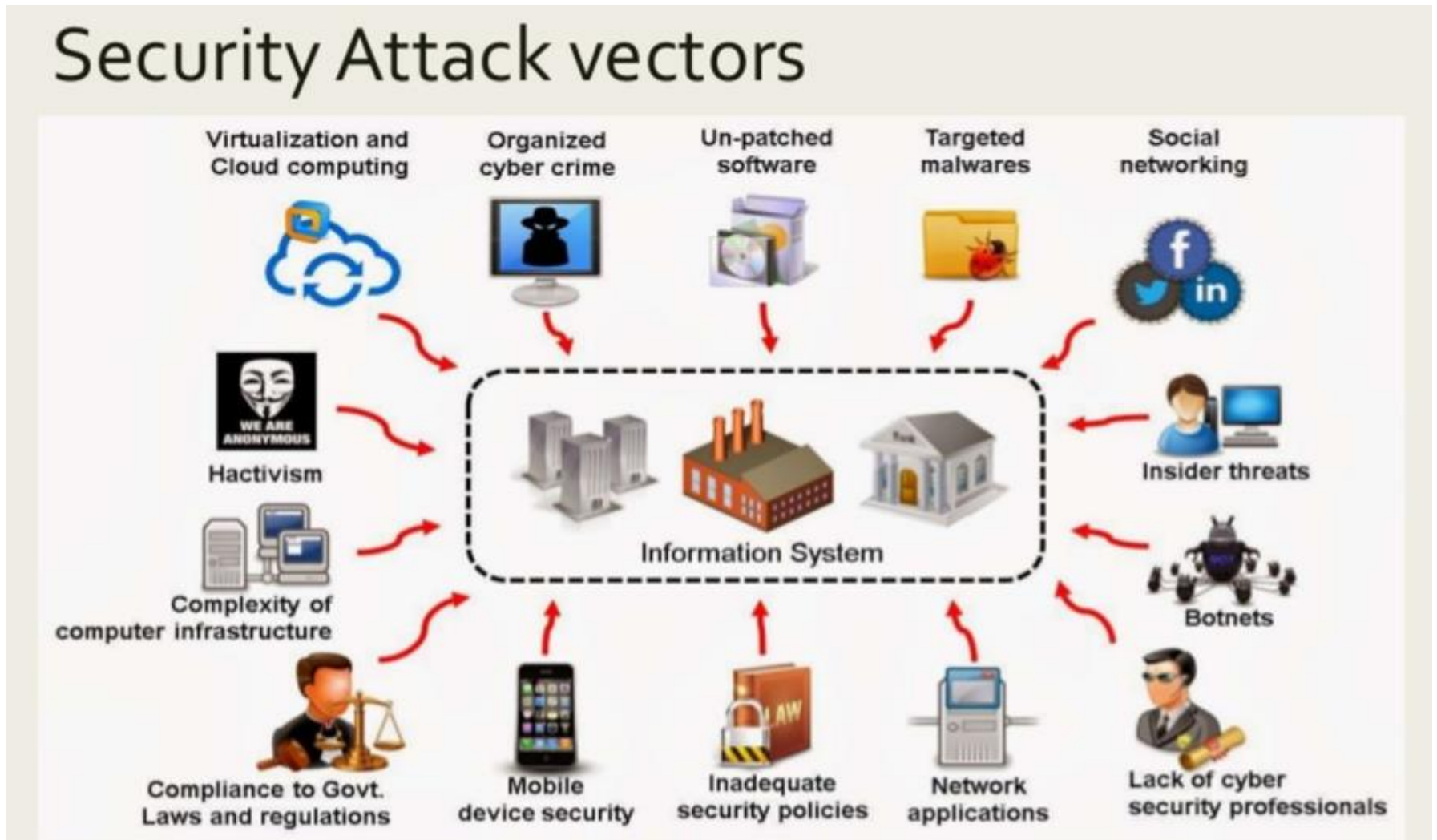
SESSION 1

INTRO AND SCENARIOS



Why are we here ?

Too many attack vectors and not enough cyber security professionals.



Today (MobCo sample):

Thanks to collected data profiles we do have the capability to take better decisions :

Flood warning

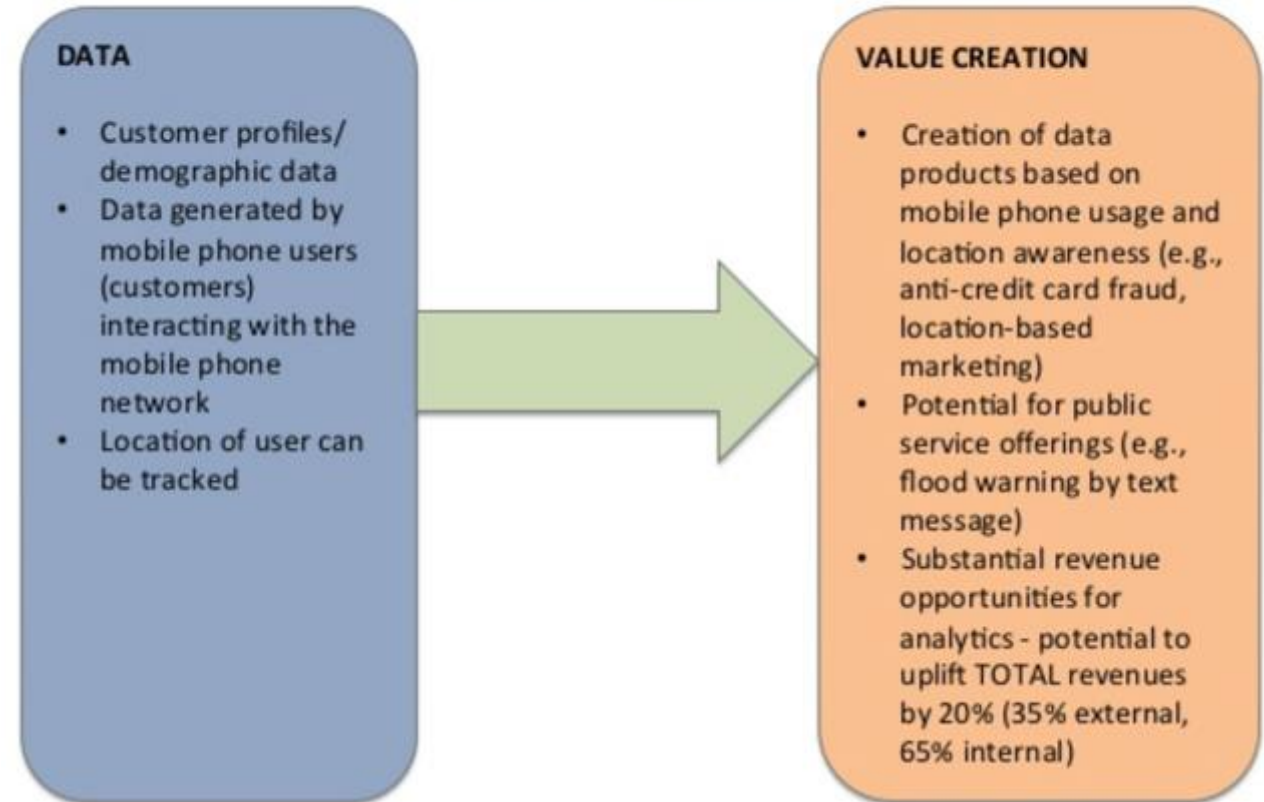
Anti-fraud solutions

Improved reliability of a service

Marketing and ...

Re-selling analytics to 3rd party

Data and value creation - MobCo

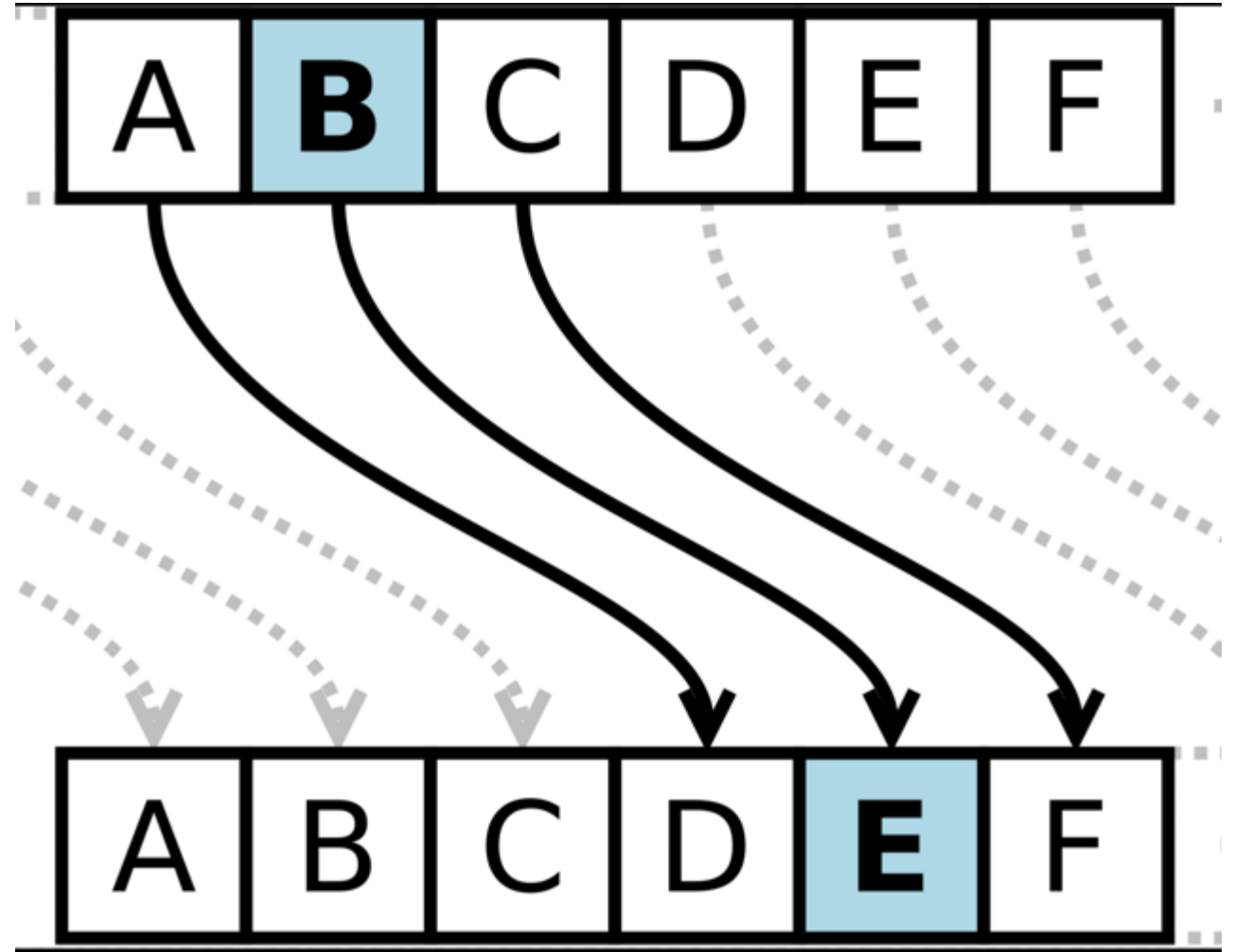


On the other side:

At Caesar time, a “key of 3” solutions was used to encrypt messages between “managers” and “remote workers”.

Hide data, protect them, discover them ... means get advantage on adversary teams

Data value can be considered at the same level of importance of cultural and mathematical skills



On every activity some one, external or internal to the corp can have:

Objectives

Method

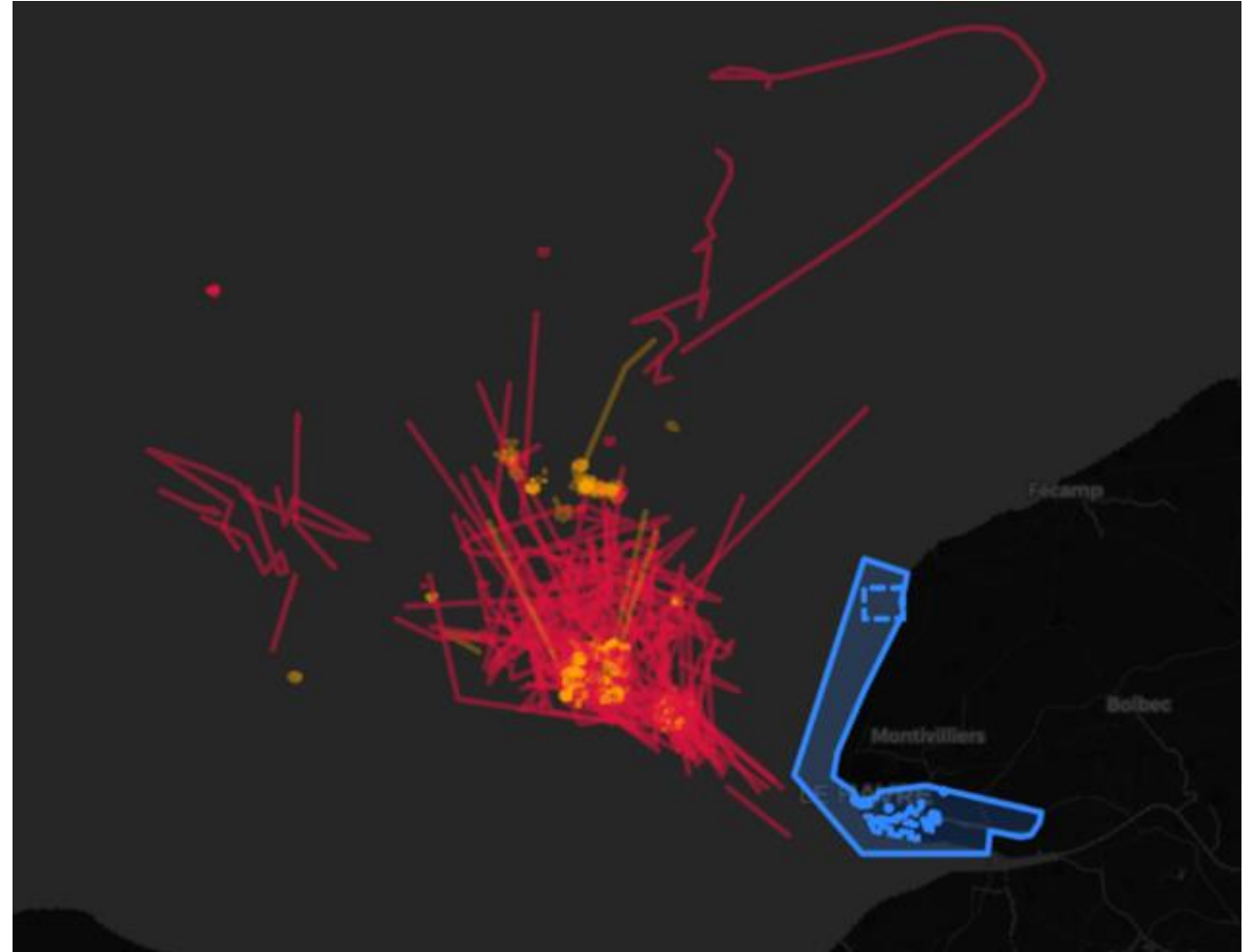
And can find vulnerabilities

Manipulating data, taking revenge, damaging reputation or disrupting business continuity when not creating fear and chaos it's the 50% resulting from attacks



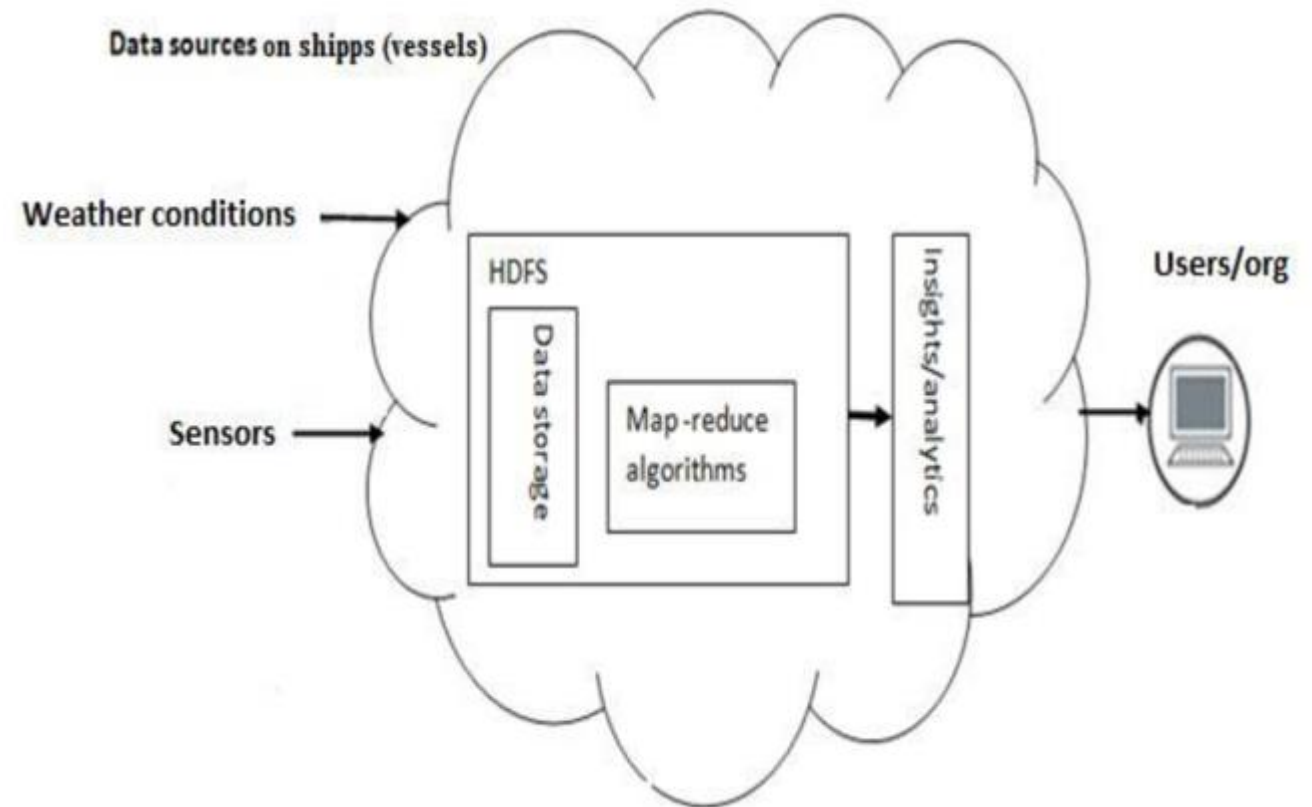
A sample in the maritime transportation:

On average, for every ship berthing in the European port, another one is waiting outside, and the environmental impact of waiting is compared to the environmental impact of berthing inside the harbours. Has been demonstrated that thanks to BIG DATA analytics this impact can be reduced by up to 80%. And Port Optimisation will be available too.



[BIG] DATA MEANS VALUE CREATION

Technologies like AIS, machine learning, and IoT are making a shift in shipping industry by introducing robots and more sensor equipped devices..



[BIG] DATA MEANS SAVING MONEY:

One of the main problems that the shipping industry is facing is the cause of misplacement of vessels on their route from source to destination. This problem has leads the industry to turn into smarter technologies like big data analytics.

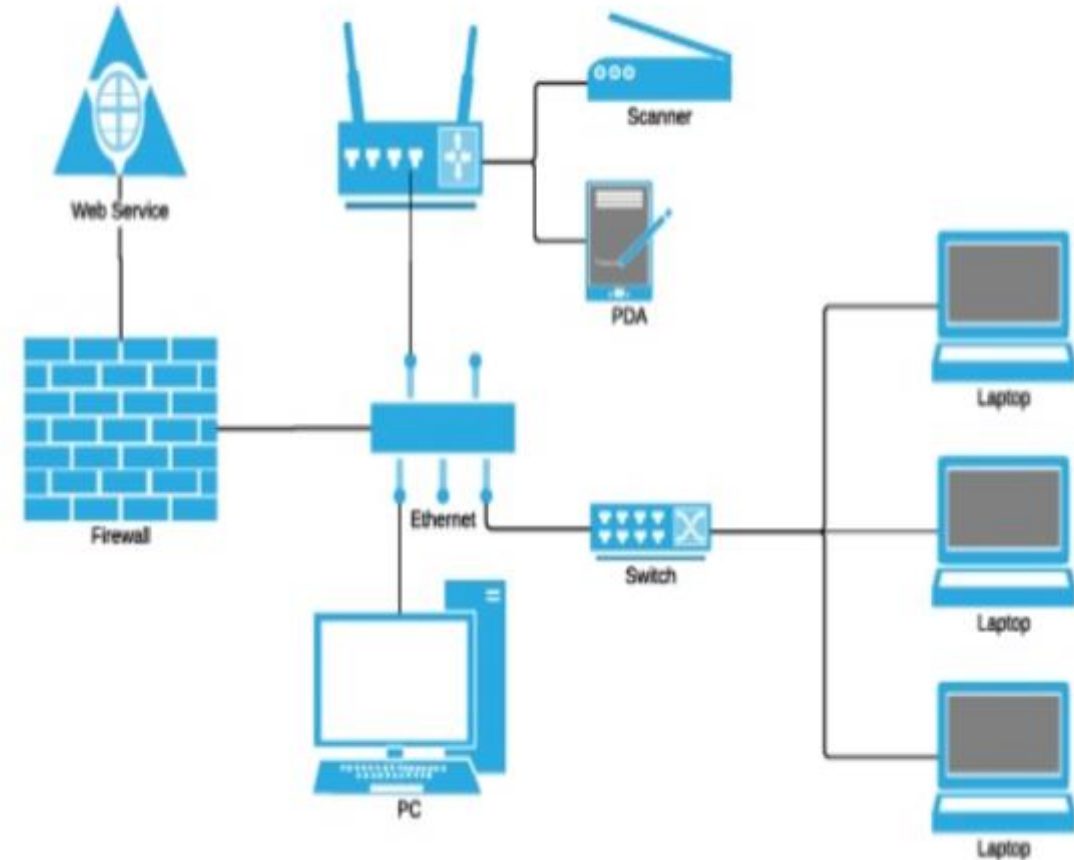
Until hackers/criminals does not disrupt it or does not hack/steal it, this becomes into a money saving investment !



LSM reefers save money with optimisation

What is a computer network ?

A **network** consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications



A network can be wired or wireless or both

PAN, LAN, MAN, WAN

Personal, Local, Metropolitan and Wide area networks are the main 4 types of networks

LAN inside your company/house

WAN = Internet

Then exists storage, virtual private,
Wireless area networks

Connection method

Wired:



Wireless:



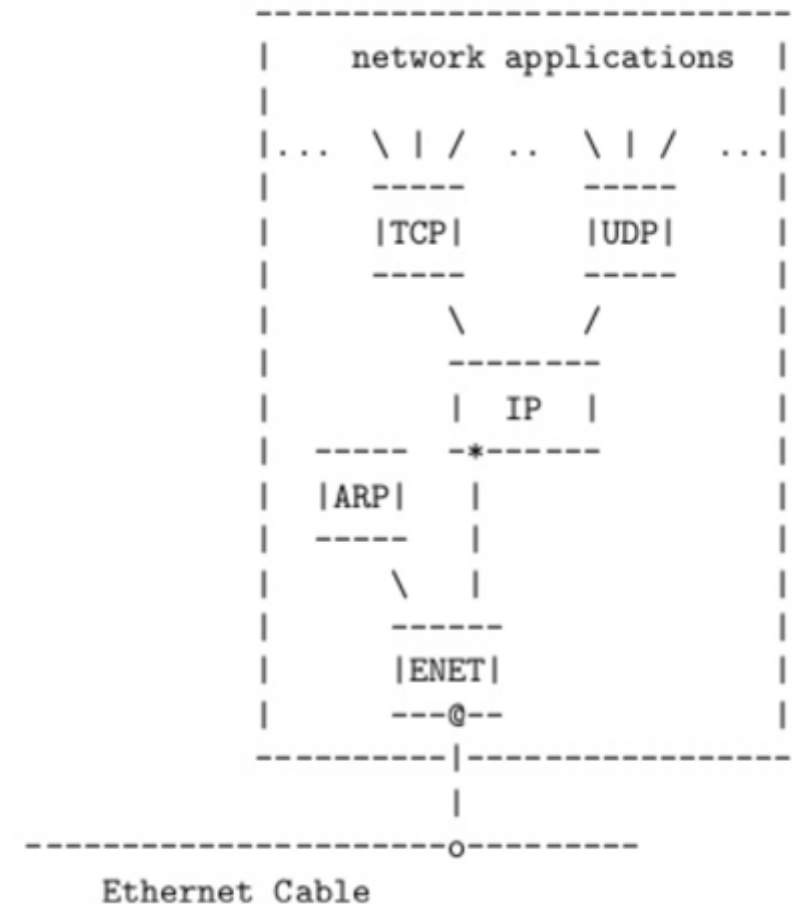
Scale

PAN, LAN, CAN, MAN, **WAN** ...

TCP/IP

Protocols

Protocols are used to permit and grant the dialogue and communication between network participants.



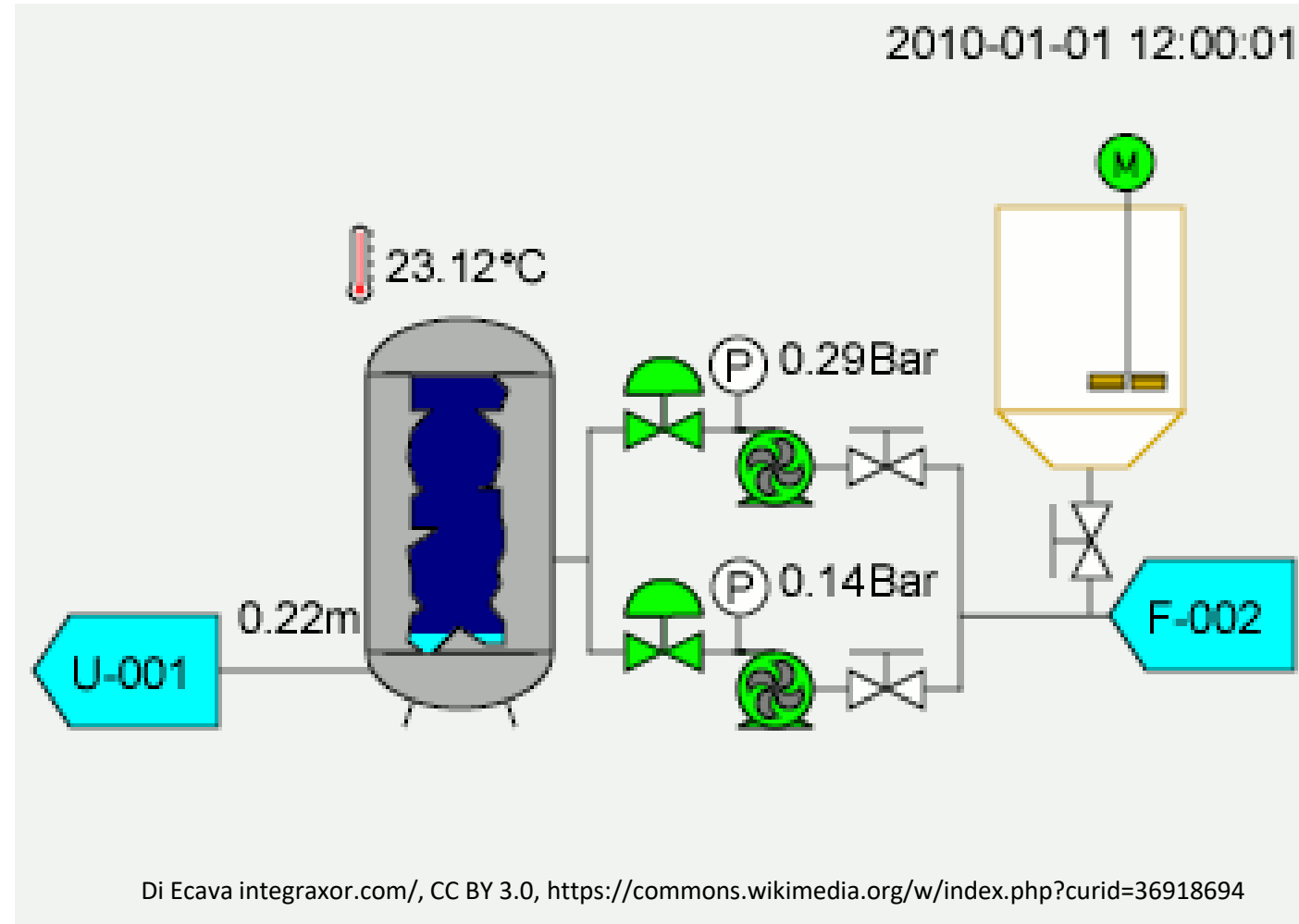
Wireless network is a **computer network** that uses wireless data connections between **network nodes**.

Wireless networking is a method by which homes, **telecommunications networks** and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. **admin telecommunications networks** are generally implemented and administered using **radio communication**. This implementation takes place at the physical level (layer) of the **OSI model** network structure.



A simple definition:

Generally, the **SCADA** system is a centralized system that monitors and controls the entire area. It is a pure software package that is positioned on top of the hardware. A supervisory system gathers data on the process and sends the commands control to the process



Components:

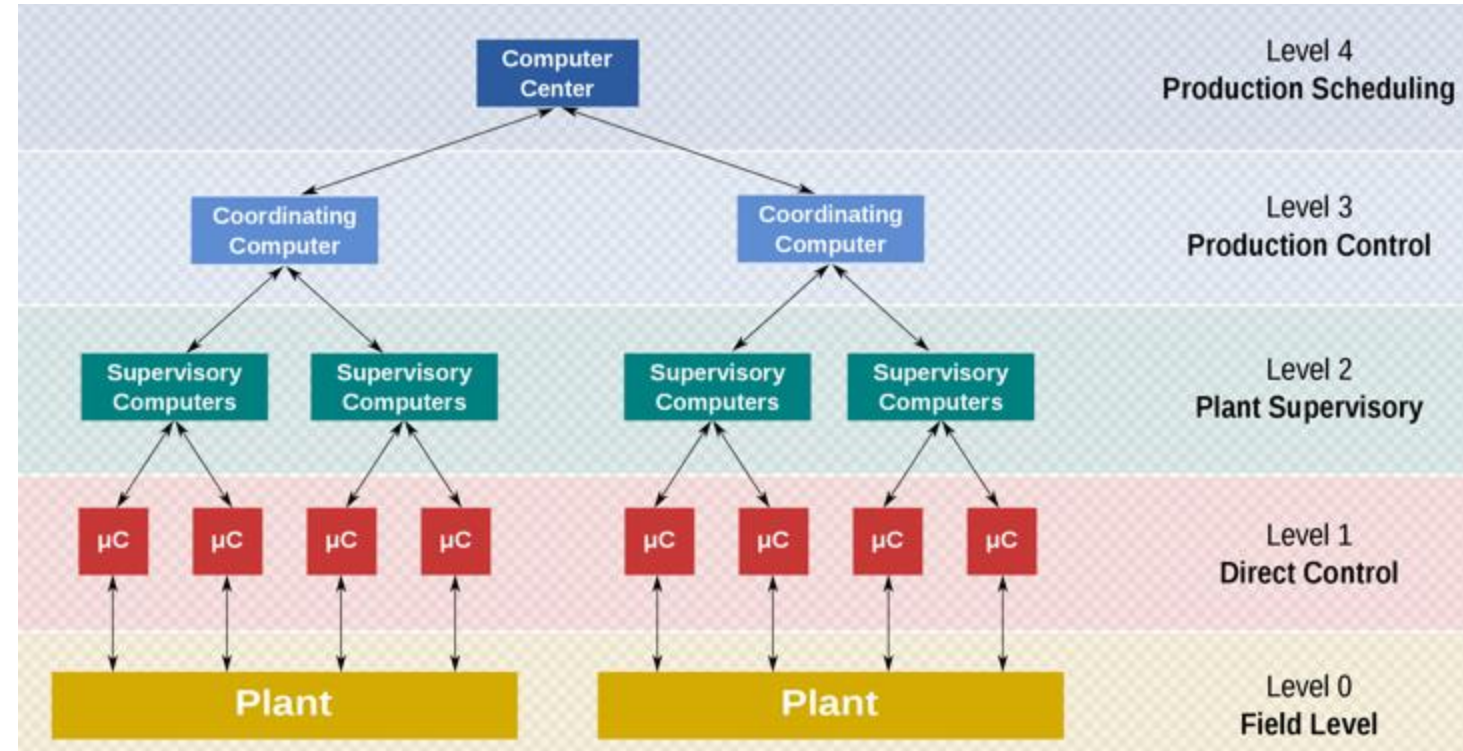
Supervisory computers

Remote terminal units

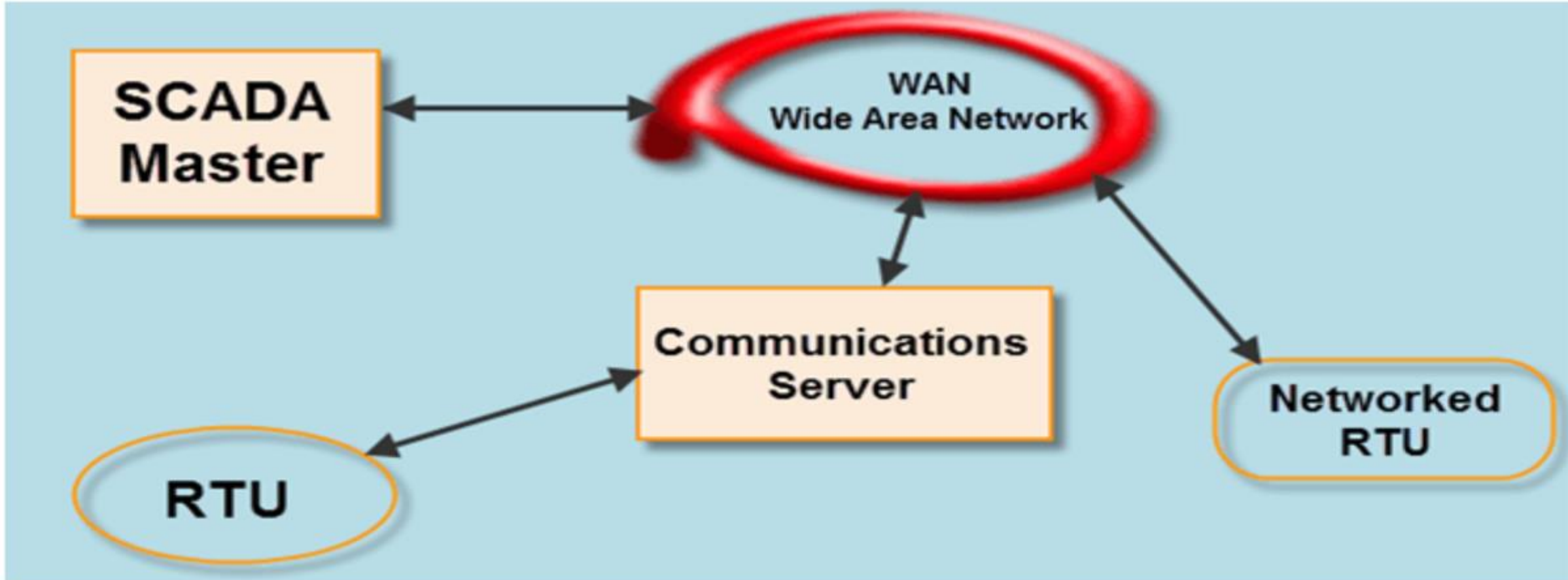
Programmable logic controllers

Communication infrastructure

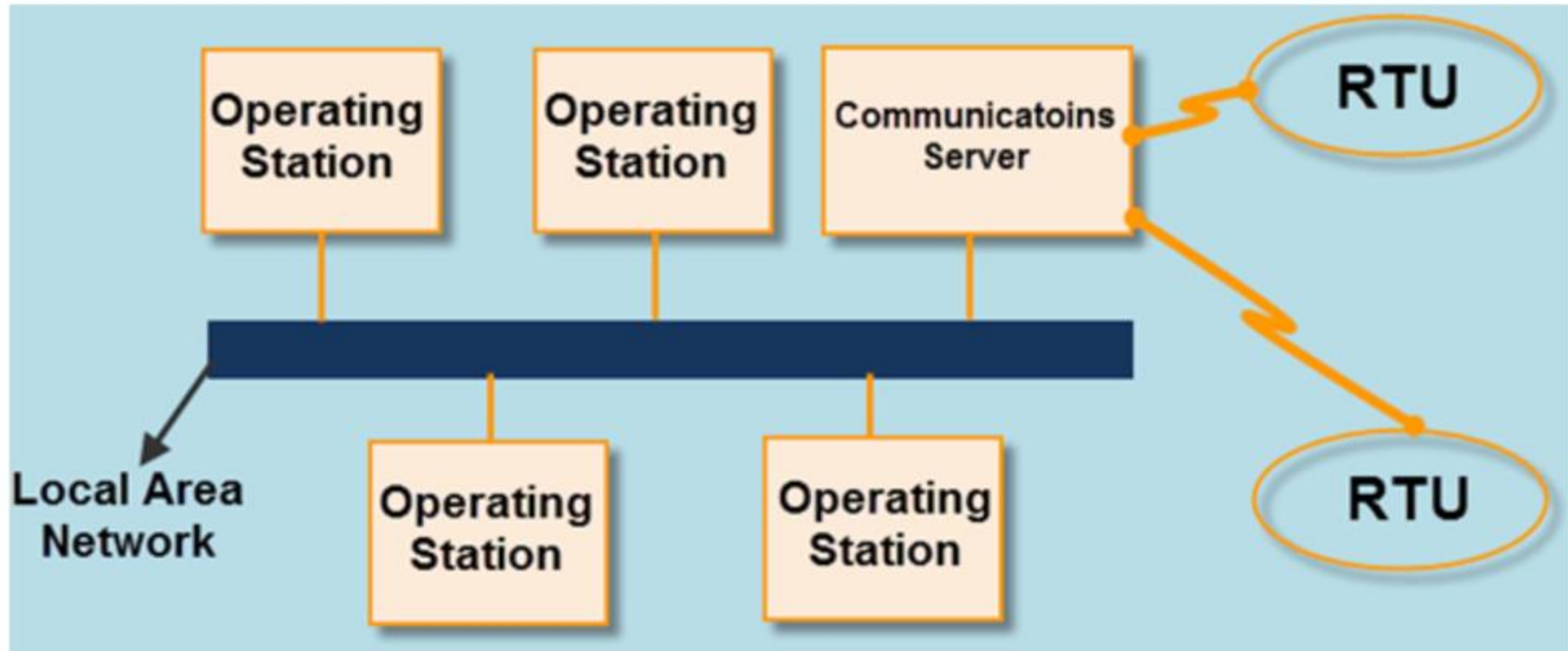
Human-machine interface



SCADA systems have traditionally used combinations of radio and direct wired connections, although SONET/SDH is also frequently used for large systems such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. Some users want SCADA data to travel over their pre-established corporate networks or to share the network with other applications. The legacy of the early low-bandwidth protocols remains, though.



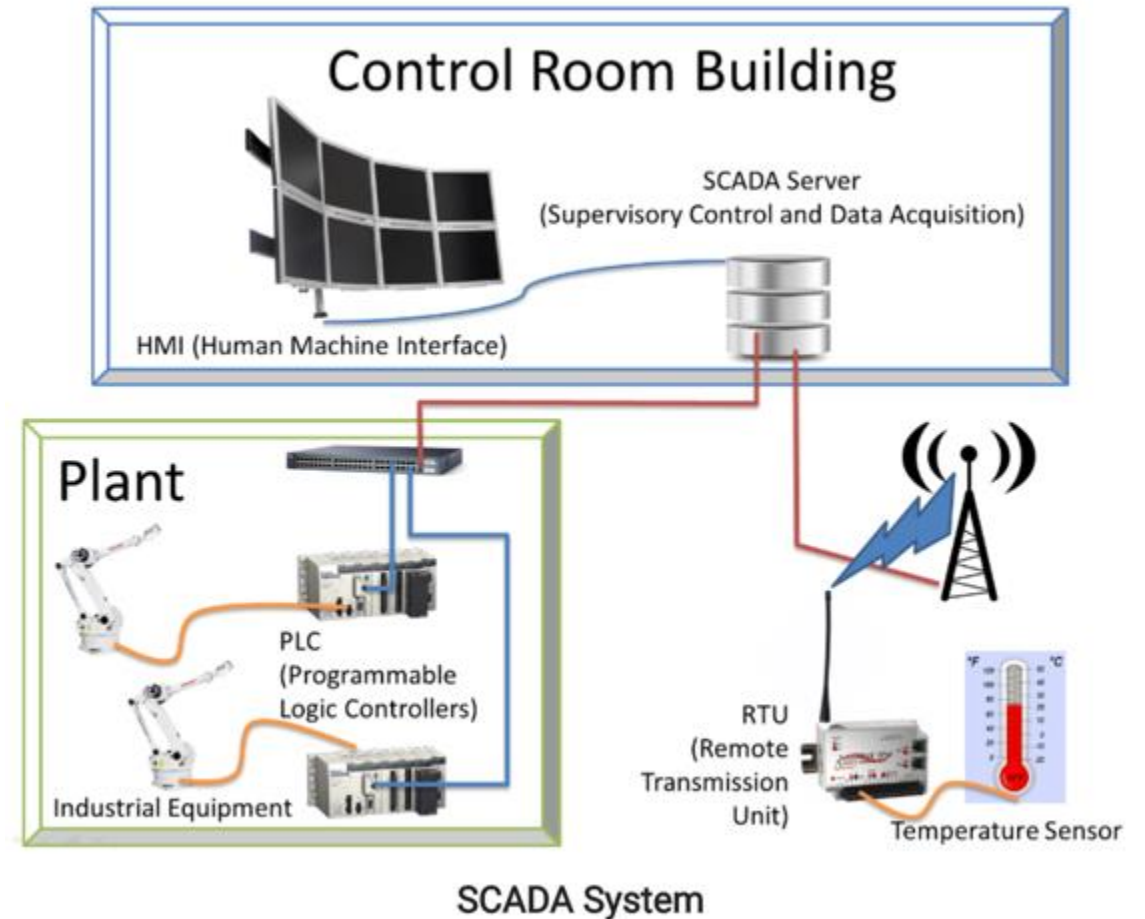
Networked SCADA Systems



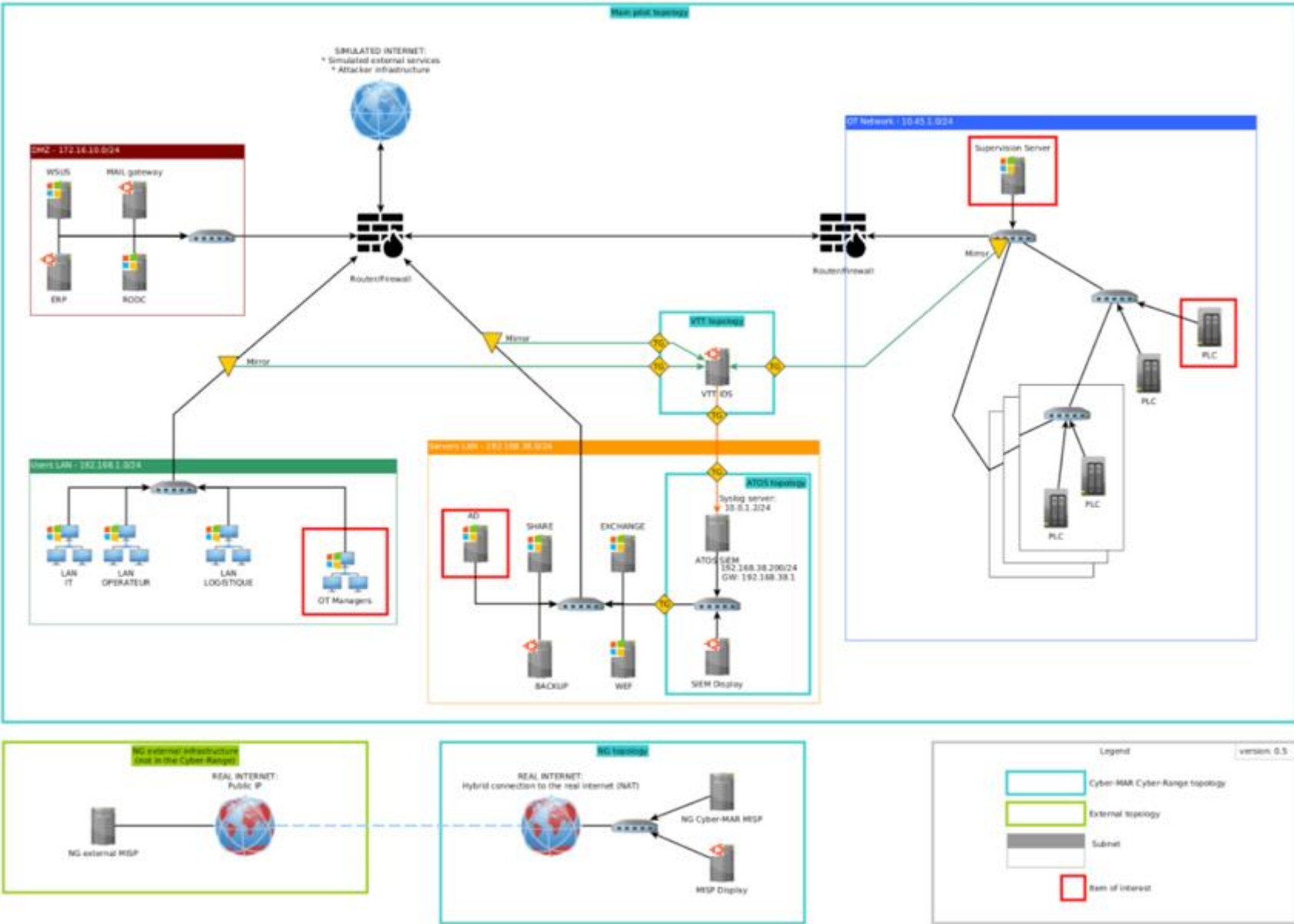
Distributed SCADA Systems

SCADA MEANING | Supervisory control and data acquisition

SCADA systems have traditionally used combinations of radio and direct wired connections, although SONET/SDH is also frequently used for large systems such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. Some users want SCADA data to travel over their pre-established corporate networks or to share the network with other applications. The legacy of the early low-bandwidth protocols remains, though.



SCADA | OUR NEXT PILOT ACTION :



Many are designed to send information only when the master station polls the RTU.

Typical legacy SCADA protocols include **Modbus RTU, RP-570, Profibus and Conitel**. These communication protocols, with the exception of Modbus (Modbus has been made open by Schneider Electric), are all SCADA-vendor specific but are widely adopted and used. Standard protocols are **IEC 60870-5-101 or 104, IEC 61850 and DNP3**.

Network simulation can be used in conjunction with SCADA simulators to perform various 'what-if' analyses.

Main diff

It is said that the best way to differentiate between a ship and a boat is to remember that **"A ship can carry a boat, but a boat cannot carry a ship."**

Technologically, **boats** are **simple** vessels with **less complicated equipment, systems and operational maintenance requirements**. Since **ships** are required to be operable for longer time-duration and travel across oceans, they are manned using **advanced engineering, heavy machinery, and navigational systems**.

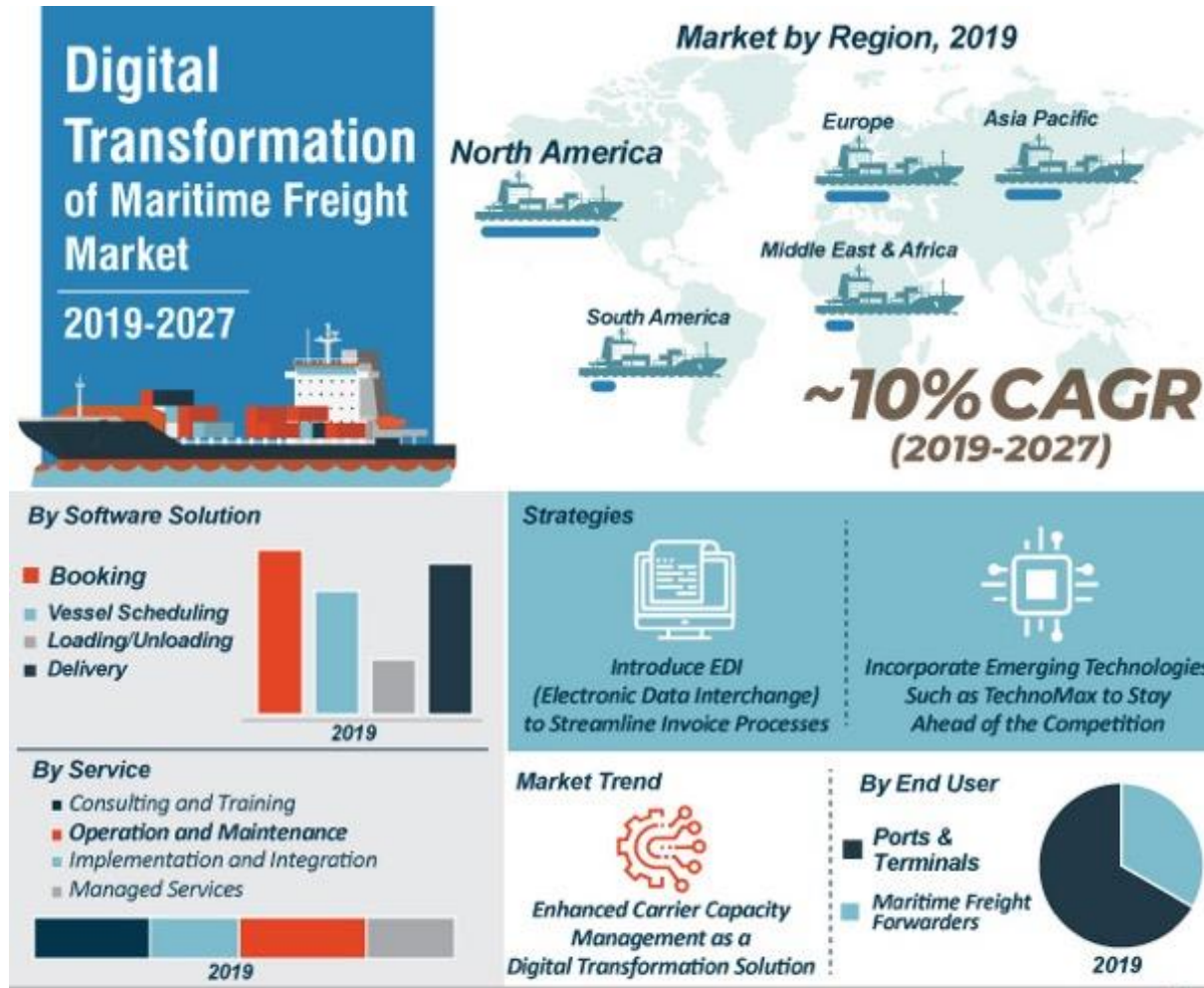
Bridge of a SHIP



Everything it's connected, including Gyro Compass, Radar, AutoPilot, ARPA (Radar Plotting automated solution), AIS (connected to VHF and Internet sat dish ...), LRIT, THD, GPS receiver ... and so on

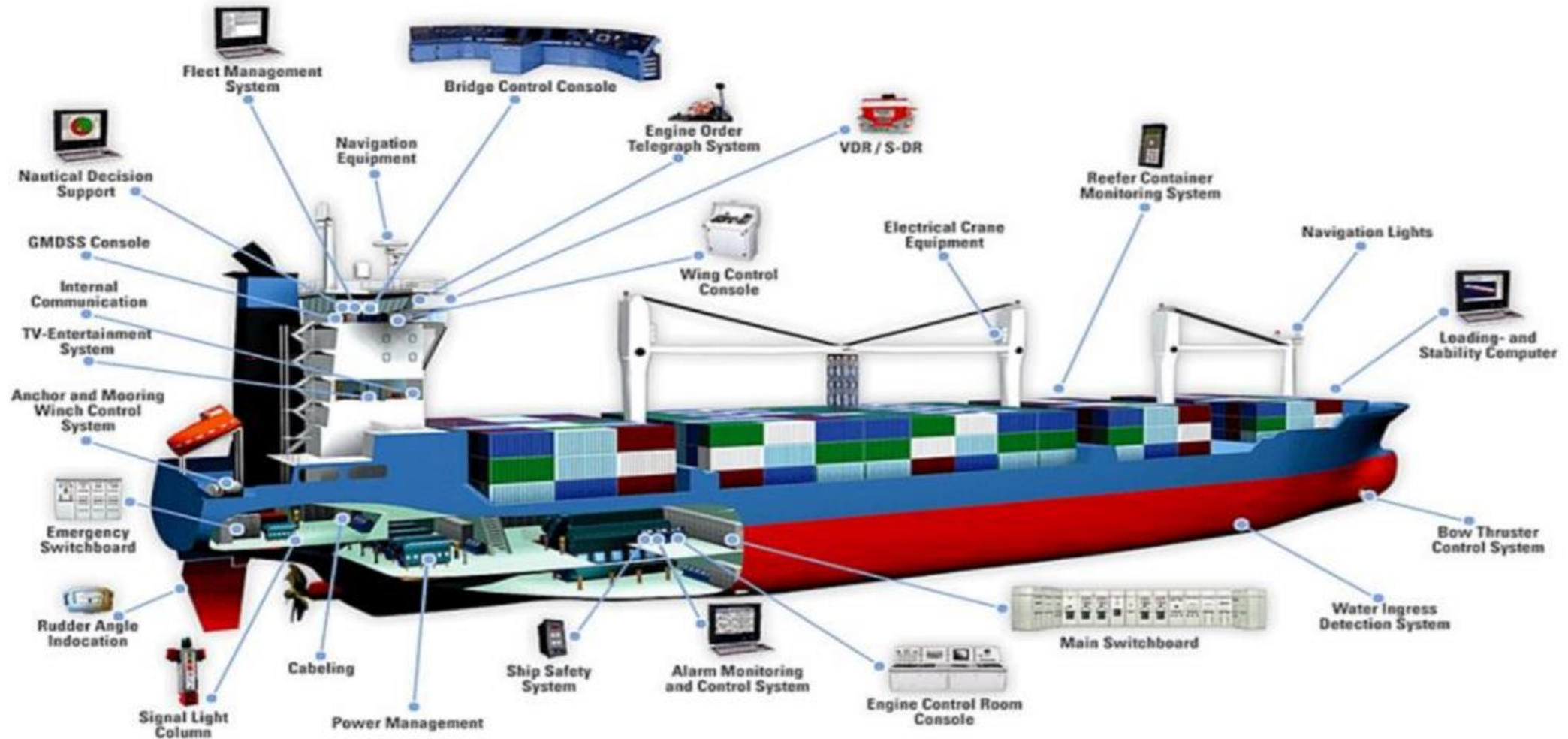


The Vessels Digitalization...



www.transparencymarketresearch.com

.... And The Attack Surface



Networking environment In a “simple” merchant ship

Usually at least 2 or 3 different networks: Crew, Business and Systems

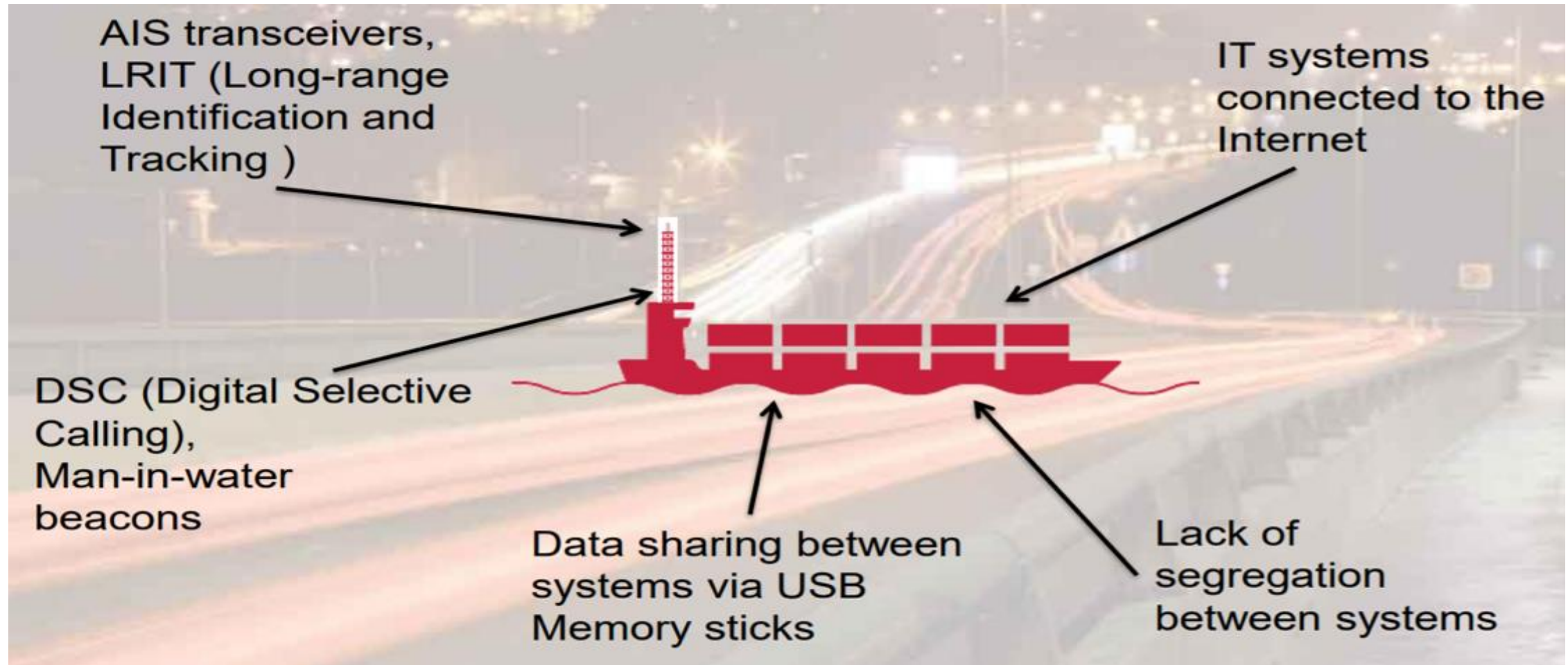
1. CREW one get also personal devices – high risk = more controls
2. BUSINESS are from 10 to 20 devices, servers, pc's and voip phones
3. SYSTEMS means for example navigation systems like cartography, 24x7 connected to get updates

Still in systems all the Naval Monitoring Devices are doubled (HW Backup) and usually not always connected

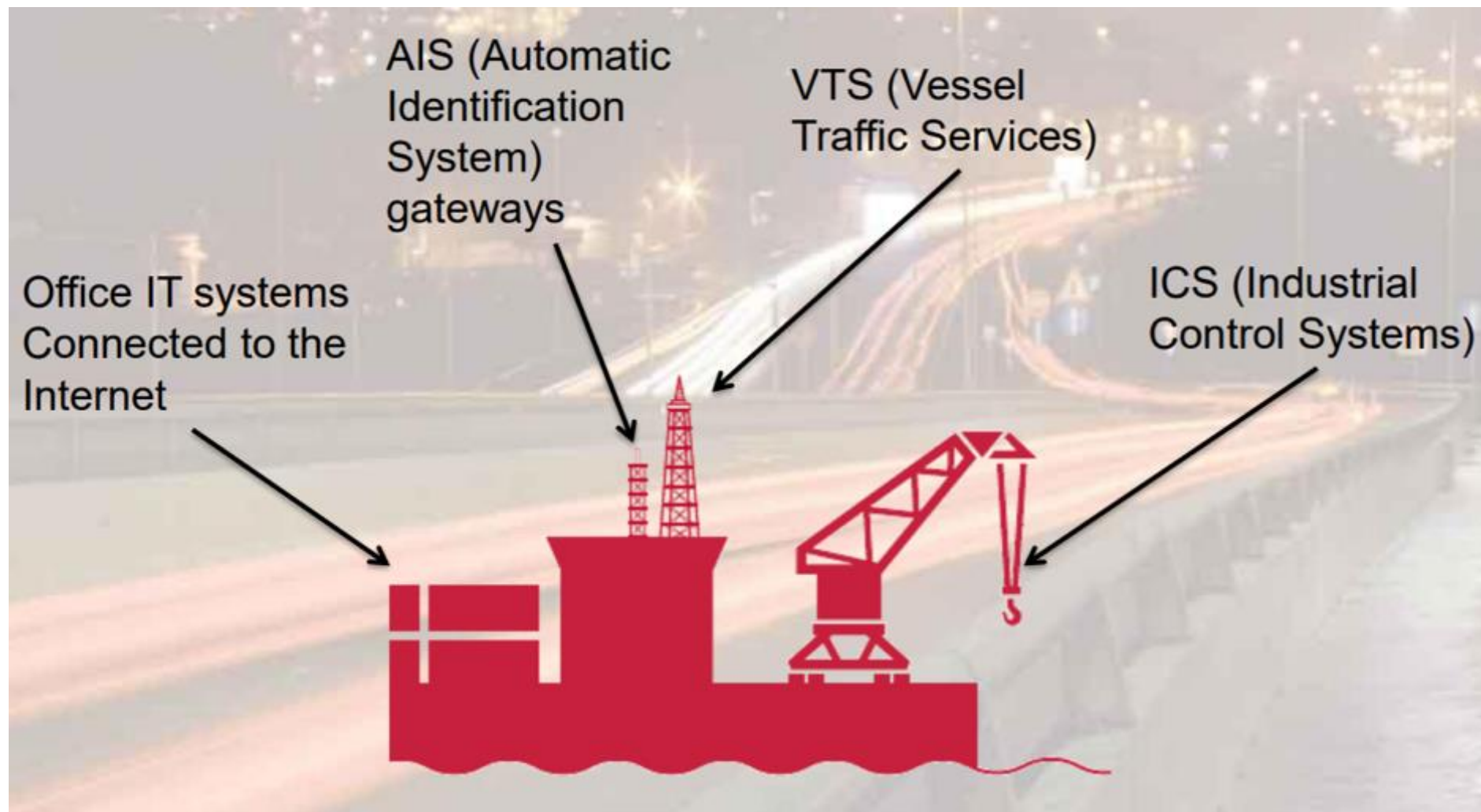
Everything, when connected to internet, uses a VPN (Virtual Private Network) to ensure secured dialogue with the internet provider.

Also, often there can be a VSAT Firewall solution or a dedicated one.

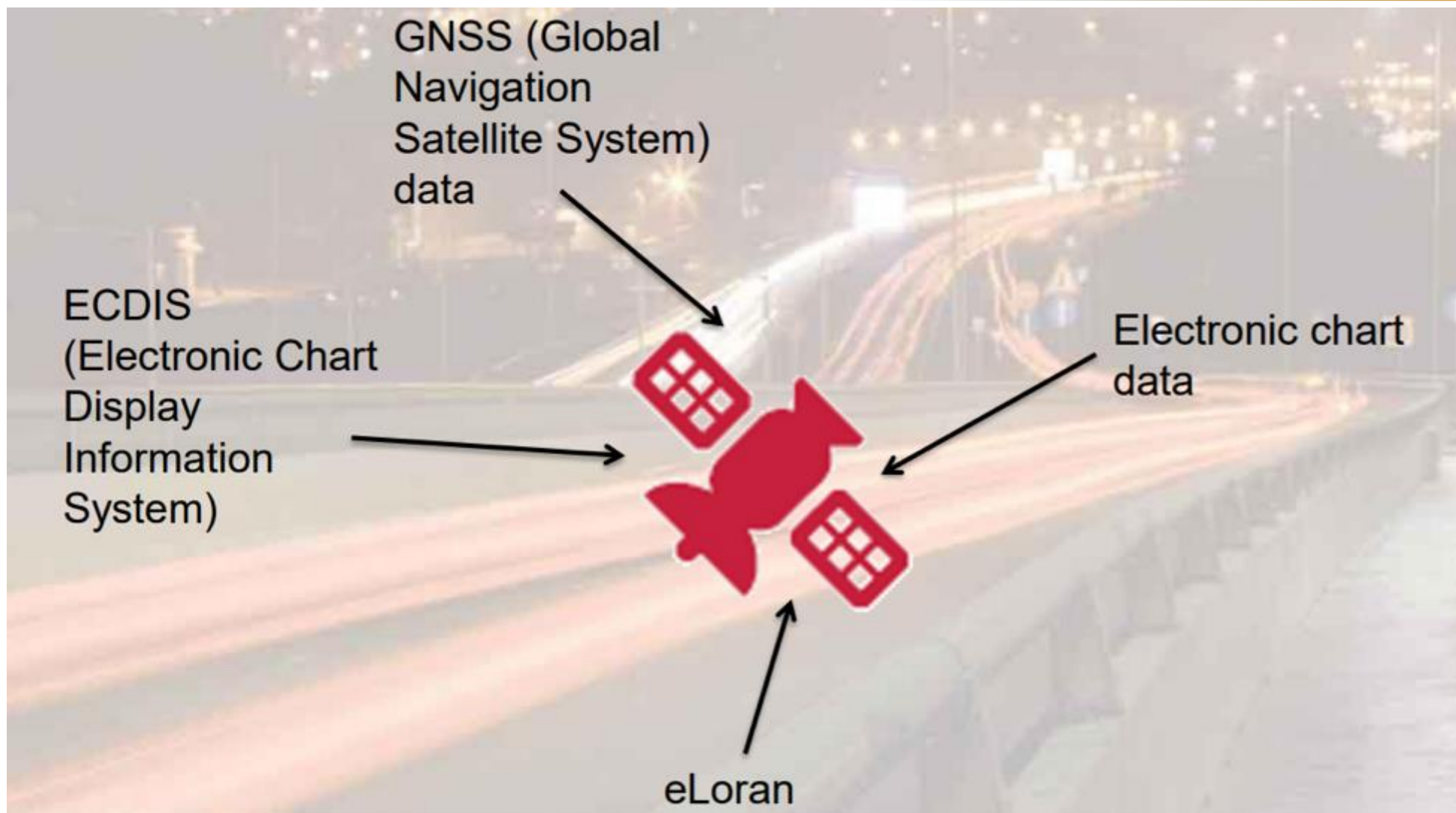
About Ship and his threats



About Hourbur



And about Navigation



Every member it's important
& there is no space for un-needed
components in the crew

Everyone need to know how systems are working,
but everyone with a different responsibility level.

TAKE-AWAY : Don't forget we talk about CYBER-
Security and everyone can be a target, and on a
luxury passenger cruise ship not only CREW, but
also guests and PASSENGERS can be attackers or
targets



No mistakes allowed

Responsibilities are formally on the Captain and his 1st Mate/Officer (Mate is also the Ship's Safety and Security Officer.)

BUT has been demonstrated that everyone need to engage with **CYBERSECURITY** with focus and at least basic skills.

No one will be excluded from protecting assets and values on board



An incredibly high cost

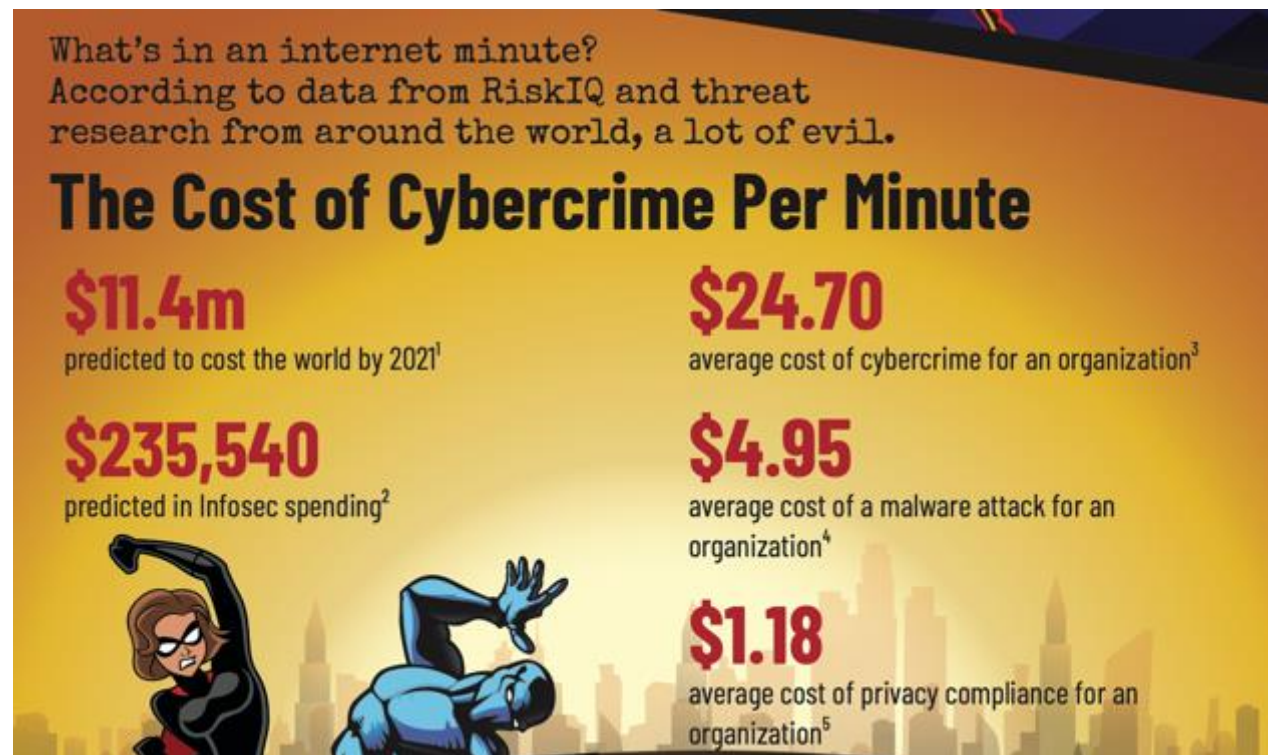
Predicted cost 11M\$ means that a crazy high value is involved into internet use and misu-use

Attacks are evolving every day

Protections are not always in place due to the «costs» or «difficulties» -

THE TRUE IS «LACK OF KNOWLEDGE»

Security it's NOT comodity

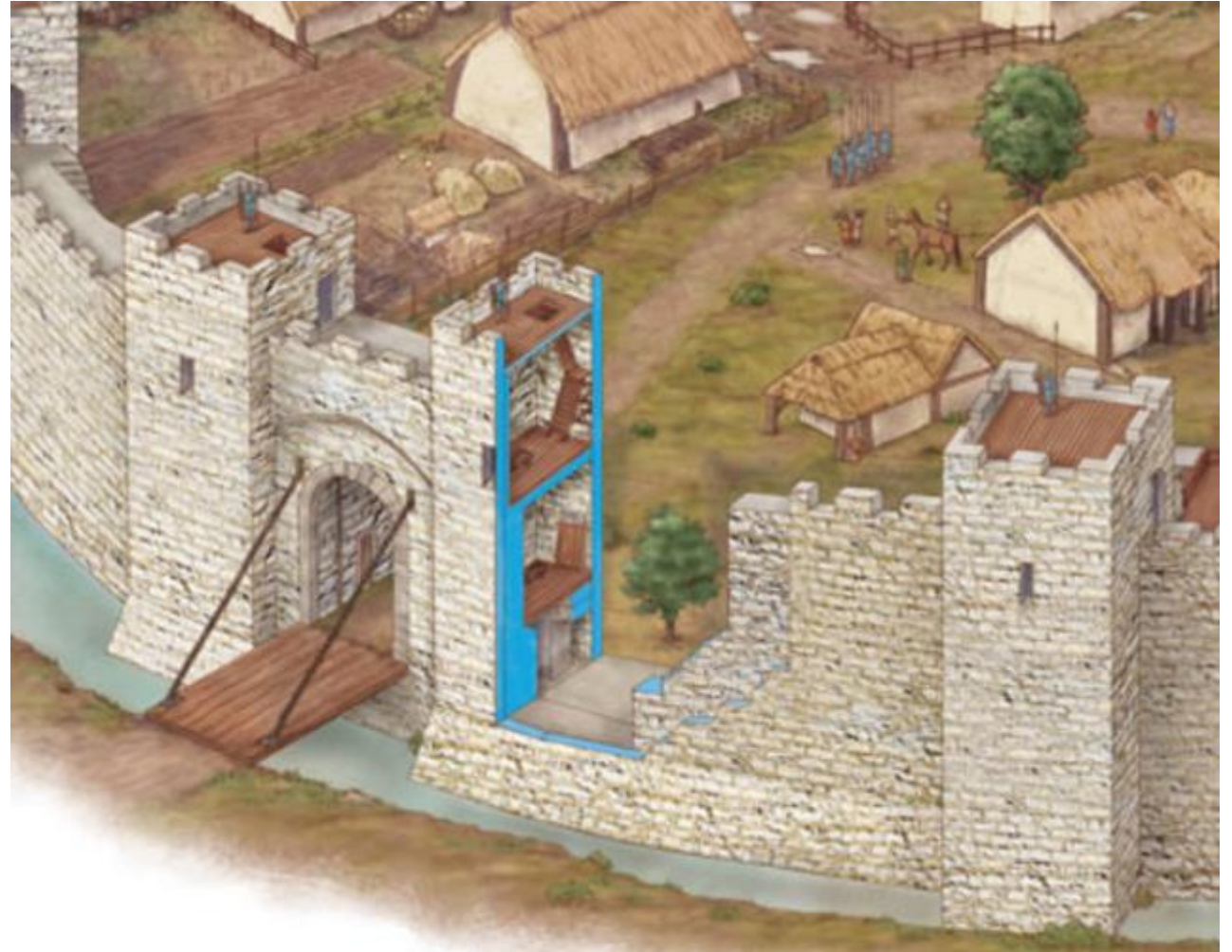


A simple ladder

«Imagine how expensive it would be to create a 20-foot brick wall around your building, and how inexpensive it is for the bad guys to buy a 30-foot ladder,»

said Steven Chabinsky, a 15-year FBI veteran and Chief Risk Officer at the cybersecurity tech firm Swascan.

«If the response to that security breach is a government mandate to build a 40-foot wall, and I spent my money on that, then the attackers buy a 50-foot ladder. Where does it end?»



RANSOM

«a sum of money demanded or paid for the release of a captive»

...the kidnappers demanded a ransom ...

In our case : someone deliver some malicious software into your devices, locking them and then asking MONEY (usually Bitcoins) to give you back the access to the data

EXPLOIT

commonly means to selfishly take advantage of someone in order to profit from them or otherwise benefit oneself ...

In our case an exploit is a code that takes advantage of a software vulnerability or security flaw. ...

Universal serial bus

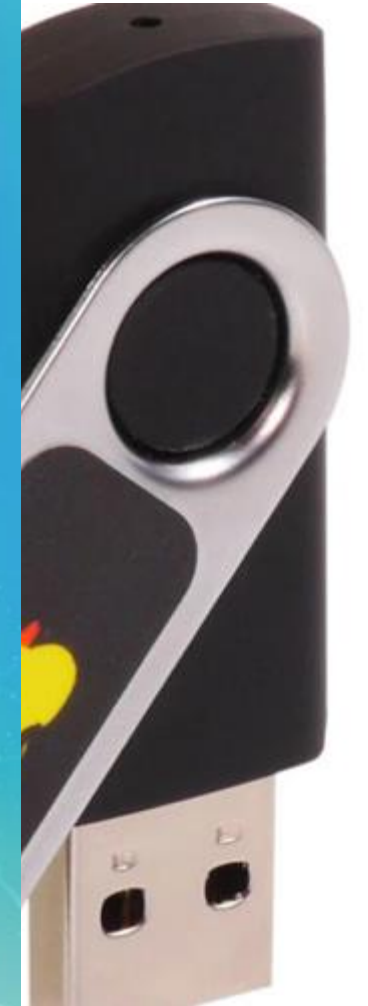
Nice, easy to use, physical and terrible because not easy to detect ...

Ready-made hw & sw:

Hacksaw, katana, very well known RUBBER DUCKy

And a well known real cases :

STUXNET, usb only, acts via C&C, infect SCADA and uses 0Days, mutable and flexible



Internet is dangerous, not only
but it is full of:

Hackers (the smallest problem)

Malware writers

Fraudsters

Blackmailers

Money launderers

Thieves and much more

And «all of them» are looking for
CASH! Money, it is all about that

While surfing around you see a
warning popup on a website
telling you to install the latest
Flash Player, and you click
“OK” to start the update.



Tiny trojan dropper downloaded ...
... and it's now hiding into your device

At least 6 different kinds

Ip Spoofing

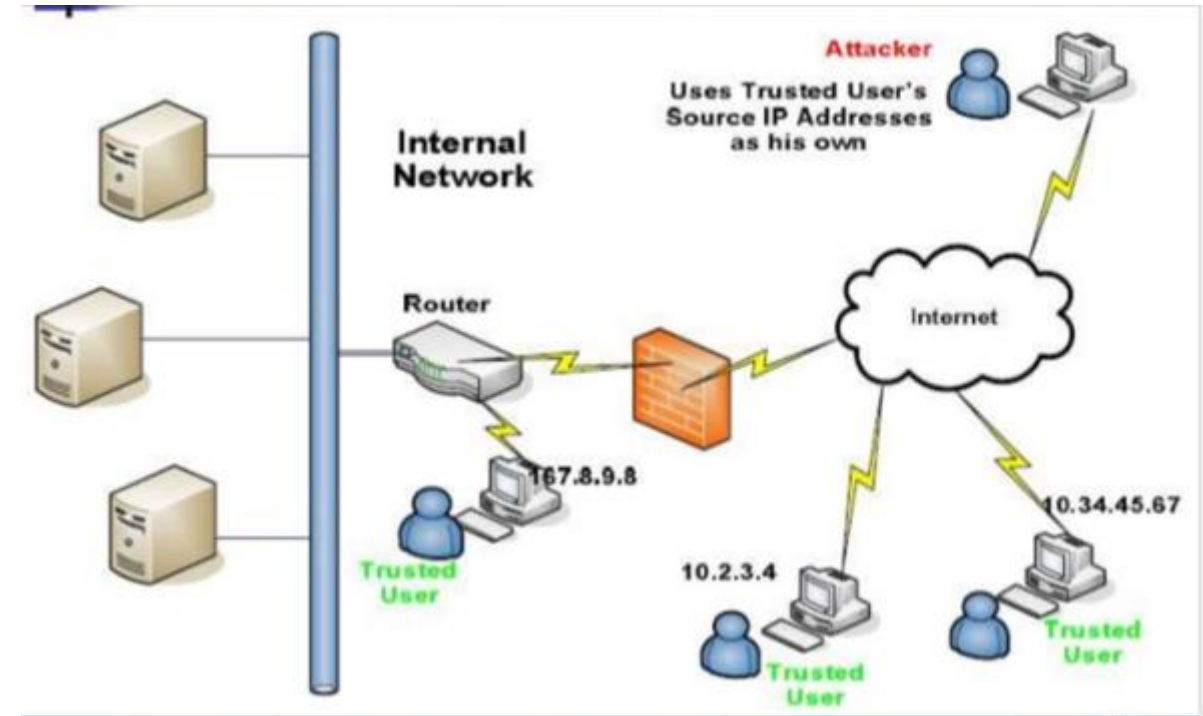
Web or URL spoofing

E-mail spoofing

Protocol spoofing

DNS spoofing

MAC spoofing



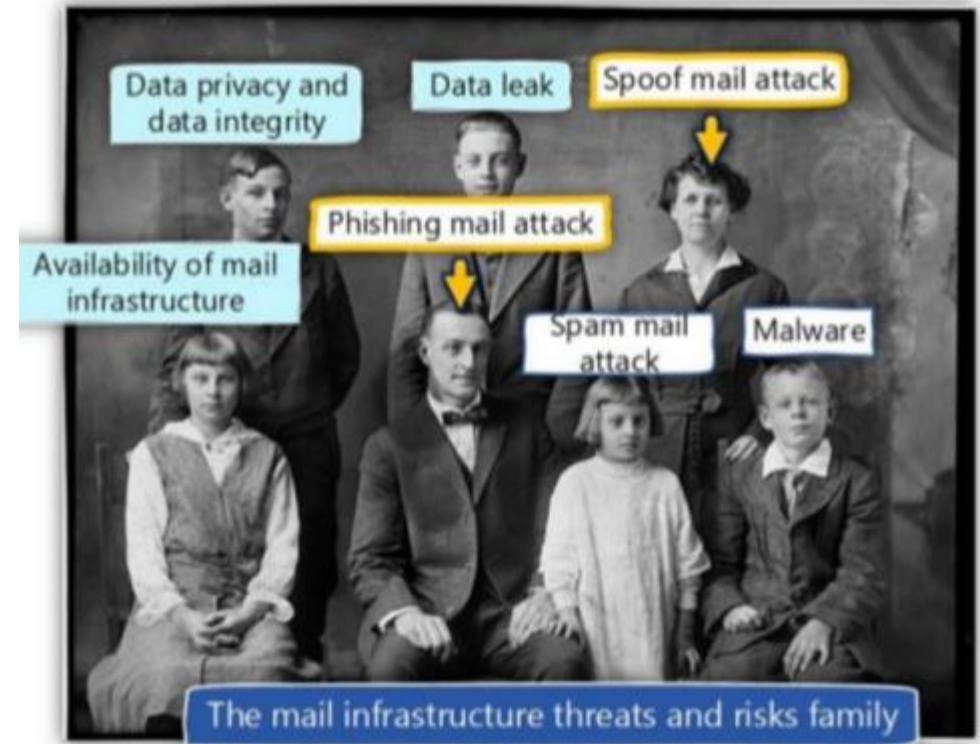
The VICTIMS think to talk with a trusted host but it's not : someone is in the middle now and read and drive the discussion

Phishing, it's cybercrime:

We were usual to SPAM emails, so UNWANTED spots on un-needed products (may be)

In the last decade attacks evolved into Phishing:

«**fraudulent attempt to obtain sensitive information** or data, such as usernames, passwords and credit card details, by disguising oneself » or better «a form of fraud in which **an attacker masquerades as a reputable entity** or person in email or other forms of communication»

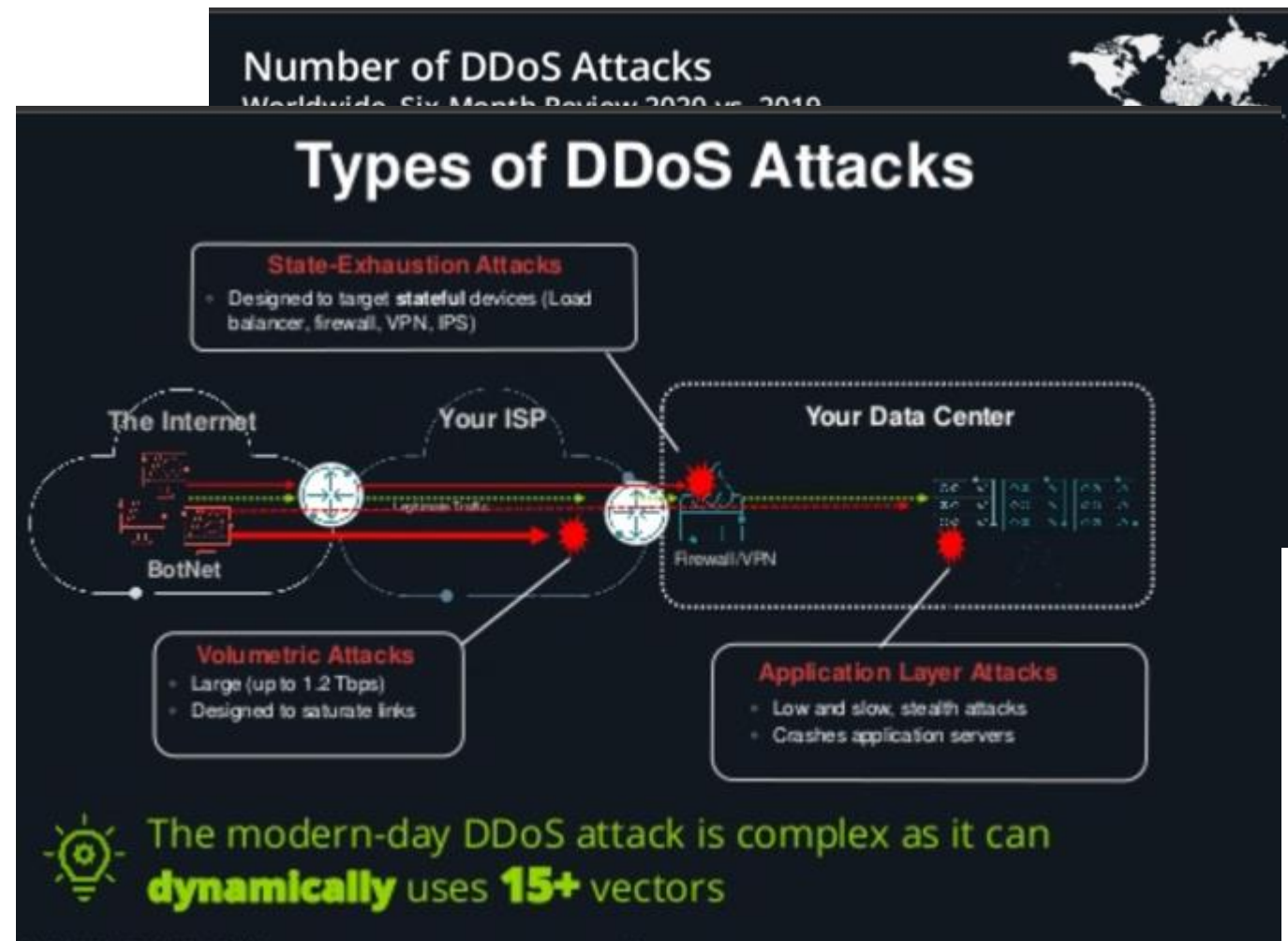


Exploiting humans

DENIAL OF SERVICE

«An interruption in an authorized user's access to a computer network, typically one caused with malicious intent»

Double «D» = multiple source so DISTRIBUTED DoS attack



DENIAL OF SERVICE





58% of Internet service providers suffered a multi-vector attack

65% of those declared that DDoS was in the top % concerns of 2019 and 2020

Victims are NO more able to sell, buy, communicate, send, receive, show, answer ... until they pay or do something to accomplish attacker requests

Telecommunications is hackers' choice

Telecommunications is number 1, 2, and 4 — out of 4 on the top sub-vertical sectors with a combined **1,991,927 attack frequency**.

Rank	Vertical	Attack Frequency	Max Attack	Classification
1	 Wired Telecommunications Carriers	1,073,851	421.5 Gbps	Information
2	 Telecommunications	575,749	348.9 Gbps	Information
3	 Data Processing, Hosting + Related Services	467,475	243.4 Gbps	Information
4	 Wireless Telecommunications Carriers	342,327	492.5 Gbps	Information

Let's understand in deep :

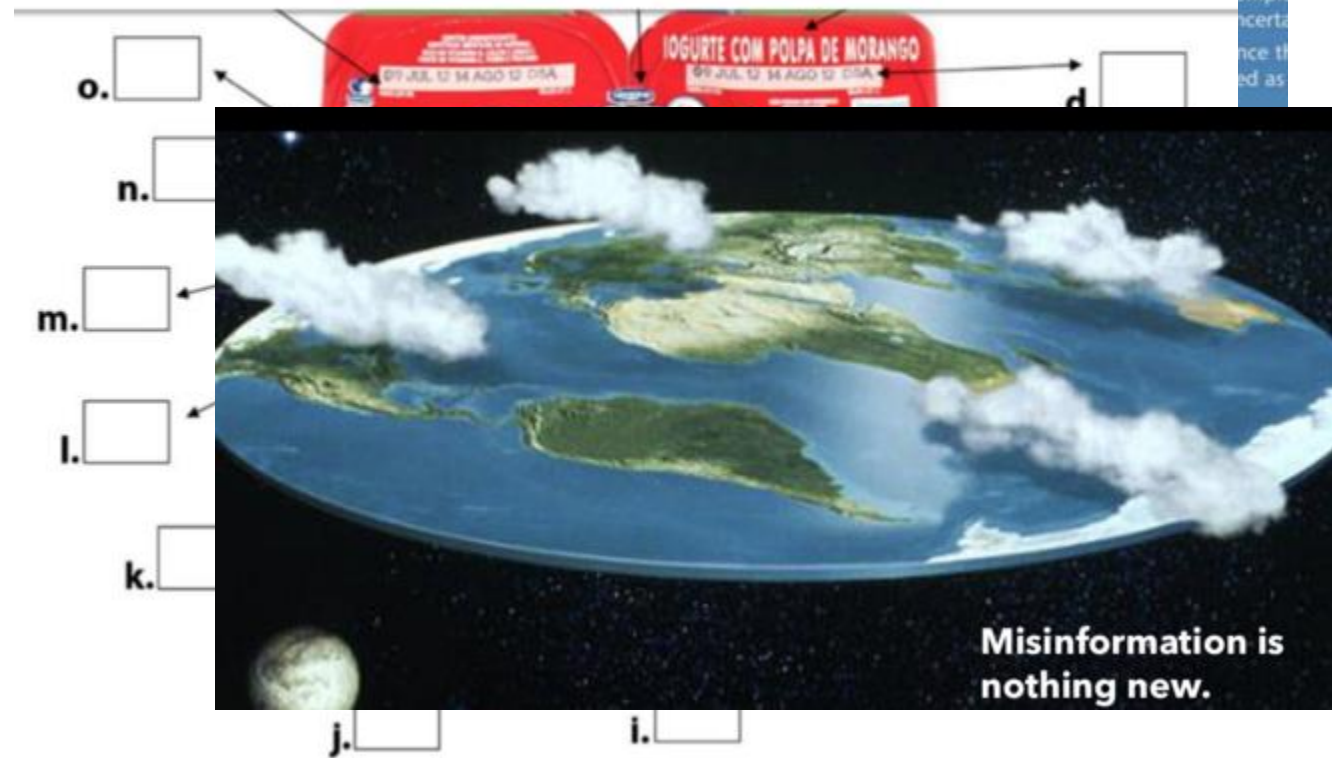
The action of disseminating deliberately false information, intentionally false or misleading is **DISINFORMATION**

while promoting a political cause or point of view is **PROPAGANDA** and information's can be false or true ...

Finally we do have **MISINFORMATION** when false or incorrect informations are shared with **NEUTRAL** intent

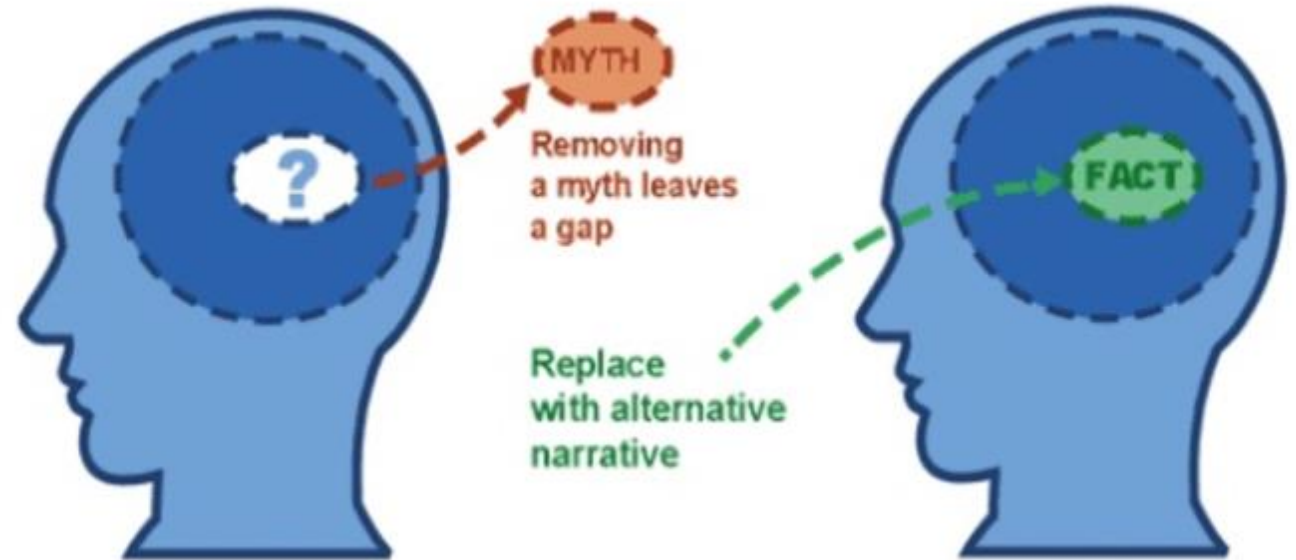
adopted by governments, corporations and non-profits to manage attitudes, partisan ideological and includes inter facts but may claim to be imp

Persuade -- Inform -- Entertain



Challenges:

1. **Exposure** to misinformation that's culturally reinforced outside the digital place
2. **Oversimplification** of the nuances data, due to lack of specific information (health, products, strategies)
3. **Worldview** and confirmation bias reinforce “don't know what you don't know” sample



The ART of Human Hacking or “how to obtain confidential information by manipulating and or deceiving people and artificial intelligence”

Social engineering attacks work because we’re imperfect creatures. The attackers know this, and they pray on our fundamental human nature to carry out their nefarious schemes. In this world of social media, they know how ready and willing we are to share personal information.

These attackers are trying to leverage our emotions. They know how primally we react to emotional triggers and exploit them accordingly.

How to obtain confidential information by manipulating and/or deceiving people and artificial intelligence

From «The Art of Deception» as a sample :

A person **gets out of a speeding ticket** by fooling the police into revealing a time when the arresting officer will be out of town and then requesting a court date coinciding with that time.

Do you remember the value of data ?

So important that we can compare every data theft or leak to and Oil&Gas Leak ...

Need to be prevented and in any case an alarm should start immediately when suspected. Damages if stay undiscovered are increasing exponentially.



Real time example

- Zeus Banking Trojan Hits Android Phones

<https://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909>

- Game Dunga

<http://blog.trendmicro.com/trendlabs-security-intelligence/one-click-billing-fraud-scheme-through-android-app-found/>

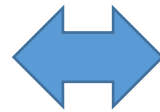
- "Your mobile number has won £850,000 IN **** Award Promo. Send your name, address and account number to bmwdept2011@live.com."

- GPS spoofing Ex:- Pokeman go (lower Android versions 6.0.1)

We told already : “it’s all about money”

Up to date, financial gains are the main reason or probably the stronger reason of cyberattacks.

75% of attacks are stealing credit cards information (to be sold or used), causing data breaches, demanding ransom with a two step procedure (crypto-locking it’s not the only trick) and stay hidden for more than 250 days in average



Economic impact:

The loss of IP and business-confidential information.

The cost of securing networks, buying cyber insurance and paying for recovery from cyber attacks

Reputational damage and liability risk for the affected company and its brand



MARITIME Economic impact:

Loss and damage to cargo.

Unexpected additional costs, e.g. storage.

Delays or disruption of supply chain.

Increased insurance premiums.

Increased prices of goods for consumers

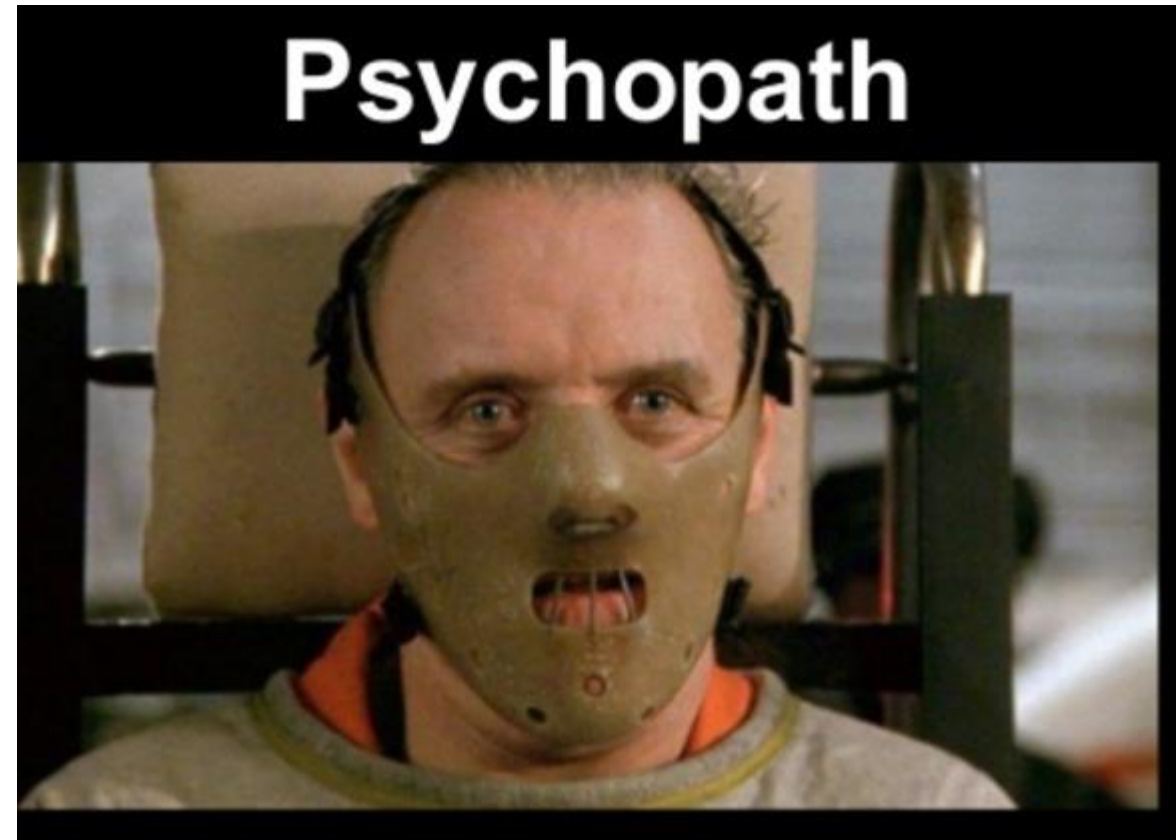


Why do people kill ?

Alcohol and drugs, mental illness, domestic argument ... then money and revenge

Why do Criminals hack and steal information?

MONEY and REVENGE or in some cases .. REVENGE and MONEY



Are Cybercriminals psychopath ?

The answer is «NOT always» :

They will eventually USE some dedicated subjects, commonly called hackers, to take advantage from the skills and to take the wanted revenge

REVENGE usually is related to Porno/Pedo cyber crimes BUT it can happen also «for REVENGE» when someone abuses of deep&dark web and buy a «revenge» activity like cryptolocking or DDoS or information stealing activity.



A specific target as a sample : AIS Systems

- Automatic tracking system for identifying and locating vessels
- 2002 – First mandate for vessels over 300GT to be equipped with a Class A type AIS transceiver.
- AIS information supplements marine radar, which continues to be the primary method of collision avoidance for water transport.
- Aid in accident investigation and in search and rescue operations.
- The information is also sent to providers such as Maritimetraffic.com, Vesselfinder.com or Aishub.net.
- Transmit in the Marine bands - Channel A 161.975 MHz (87B) & Channel B 162.025 MHz (88B).



AIS can send up to 27 types of messages

- Message 18 is sent between anywhere 30 seconds and 3 minutes to report the vessels position.
- Message 14 is a safety related broadcast used in emergencies.

Description	Value	Value Description
Vessel Name		
NMEA Sentence	!AIVDM,1,1,A,>3a`Tn1@E	
Sentence Type	!AIVDM	
Fragments in this message	1	
Fragment No	1	
Sequential Message ID	{none}	
Radio Channel	A	
Payload	>3a`Tn1@E=80tpiT	96 bits (16 6-bit words)
Fill bits * CRC check	0°52	
AIS Message		96 bits (12 8-bit words)
AIS Message Type	14	Safety Related Broadcast Message
Repeat Indicator	U	Repeatable
MMSI	244 983 000	Netherlands (Kingdom of the)
Spare	0	2 bits
Text	TEST ONLY	9 characters

- AIS communications do not employ authentication or integrity checks.
- Communication is made over RF
- Anyone with a cheap RF receiver can also “listen” to these messages.

(Range dependent)

Maritime security - AIS ship data

At its 79th session in December 2004, the Maritime Safety Committee (MSC) agreed that, in relation to the issue of freely available automatic information system (AIS)-generated ship data on the world-wide web, the publication on the world-wide web or elsewhere of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities and was undermining the efforts of the Organization and its Member States to enhance the safety of navigation and security in the international maritime transport sector.

The Committee condemned the regrettable publication on the world-wide web, or elsewhere, of AIS data transmitted by ships and urged Member Governments, subject to the provisions of their national laws, to discourage those who make available AIS data to others for publication on the world-wide web, or elsewhere from doing so.

In addition, the Committee condemned those who irresponsibly publish AIS data transmitted by ships on the world-wide web, or elsewhere, particularly if they offer services to the shipping and port industries.

AIS Spoofing

Hackers can send specially crafted messages that could mimic the location of an existing vessel, or even create a fake vessel and place it on its own virtual course.

Fake CPA

Hackers create a fake CPA (closest point of approach) alert.

Ship Hijacking

Hackers download the data of an existing ship, changing some of the parameters and submitting it to the AIS service.

Man-in-the-water

Because of maritime laws and best practices, everyone needs to address this type of an alert.

Replay Attacks

Hackers capture and store AIS data and replay spoofed messages in specific timeframes

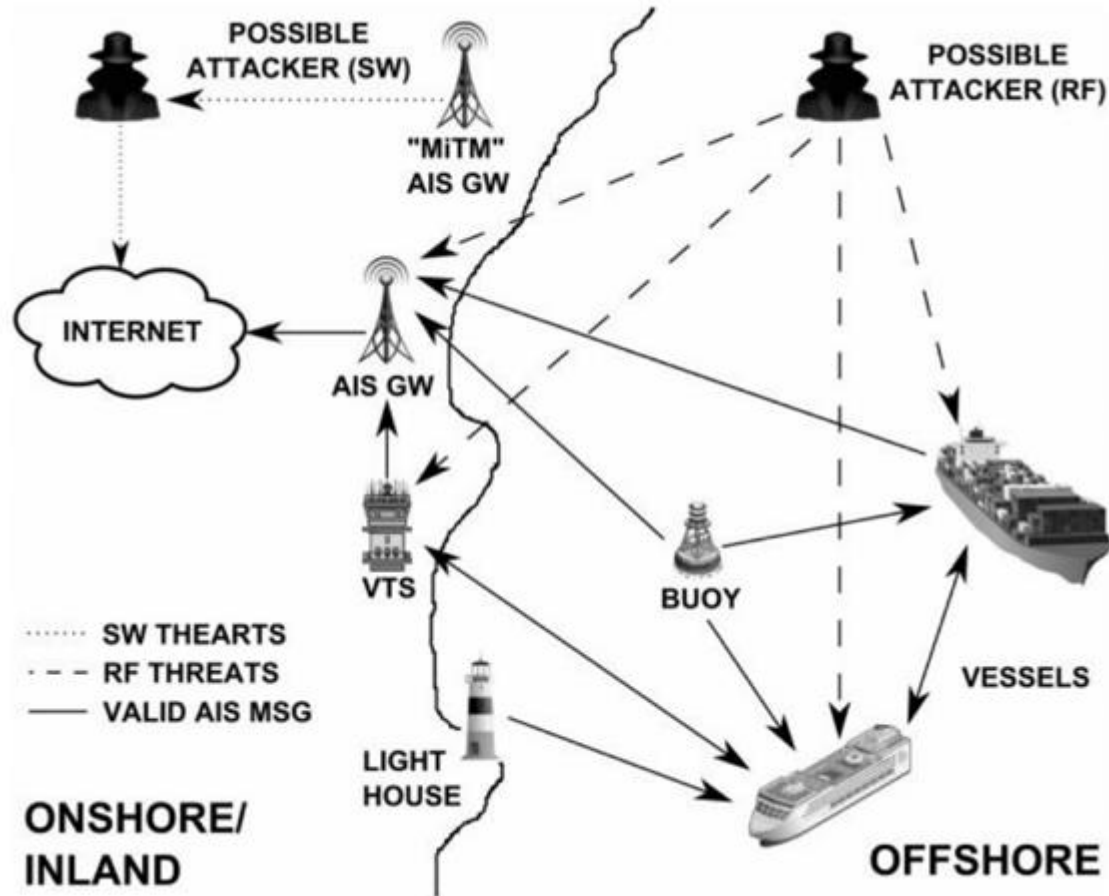
Arbitrary weather forecast

Hackers impersonate actual issuers of weather forecast such as the port authority and arbitrarily change the weather forecast delivered to ships.



- Modification of all ship details such as position, course, cargo, flagged country, speed, name & MMSI
- Creation of fake vessels e.g. having an vessel with nuclear cargo show up off the coast of the US
- Create and modify Aid to Navigations (AToN) entries, such as buoys and lighthouses.
- Research has been published in 2013 but since then there was not an improvement on the protocol
- ITU Radiocommunication Sector (ITU-R); the developers of the AIS standard and the protocol specification have acknowledged the problem





Even via RF the hackers have 4 attack vectors:

- AIS Gateway
- Vessel Traffic Service
- Vessels
- Offshore

An exaggerated example



1. 300 ton ships should not drive down the main street of a city

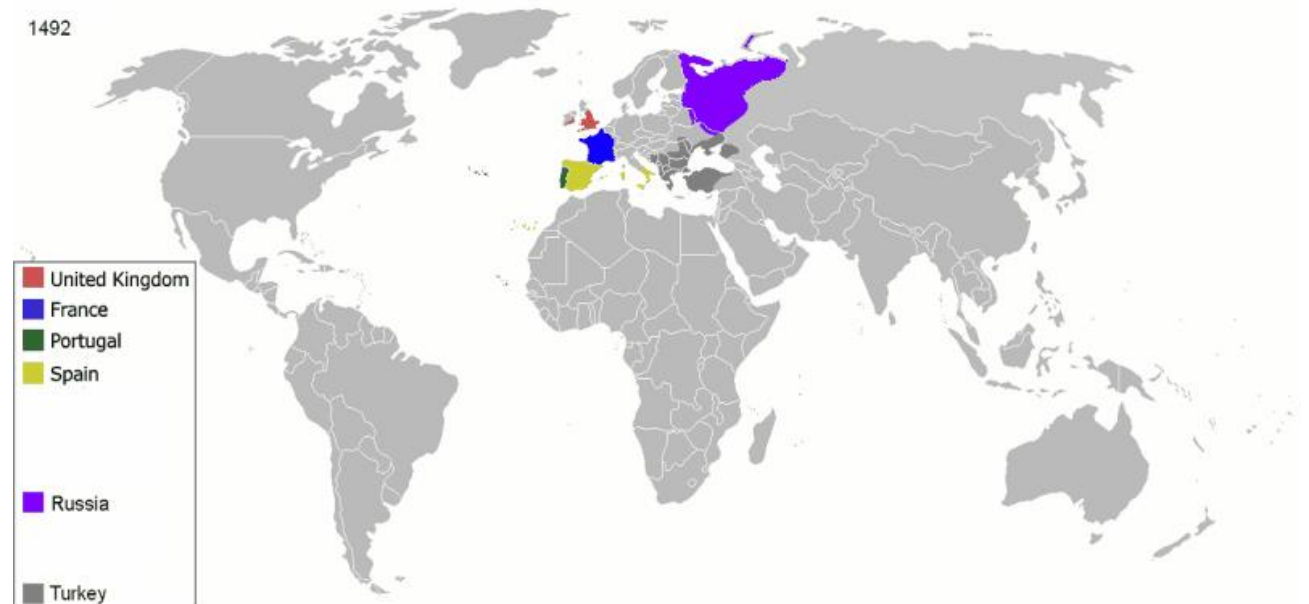
ROLE OF CYBER RANGE |

As per his name:
it's a testing platform, it's a place where to measure risks and take decisions in a LAB with no real human risk but with the best real life view and simulation.

It's a virtual environment that use actual network equipment, as required to simulate real life.

In our case, it's a large, complex, locally and remotely accessible infrastructure where all equipment and devices are provided by the cyber range vendor/operator, and malware and attacks may be safely run without fear of contaminating the business network

WE CANNOT FORGET THE IMPORTANCE BOATS ...



SESSION 2

ATTACKS IN DEEP

For whom survived to session 1



CISO being prepared with a strong cybersecurity posture:



Hackers:



Common or uncommon ?

Malware. A malicious software, including spyware, ransomware, viruses, and worms. ...

Phishing. ...

Man-in-the-middle **attack.** ...

Denial-of-service **attack.** ...

SQL injection. ...

Zero-day exploit. ...

DNS Tunneling.

And many more

- **Fraudulent emails** (75%) remain the most widely used and successful attack on businesses and individuals alike. Most cyber attacks start with phishing emails, exploiting human vulnerabilities, and infecting computers with ransomware or other types of malware. Advanced malicious tools, phishing kits and targeted attacks on specific businesses are expected in 2019.
- **Viruses/spyware/malware** (24%) is the second most common attack that will continue bringing sizeable damage. Viruses lead to various malicious effects including deleting or stealing information, downloading malicious programs, providing hackers with unauthorized access to the computer, and more. Spyware allows criminals to collect user information, credit card credentials, user passwords, and other personal information.
- **Ransomware** (15%) is the growing threat that allows bad actors to automate the attacks, and thus increase their scale and profits from hacks. It blocks the user or the company from the computer or the whole network demanding money compensations. It's on the boom targeting high-net-worth victims.
- **Unauthorized access** (15%) can be performed via various malicious techniques and instruments. It leads to information theft that many organizations are now suffering from.
- **Denial-of-service attacks** (12%) are aimed at preventing users from server access. This type of cybercrime can lead to noticeable disruption or complete unavailability of the server, causing further network intrusion and loss of sensitive data.

ATTACKS IN DEEP | "bad things" ...

AT LEAST 8

BUGS

WORMS

VIRUS

BOTS









TROJAN HORSES

RANSOMWARE

ADWARE

SPYWARE

Types of Malware

 <p>BUGS A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.</p>	 <p>WORMS A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.</p>
 <p>VIRUS A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.</p>	 <p>BOTS A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.</p>
 <p>TROJAN HORSES Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.</p>	 <p>RANSOMWARE Ransomware denies access to your files and demands payment, through Bitcoin in order for access to be granted again.</p>
 <p>ADWARE A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.</p>	 <p>SPYWARE A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.</p>

RANSOMWARE

is malicious software, or malware, that encrypts the information on a person's computer like documents, photos and music.

It will not release these files until the user pays a fee — or ransom — to unlock these files and get them back. Ransomware has quickly become the most profitable type of malware ever seen, on its way to becoming a \$1 billion annual market.

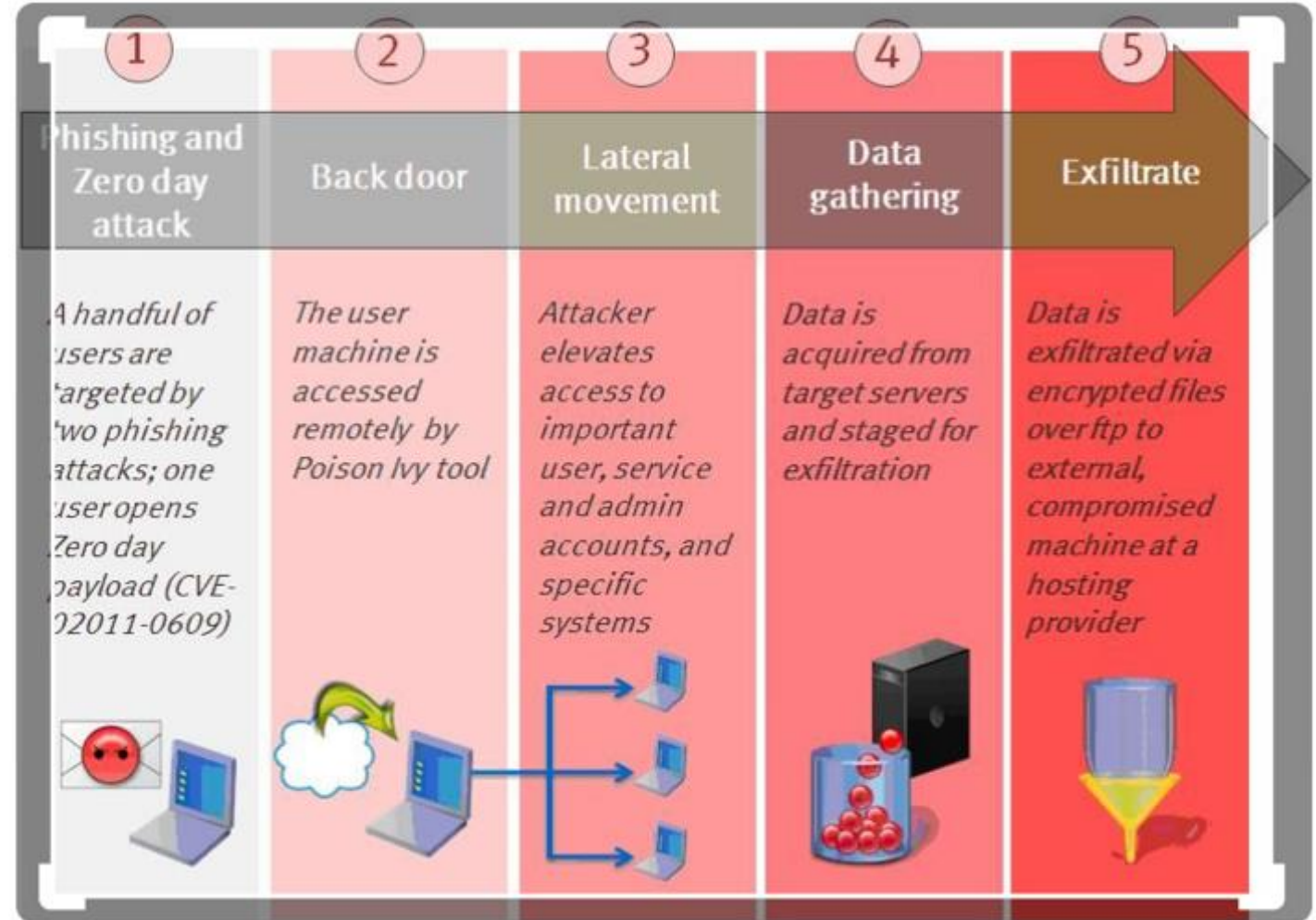
Ransomware is typically distributed through a few main avenues. These include email phishing, malvertising (malicious advertising), and exploit kits.

After it is distributed, the ransomware encrypts selected files and notifies the victim of the required payment.

Attack anatomy (simplified version)

After studying the target, from wifi or usb or email someone delivers into a first victim unit a software

This one will start the process



War Driving and Rogue AP

Most common cases

War driving is the practice of attempting to sniff out unprotected or poorly protected wireless networks

Rogue AP Attack is made by installing/activating an unauthorized AP used by USERS

Evil twin attack is an unauthorized AP, with an SSID similar or equal to the original one and will get all users keystrokes



War Driving and Rogue AP

Most common cases

War driving is the practice of attempting to sniff out unprotected or poorly protected wireless networks

Rogue AP Attack is made by installing/activating an unauthorized AP used by USERS

Evil twin attack is an unauthorized AP, with an SSID similar or equal to the original one and will get all users keystrokes



Summary

Jamming : so many packets here ... that nothing will work anymore – less working on 802.11.n/ac

BlueJacking/snarfing attacks were the first is DOS similar – many requests, no way to answer while the second is connection without other party auth

NFC attack – easy like everyone know : that's enough to READ at low distance the infos (ex. Contactless Credit cards ...)



Summary

Jamming : so many packets here ... that nothing will work anymore – less working on 802.11.n/ac

BlueJacking/snarfing attacks were the first is DOS similar – many requests, no way to answer while the second is connection without other party auth

NFC attack – easy like everyone know : that's enough to READ at low distance the infos (ex. Contactless Credit cards ...)



Types of NFC transactions
PHOTO: GLOBAL TAG

WSN wireless sensor network

Collection of sensor nodes, small, low cost, short distance comm capabilities and ...

VULNERABLE :

Limited processing capabilities

Inability to secure wireless medium

Physical tampering

Limited power



Attacks :

DOS that make the sensor unavailable

JAMMING since they don't use spread spectrum technology

HELLO FLOOD attacks

WORMHOLE attacks – disrupt routing

Wireless encryption

Unfortunately **ALL** the actual wi-fi deployed encryption standards

CAN BE BROKEN

From 3 to 5 seconds to find a 8 to 10 digit WEP key

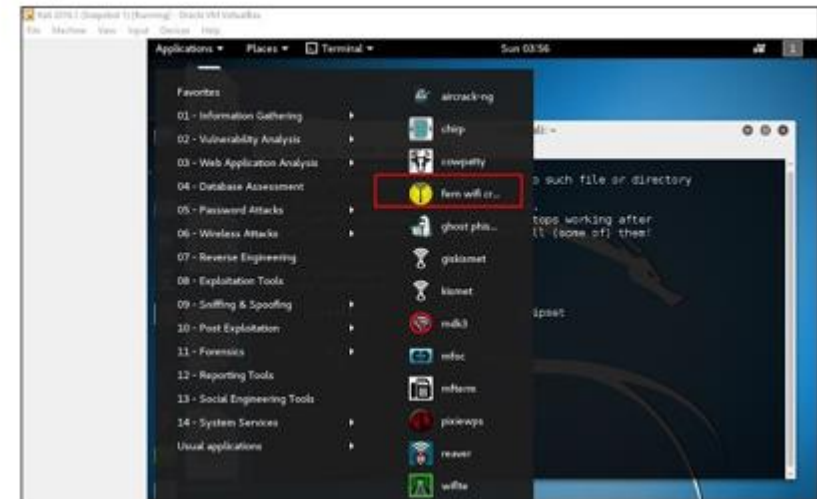
From 30 to 180 seconds to build a WPA key if shorter than 10 digits

Forget WPS al all – disable it on every device, brute force attacks available since 2011 and never solved

Receiving enough packets, the attacker can start the key cracking process

Being able to find/read/sniff the initialization vector means getting enough material to rebuild the key.

Step 1 – Applications → Click "Wireless Attacks" → "Fern Wireless Cracker".



Wireless encryption

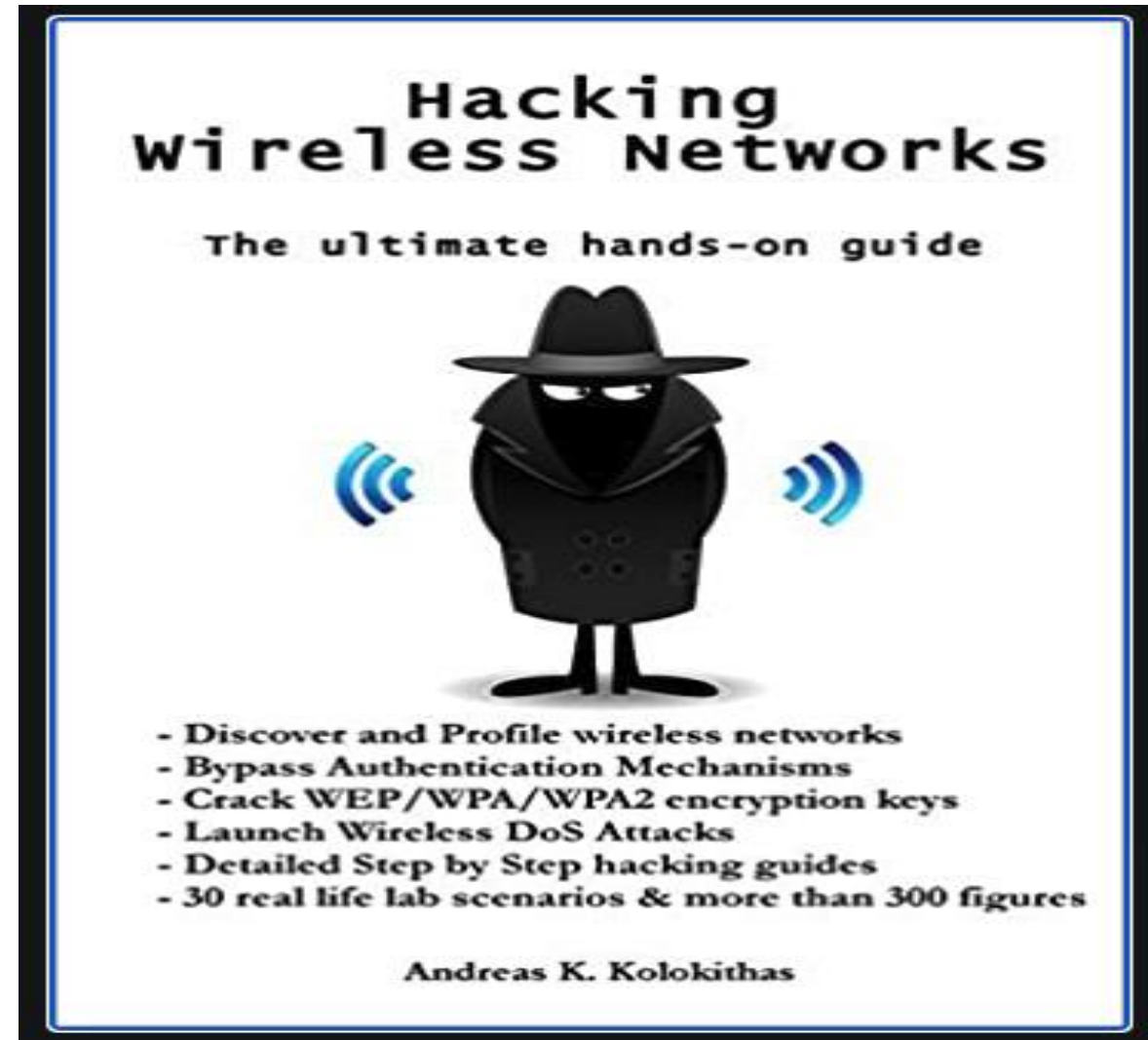
Unfortunately **ALL** the actual wi-fi deployed encryption standards

CAN BE BROKEN

From 3 to 5 seconds to find a 8 to 10 digit WEP key

From 30 to 180 seconds to build a WPA key if shorter than 10 digits

Forget WPS al all – disable it on every device, brute force attacks available since 2011 and never solved

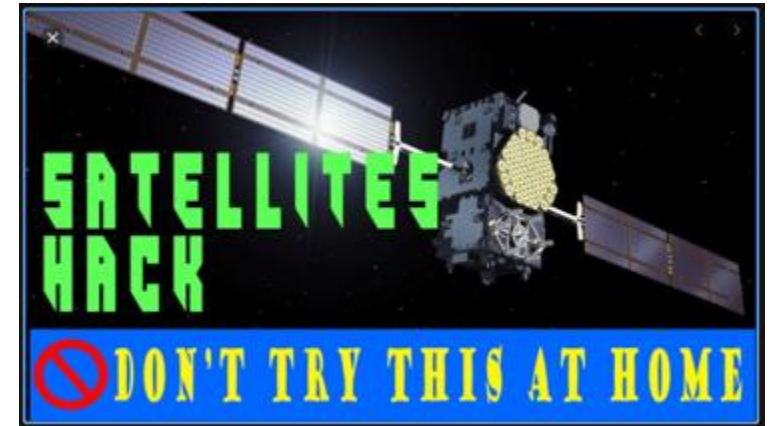


Main vulns :

Inconsistent software patching, weak encryption, and old IT equipment are key vulnerabilities to satellite networks.

Legacy satellite communications platforms are not easily updated and must undergo significant testing to ensure that upgrades for communications, encryption, or improved operability with next-generation platforms will not interfere with other, possibly critical, system functions.

High presence of legacy IT or OT system vulnerabilities «embedded» and left alone ...



And ground systems ?

Ground systems are the most vulnerable weak points in a hierarchy that starts with the TT&Cs/Satellite Operations Centers (SOCs) and flows down through the Network Operation Centers (NOCs) and gateways, teleports, and earth terminals



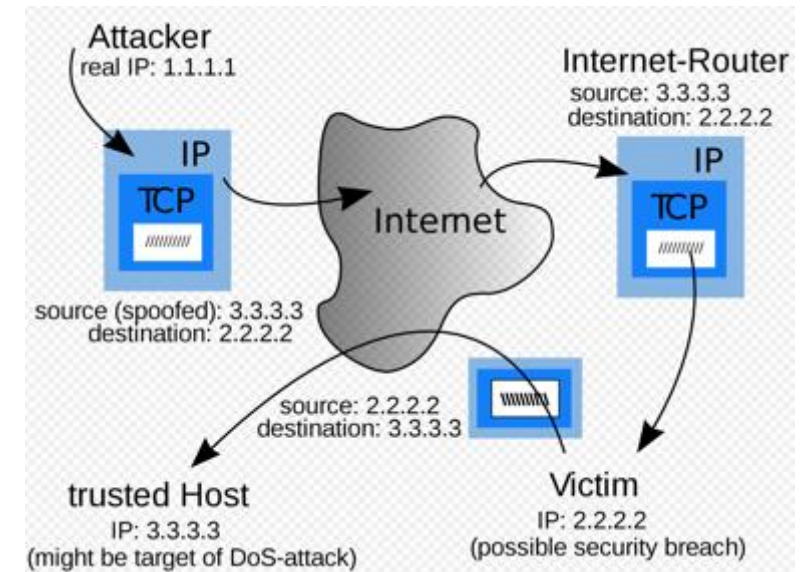
Worst case scenario :

Hijacking is illegal transmission using a satellite, or taking control of a signal such as a broadcast and switching it with another (Paganini, 2013). Whereas Controlling is the most difficult form of hacking, in which hackers control an orbiting satellite by breaching and taking control over the TT&C ground station, payload, or/and bus that.

Ip spoofing :

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

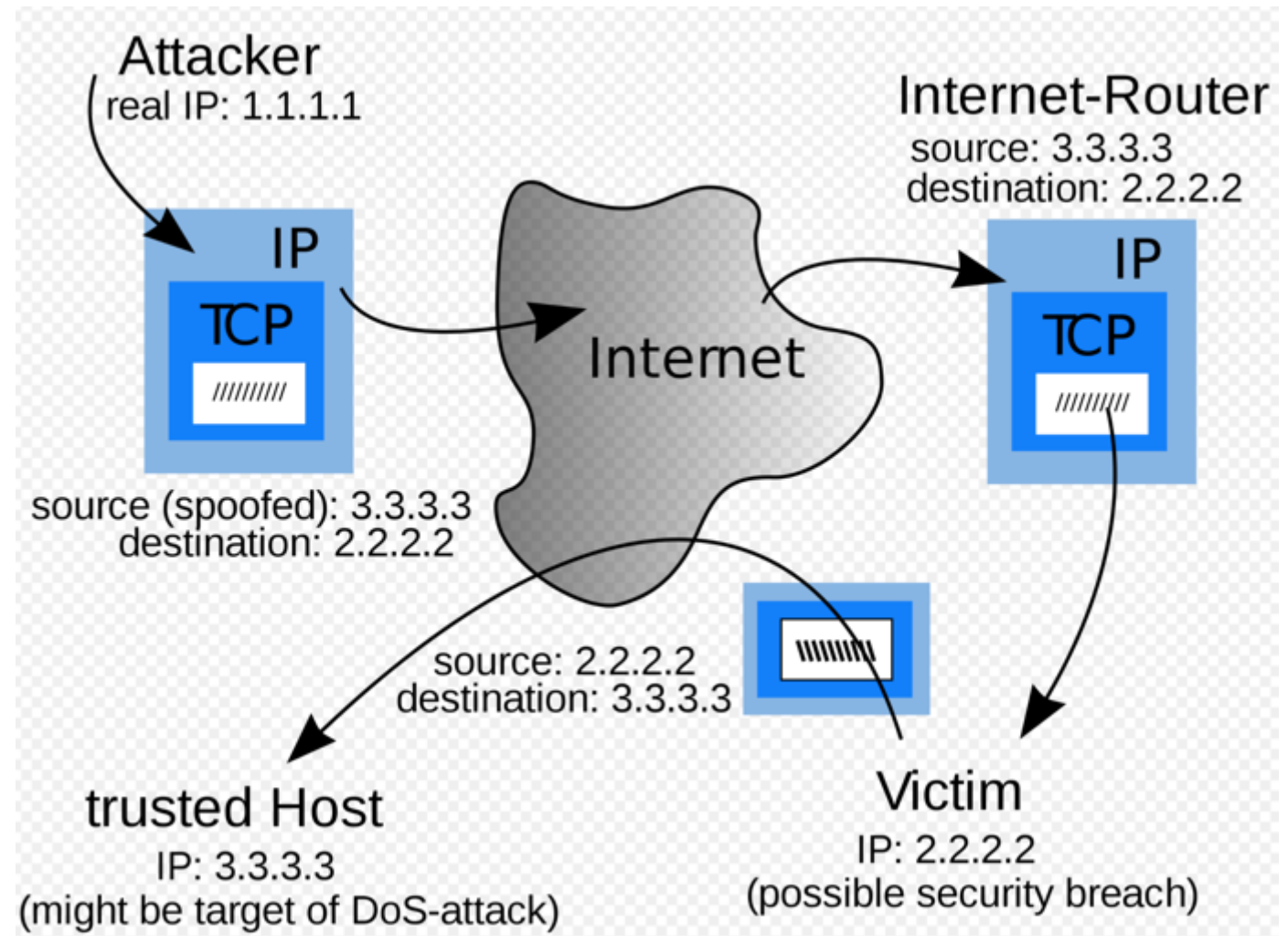
DDoS attacks will often utilize spoofing with a goal of overwhelming a target with traffic while masking the identity of the malicious source, preventing mitigation efforts. If the source IP address is falsified and continuously randomized, blocking malicious requests becomes difficult. IP spoofing also makes it tough for law enforcement and cyber security teams to track down the perpetrator of the attack.



Ip spoofing :

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

DDoS attacks will often utilize spoofing with a goal of overwhelming a target with traffic while masking the identity of the malicious source, preventing mitigation efforts. If the source IP address is falsified and continuously randomized, blocking malicious requests becomes difficult. IP spoofing also makes it tough for law enforcement and cyber security teams to track down the perpetrator of the attack.



Email spoofing, or whaling and spear phishing :

Email spoofing is a very popular attack method. The sender modifies message headers so that emails appear as sent from someone else. Hackers use it, for example, to impersonate employees of a company to obtain login credentials, personal data, or other confidential information.

```
mail from: dude1@domain1.com
rcpt to: dude2@domain2.com
data
-----
From: Dude1 <dude1@domain1.com>
Subject: Nice To Meet You!
Date: February 13, 2018 3:30:58 PM PDT
To: dude1 <dude1@domain1.com>
Reply-To: dude2 <dude2@domain2.com>
-----
Hi Dude1,
It's nice to meet you!
```

Envelope

Header / Body

The box in red above highlights the email's envelope. Normally the envelope fields are filled out for the sender automatically during the translation of the header. Neither the sender nor the recipient usually sees this information. The stuff in blue is the header and body. This is the stuff you normally see when you open an email that was sent to you.

It is possible for the sender to tinker with the message header and spoof the sender's identify so the email looks like it is from someone other than Dude1. Let's break down how.

Say you have a friend that likes to play practical jokes on you. And you receive an email from them that says this:

```
mail from: dude1@domain1.com
rcpt to: dude2@domain2.com
data
-----
From: BossMan <bossman@domain1.com>
Subject: Raise!
Date: February 13, 2018 3:30:58 PM PDT
To: dude1 <dude1@domain1.com>
Reply-To: BossMan <dude2@domain2.com>
```

The structure of email

Why can't we just harden email like we do a firewall and turn it into a tank? Because email wasn't built with security in mind. It was invented in the 1960's and the original standard, RFC 822, was written in 1982. Updated standards weren't written until 2008, which contain the current email structure that we all know and are comfortable with.

Email as we know it today consists of three major sections:

The envelope The message header The message body ...

The structure of SPOOFED email

Usually the envelope fields are correct, **but the From and Reply-To are false**. When Dude1 receives this email, he may think it's from his boss. When he hits "Reply" all he'll see in the To: field is the "BossMan" name, but it will go back to his friend who spoofed the email, Dude2.

According to the FBI, this type of scam has siphoned more than \$2.3 billion from more than 17,000 victims—and those are just reported incidents. Impostor emails succeed for three primary reasons:

They look and feel legitimate

They do not include a malicious link or malware attachment

They do not arrive in high enough volumes to raise red flags in most anti-spam tools

What is Jamming ?

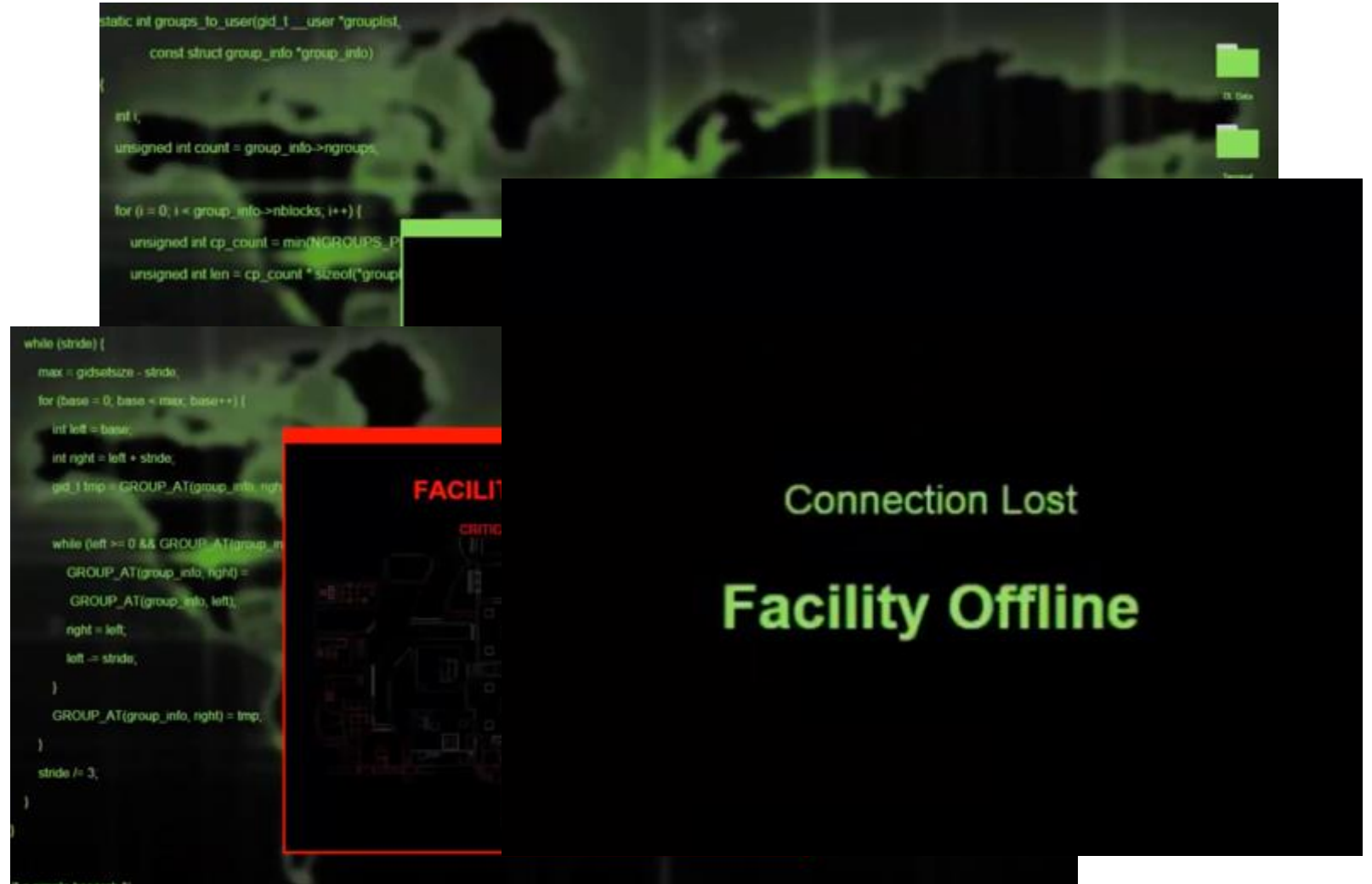
Jamming is a technique in which a receiver is overloaded with a high power transmission of jamming signal from another transmitter.

It's an INTENTIONAL radio noise, created to block a receiver from getting required radio signal



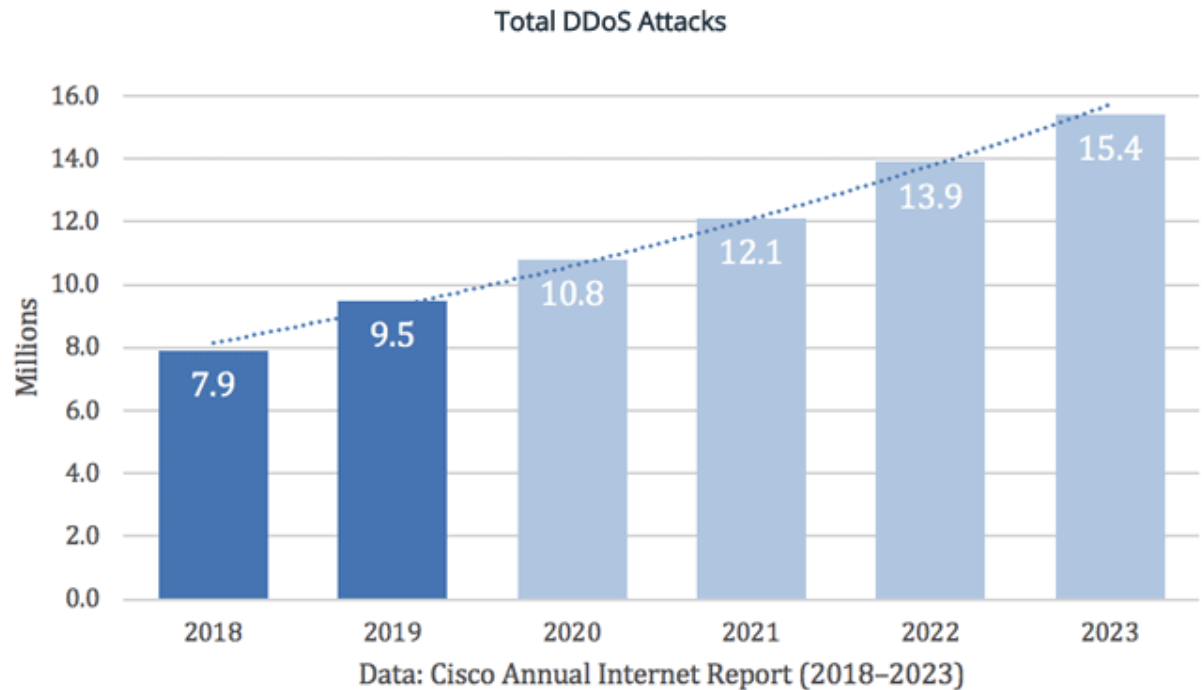
Denial-of-service

(DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor



The first known Distributed Denial of Service attack

Occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack.



5 top DDoS attacks of the last 10 years

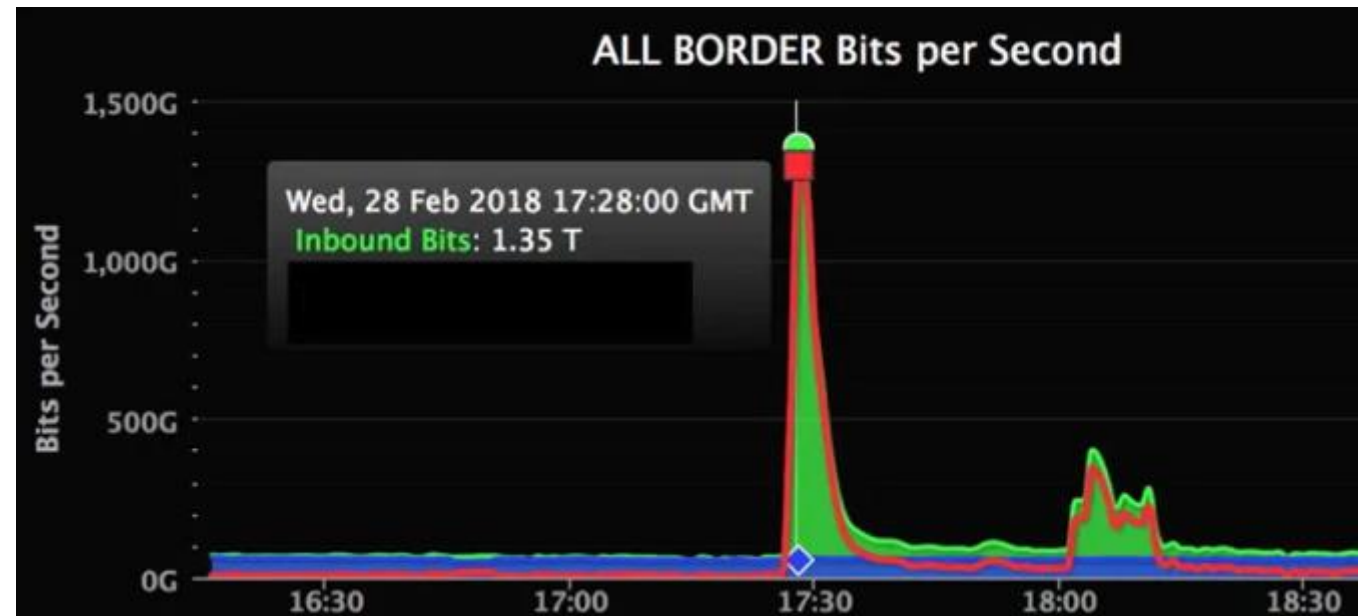
The AWS DDoS Attack in 2020

The Mirai Krebs and OVH DDoS Attacks in 2016

The Mirai Dyn DDoS Attack in 2016

The GitHub Attack in 2018

The Six Banks DDoS Attack in 2012



Some DoS and DDoS technique :

DNS flood where an attacker floods a particular domain's DNS servers in an attempt to disrupt DNS resolution for that domain. If a user is unable to find the phonebook, it cannot lookup the address in order to make the call for a particular resource

Memcached attack is a type of cyber attack in which an attacker attempts to overload a targeted victim with internet traffic. The attacker spoofs requests to a vulnerable UDP memcached* server, which then floods a targeted victim with internet traffic, potentially overwhelming the victim's resources.

SYN flood (half-open attack) is a type of DDoS which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

Common DDoS Attacks	DDoS Attac
Memcached DDoS Attack	
NTP Amplification Attack	gation st
DNS Amplification Attack	n solutions
SSDP Attack	each invol
DNS Flood	capable c
HTTP Flood	structure u
SYN Flood Attack	based DD
UDP Flood Attack	
Ping (ICMP) Flood Attack	ive solutio
Low and Slow Attack	e growing
Application Layer Attack	l, and ther
Layer 3 Attacks	s capable
Cryptocurrency Attacks	
ACK Flood Attack	e to create
QUIC Flood Attack	al time. Th
Smurf Attack (historic)	work is a c
Ping of Death (historic)	a seatbel!

but when that time comes it be
the success of any protection s
reliability engineers working 24
Redundancy, failover and an ex
of the platform.

Misinformation can be a WEAPON

Covid-19 fake news exploited thanks to false information shared by misinformed or misguided individuals. Someone went in wrong direction due to those informations And died



Real or Fake News Card Game, Party Games

«Believe me or not It's the era of testing IQ and Intelligence as well as learning how Misinformation works»

«DAILY LANE CLOSURES DUE TO ZOMBIES»
hacked sign caused 9% vehicles to exit from the highway at that time



Phishing it's already a Social Engineering attack.

1. *Spear Phishing*
2. *Pretexting*
3. *Vishing*
4. *Baiting*
5. *Tailgating*

6. *And «talking with people», by phone or in person !*

A Coordinated Social Engineering Attack Hacks Twitter.

Where has Privacy gone?



PREFER INDIAN! PREFER PIXALIVE!

INSTALL NOW

GET IT ON Google Play

Download on the App Store

Scareware, baiting, phishing and spear phishing

Given that social engineering attacks remain the most commonly used techniques, it becomes obvious that hackers focus on exploiting the human factor as a weakness. Even the well-designed security systems could be undermined via a single malicious act aimed at the human factor.

The weak links in your organization's cybersecurity system can come in many forms but it doesn't mean that the system can't be protected effectively.

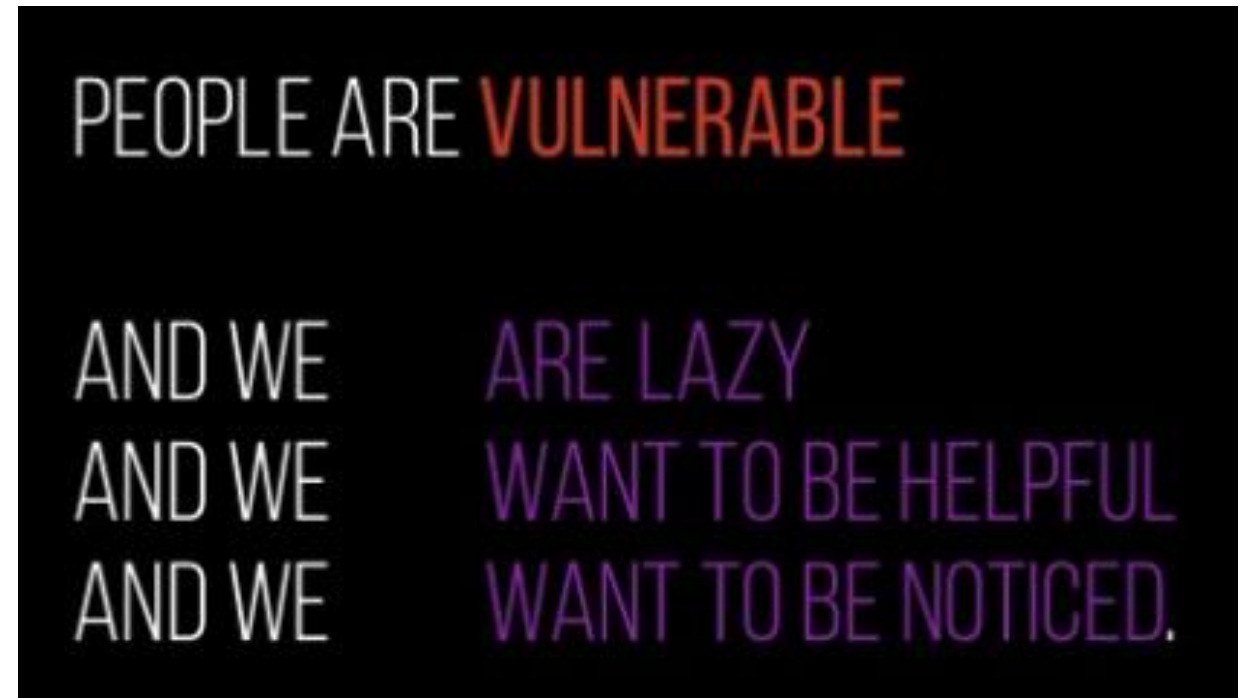
Measuring people vulnerabilities ?

People shame and blame

People make others feel bad for their behavior

And people avoid testing because it makes them feel vulnerable

And YOU don't like to feel vulnerable, isn't it ?



What can be stolen ?

1. Supplier list
2. Testing procedures
3. Prototypes
4. Corporate strategies
5. Staff details, including personal infos
6. Company capabilities and weaknesses
7. Ideas
8. Designs
9. Chemical formulas
10. Business methods
11. You can add “everything” here

Why ?

1. Money
2. Money
3. Guess

How ?

USB attacks

Phishing emails

An interesting dinner

A strange SMS

Or the well known
“Evil Maid attack” that
still works



Was 2009 when ...

... **Alex Tereshkin** got some spare time and implemented the **Evil Maid** TrueCrypt system disk encryption of a small bootable **USB** that allows to perform the attack in a “plug-and-play” way.

The whole infection procedure is very quick, in a few minutes, and **it's well suited for hotel maids**

... But then you have an appointment at the hotel SPA (at least this little fun you can have on a business trip, right?). Obviously you don't want to look so geeky and you won't take your laptop with you to the SPA, will you? The Evil Maid just waited for this occasion... She sneaks again into your room and powers up your laptop. She presses a magic key combo, which results in the Evil Program displaying the sniffed decryption password. Now, depending on their level of subtleness, she could either steal your whole laptop or only some more important data from the laptop. Your system disk encryption software is completely useless against her now.

a hotel room and go down for a breakfast... Meanwhile an Evil Maid enters your room. She holds an Evil USB stick in her hand and plugs it into your laptop and presses the power button. The system starts and boots from the USB. Your [BluePillBoot](#) (or [BluePillBoot I EEPROM](#)). This Evil program bypasses the encryption and restores the data back to the system. You can't brush your teeth after breakfast, refrain from not taking a shower, you just need to enter the password, whatever. Your system will be prompted, like if you don't know the password, it possibly know the password has not been loaded a moment ago from the MBR or a PCI EEPROM? It can not! So, you enter the valid password, your system gets the

SMS Malware and via E-Mails :

6 years ago : Pony Loader, also referred to as Fareit, has been around for a few years and has the ability to steal sensitive information from a victim's computer and install additional malware. This may include taking stored credentials for email, web and FTP accounts. In the past, Pony has been used to distribute the P2P GameOver Zeus Trojan.



Insight at SCADA hacking incident

Stuxnet. ...

Night Dragon. ...

Duqu, Flame, and Gauss. ...

Shamoon - Saudi Aramco and RasGas. ...

Target Stores. ...

New York Dam. ...

Havex. ...

German Steel Mill

Stuxnet

In 2010, Stuxnet was the one of the most complex malware known. It infected control system networks and it was presumed by some to have damaged as many as one-fifth of the nuclear power centrifuges in Iran.

The Stuxnet malware was a wake-up call to SCADA systems around the world because it was considered ***the first known threat to target specifically SCADA systems in order to control networks***. The US Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Team ([ICS-CERT](#)) issued multiple guidelines on how to defend against the Stuxnet malware, which also infected systems in the US.

Duqu, Flame, and Gauss / 1

In 2011, Hungarian cyber security researchers discovered three ***information-stealing malware***: Duqu, Flame, and Gauss. It is believed that these three malware are related since they all use the same framework.

Duqu was a malware designed to perform information gathering. It was designed to attempt to hide data transmissions as normal HTTP traffic by attaching encrypted data to be extracted in a .jpg file.

Flame is a complex malware designed to steal information by using: Microphones. Web cams. Key stroke logging. Extraction of geolocation data from images.



Duqu, Flame, and Gauss / 2

The malware **Gauss** is also intended for information stealing. It gathered the following information from the attacked systems:

Passwords, cookies, and browser history by intercepting user sessions in different browsers.

An important point to keep in mind from the Duqu, Flame, and Gauss information-stealing malware is **how complex attacks can be.**



-  www.Cyber-MAR.eu
-  [Cyber_MAR](#)
-  [Cyber-MAR EU Project](#)
-  [Cyber-MAR](#)
-  info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Partner's logo

Speaker, Institution



Contact details of the speaker



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389