

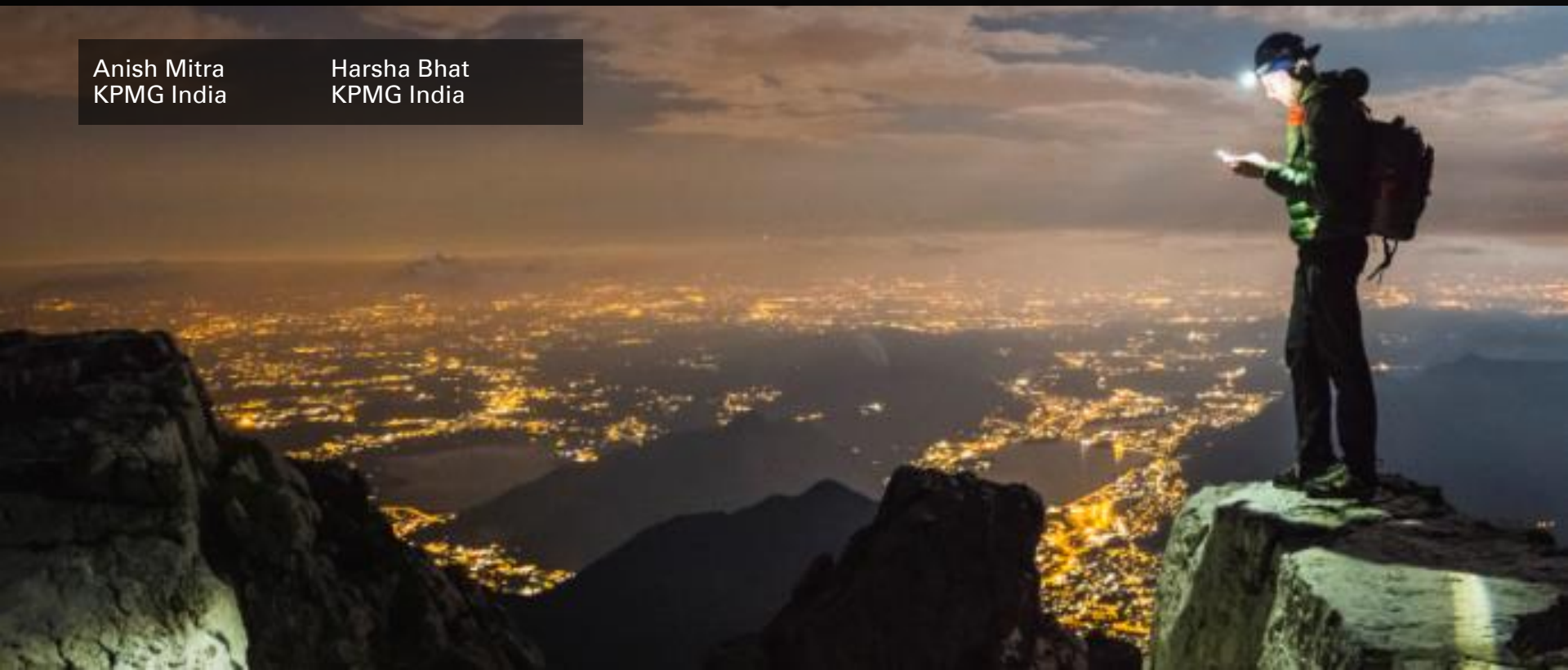


Who turned off the lights!

The State of Industrial Control System Security Implementation

Anish Mitra
KPMG India

Harsha Bhat
KPMG India

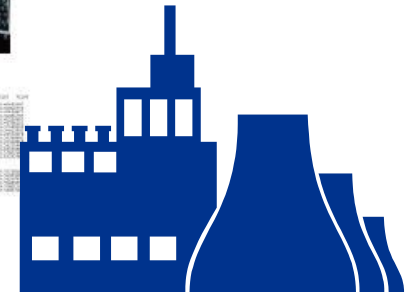


Introduction | Industrial Control Systems

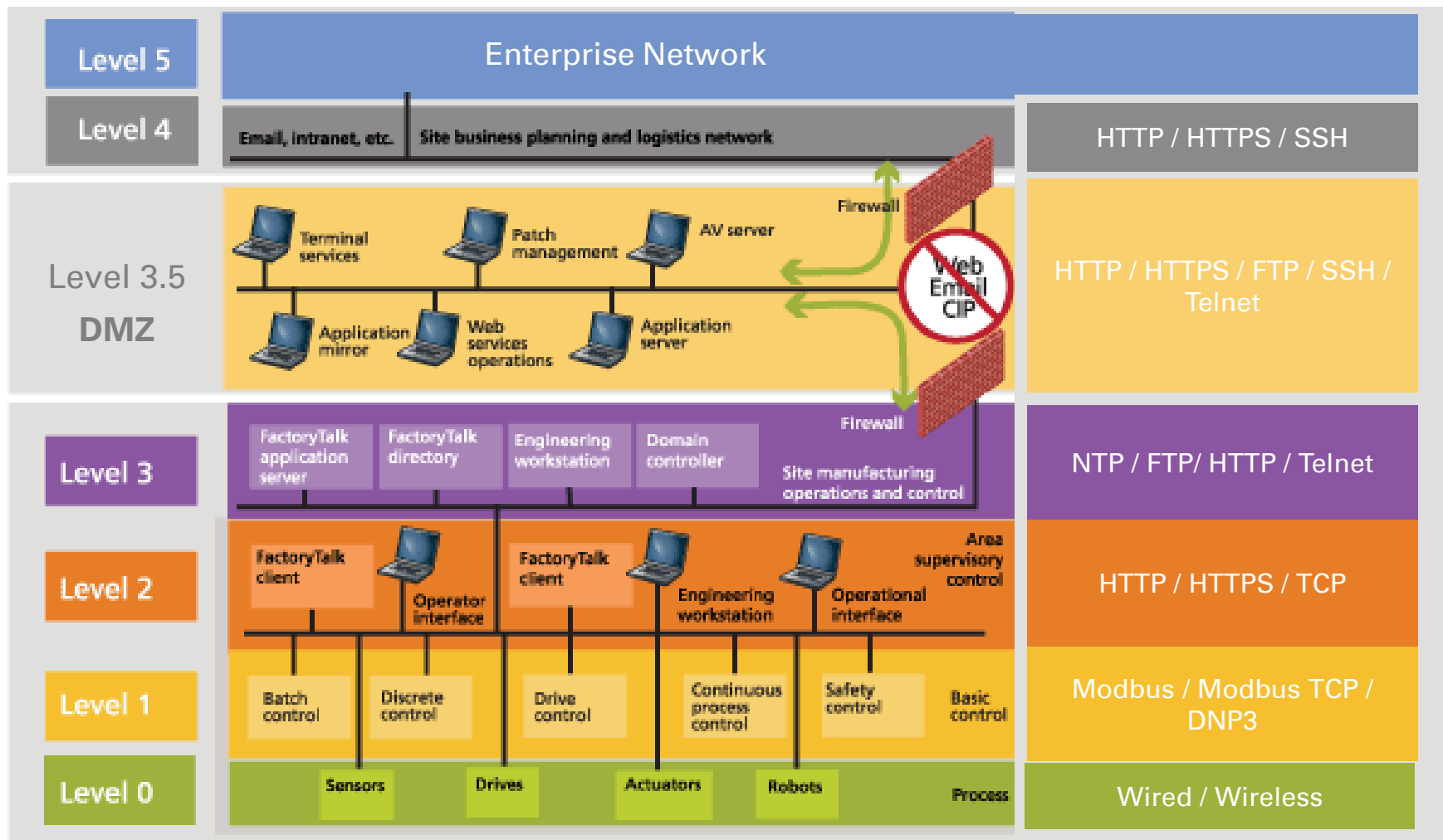
What are Industrial Control Systems?

Industrial control system (ICS) is a term used to describe an umbrella of control systems and automation instrumentation that include logic controllers, networks, servers and application software

- ➔ **Sensors and actuators:** allow interaction with the physical world (pressure sensor, valves, motors, ...)
- ➔ **Local HMI:** Human-Machine Interface, permits the supervision and control of a subprocess
- ➔ **PLC:** Programmable Logic Controller : manages the sensors and actuators
- ➔ **Supervision screen:** remote supervision of the industrial process
- ➔ **Data historian:** Records all the data from the production and Scada networks and allows exporting to the corporate IS (to the ERP for instance)



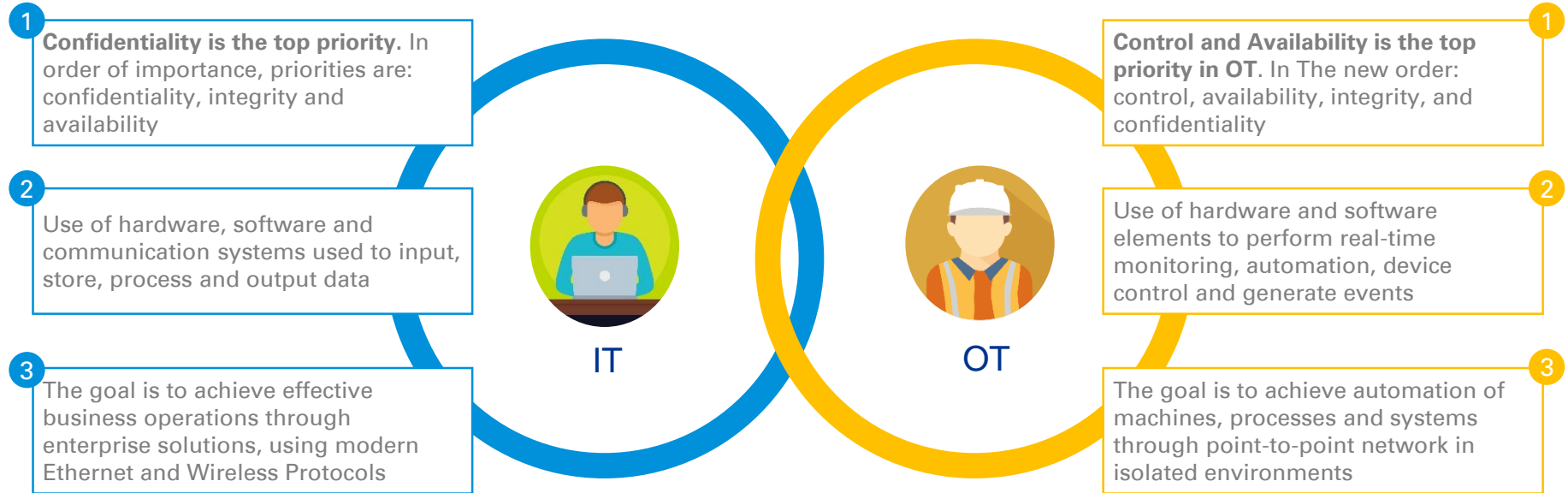
Purdue Model | Blueprint of Standard OT Network



ICS Threat Landscape

IT	Enterprise Infrastructure	Level 4	<ul style="list-style-type: none"> Malware Injection through USB Drives Vulnerable version of software in use Lack of adequate security policies Lack of intrusion detection and prevention systems 	<ul style="list-style-type: none"> Untrained professionals Lack of awareness Improper segmentation of legacy systems Change management Patch management Configuration management Asset Management Virtual environment Backup management Supply chain Decommissioned devices Identity and access management Undefined policies and procedures
	Antivirus, Terminal Services, Patch Management	Level 3.5	<ul style="list-style-type: none"> Remote access to OT system Misconfigured firewall IT Related Risks Improper logging and monitoring Improper network segmentation. 	
OT	Historian, Active Directory, Engineering Stations	Level 3	<ul style="list-style-type: none"> Default configurations are used OS and application security patches Inadequate testing of security changes 	
	SCADA/ Historian / Application Server	Level 2	<ul style="list-style-type: none"> Insecure remote access on ICS components Dual network interface cards (NIC) to connect networks 	
	PLC/ DCS / RTU/ Local HMI	Level 1	<ul style="list-style-type: none"> Insecure transport layer security Lack of authentication and authorization Denial of Service Data unprotected on portable device 	
	Sensors, Pre-Actuators & Actuators	Level 0	<ul style="list-style-type: none"> Physical Damage Hardware Tampering Malicious Hardware Mounting Electromagnetic Interference and Discharge 	

When worlds collide | The IT-OT Security Convergence



Convergence of IT and OT domains have given rise to shared Cyber Security concerns



Open-ended access to all devices emerging out of the IT network which allow remote control of OT devices



Wide range of OT protocols which use cleartext communication that allows eavesdropping



Advanced threat vectors acting on the OT network causing not only data loss but potentially could harm the human life as well

IIoT / SMART Factories | Changing Attack Vectors

Drivers for IIoT / Smart Factory and Security

Smart Maintenance Systems

- Autonomous maintenance systems would add more attack vectors to the picture

Self-driving vehicles

- The attack vectors on wireless communication would add-on due to autonomous vehicles on the shop floors

Robotic Fixtures

- The robotic fixtures would be maintained and controlled through mobile apps

Smart Supply Network

- Connected inventory tracking and supply chain

Mobile Workforce

Attack Gains



Intellectual Property



Service Disruption



Physical Harm



Monetary Gains

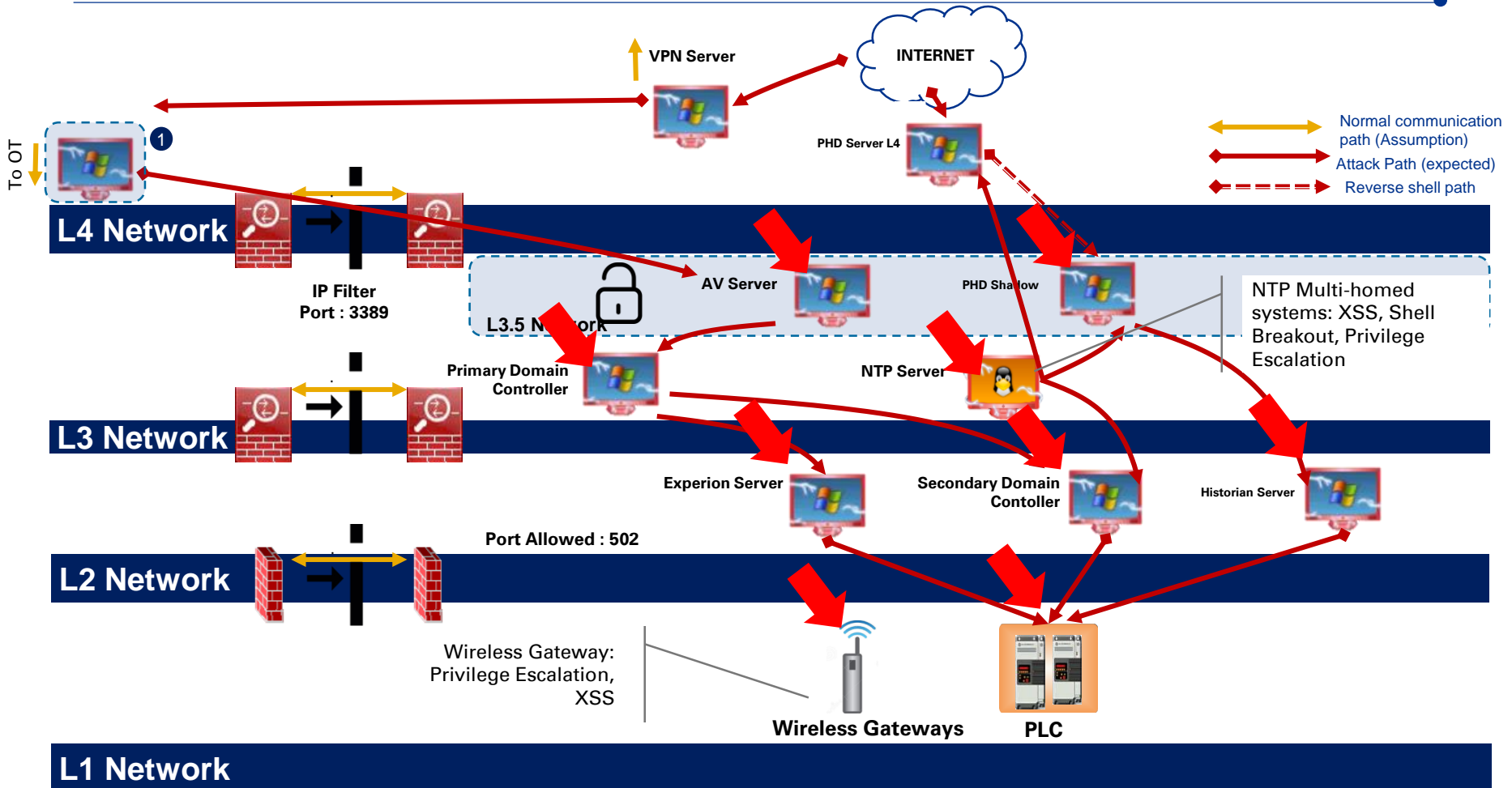
Why is it difficult?

- Different vendors and service providers
- Lack of vendor support for security updates
- Proprietary software and protocols
- Lack of support for network security controls
- Lack of interoperability
- Lack of support for security unified monitoring and operations

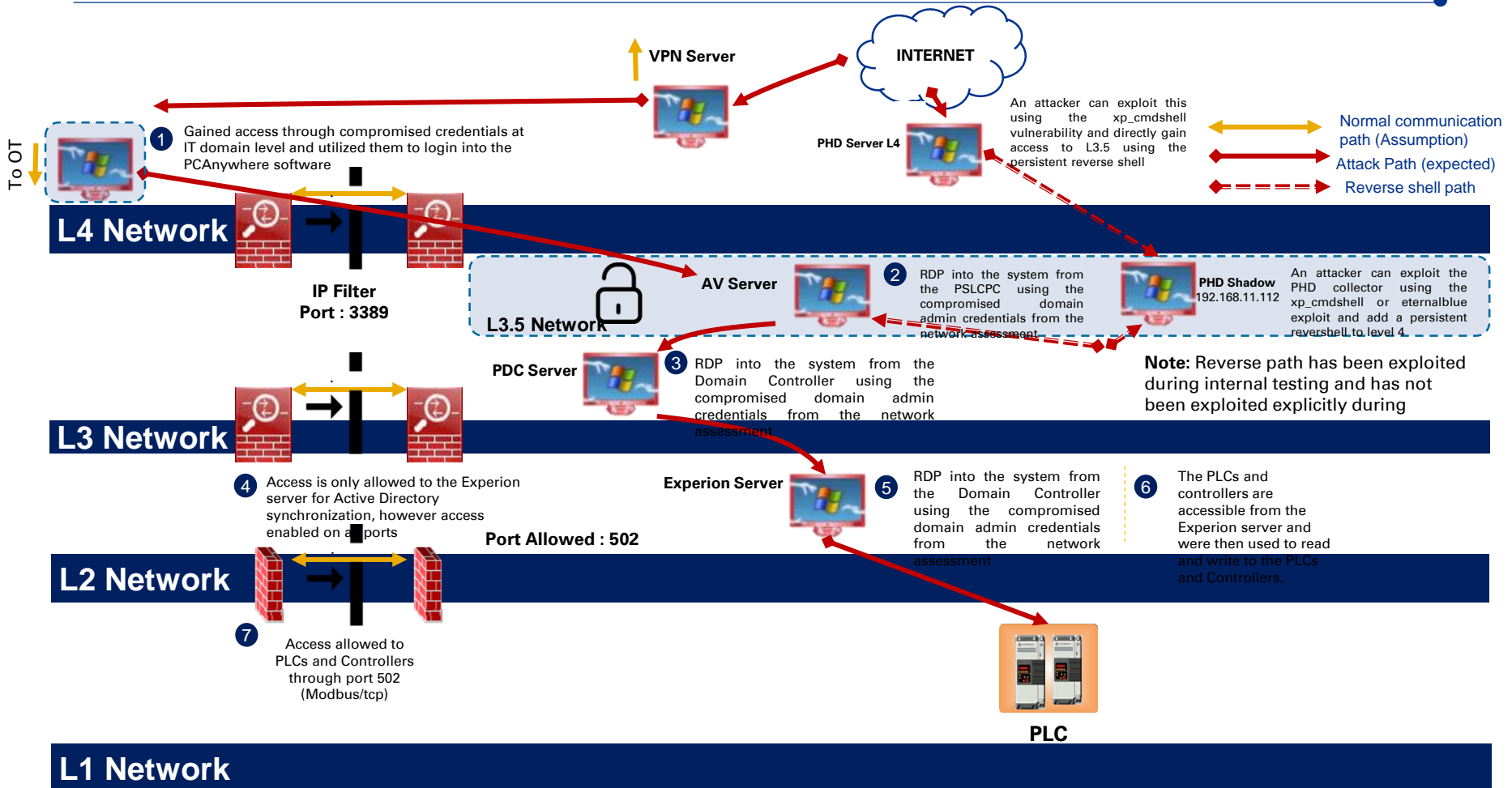
New Attack Vectors ?

- 802.15 Wireless HART Protocol
- Cloud Services connected to ICS infrastructure
- External services in the cloud environment
- Supplementary IT Services which may be vulnerable

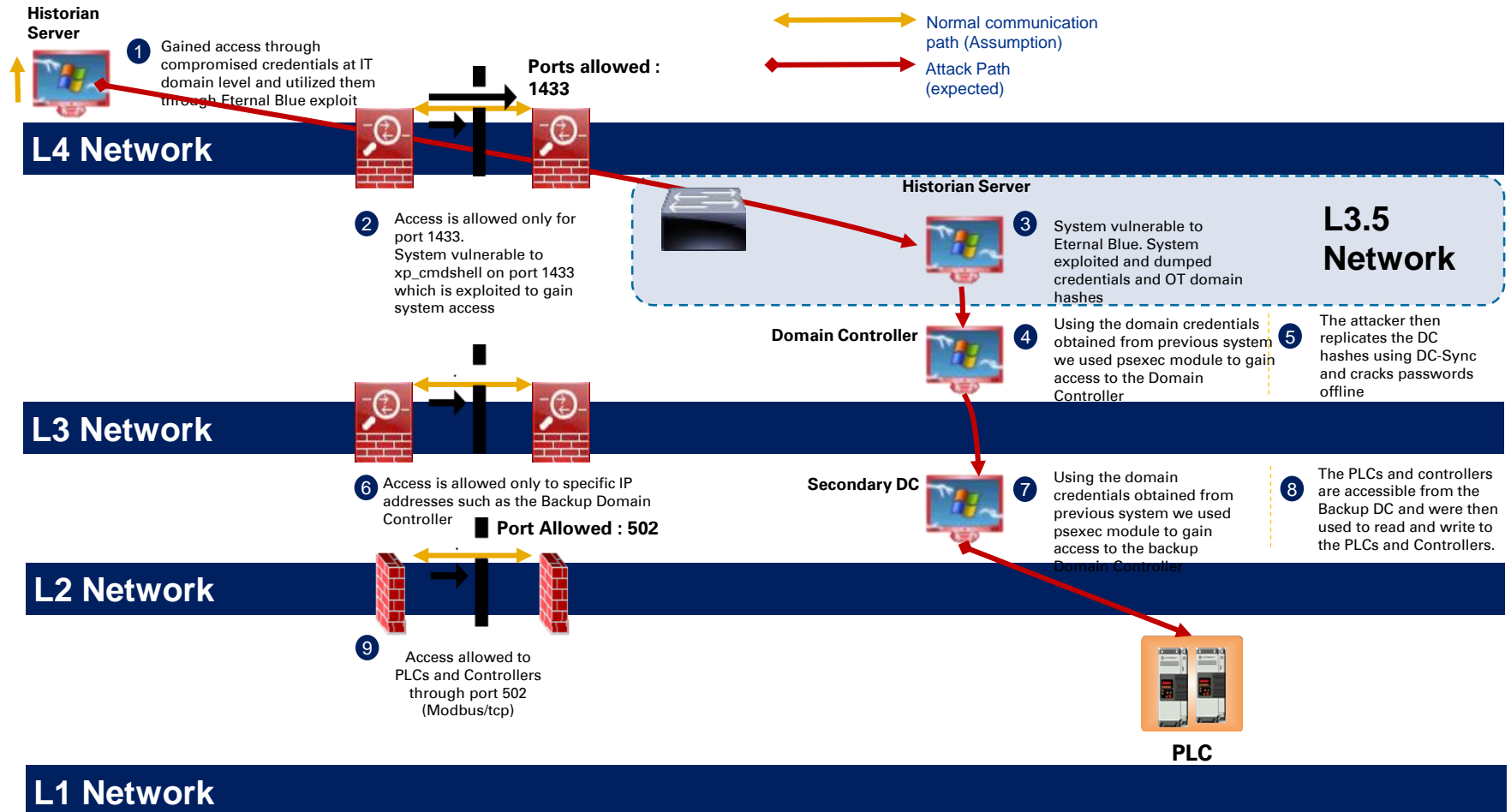
Open the pod bay doors | Brief explanation of the attack vectors



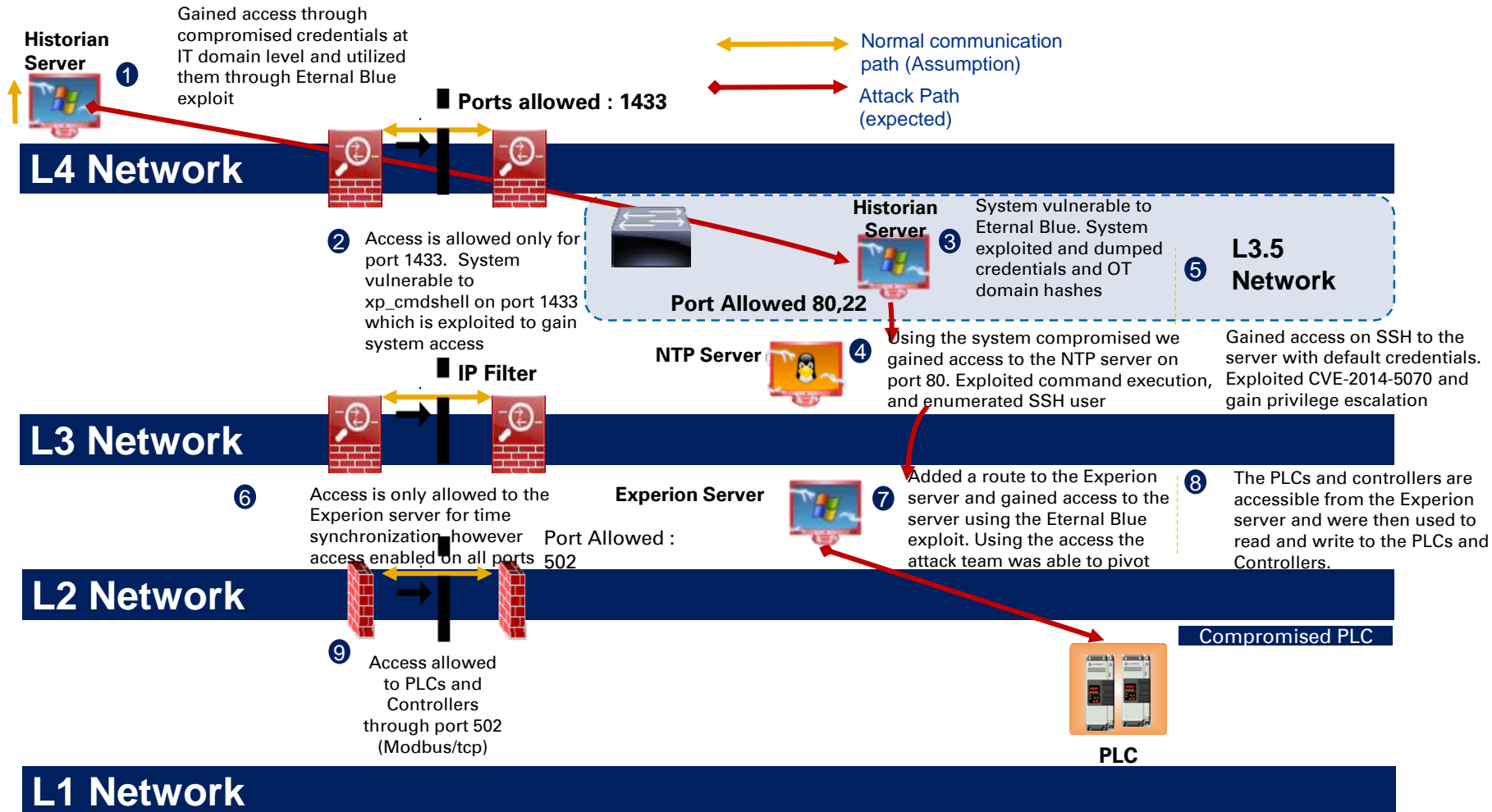
Reaching the heart of the system | Attack Path - 1



Reaching the heart of the system | Attack Path - 2



Reaching the heart of the system | Attack Path - 3



Destruction Ensues | Demonstration of what can happen

DEMO

Arms and Ammo

PLC Testing

- **mbtget** - Simple perl script for make some modbus transaction from the command line
- **ControlThings** - Platform consisting of all tools required to test the OT / IoT environment
- **pymodbus**: Python library for Modbus protocol implementation using twisted for its asynchronous communications core
- **pyModbusTCP**: A simple Modbus/TCP client library for Python.
- **EXPLIoT**: Framework for IoT Hacking

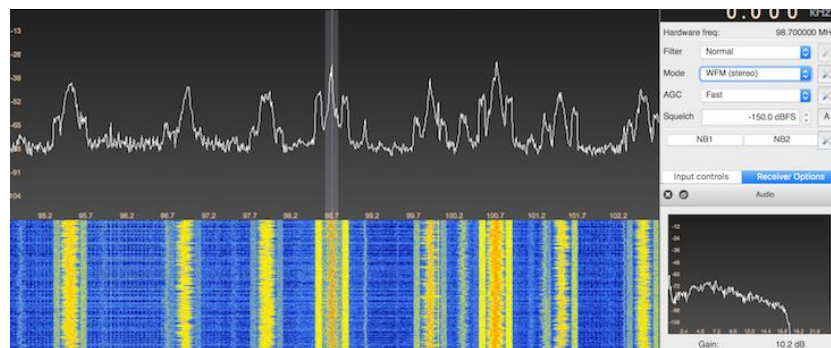
Wireless HART Testing

- **HackRF w/ GNURadio and gqrx**: Wireless HART communication interface
- **WirelessHART-Parser**: Analysis of the WirelessHART communications in the air
- **Wireshark**: You know why

OT Environment Testing

- Metasploit, nmap, JTR, aircrack-ng, Nessus, BurpSuite, Ettercap, sqlmap,

```
root@CybatiWorks-1:~# mbtget 172.16.192.2 -n 7
values:
1 (ad 00000) : 0
2 (ad 00001) : 1
3 (ad 00002) : 0
4 (ad 00003) : 1
5 (ad 00004) : 0
6 (ad 00005) : 0
7 (ad 00006) : 0
```



No.	Time	Source	Destination	Protocol	Length	Info
11...	454.610432	2a03:2880:f201:...	2601:1c0:cf00:...	TLSv1.2	105	Encrypted Alert
11...	454.610432	2a03:2880:f201:...	2601:1c0:cf00:...	TCP	74	443 → 60522 [FIN, ACK] Seq=
11...	454.610477	2601:1c0:cf00:8...	2a03:2880:f20...	TCP	74	60522 → 443 [RST, ACK] Seq=
11...	454.616387	AsustekC_35:e4:...	IntelCor_38:b...	ARP	42	Who has 192.168.29.250? Tel
11...	454.616412	IntelCor_38:be:...	AsustekC_35:e...	ARP	42	192.168.29.250 is at 7c:5c:
11...	454.629407	2a03:2880:f201:...	2601:1c0:cf00:...	TLSv1.2	660	Application Data
11...	454.629604	2601:1c0:cf00:8...	2a03:2880:f20...	TLSv1.2	105	Encrypted Alert
11...	454.629865	2601:1c0:cf00:8...	2a03:2880:f20...	TCP	74	60533 → 443 [FIN, ACK] Seq=
11...	454.649158	2a03:2880:f201:...	2601:1c0:cf00:...	TLSv1.2	105	Encrypted Alert
11...	454.649364	2601:1c0:cf00:8...	2a03:2880:f20...	TCP	74	60533 → 443 [RST, ACK] Seq=

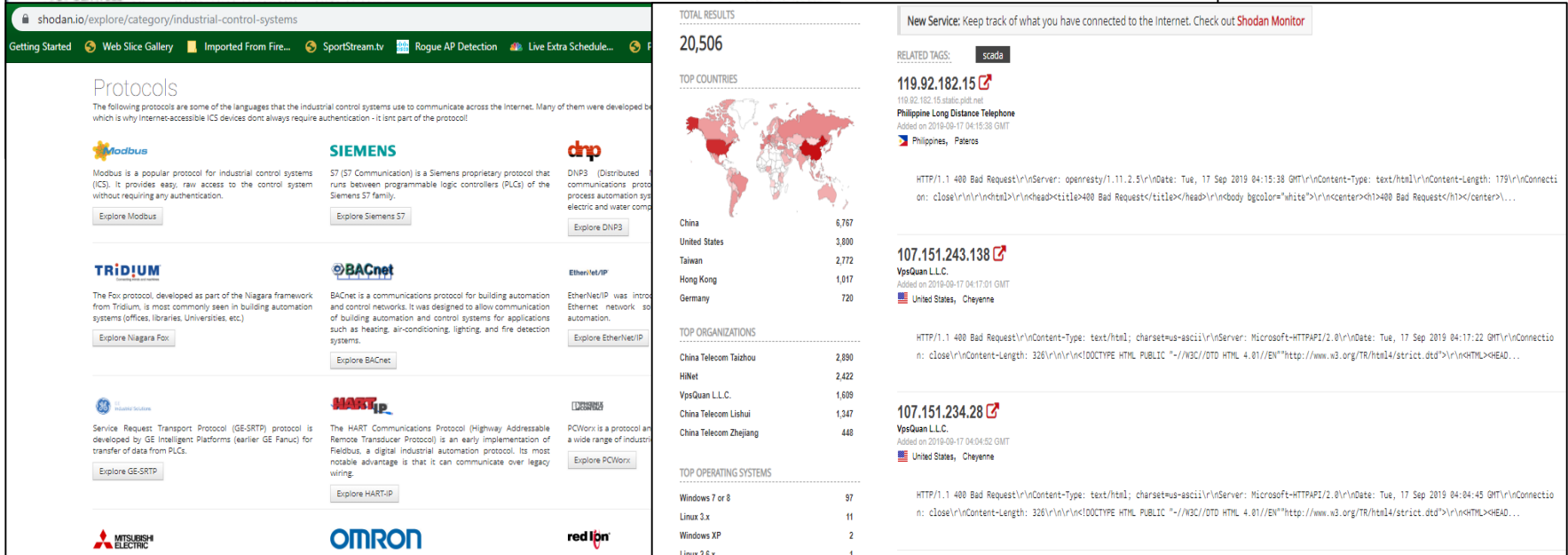
> Frame 4650: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c:1c:87:2c)
> Internet Protocol Version 4, Src: 192.168.29.250, Dst: 23.92.23.135
> Transmission Control Protocol, Src Port: 60424, Dst Port: 443, Seq: 2428, Ack: 931, Len: 54

The World is your Playground | critical Infrastructure on the Internet

Devices exposed on the internet and operate on Insecure Modbus TCP protocols



Devices on the internet on SIEMENS protocols




Explore by protocol / type

Maritime Security | AIS / ECDIS Information

Is this information you would want pirates or enemies to see?

SWEDISH WARSHIP K31
Military ops



Details Track Add photo Fleet

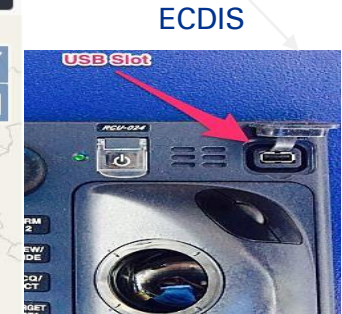
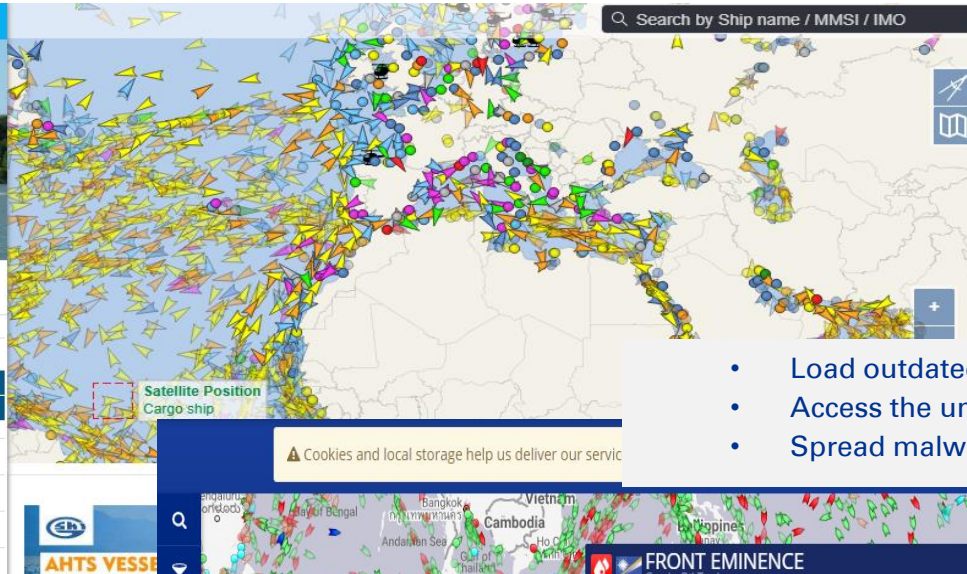
Destination: TRANSIT ETA: -

PORT CALLS

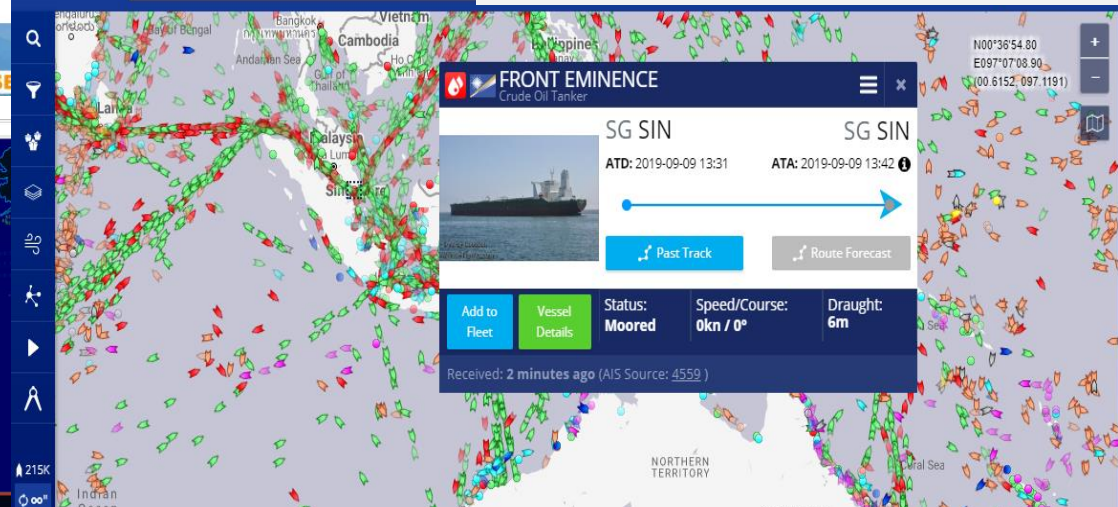
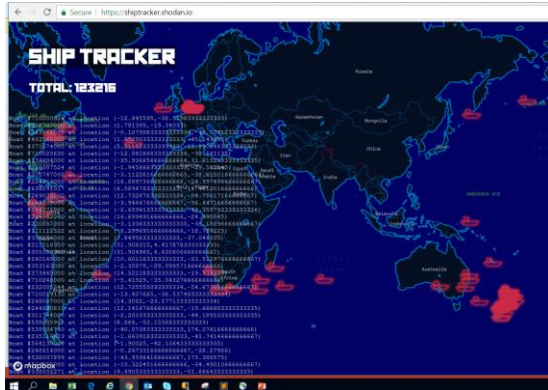
AIS DATA

Course	Speed	Current draught
283.0°	8.9 kn	-
GT	Built	IMO number
-	-	-
DWT	Size	MMSI
-	-	265823000

Last report
41 hours (Sep 17, 2019 15:29 UTC)



- Load outdated maps
- Access the underlying operating system
- Spread malware/ransomware



Maritime Security | It is happening...

The screenshot shows the IHS Fairplay Maritime Portal website. At the top, there is a navigation bar with links: IHS Markit Maritime Portal | Magazine Digital Editions | DPC Awards | Safety at Sea Awards | Webcasts | Whitepapers. Below this is a large blue banner with the 'Fairplay' logo on the left and a search bar on the right that says 'Search for articles or companies' with a magnifying glass icon. Under the banner is a secondary navigation bar with links: Commerce | Bulk | Container | Tankers | Markets | Safety & Regulation | Ports | Dredging. Below the navigation bar, the breadcrumb trail reads 'Fairplay > Safety & Regulation'. The main headline of the article is 'Hackers took ‘full control’ of container ship’s navigation systems for 10 hours'. Below the headline, it says 'Tanya Blake, editor, Safety at Sea | 22 November 2017'. At the bottom of the article preview, there are icons for Print, Email, Twitter, LinkedIn, Facebook, and Google+.

IHS Markit Maritime Portal | Magazine Digital Editions | DPC Awards | Safety at Sea Awards | Webcasts | Whitepapers

Fairplay Search for articles or companies

Commerce | Bulk | Container | Tankers | Markets | Safety & Regulation | Ports | Dredging

[Fairplay > Safety & Regulation](#)

Hackers took ‘full control’ of container ship’s navigation systems for 10 hours

Tanya Blake, editor, Safety at Sea | 22 November 2017

Print Email Twitter LinkedIn Facebook Google+

A “pre-warning”, about what will happen in the future of shipping, with pirates using hacking to gain control and entry to vessels in order to carry out kidnap and ransom

Source: HIS Fairplay

Had to bring IT experts on board

The 10-hour attack was carried out by “pirates” who gained full control of the vessel’s navigation system intending to steer it to an area where they could board and take over. The crew attempted to regain control of the navigation system but had to bring IT experts on board, who eventually managed to get them running again after hours of work

Suddenly the captain could not manoeuvre

In February 2017 hackers reportedly took control of the navigation systems of a German-owned 8,250 teu container vessel en route from Cyprus to Djibouti for 10 hours.



Questions?



Thank you