# Latest Developments in Cyber Safety

Chris Johnson,
Cyber Defense Group,
University of Glasgow.
johnson@dcs.gla.ac.uk

CEO Conference, Copenhagen,
15-16 May 2019

# Key Messages

- Good progress but investments being wasted:
  - Consultants expensive and ineffective, many projects fail.

- Low Cost solutions:
  - METRIC driven Cyber Security (NIS: CAF, ECTRL/CANSO);
  - Integrated Approach to Safety & Cyber Security Risks.

HUAWEI Industry Insights Spotlight Solutions & Products & Services Support

Home > Success Stories > Vodafone Spain Achieves the Largest DOCSIS 3.1 Network Transformation in Europe

# Vodafone Spain Achieves the Largest DOCSIS 3.1 Network Transformation in Europe


Recently, Vodafone Spain completed the deployment of 12,000 Distributed Converged Cable Access Platform (D-CCAP) sites. In the second quarter of 2018, Vodafone Spain will complete the DOCSIS 3.1 upgrade of its nation-wide network covering 7.9 million coaxial lines and provide up to 1 Gbps access broadband and services on the live network. This is the largest DOCSIS 3.1 network reconstruction project in Europe so

HUAWEI Phones, PC & More For Business Industry Insights About Huawei

Home > Press Center > News

# Huawei and Swisscom strengthen their partnership in the network infrastructure

Huawei and Swisscom jointly build IP metro network

2017.06.30

Liebefeld/Worblaufen, 30th
strengthen their partnershi
Swisscom next generation

The rapid developments in
about increasing service div
network that needs to be a
costs.

To meet this challenge, Swi
incremental architectural c
agility, and cost effectivene
partner able and willing to
edge technologies.

To support Swisscom's busi
oriented CloudMetro soluti

HUAWEI Phones, PC & More For Business Industry

Home > About Huawei > Publications > WinWin > WinWin Issue 08

# Telefonica o2 Germany: Improving service innovation through service network optimization

Dec 10, 2011

Telefónica o2 Germany was determined to leverage its fixed and IMS network assets to create the necessary synergies for the organic growth of its mobile business. To realize this strategic target, and lay the foundation for a future competitive edge in service innovation, the operator has started a journey of service network optimization.

## Aiming for synergy among fixed, mobile and IMS

Telefónica o2 Germany (o2) operates in the cutthroat German market, where competition from

# Poland arrests Huawei, Orange executive suspicion of spying

Authorities search offices of Huawei, Orange and the teleco regulator to confiscate data and documents.

By LAURENS CERULUS | 1/11/19, 10:20 AM CET | Updated 1/11/19, 8:19 PM CET

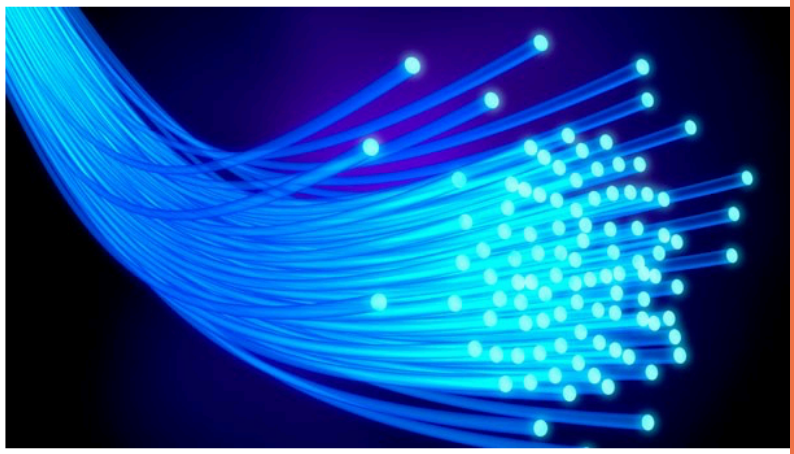
Polish security officials arrested two telecom executives on suspicion of v with Chinese intelligence services, the Polish government confirmed on

One suspect is a Chinese national, identified by authorities as Weijing W.

# BT Core Network trials break world speed records

May 25, 2016

Share Twee



**BT and Huawei deliver 2Tbps speeds over a live core fibre link between Dublin and London. Trial wins Global Telecoms Business Awards for innovation in London last night.**

New trials by BT and Huawei have achieved the fastest ever speeds of 2 Terabits per second (Tbps) over a live core network link which spans more than 700km between Dublin and London, in another world-first for BT's team of researchers at Adastral Park, Ipswich.

In 2014 BT used optical superchannel technology to deliver record breaking speeds over a closed trial network. Now, the company has successfully applied the same

stomer traffic between Dublin

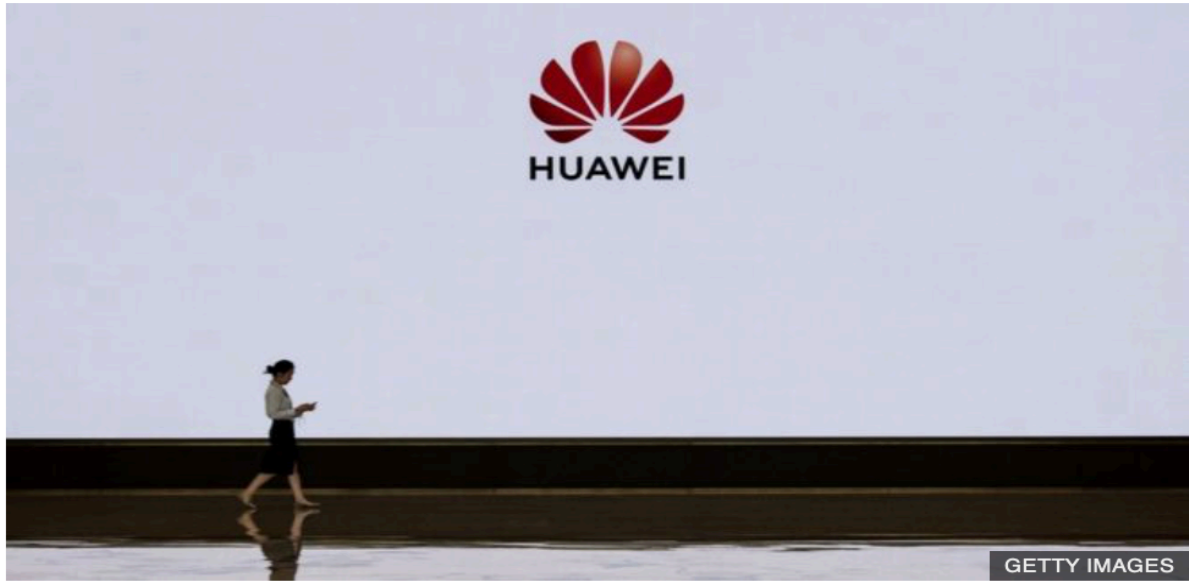
fully transmitted speeds of
etwork between the BT Labs in
previous record of 3Tbps set in
ost 200 HD quality films in one

ny's labs – using Terabit
ow BT to avoid a 'capacity
sting core optical networks
achieved by increasing the

# European ATM would collapse without Huawei

# Huawei says willing to sign 'no-spy' agreements

15 May 2019 Share




**Huawei is "willing to sign no-spy agreements with governments" including the UK, its chairman Liang Hua said.**

It follows concerns from some countries that China could use products made by the telecoms firm for surveillance.

The Chinese company has denied that its work poses any risks of espionage or





# Trump declares national emergency over IT threats

16 May 2019 Share


Donald Trump signed the order on Wednesday

# 'Very Abnormal' Russian Satellite Doesn't Seem So Threatening, Experts Say

By Mike Wall, Space.com Senior Writer | August 16, 2018 05:35pm ET





An artist's illustration of a satellite-servicing spacecraft approaching its target. On Aug. 14, 2018, a US diplomat said that a Russian satellite described as a "space apparatus inspector" has been exhibiting "very abnormal" (and therefore concerning) behavior on orbit.
Credit: SSL

It's unclear exactly why American officials are so worked up about a Russian satellite's recent activities, experts say.

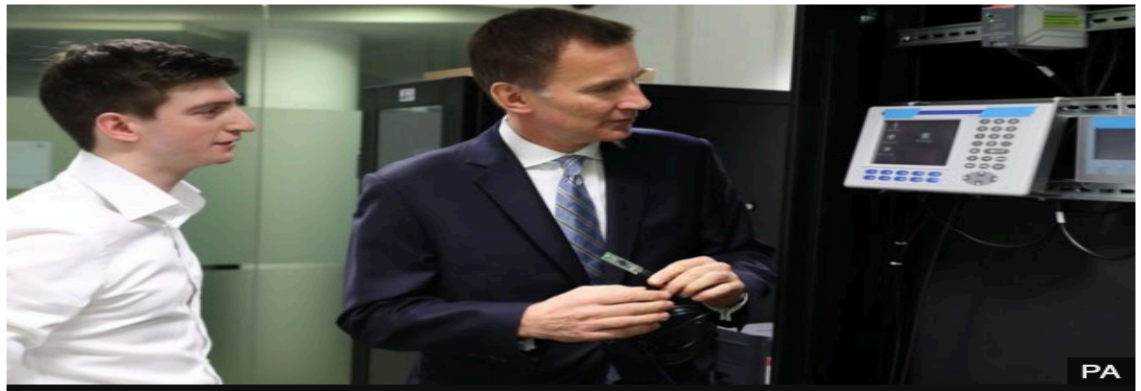
On Tuesday (Aug. 14), a high-ranking member of the U.S. State Department raised concerns about the satellite, describing its on-


OPEN
RTL1090 - (c) jetvision.de - B:103
BETA
1090.000 MHz
STOP
Tuner gain set to AUTO
Freq correction: 0 ppm
Freq set: "1090000000 Hz"
Buffer cleared
DO-260A/B symbols: . . . . . .
Started ...
*5D 40 72 B8 00 00 0D; [ 99]
*5D 40 72 B8 00 00 0D; [ 87]
*5D 40 72 B8 00 00 00; [ 73]
*20 00 06 9E 40 72 B8; [ 48]
*A8 00 0B BA B0 D8 00 00 00 00 40 72 B8; [ 38]
*02 A1 86 9F 40 72 B8; [ 76]
*5D 40 72 B8 00 00 00; [ 56]
*20 00 06 B0 40 72 B8; [ 27]
*20 00 06 B1 40 72 B8; [ 36]
*5D 40 72 B8 00 00 00; [ 31]
*20 00 06 B2 40 72 B8; [ 59]
*02 A1 86 B2 40 72 B8; [ 45]
*02 A1 86 B3 40 72 B8; [ 65]
*A8 00 0B BA 80 98 73 1E 40 04 7B 40 72 B8; [ 63]
*02 A1 86 B3 40 72 B8; [ 34]
*02 A1 86 B5 40 72 B8; [ 41]
*A8 00 0B BA 20 08 51 76 1D 58 20 40 72 B8; [ 47]
*20 00 06 B5 40 72 B8; [ 42]
*02 A1 86 B6 40 72 B8; [ 19]
List
Table
Stats
H/SI
>10
>20
>40
>80
>120
>180
UDP
BS
TCP
HTTP
47 ms
5/sec
THR: -78db [9]
Port:31011
....
R820T-00000001


SAT
ADS-B
GPS
SkyEcho

# Cyber-attacks: Jeremy Hunt says democratic elections 'vulnerable'

7 March 2019 | Share




Jeremy Hunt met cyber security experts during his visit to Glasgow University

**Cyber-attacks could turn elections into "tainted exercises" that undermine Western democracies, the foreign secretary has said.**

In a speech in Glasgow, Jeremy Hunt said authoritarian regimes view democratic elections as "key vulnerabilities" to be targeted.

But he stressed there was no evidence of successful interference in UK polls.

Mr Hunt called for economic and diplomatic sanctions to be part of the response to attacks.

He added that the government was expanding its network of "cyber attaches" - diplomats working with governments around the world to address the problem.

- The risks of cyber-conflict with Russia

Top Stories

**No clear winner in Israeli election**
Exit polls prompt both ex-military chief Benny Gantz and PM Benjamin Netanyahu to claim victory.
2 hours ago

**Tusk suggests Brexit delay of up to a year**
5 hours ago

**Japanese F-35 fighter crashes into Pacific**
1 hour ago



Features

Modi's India

THE TIMES
SCOTLAND
TUESDAY NOVEMBER 1 2016 | THETIMES.CO.UK | NO 72016
Printed in Scotland
80p to subscribers £1.40

## Meet Harry's girl

Has the prince finally found his match? Talent

## Hurt of the past

Laidlaw ready to tackle Australia one year on Sport

# Britain will strike back at foreign cyberthreat

### Chancellor unveils £2bn plan to target hackers

Francis Elliott Political Editor

Britain will "strike back" against cyberattacks by foreign governments and criminal hackers, the chancellor is to pledge today.

The country must take an aggressive approach to protect the economy, infrastructure and individuals' privacy from hostile forces, Philip Hammond will say. The risk of hackers targeting air traffic control and power grid networks is among the biggest concerns.

Announcing a £19 billion programme to improve cyberdefences, Mr Hammond will make the government's most explicit threat to deploy newly developed offensive capabilities against attackers, whether they be lone teenagers or foreign states.

His comments come after a series of attacks on the West for which Russia has been blamed. Last month Joe Biden, the US vice-president, threatened a revenge cyberattack on President Putin, who was accused of seeking to use hacking to influence the presidential election. There have also been espionage fears over plans to use Chinese technology in a nuclear plant in Essex.

Mr Hammond will warn that Britain is increasingly vulnerable to cyberattacks because of the proliferation of "smart" household items. Last week The Times reported that wi-fi-enabled devices including cameras, coffee makers and baby monitors — part of the so-called internet of things — can be accessed, leaving owners at risk of surveillance, burglary and blackout.

Ageing commercial IT systems, a growing shortage of computer security experts and the rise of "user-friendly"

threat, the chancellor will tell more than 4,000 experts at a Microsoft conference in London today.

As part of a new national cybersecurity strategy, he will announce the creation of a national research institute to tackle the most pressing weaknesses. Improving the safety of devices such as smartphones and laptops, beyond the use of simple passwords will be a priority, along with protecting infrastructure.

The chancellor's threat to turn Britain's cyberwarfare capabilities against "hostile actors" is likely to be the most controversial element of his announcement. "Our new strategy ... will allow us to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked," he will say.

Although he will not name any state, his speech comes after the US threatened Mr Putin with a retaliatory strike over a series of hacks designed to undermine Hillary Clinton's campaign. Mr Biden said that the administration was "sending a message" to Mr Putin last month after the US accused Moscow of using hacking to influence the election. "We have the capacity to do it. It will be at the time of our choosing, and under the circumstances that have the greatest impact," he said.

Mr Hammond will be more circumspect but will make clear that Britain would not allow a state-sponsored cyberattack to go unpunished.

George Osborne, his predecessor as chancellor, announced last year that Britain had developed a "dedicated ability to counterattack in cyberspace" and that a joint Ministry of Defence and GCHQ taskforce would develop the capability. Mr Hammond will

Continued on page 2, col 3

Mark Carney leaving No 10 yesterday after talks with Theresa May. The Bank of England governor cited Brexit and family considerations for his decision to quit

## Carney to quit as Bank chief in 2019

Sam Coates Deputy Political Editor

Mark Carney surprised the government last night by turning down a plea to stay in his post until 2021 after ministers backing him in Downing Street.

The governor of the Bank of England said that he would leave in June 2019 — the earliest opportunity to depart after Brexit. Mr Carney, 52, was originally due to step down in 2018, at the end of a three-year extension, which he had been backed publicly by Philip Hammond, the chancellor.

Last month, however, Theresa May used her speech to the Conservative Party conference to warn of the "international elite", which some Tory MPs saw as a swipe at the Canadian governor. No 10 was blamed for aggravating relations by failing to show the

Yesterday Mr Carney said he was happy to stay until the conclusion of the Article 50 process — expected March 2019 — to help to secure "orderly transition" as Britain leaves the EU, but not beyond that point. There had been reports that he would remain 2008 will represent "the

days for the UK".

In a letter to the chancellor, the governor cited Brexit and family considerations. His wife, Diana, and their children are understood to be not to Canada a year earlier than his original decision to serve for five was driven by personal considerations which had not changed, "but circumstances clearly have, most the UK's decision to leave the wrote. He has previously indicated interest in Canadian politics. try's next federal elections are to be in October 2019.

Last December Mr Carney that he was open to continuing post until 2021 because he'd "more" to do. This year he was by Brexit-supporting Tories Lord Lawson of Blaby chancellor, and the ex-cabinet Michael Gove, who described for enthusiastically backing

His decision to step down after the lowest point between the Bank and since the 2008 financial Gordon Brown's government

Continued on page 9, col

## Applications

# Where is MIL-STD-1553?

MIL-STD-1553 was originally used in military aerospace platforms. The standard has now expanded beyond its traditional domain to encompass applications of for combat vehicles, ships, satellites, missiles, the International Space Station Program, and advanced commercial avionic applications.

MIL-STD-1553 has been designed into important military and commercial applications.

## Military Aerospace

Military aircrafts utilize MIL-STD-1553 data buses, which allow complex electronic subsystems to interact with each other and the on-board flight computer. This is the military data bus is the lifeline of the aircraft. The data bus products function as the interface between the sub-system electronics and the 1553 data bus.

MIL-STD-1553 has been designed into the following aircrafts:

- Airbus A-400M Turboprop Military Transport
- Alenia C-27J Spartan Military Transport Aircraft
- Bell-Boeing V-22 Osprey Vertical and Short Takeoff and Landing (V/STOL) Helicopter
- Boeing AH-64 Apache Attack Helicopter
- Boeing B-1 Lancer Strategic Bomber
- Boeing B-52 Stratofortress Strategic Bomber
- Boeing EA-18G Growler Electronic Warfare Aircraft
- Boeing F/A-18 Hornet Multirole Fighter
- Boeing F-15 Eagle Tactical Fighter
- Boeing C-17 Globemaster III Military Transport Aircraft
- Boeing KC-135 Stratotanker
- Boeing RC-135 Reconnaissance Aircraft
- Boeing X-45A Joint Unmanned Combat Air System (J-UCAS)
- Boeing/Sikorsky RAH-66 Comanche Reconnaissance and Attack Helicopter
- Dassault Mirage Jet Fighter
- Dassault Rafale Multirole Fighter
- Eurofighter EF-2000 Typhoon Multirole Fighter
- Fairchild Republic A-10 Thunderbolt II Jet
- General Atomics MQ-1 Predator Unmanned Aerial Vehicle (UAV)
- General Dynamics F-16 Fighting Falcon Jet Fighter
- Hawker Hunter Fighter
- Lockheed AC-130 Ground Attack Fixed-Wing Gunship
- Lockheed C-5 Galaxy Military Transport Aircraft
- Lockheed C-130 Hercules Military Transport Aircraft
- Lockheed F-117 Nighthawk Stealth Attack Aircraft
- Lockheed P-3 Orion Maritime Patrol Aircraft
- Lockheed Martin F-22 Raptor Stealth Air Superiority Fighter
- Lockheed Martin F-35 Lightning II Joint Strike Fighter
- Lockheed Martin KC-103 Tanker
- McDonnell Douglas KC-10 Extender Air-to-Air Tanker
- Mitsubishi F-2 Multirole Fighter
- Northrop Grumman B-2 Spirit Stealth Bomber
- Northrop Grumman E-2C/D Hawkeye Airborne Early Warning (AEW) Aircraft
- Northrop Grumman EA-6B Prowler Electronic Warfare Aircraft
- Northrop Grumman RQ-4 Global Hawk Surveillance Unmanned Aerial Vehicle (UAV)
- Panavia Tornado Multirole Fighter
- Sikorsky SH-60 Seahawk Multimission Maritime Helicopter
- Sikorsky SJ-60K  Seahawk Multimission Maritime Helicopter
- Sikorsky UH/MH-60 Black Hawk Utility Helicopter

# Implementation of the NIS Directive in France

This page gives state of play of the implementation of the NIS Directive in France and points of contact. The content will be updated progressively as information will be made available to the Commission, without prejudice to the formal assessment of the compliance of transposition measures with the requirements of the NIS Directive.

## Status of transposition

Transposed.

## National strategy on the security of network and information systems

The strategy is available online.

## Single point of contact

Agence nationale de la sécurité des systèmes d'information (ANSSI)

Address: Boulevard de la Tour-Maubourg 51, 75700 Paris 07 SP

Email: nis@ssi.gouv.fr

## National competent authority for DSPs

Same as Single point of contact.

## National competent authorities for OES

Details tbd.

## National CSIRT

CERT-FR


About Cybersecurity

- Policies
- Blog posts
- News
- Events
- Projects
- Funding
- Consultations
- Reports and studies
- Laws
- Frequently Asked Questions

Related topics

- eCommerce
- eHealth
- Internet of Things

## National competent authority for DSPs

Information Commissioner's Office (ICO)

Email: nis@ico.org.uk

Contact Hours: Monday-Friday 09:00-17:00

## National competent authorities for OES

### Energy (Electricity)

**England, Scotland and Wales** - Department for Business, En
Industrial Strategy, and the Office of Gas and Electricity Mar

Email: nis.energy@beis.gov.uk and cybersecurityteam@ofgem.g uk

Phone: +44 (0)20 7901 7000
Contact Hours: Monday-Friday 09:00-17:00

**Northern Ireland** - Department of Finance Northern Ireland
Email: nis.ca@finance-ni.gov.uk

Contact Hours: Monday-Friday 09:00-17:00

### Energy (Oil)

**England, Scotland and Wales** - Department for Business, Energy & I
Health & Safety Executive (HSE)
Email: nis.cyber.incident@hse.gov.uk and nis.energy@beis.gov.uk
Contact Hours: Monday-Friday 09:00-17:00

**Northern Ireland** - Department of Finance Northern Ireland
Email: nis.ca@finance-ni.gov.uk
Contact Hours: Monday-Friday 09:00-17:00

### Energy (Gas)

**England, Scotland and Wales** - Department for Business,
Gas and Electricity Markets
Email: nis.energy@beis.gov.uk and cybersecurityteam@ofge

Contact Hours: Monday-Friday 09:00-17:00

Health & Safety Executive (for some gas storage & transmission)

Email: nis.cyber.incident@hse.gov.uk

Contact Hours: Monday-Friday 09:00-17:00

**Northern Ireland** - Department of Finance Northern Ireland

eCommerce

eHealth

Internet of Things

Trust Services and eIdentification

| Country | Fines | Country | Fines |
|---|---|---|---|
| **Austria** | €50,000 - €100,000 | Italy | €150,000 |
| **Belgium** | - | Latvia | €10,000 |
| **Bulgaria** | Unspecified | Lithuania | TBC |
| **Croatia** | - | Luxembourg | - |
| **Cyprus** | €8,000-€10,000+ 6 months | Malta | - |
| **Czech Republic** | €200,000 | Netherlands | €5,000,000 (breach) + €1,000,000 (non-cooperation) |
| **Denmark** | 12 different sectoral bills - tbc | Poland | €35,000-<br>€230,000 |
| **Estonia** | €20,000 | Portugal | €5,000-€25,000 (person), €10,000-€50-000 (legal entity) for serious offences, reduced by half if negligent |
| **Finland** | Unspecified | Romania | €670-€11,000 (repeated up to €22,000), up to 5% of turnover. |
| **France** | €75,000 or<br>€100,000 or<br>€150,000 tiers | Slovakia | €300 or 1% of annual turnover, with maximum of €300 000. |
| **Germany** | €50,000 for negligence | Slovenia | €10 000 -€50 000 EURO (large companies) €500-€10 000 (Small) |
| **Greece** | - | Spain | TBC |
| **Hungary** | €165 –<br>€16,500 repeated every 2 months | Sweden | €500-€100,000 |
| **Ireland** | TBC | UK | €17,000,000 |

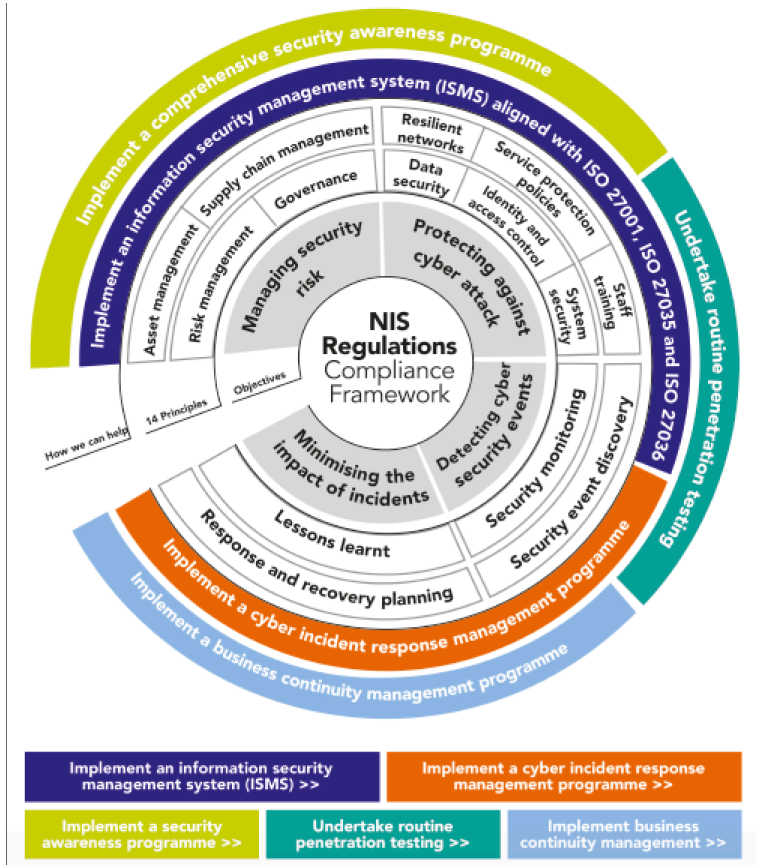
| Country | Fines | Country | Fines |
|---|---|---|---|
| **Austria** | €50,000 - €100,000 | Italy | €150,000 |
| **Belgium** | - | Latvia | €10,000 |
| **Bulgaria** | Unspecified | Lithuania | TBC |
| **Croatia** | - | Luxembourg | - |
| **Cyprus** | €8,000-€10,000+ 6 months | Malta | - |
| **Czech Republic** | €200,000 | Netherlands | €5,000,000 (breach) + €1,000,000 (non-cooperation) |
| **Denmark** | 12 different sectoral bills - tbc | Poland | €35,000-<br>€230,000 |
| **Estonia** | €20,000 | Portugal | €5,000-€25,000 (person), €10,000-€50-000 (legal entity) for serious offences, reduced by half if negligent |
| **Finland** | Unspecified | Romania | €670-€11,000 (repeated up to €22,000), up to 5% of turnover. |
| **France** | €75,000 or<br>€100,000 or<br>€150,000 tiers | Slovakia | €300 or 1% of annual turnover, with maximum of €300 000. |
| **Germany** | €50,000 for negligence | Slovenia | €10 000 -€50 000 EURO (large companies) €500-€10 000 (Small) |
| **Greece** | - | Spain | TBC |
| **Hungary** | €165 –<br>€16,500 repeated every 2 months | den | €500-€100,000 |
| **Ireland** | TBC | UK | €17,000,000 |

| Country | Fines | Country | Fines |
|---|---|---|---|
| **Austria** | €50,000 - €100,000 | Italy | €150,000 |
| **Belgium** | - | Latvia | €10,000 |
| **Bulgaria** | Unspecified | Lithuania | TBC |
| **Croatia** | - | Luxembourg | - |
| **Cyprus** | €8,000-€10,000+ 6 months | Malta | - |
| **Czech Republic** | €200,000 | Netherlands | €5,000,000 (breach) + €1,000,000 (non-cooperation) |
| **Denmark** | 12 different sectoral bills - tbc | Poland | €35,000-<br>€230,000 |
| **Estonia** | €20,000 | Portugal | €5,000-€25,000 (person), €10,000-€50-000 (legal entity) for serious offences, reduced by half if negligent |
| **Finland** | Unspecified | Romania | €670-€11,000 (repeated up to €22,000), up to 5% of turnover. |
| **France** | €75,000 or<br>€100,000 or<br>€150,000 tiers | Slovakia | €300 or 1% of annual turnover, with maximum of €300 000. |
| **Germany** | €50,000 for negligence | Slovenia | €10 000 -€50 000 EURO (large companies) €500-€10 000 (Small) |
| **Greece** | - | Spain | TBC |
| **Hungary** | €165 –<br>€16,500 repeated every 2 months | Sweden | €500-€100,000 |
| **Ireland** | TBC | UK | €17,000,000 |

# European NIS Coordination Group

- CG 01/2018 - Reference on security measures for OES
- CG 02/2018 - Reference on incident notification for OES
- CG 03/2018 - Compendium on cyber security of election technology
- CG 04/2018 - Cybersecurity incident taxonomy
- CG 05/2018 - Guide on notification of OES incidents (formats & procedures)
- CG 06/2018 - Guide on notification of DSP incidents (formats & procedures)
- CG 07/2018 - Reference on identification of OES (cross-border impact)
- CG 01/2019 - Voluntary information exchange cross-border dependencies

# NCSC Cyber Assessment Framework (CAF)

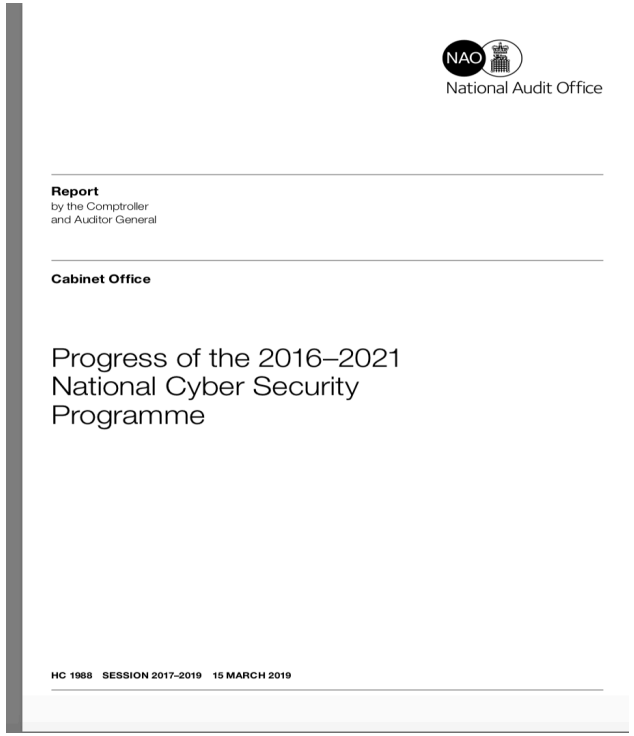



- Each principle -> specific outcomes.
- With indicators of good practice.
- Auditor use IGPs to assess if organisation applied principle.

| | | | Maturity levels | | | | |
|---|---|---|---|---|---|---|---|
| **Function** | **Category** | **Description (from NIST)** | **Level 0 - Non-existent** | **Level 1 – Partial** | **Level 2 – Defined** | **Level 3 – Assured** | **Level 4 – Adaptive** |
| LEAD AND GOVERN | Leadership and governance | Top management demonstrate leadership and commitment to cybersecurity. The policies needed to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | No overarching policy, strategy or plan | Policy established, together with parts of a strategy or plan; roles & responsibilities are established but no or weak link with top management | Policy supported by a strategy and plan approved by top management; key risks are accepted by top management | Plan is funded and, with visible top management commitment, delivering intended improvements across the organisation | Updated regularly to reflect progress, threats and risks |
| | Cybersecurity Management System (CyberSecMS) | The organisation has a set of interacting elements that establishes security policies and security objectives, and processes to achieve those objectives. | No documented CyberSecMS | Parts of a CyberSecMS documented, resourced and applied, but independently of other depts/systems | Fully operational CyberSecMS, that is externally audited CyberSecMS, and with links to other parts of the SecMS and the QMS and SMS | Certified CyberSecMS, with KPIs defined and tracked, and CyberSecMS/QMS/SMS processes are coordinated | Regular review against new good practices; KPIs show continual improvement; Certified Integrated Management System (IMS) |

| Function | Category | ANSP | Supplier 1 | Supplier 2 | Supplier 3 | Supplier 4 | Supplier 5 |
|---|---|---|---|---|---|---|---|
| LEAD AND GOVERN | Leadership and governance | 3 | 3 | 3 | 2 | 1 | 1 |
| | Cyber Security Management System (CyberSecMS) | 2 | 3 | 2 | 2 | 2 | 1 |
| IDENTIFY | Asset Management | 4 | 4 | 3 | 2 | 2 | 1 |
| | Risk Assessment | 1 | 3 | 3 | 1 | 2 | 1 |
| | Information sharing | 2 | 3 | 2 | 1 | 1 | 0 |
| | Supply Chain Risk Management | 2 | 3 | 3 | 2 | 1 | 0 |
| PROTECT | Identity Management and Access Control | 3 | 4 | 2 | 2 | 3 | 2 |
| | Human-centred security | 1 | 3 | 3 | 2 | 2 | 0 |
| | Protective Technology | 3 | 4 | 2 | 3 | 1 | 1 |
| DETECT | Anomalies and Events | 3 | 2 | 2 | 2 | 2 | 0 |
| RESPOND | Response Planning | 2 | 3 | 3 | 3 | 0 | 0 |
| | Mitigation | 3 | 3 | 2 | 2 | 0 | 1 |
| RECOVER | Recovery Planning | 3 | 3 | 3 | 1 | 2 | 1 |

# Need for Metrics: NAO March 2019



National Audit Office

**Report**
by the Comptroller
and Auditor General

**Cabinet Office**

Progress of the 2016–2021
National Cyber Security
Programme

HC 1988 SESSION 2017–2019 15 MARCH 2019

## Key facts

**£1.3bn**
National Cyber Security Programme budget 2016-21

**£648m**
remaining funding for the final two years of the five-year Programme

**3**
number of the Programme's 12 objectives for which the Department assesses the supporting projects are all currently on track

| | |
|---|---|
| **8** | number of the Programme's 12 objectives where at least 80% of the projects that support the objective are currently on track, with fewer than 80% on track against the twelfth objective |
| **1** | number of the National Cyber Security Strategy's 12 strategic outcomes for which the Department has 'high confidence' in its assessment that it will be met by 2021 |
| **11** | number of strategic outcomes we are unable to report progress on for national security reasons. However, we can report that the Department has 'moderate confidence' in the evidence supporting progress in achieving four of them and 'low confidence' in a further six. The twelfth strategic outcome – 'understanding the cyber threat' – is fully excluded from the analysis |
| **326** | metrics the Department has identified to track performance of both the Programme and the Strategy. However, one-third (107) of these are currently not being measured, either because the Department has low confidence in the evidence underpinning a metric or it is planned as a future measure of performance |
| **£169 million** | value of Programme expenditure loaned or transferred in the first two years to support other activities, representing 37% of funding |
| **72%** | percentage of large UK companies reporting a cyber-attack in the previous 12 months, with 9% of those reporting multiple attacks per day |
| **1,100+** | number of cyber security incidents dealt with by the National Cyber Security Centre since its formation in October 2016 |

# Key Messages

**Progress but significant investment being wasted:**

Ineffectiveness consultants, many projects fail.

**Low Cost solutions:**

| | |
|---|---|
| METRIC driven Cyber Security; | Integrated Approach to Safety & Cyber Security Risks. |

# We need tools and techniques to:

Systems Approaches address these challenges.

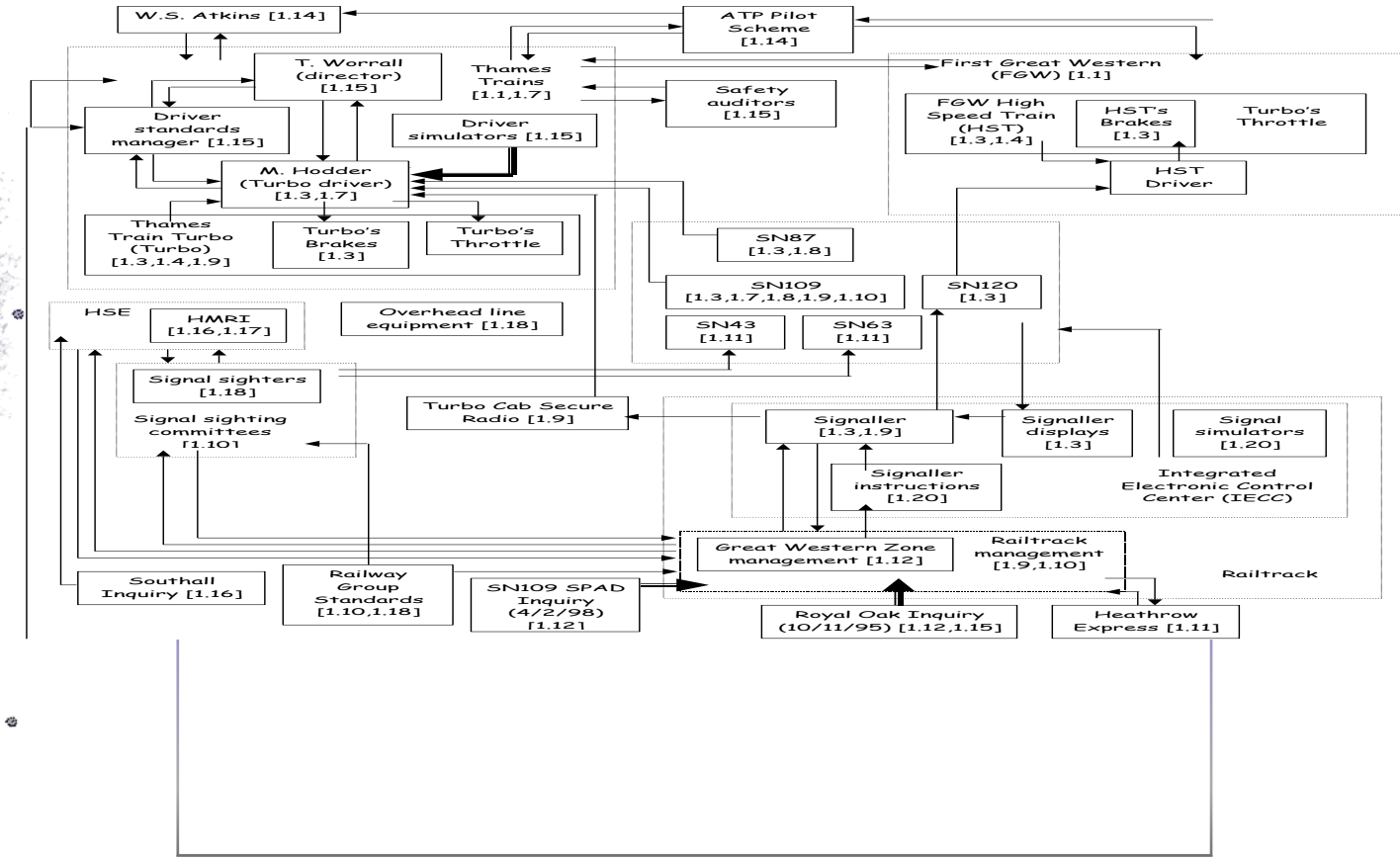
- Manage complexity and scale.
- Understand humans, digital and physical systems.
- Bring safety and cyber security thinking together.
- Maximise expertise from both domains.

# 1. Identify Subset of Threats

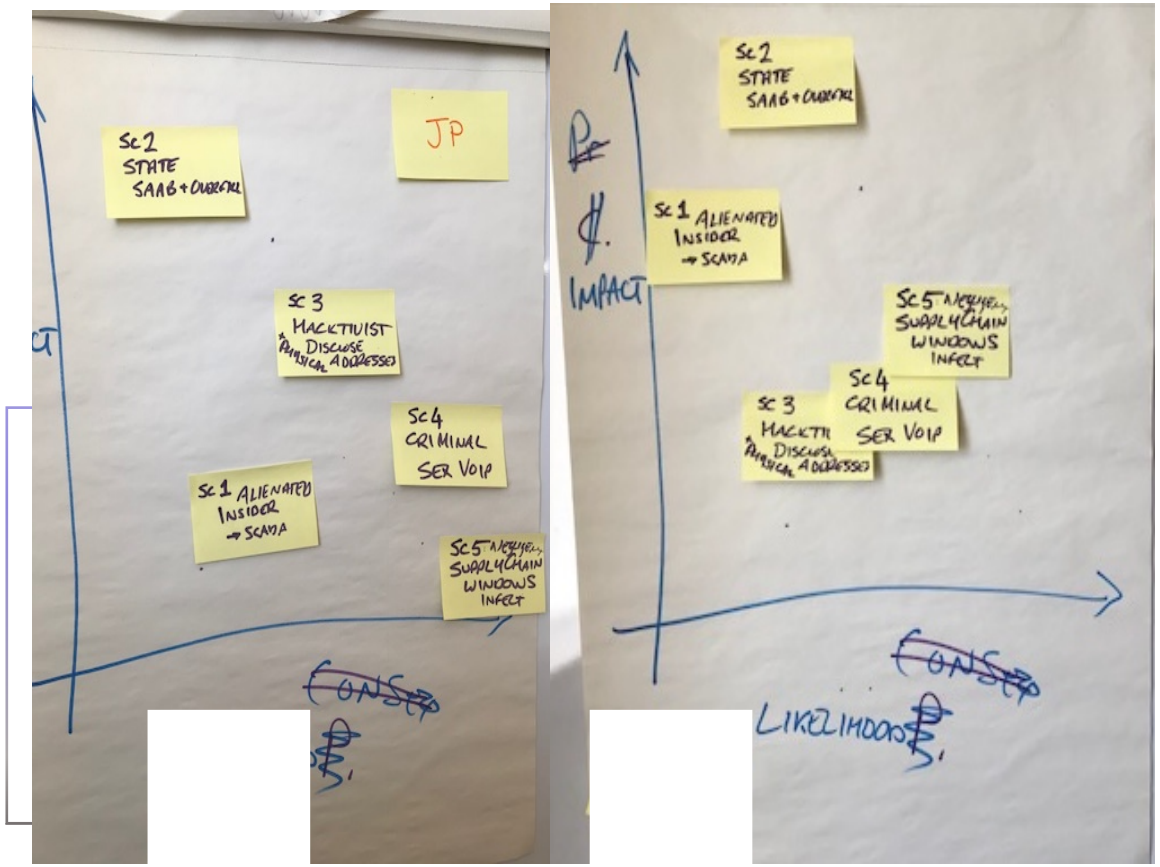
# 2. Check for Completeness

| | 1. Weakest point | 2. Loss of operational data | 3. Hidden code | 4. Collateral damage | 5. SCADA and ICS |
|---|---|---|---|---|---|
| Insiders | | (X) | X | | (X) |
| Supply Chain | | | X | | (X) |
| Hacktivists | X | X | | | |
| Nation State | | | | (X) | X |
| Criminals | (X) | | | X | |

# 3. Socio Technical Modelling



# 4. Rank Threat Scenarios to Assess Risk



# 5. Identify and Prioritise Control

| | Cyber Threat Scenarios | | | | |
|---|---|---|---|---|---|
| | 4 Collateral damage | 1. Weakest point | 3. Hidden code | 2. Loss of operational data | 5. SCADA and ICS |
| Two Factor Authentication | Required | N/A | N/A | N/A | Recommd |
| De-militarized Zones | Optional | Required | Required | N/A<br>N/A | Recommd |
| Counter 3 | N/A | Recommd | N/A | Required | N/A |
| Counter 4 | N/A | Required | N/A | N/A | N/A |
| Counter 5 | Recommd | N/A | Recommd | Required | N/A |

# 5. Identify and Prioritize Controls

- If you had £10,000 what two things would you do?
- If you had £100,000 what two things would you do?
- If you had £1 million what two things would you do?

# Key Achievements

- Input from industry, military, academia and government.
- Socio-Technical Foundations.
- Pragmatic, scalable and relevant.

# Key Messages

- Good progress but investments being wasted:
  - Consultants expensive and ineffective, many projects fail.

- Low Cost solutions:
  - METRIC driven Cyber Security (NIS: CAF, ECTRL/CANSO);
  - Integrated Approach to Safety & Cyber Security Risks.

# Any Questions?