Emerging Threats Related to National Critical Information Infrastructure and Internet of Things (IoT)

Sameer Sharma
ITU

Tehran , Iran
12-16 May 2018

Meet us

ITU at a glance

What we do

‘Committed to Connecting the World’

3 Sectors

ITU Radiocommunication

Coordinating radio-frequency spectrum and **assigning** orbital slots for satellites

ITU Standardization

Establishing global standards

ITU Development

Bridging the digital divide

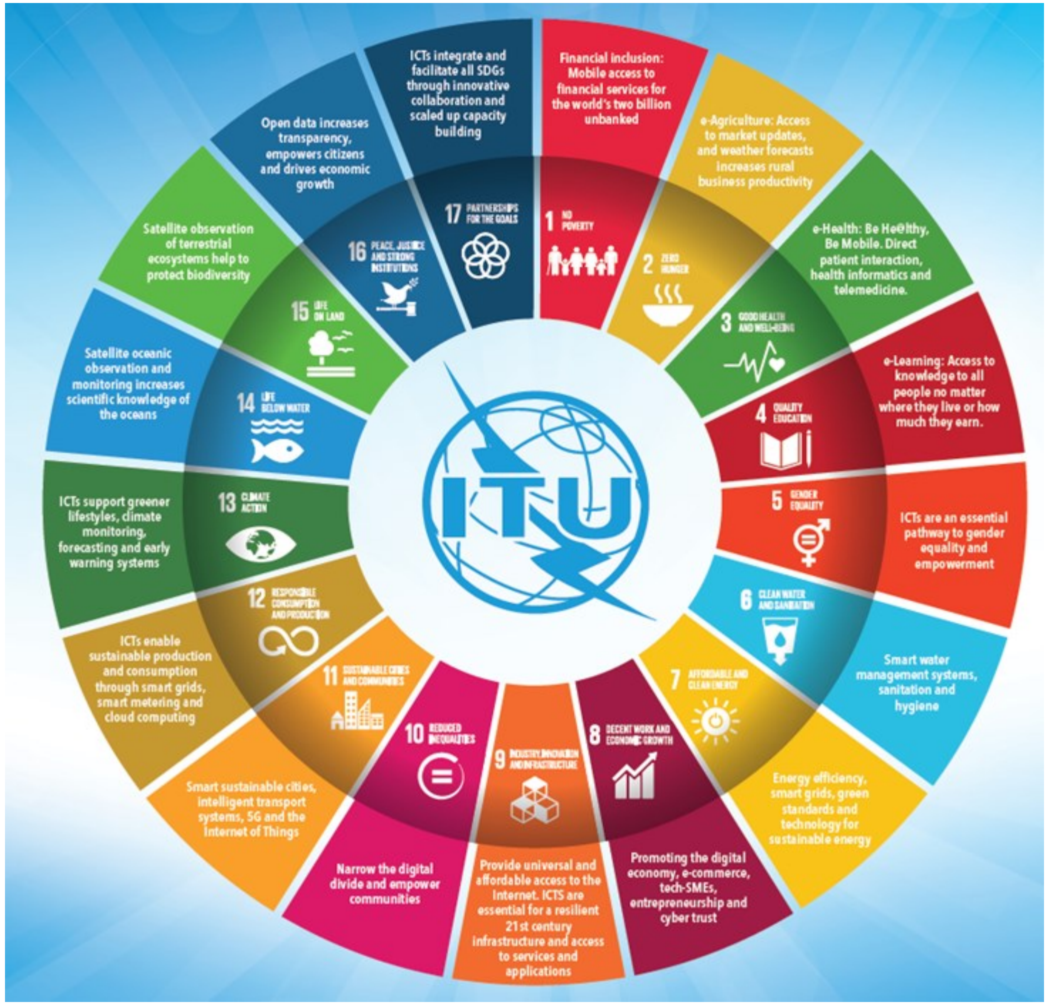
193	+700	+150
MEMBER STATES	INDUSTRY & INTERNATIONAL ORGANIZATIONS	ACADEMIA MEMBERS

MEMBERSHIP

ICTs and the SDGs

fast forward together
#ICT4SDG

*"The spread of information and communication technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies, as does scientific and technological innovation across areas as diverse as medicine and energy". **Agenda for Sustainable Development (Paragraph 15)***



1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
ITU

Financial inclusion: Mobile access to financial services for the world's two billion unbanked

e-Agriculture: Access to market updates, and weather forecasts increases rural business productivity

e-Health: Be He@lthy, Be Mobile. Direct patient interaction, health informatics and telemedicine.

e-Learning: Access to knowledge to all people no matter where they live or how much they earn.

ICTs are an essential pathway to gender equality and empowerment

Smart water management systems, sanitation and hygiene

Energy efficiency, smart grids, green standards and technology for sustainable energy

Promoting the digital economy, e-commerce, tech-SMEs, entrepreneurship and cyber trust

Provide universal and affordable access to the Internet. ICTS are essential for a resilient 21st century infrastructure and access to services and applications

Narrow the digital divide and empower communities

Smart sustainable cities, intelligent transport systems, 5G and the Internet of Things

ICTs enable sustainable production and consumption through smart grids, smart metering and cloud computing

ICTs support greener lifestyles, climate monitoring, forecasting and early warning systems

Satellite oceanic observation and monitoring increases scientific knowledge of the oceans

Satellite observation of terrestrial ecosystems help to protect biodiversity

Open data increases transparency, empowers citizens and drives economic growth

ICTs integrate and facilitate all SDGs through innovative collaboration and scaled up capacity building

Fast forward the SDGs

Many of the Sustainable Development Goals (SDGs) will not be met unless we accelerate the pace of change. We need information and communication technologies (ICTs) to meet the SDGs.

Talk to us today about how ICTs can help achieve the SDGs.

fast forward together
#ICT4SDG

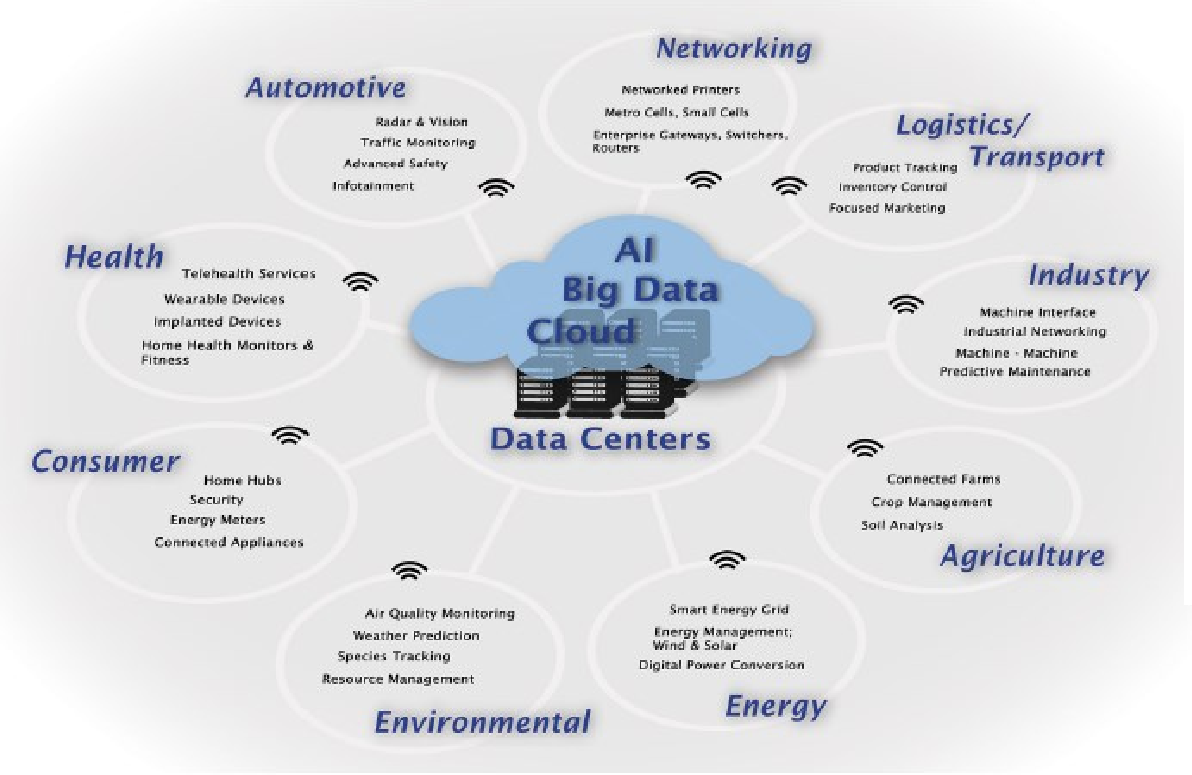
ICTs are catalytic drivers to enable the achievement of all the SDGs

Specifically referenced in the SDG targets:

- SDG4 Quality Education (4b)
- SDG5 Gender Equality (5b)
- SDG9 Industry, innovation and Infrastructure (9c)
- SDG 17 Partnerships for the Goals (17.8, as a means of implementation)

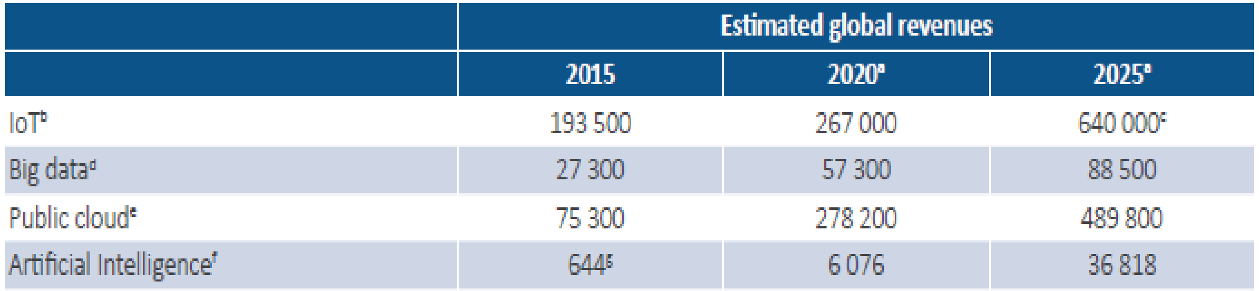
IOT, Big Data and Artificial Intelligence – The New Drivers of ICT Ecosystem

Figure 4.1: IoT, cloud computing, big data and artificial intelligence – the new drivers of the ICT ecosystem



Source: ITU.

Table 4.2: Estimated global market sizes for selected advanced ICTs (USD millions)



	Estimated global revenues		
	2015	2020[a]	2025[a]
IoT[b]	193 500	267 000	640 000[c]
Big data[d]	27 300	57 300	88 500
Public cloud[e]	75 300	278 200	489 800
Artificial Intelligence[f]	644[g]	6 076	36 818

[a] Forecast. [b] Statista (2017b); Hunke et al. (2017). [c] Estimate based on expected compound annual growth rate. [d] Statista (2016, p. 22). [e] Statista (2017a, p. 13). [f] Kaul and Wheelcock (2016). [g] Information for 2016.

Sources: Statista (2016, 2017a, 2017b), Hunke et al. (2017), Kaul and Wheelcock (2016).

Key Cybersecurity Challenges

- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software for ICT-based applications
- Lack of appropriate national and global organizational structures to deal with cyber incidents
- Lack of information security professionals and skills within governments; lack of basic awareness among users
- Lack of international cooperation between industry experts, law enforcements, regulators, academia & international organizations, etc. to address a global challenge
- Complexity of ICTs imply a need for the ability to respond, not just protect, as cybersecurity incidents will happen even if protective measures are deployed.

Cybersecurity not seen yet as a cross-sector, multi-dimensional concern.

Still seen as a technical/technology problem.

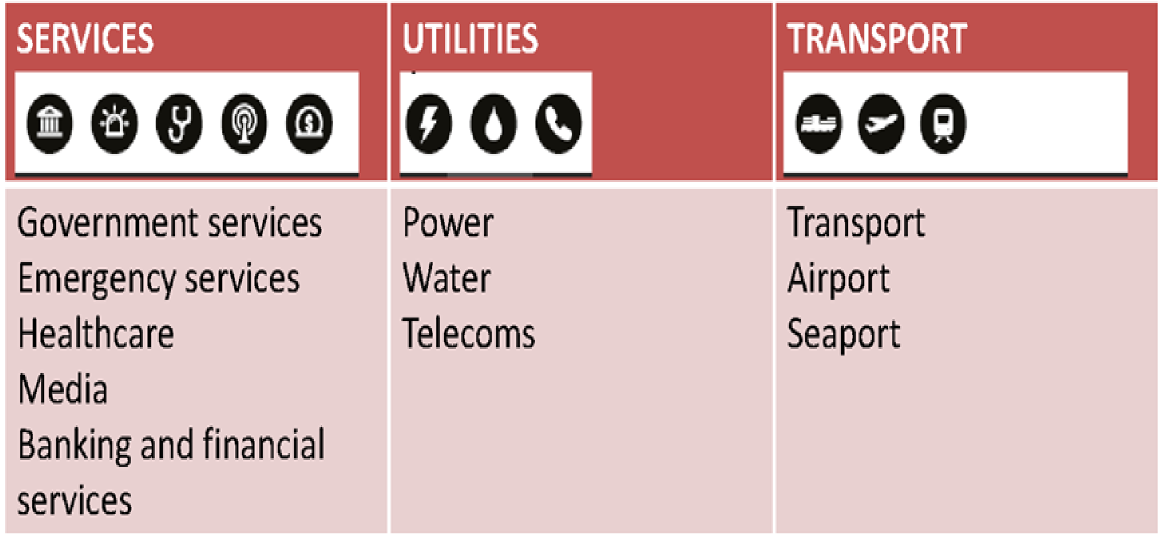
The National Critical Information Infrastructure

National CII : Singapore

Singapore

Definition of Critical National Infrastructure

“CIIs are computers or computer systems that are necessary for the continuous delivery of essential services that Singapore relies on, the loss or compromise of which will lead to a debilitating impact on national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. Currently, essential services have been identified in 11 sectors, including utilities, banking and finance, media, info-communications, healthcare and transportation.”



SERVICES	UTILITIES	TRANSPORT
Government services Emergency services Healthcare Media Banking and financial services	Power Water Telecoms	Transport Airport Seaport

Sectors

The Cyber Security Agency of Singapore (CSA) - Singapore

National CII : Malaysia

Malaysia

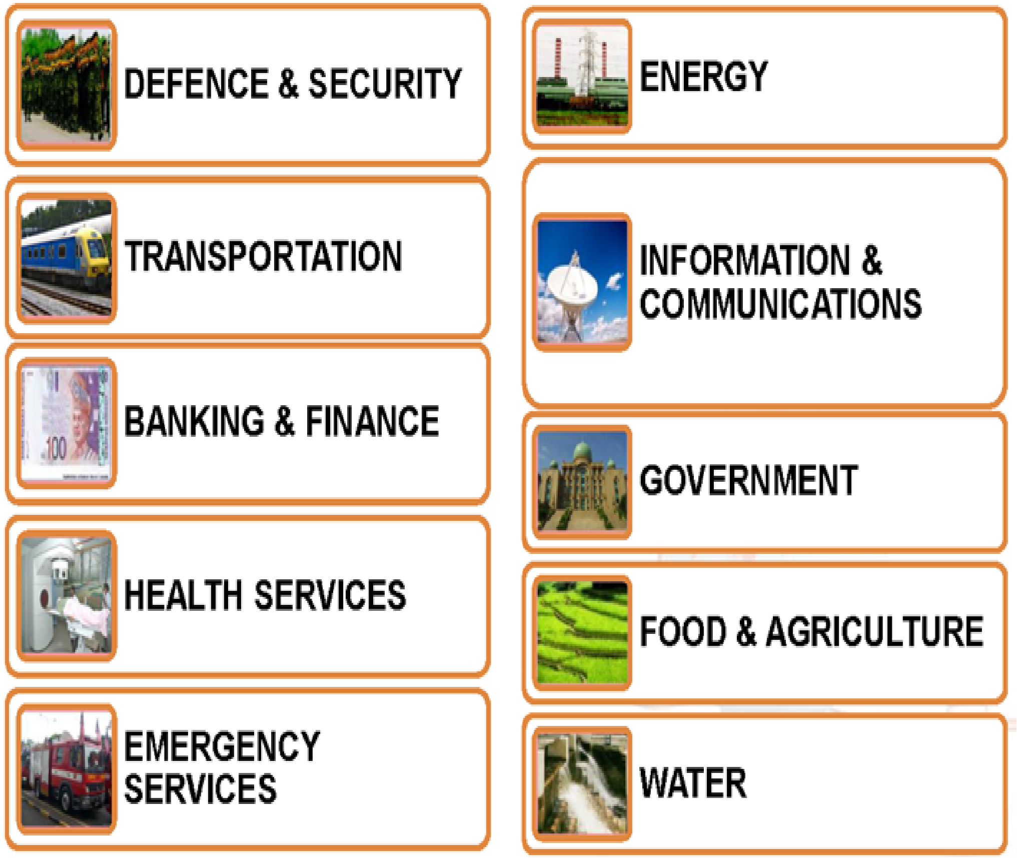
Definition of Critical National Infrastructure

“Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on:

- National economic strength; Confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living.
- National image; Projection of national image towards enhancing stature and sphere of influence.
- National defence and security; guarantee sovereignty and independence whilst maintaining internal security.
- Government capability to functions; maintain order to perform and deliver minimum essential public services.
- Public health and safety; delivering and managing optimal health care to the citizen.”

CyberSecurity Malaysia - Malaysia -

Sectors



DEFENCE & SECURITY

TRANSPORTATION

BANKING & FINANCE

HEALTH SERVICES

EMERGENCY SERVICES

ENERGY

INFORMATION & COMMUNICATIONS

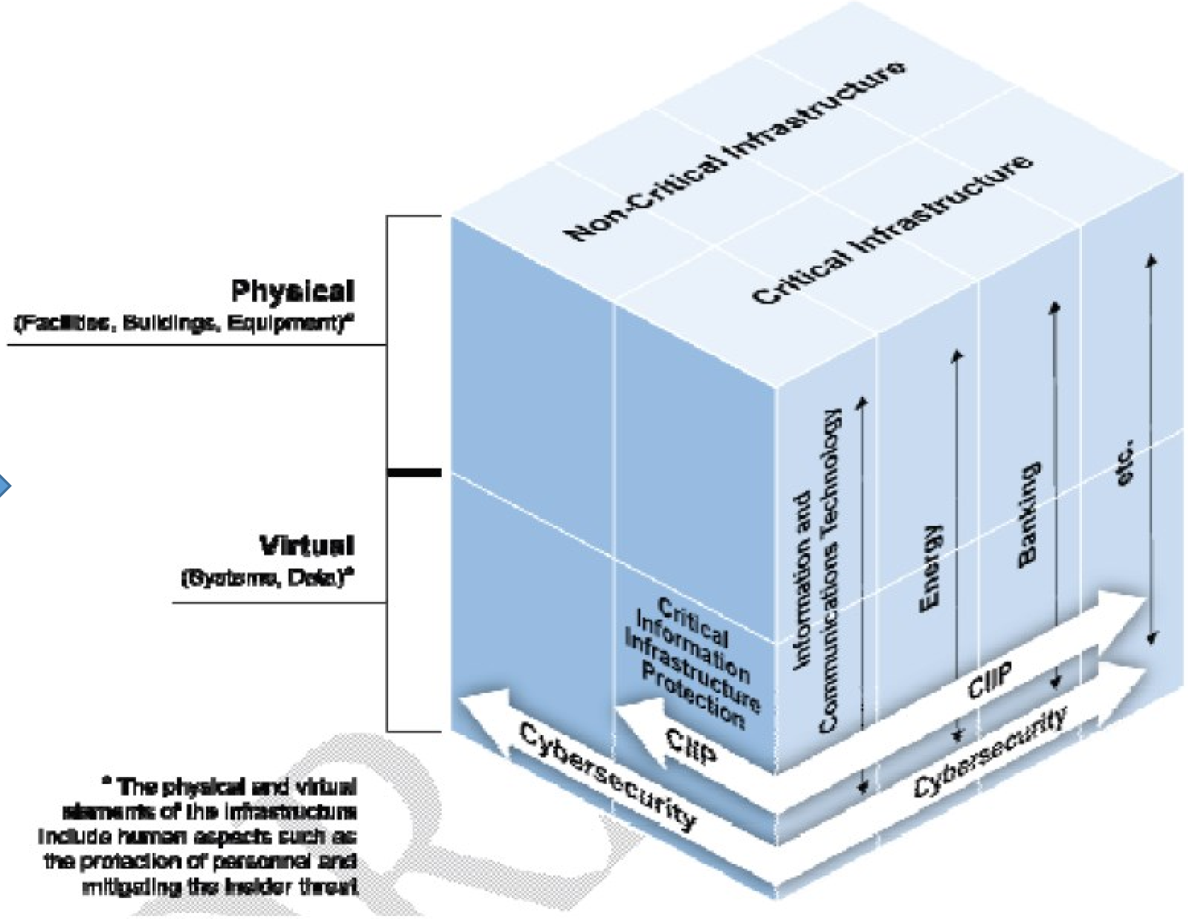
GOVERNMENT

FOOD & AGRICULTURE

WATER

Critical Information Infrastructure (CII)

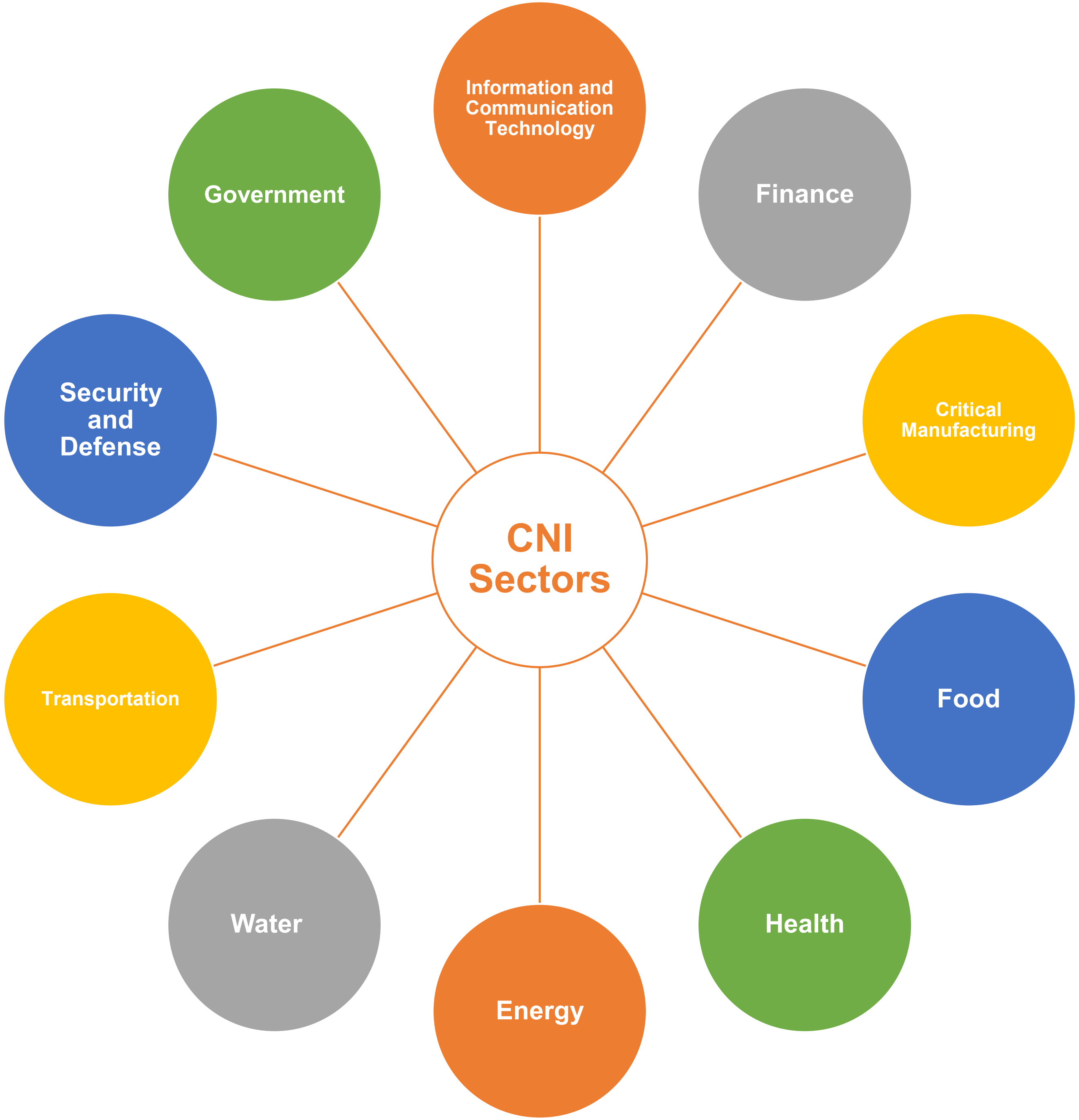
The Conceptual Relationship Between Critical Information Infrastructure Protection and Cybersecurity.


Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
Non-Critical Infrastructure
Critical Infrastructure
Information and Communications Technology
Energy
Banking
etc.
Critical Information Infrastructure Protection
CIIP
CIIP
Cybersecurity
Cybersecurity

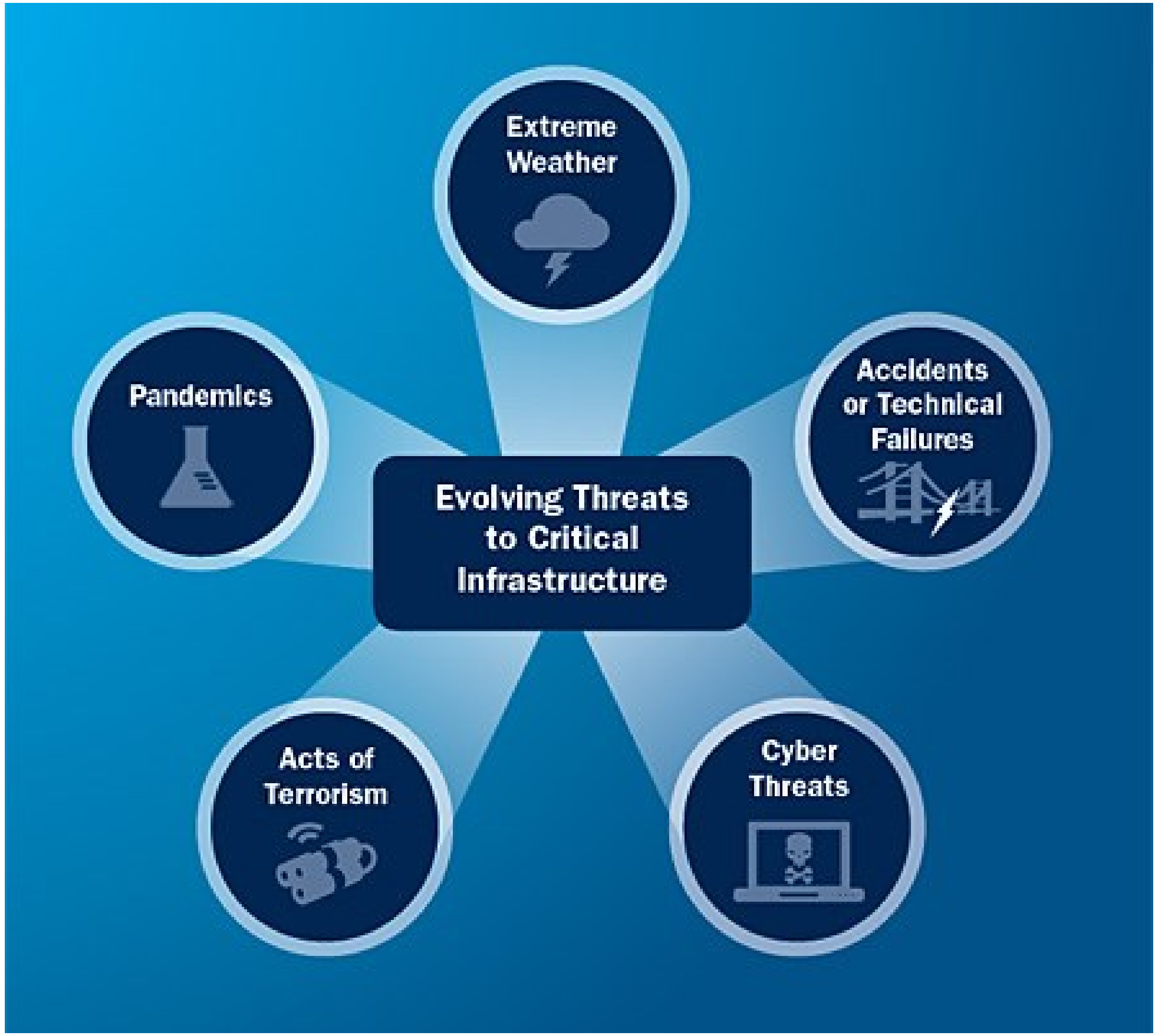
* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat

Source : ITU –D Study Group Q.22/1 report on best practices for a national approach to cybersecurity:

In General, we can identify 10 Critical National Infrastructure sectors :



Threats to Critical National Infrastructure


Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

Source : https://emilms.fema.gov

Threats to Critical National Infrastructure-I

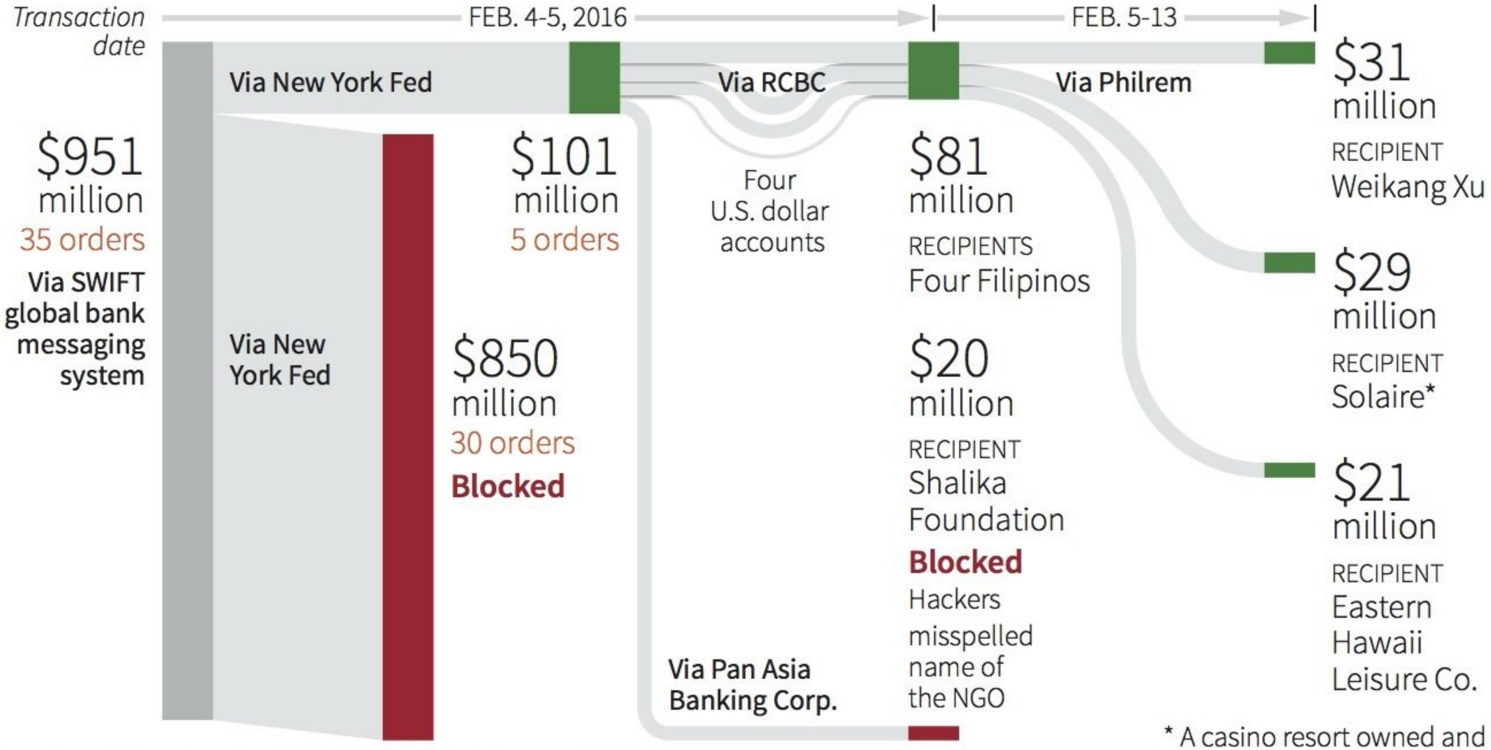
Bangladesh Bank

4 February 2016

Bangladesh Bank heist

In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines.

THE MONEY TRAIL



Transaction date

FEB. 4-5, 2016

FEB. 5-13

$951 million
35 orders
Via SWIFT global bank messaging system

Via New York Fed

$101 million
5 orders

Via New York Fed

$850 million
30 orders
Blocked

Via RCBC

Four U.S. dollar accounts

Via Pan Asia Banking Corp.

$81 million
RECIPIENTS
Four Filipinos

$20 million
RECIPIENT
Shalika Foundation
Blocked
Hackers misspelled name of the NGO

Via Philrem

$31 million
RECIPIENT
Weikang Xu

$29 million
RECIPIENT
Solaire*

$21 million
RECIPIENT
Eastern Hawaii Leisure Co.

* A casino resort owned and operated by Bloomberry Resorts

Sources: Philippines Court of Appeals documents; Reuters

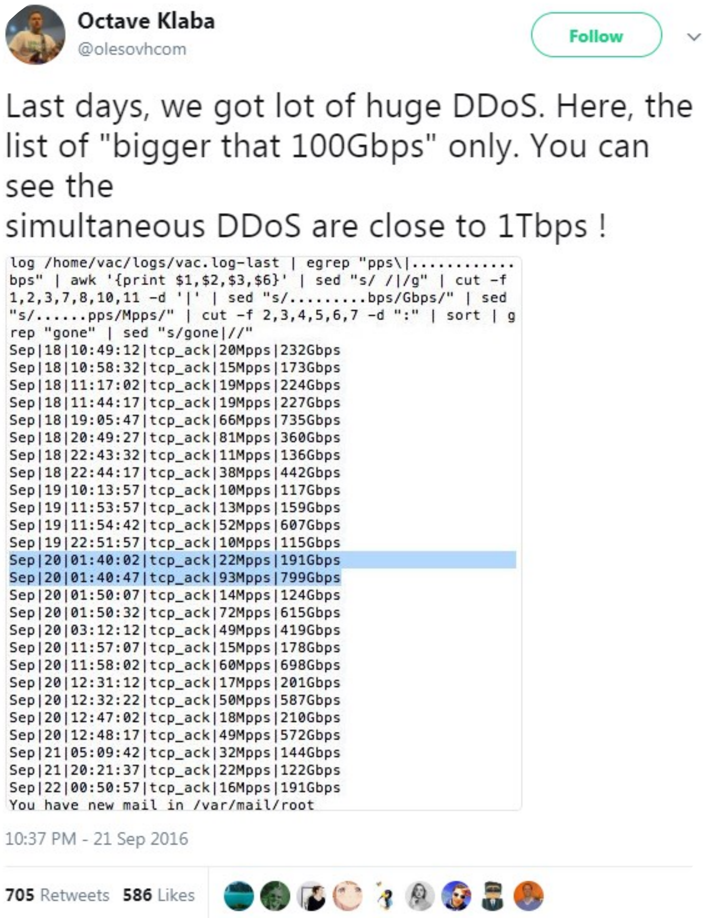
W. Foo, 31/03/2016

REUTERS

Threats to Critical National Infrastructure-II

Mirai Botnet (未来)

September and October 2016



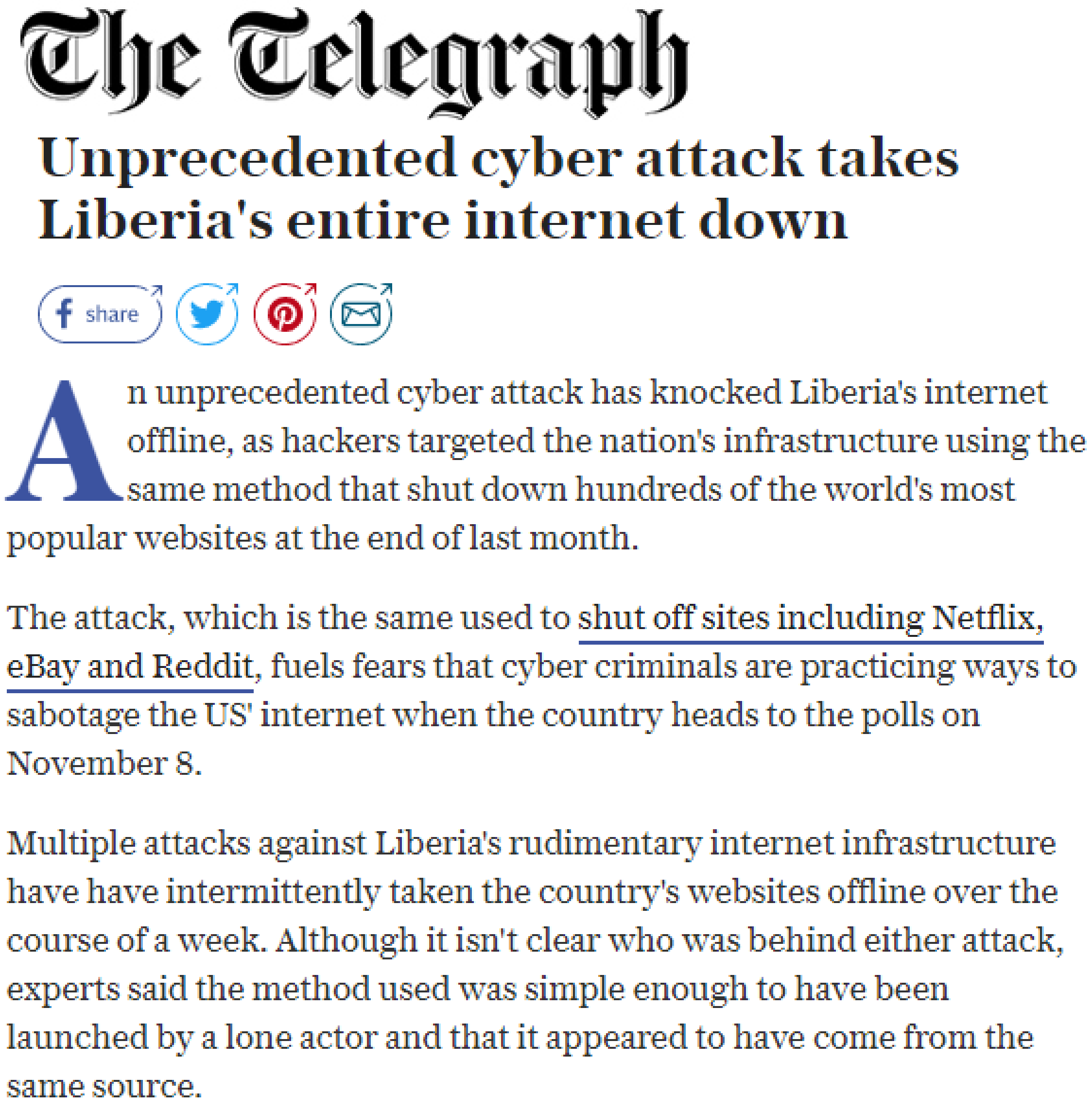
Octave Klaba
@olesovhcom

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the
simultaneous DDoS are close to 1Tbps !

```
log /home/vac/logs/vac.log-last | egrep "pps\|............
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

10:37 PM - 21 Sep 2016

705 Retweets **586** Likes



The Telegraph

Unprecedented cyber attack takes Liberia's entire internet down

An unprecedented cyber attack has knocked Liberia's internet offline, as hackers targeted the nation's infrastructure using the same method that shut down hundreds of the world's most popular websites at the end of last month.

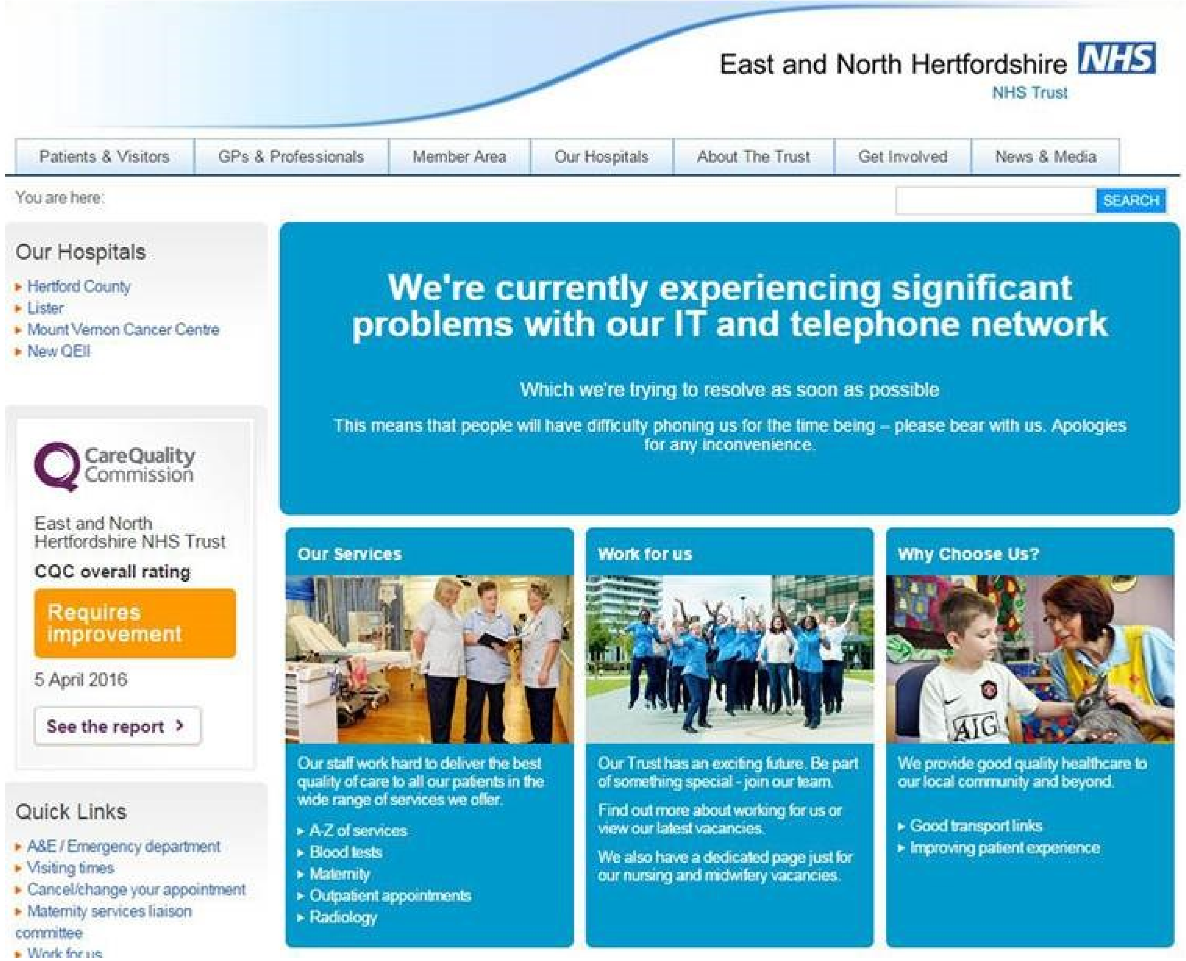
The attack, which is the same used to shut off sites including Netflix, eBay and Reddit, fuels fears that cyber criminals are practicing ways to sabotage the US' internet when the country heads to the polls on November 8.

Multiple attacks against Liberia's rudimentary internet infrastructure have have intermittently taken the country's websites offline over the course of a week. Although it isn't clear who was behind either attack, experts said the method used was simple enough to have been launched by a lone actor and that it appeared to have come from the same source.

Threats to Critical National Infrastructure-III

WannaCry Ransomware

May 2017



East and North Hertfordshire NHS
NHS Trust

Patients & Visitors | GPs & Professionals | Member Area | Our Hospitals | About The Trust | Get Involved | News & Media

You are here:

SEARCH

Our Hospitals
- Hertford County
- Lister
- Mount Vernon Cancer Centre
- New QEII

CareQuality Commission

East and North Hertfordshire NHS Trust

CQC overall rating

Requires improvement

5 April 2016

See the report ›

Quick Links
- A&E / Emergency department
- Visiting times
- Cancel/change your appointment
- Maternity services liaison committee
- Work for us

We're currently experiencing significant problems with our IT and telephone network

Which we're trying to resolve as soon as possible

This means that people will have difficulty phoning us for the time being – please bear with us. Apologies for any inconvenience.

Our Services

Our staff work hard to deliver the best quality of care to all our patients in the wide range of services we offer.

- A-Z of services
- Blood tests
- Maternity
- Outpatient appointments
- Radiology

Work for us

Our Trust has an exciting future. Be part of something special - join our team.

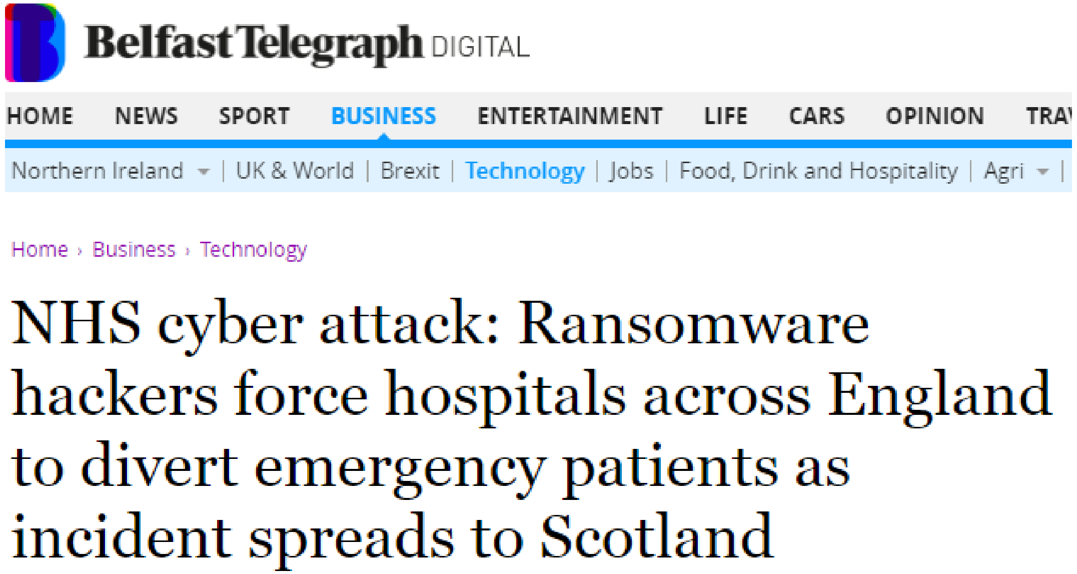
Find out more about working for us or view our latest vacancies.

We also have a dedicated page just for our nursing and midwifery vacancies.

Why Choose Us?

We provide good quality healthcare to our local community and beyond.

- Good transport links
- Improving patient experience



Belfast Telegraph DIGITAL

HOME | NEWS | SPORT | BUSINESS | ENTERTAINMENT | LIFE | CARS | OPINION | TRA

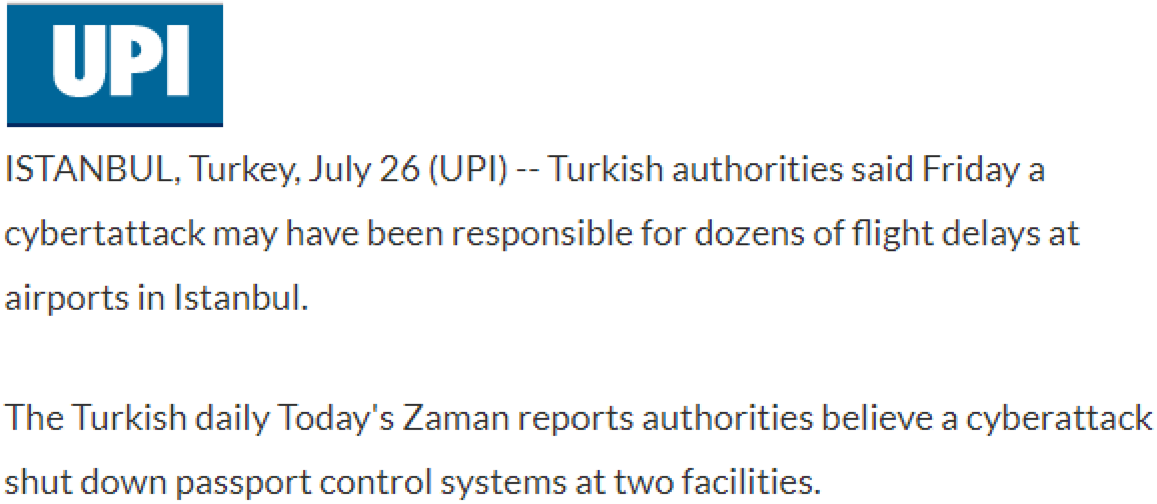
Northern Ireland | UK & World | Brexit | Technology | Jobs | Food, Drink and Hospitality | Agri |

Home › Business › Technology

NHS cyber attack: Ransomware hackers force hospitals across England to divert emergency patients as incident spreads to Scotland

Threats to Critical National Infrastructure-IV

Istanbul Airports
July 2016

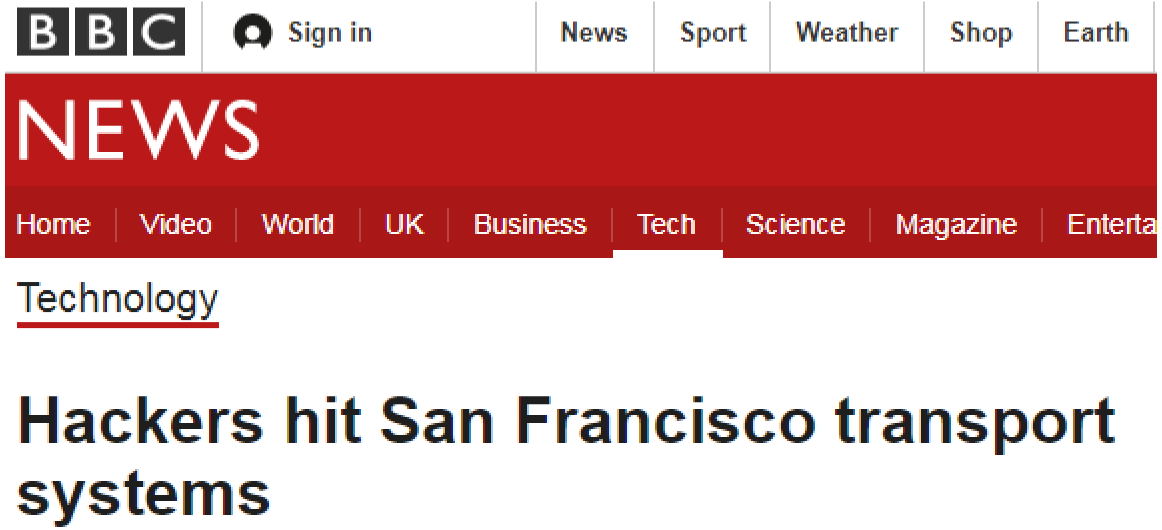


UPI

ISTANBUL, Turkey, July 26 (UPI) -- Turkish authorities said Friday a cybertattack may have been responsible for dozens of flight delays at airports in Istanbul.

The Turkish daily Today's Zaman reports authorities believe a cyberattack shut down passport control systems at two facilities.

San Francisco train system
November 2016

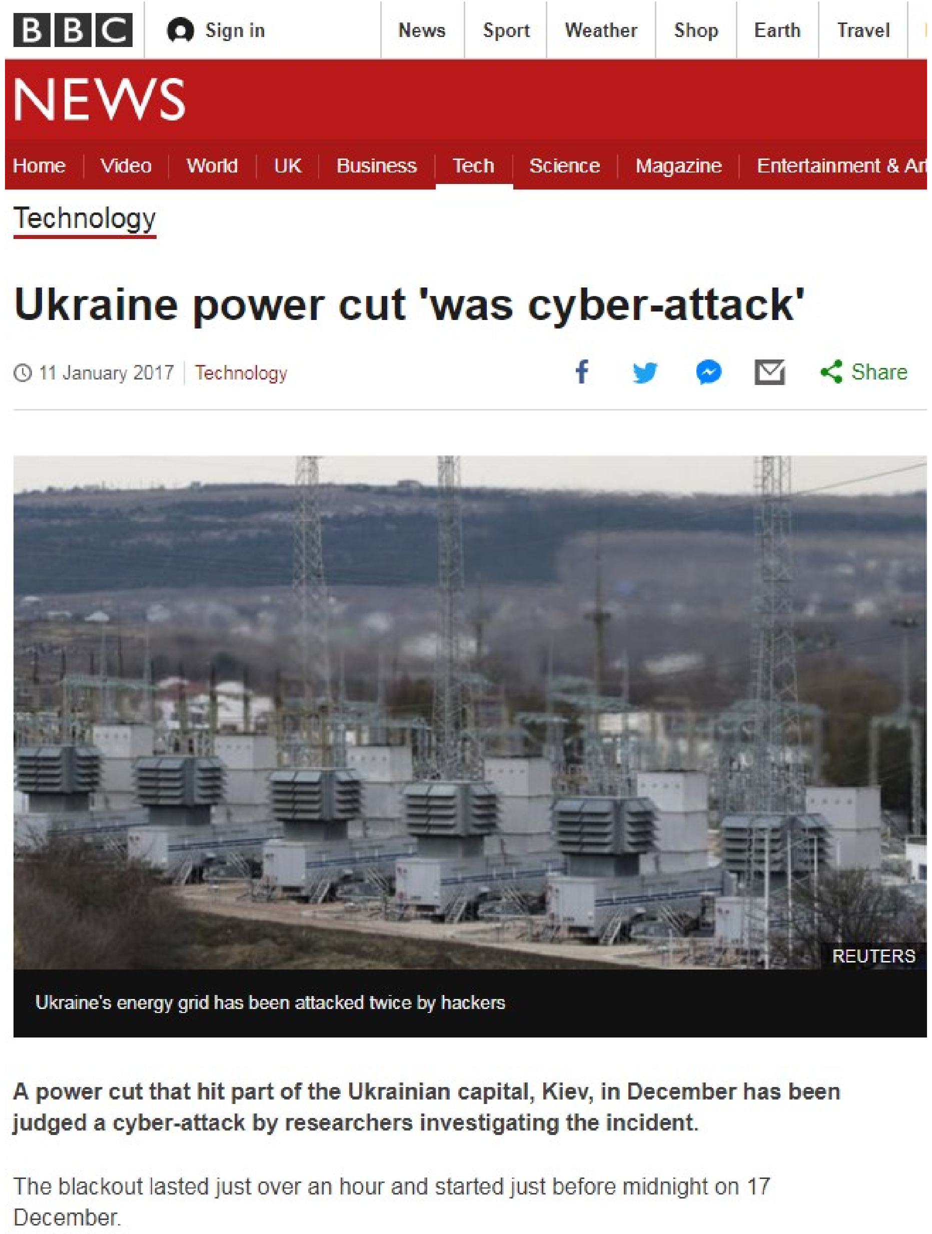


Technology

Hackers hit San Francisco transport systems

Threats to Critical National Infrastructure-V

Kiev's power grid
December 2016



Technology

Ukraine power cut 'was cyber-attack'

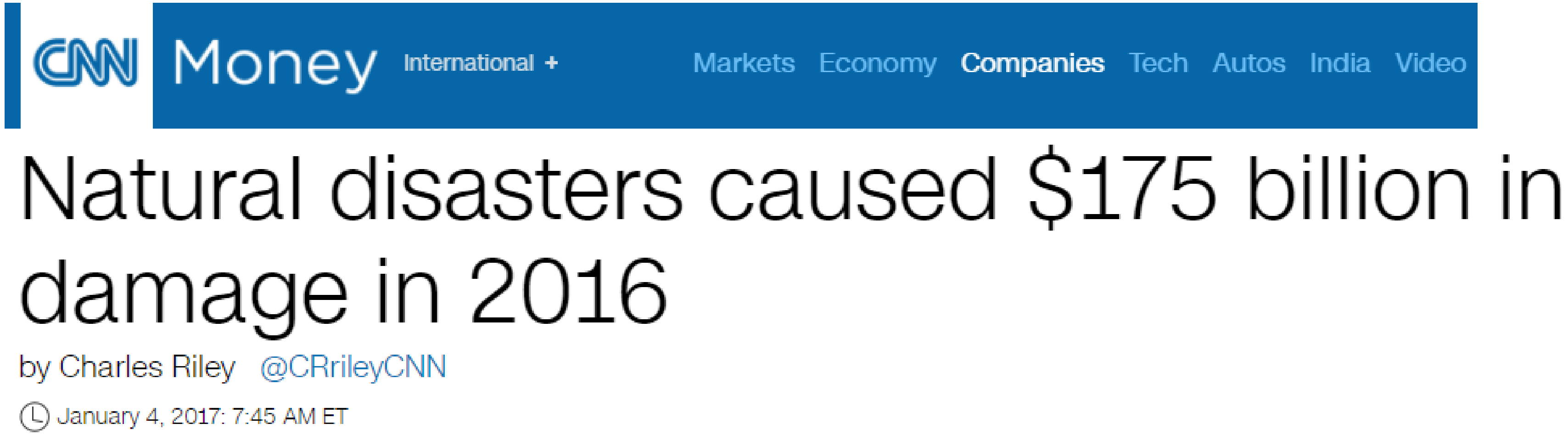
11 January 2017 | Technology

Ukraine's energy grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

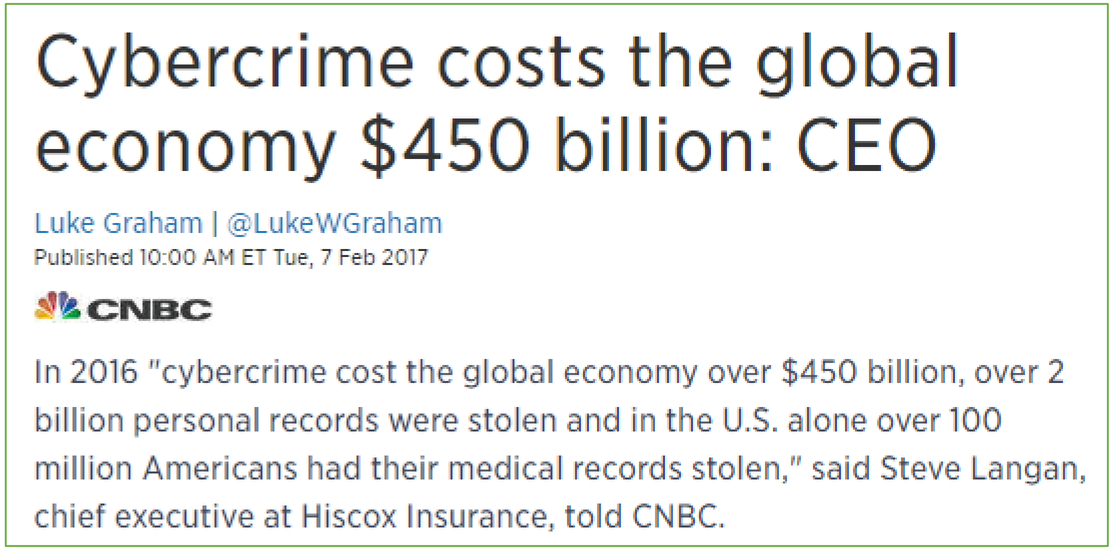
Threats to Critical National Infrastructure-VI



Natural disasters caused $175 billion in damage in 2016

by Charles Riley @CRrileyCNN

January 4, 2017: 7:45 AM ET



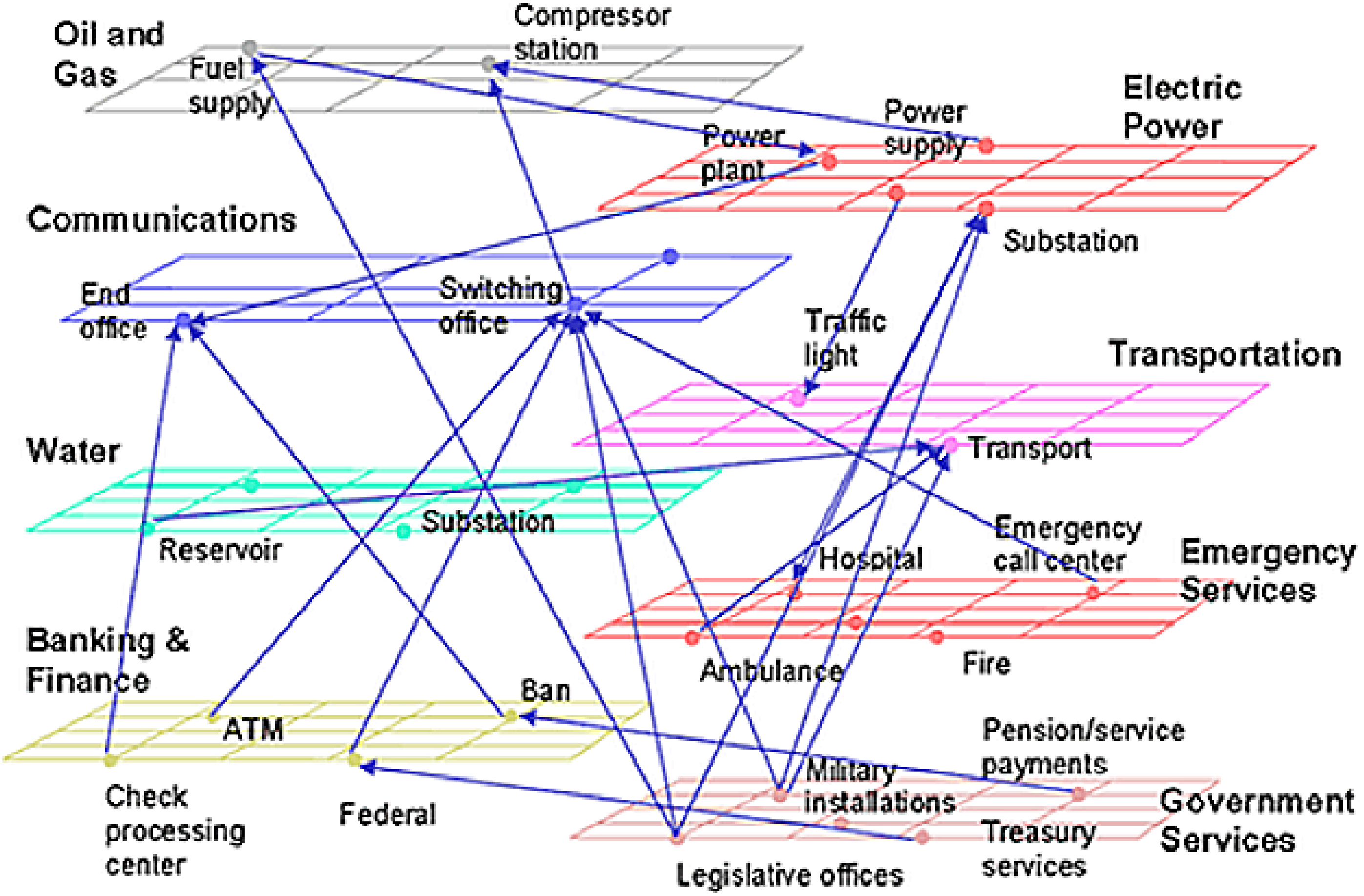
Cybercrime costs the global economy $450 billion: CEO

Luke Graham | @LukeWGraham

Published 10:00 AM ET Tue, 7 Feb 2017

In 2016 "cybercrime cost the global economy over $450 billion, over 2 billion personal records were stolen and in the U.S. alone over 100 million Americans had their medical records stolen," said Steve Langan, chief executive at Hiscox Insurance, told CNBC.

Threats to Critical National Infrastructure-VII



Cascade effect

Source : NSA

Interconnected Nature of Critical Infrastructure

Internet of Things (IoT)

Internet of Things

The ITU-T's definition of the IoT calls it "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"

What Is It?

"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication" (ITU-T)

Who Makes It?

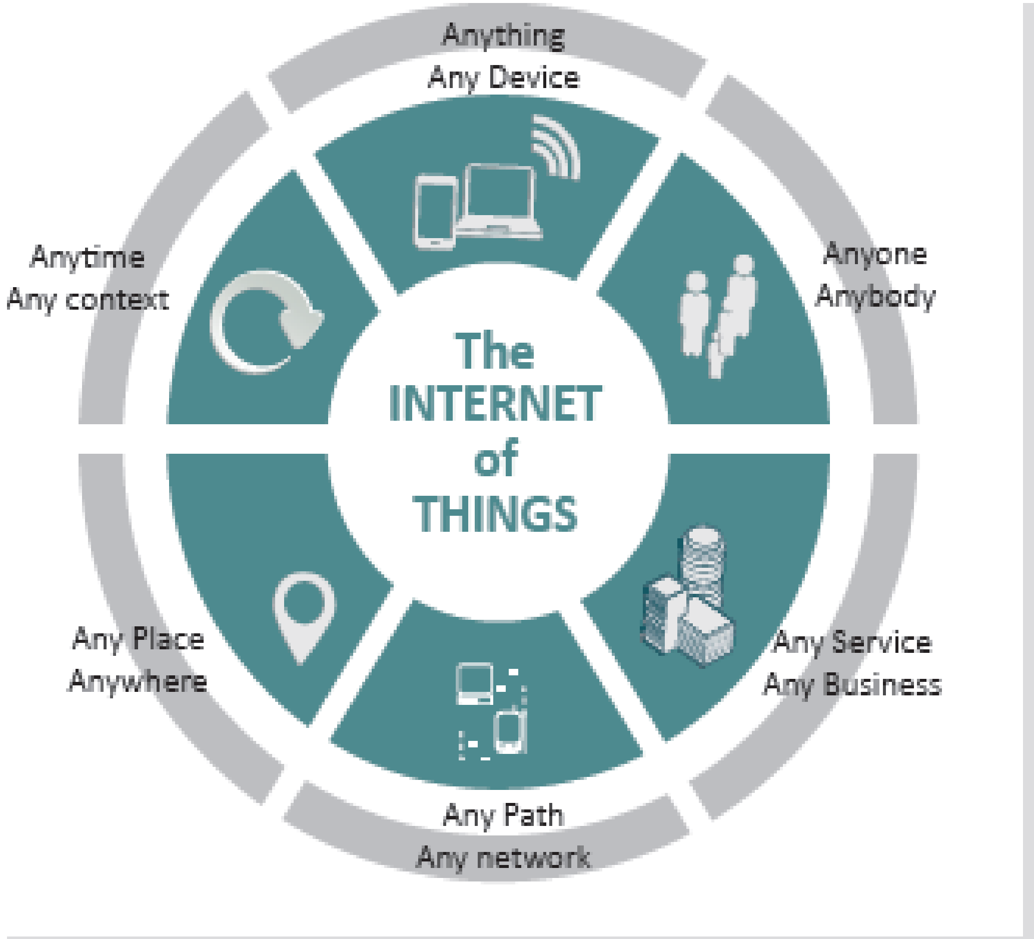
Device manufacturers, network operators, application platforms, software developers and (cloud-based) data analytics services providers

How Is It Accessed?

Connection of IoT devices via Wi-Fi, Bluetooth, mobile phone networks, specialized radio networks, global Internet

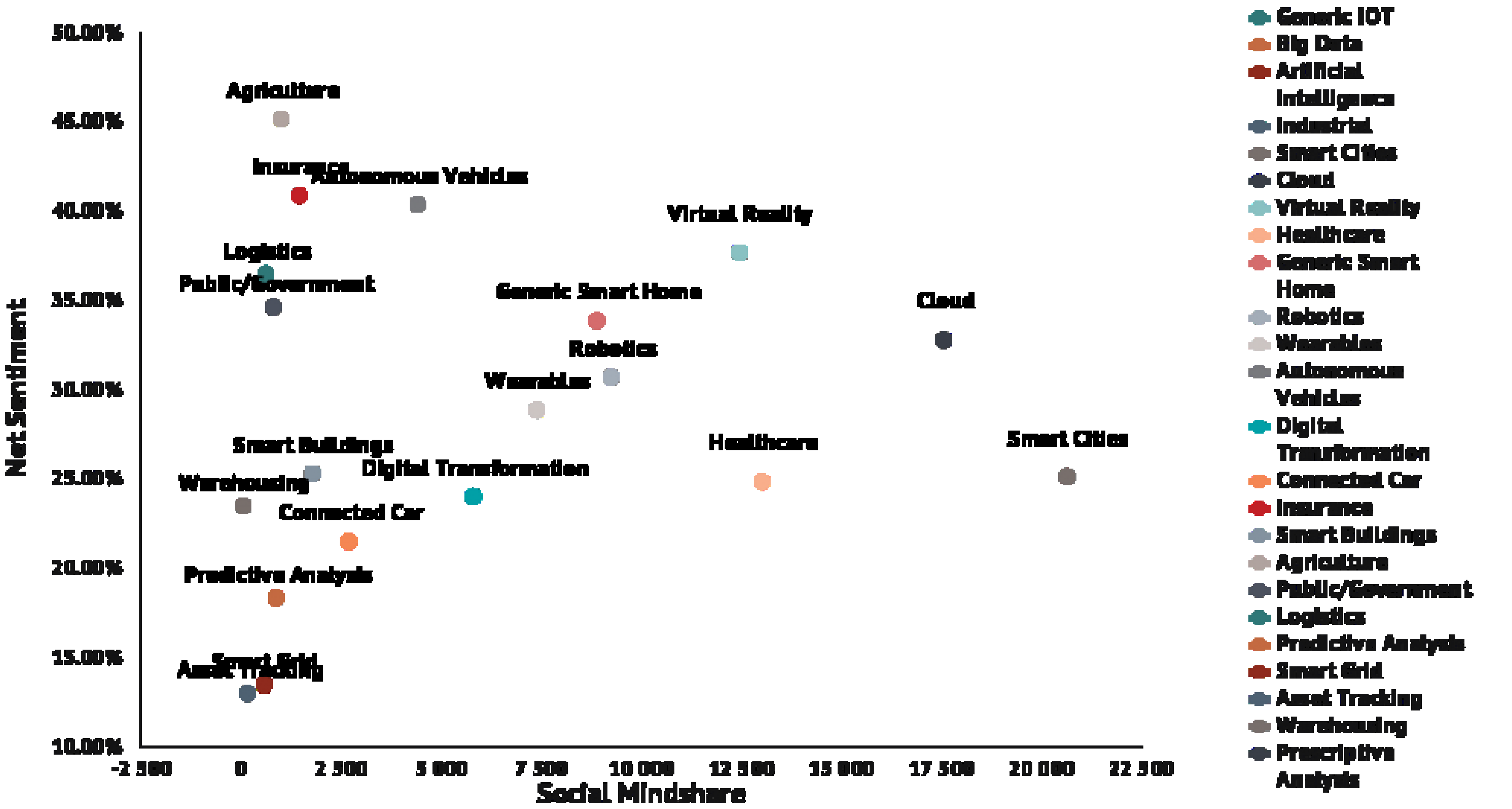
Main current areas of investment

- Smart cities
- Smart metering & grids
- Connected vehicles
- Healthcare



IoT as defined in ITU-T [ITU-T Y.2060]

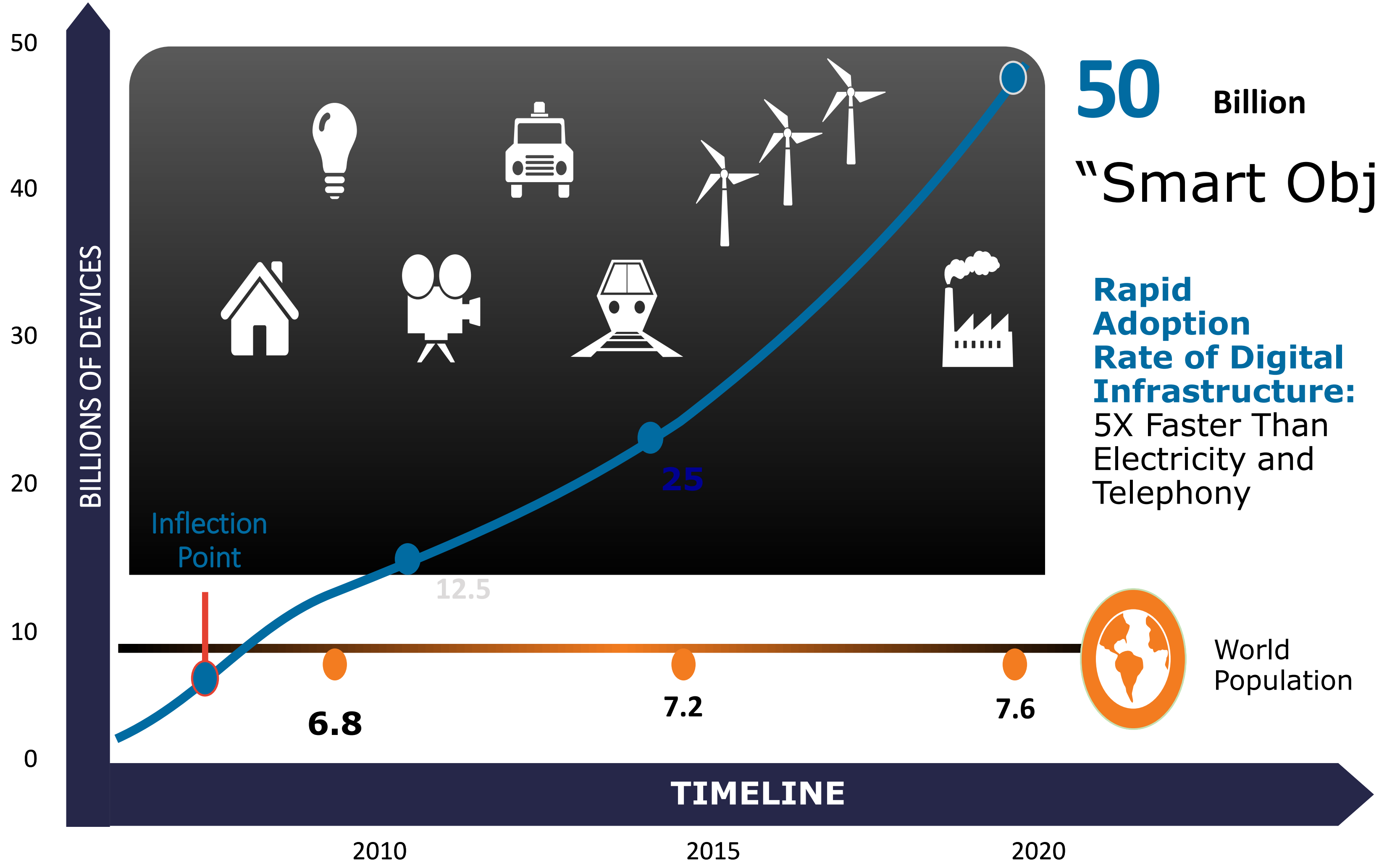
IOT Applications



For period 4/1/17 thru 6/30/17, Sources included: twitter, blog, board, facebook

©Argus Insights

IoT Is Here Now – and Growing!



50 **Billion**

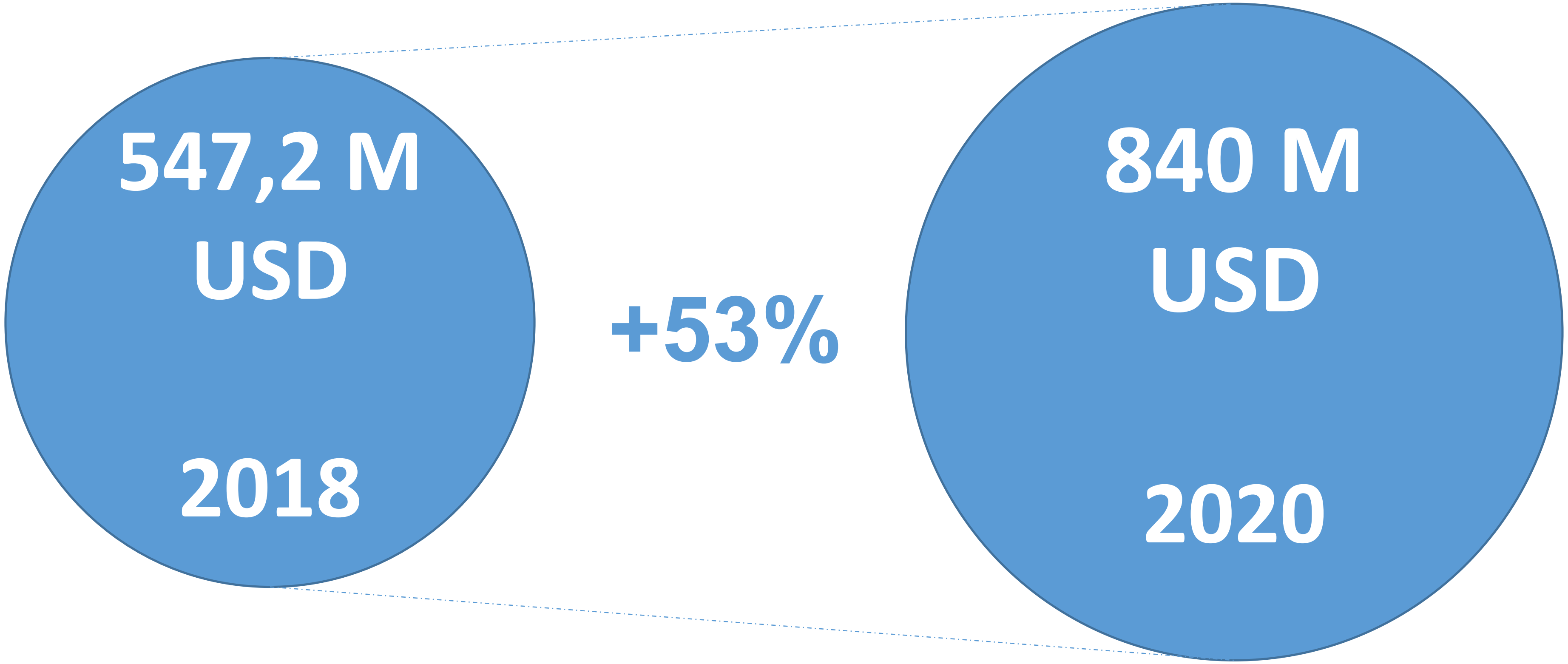
"Smart Objects"

Rapid Adoption Rate of Digital Infrastructure: 5X Faster Than Electricity and Telephony

World Population

Source: Cisco IBSG, 2011

The IoT Security Market



547,2 M USD

2018

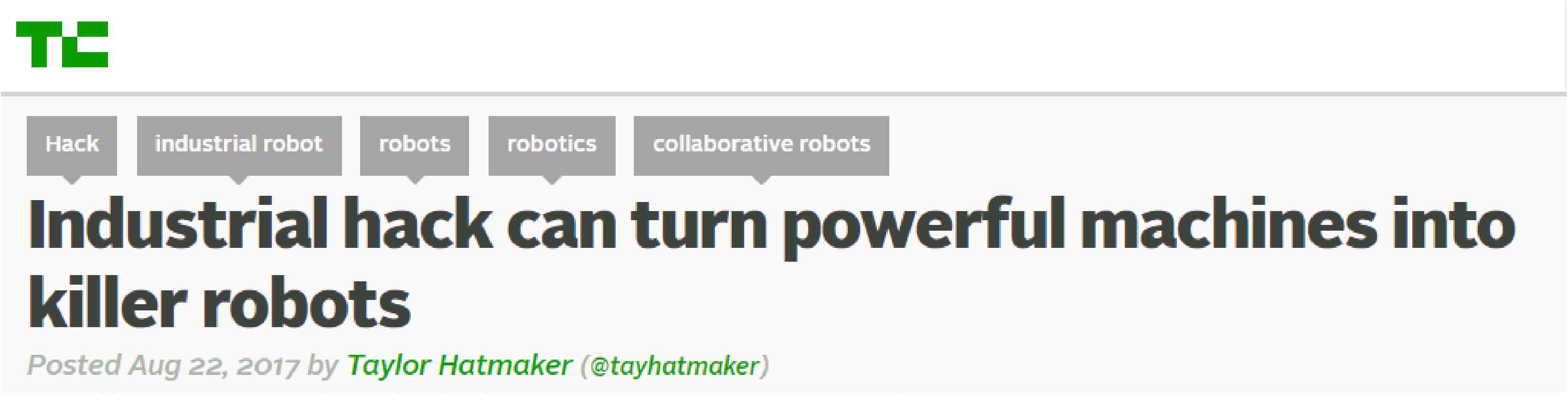
+53%

840 M USD

2020

http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/IoT-Another-opportunity-to-build-in-security-from-the-start

IoT’s security – Some Recent News

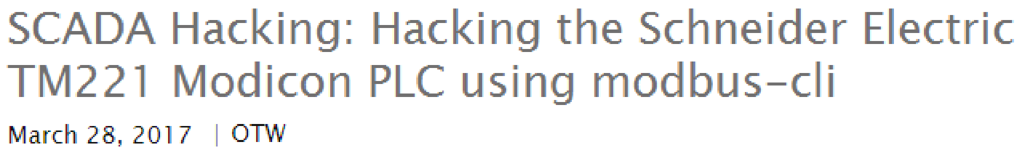


Hack | industrial robot | robots | robotics | collaborative robots

Industrial hack can turn powerful machines into killer robots

Posted Aug 22, 2017 by Taylor Hatmaker (@tayhatmaker)

https://techcrunch.com/2017/08/22/universal-robots-exploit-ioactive/



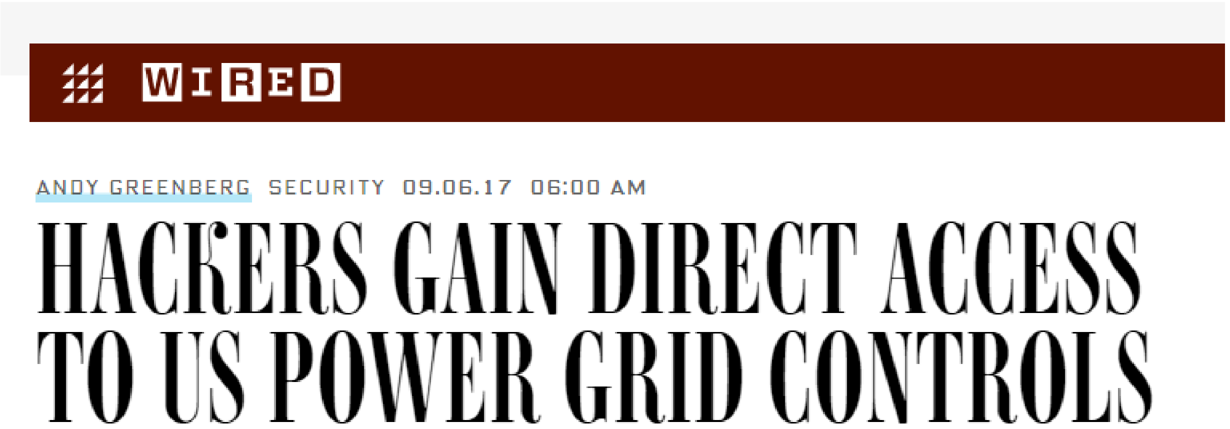
SCADA Hacking: Hacking the Schneider Electric TM221 Modicon PLC using modbus-cli

March 28, 2017 | OTW

https://www.hackers-arise.com/single-post/2017/03/28/SCADA-Hacking-Hacking-the-Schneider-Electric-TM221-Modicon-PLC-using-modbus-cli

SCADA

Supervisory Control And Data Acquisition



WIRED

ANDY GREENBERG SECURITY 09.06.17 06:00 AM

HACKERS GAIN DIRECT ACCESS TO US POWER GRID CONTROLS

https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

IoT Security goes beyond $

IoT security failures can cause both

- Financial loss
- and physical harm

http://eftm.com.au/2015/02/robots-helping-out-not-taking-over-on-the-audi-production-line-19389

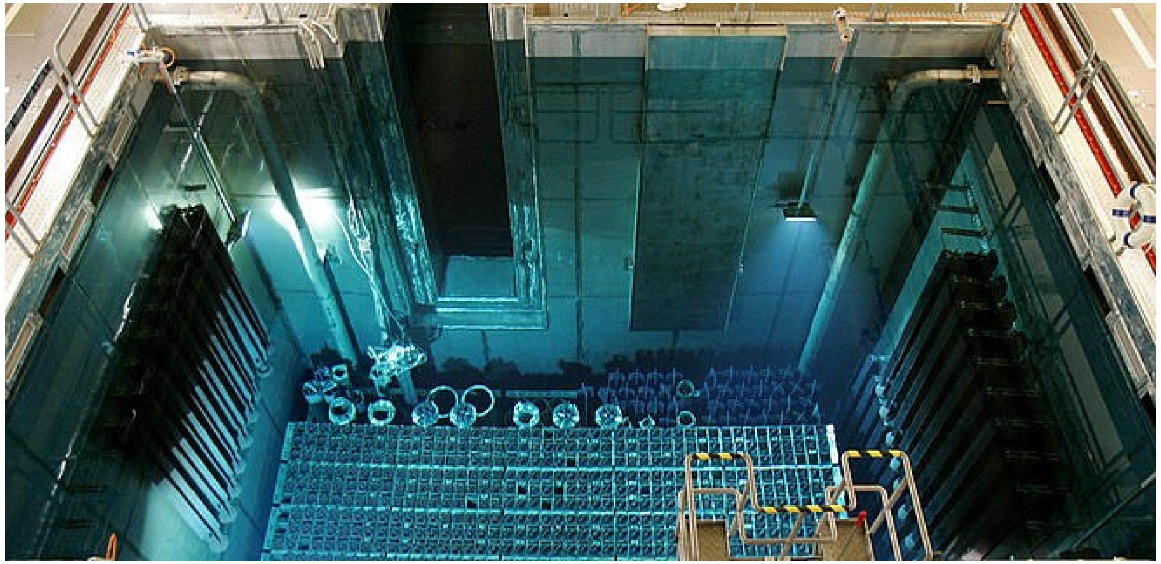


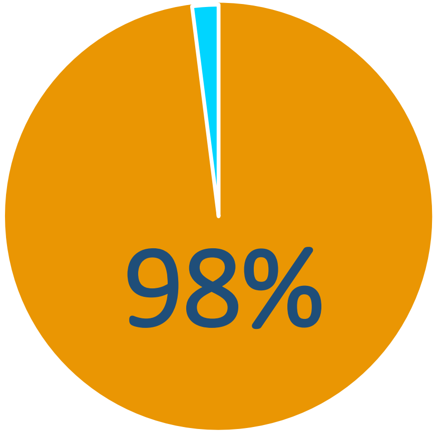
Image source: https://www.allianz.com/en/about_us/open-knowledge/topics/environment/articles/110317-nuclear-power-a-beginners-guide.html/

Source: https://www.sjm.com

IoT Security – Two risks

- Devices do something there are not supposed to do
  - ✓Example: fridges / webcams used as part of a DDoS attack (Cf. Mirai botnet)
- Devices do exactly what they are intended to do but in a devious way
  - ✓Example: Nuclear power plant enrichment centrifuges rapidly speeding up and then suddenly slow down, potentially damaging them (Stuxnet)

Looks like for IoT devices



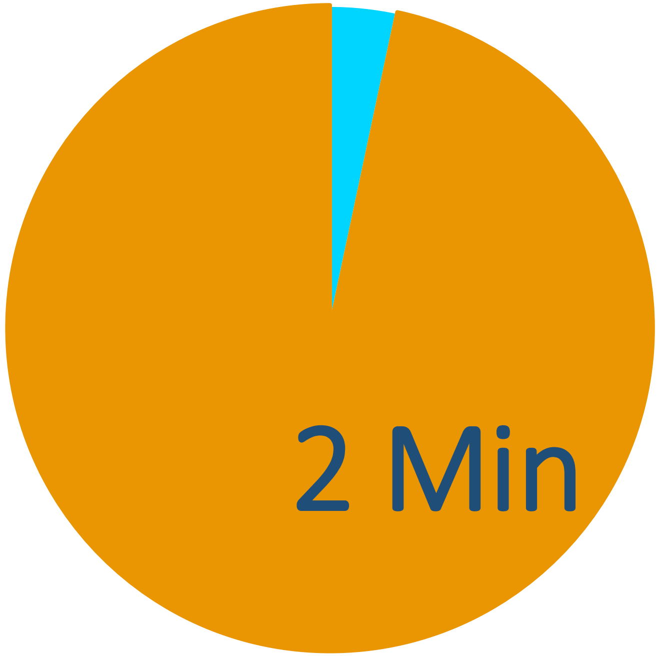
of web interfaces and administrative panels had fundamental security problems

Such as:

- ❖Hardcoded and unmodifiable admin credentials
- ❖Outdated software (e.g. web server)
- ❖Lack of HTTP traffic encryption,
- ❖Various critical vulnerabilities in the interface

Source: https://www.htbridge.com/news/application-security-trends-report-2017.html

An easy target…



Time it took for an IoT device to be attacked
(peak time during Mirai botnet period)

Source: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

IoT Device

You need only one vulnerability in only one part of the device to compromise the whole system

ITU : I Thank U