C4I 2017

2nd International Conference on C4I Alliance against Terrorism. Strategies and Capabilities

The Evolving Landscape of Cyber Breaches and Lacking Crisis Management Plan

Dr. Anibal Villalba
Senior Adviser to the President of the National Cyber Security Council
Kingdom of Spain

avillalba@oc.mde.es

Riyadh, 19 October 2017

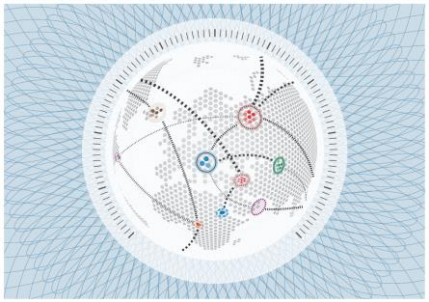
The Evolving Landscape of Cyber Breaches and Lacking Crisis Management Plan

- Cyberspace, cyber breaches, cyber risks.
- Cyber attacks within other global risks.
- Economic impact of cyber attacks.
- Cyber attacks against public sector. Spain.
- Global cyber attack. Wannacry.
- How do we organise? Do we have a plan?
- Cooperation as a must.
- Cyberterrorism and the role of Intelligence.

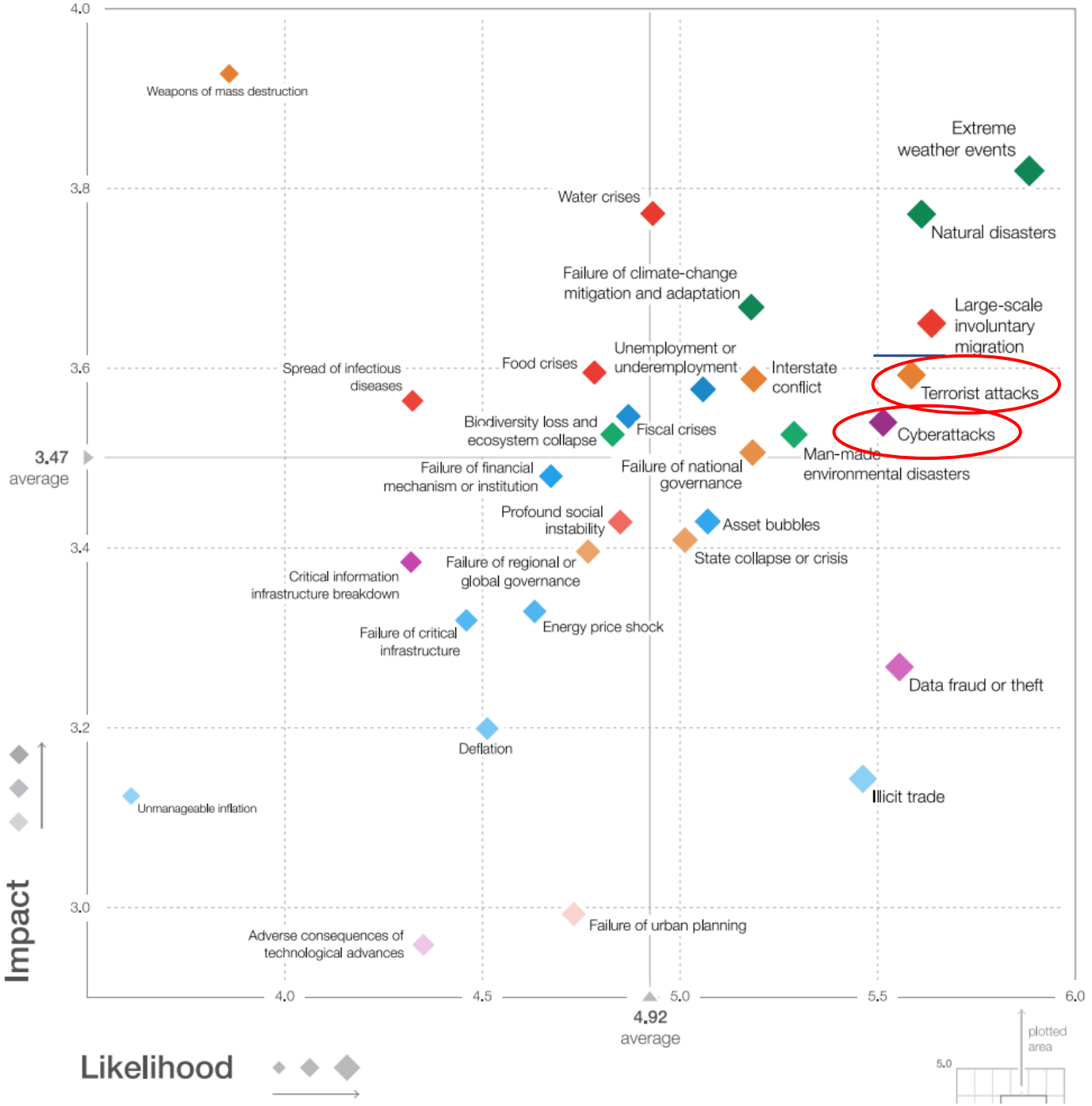
2017 This Is What Happens In An Internet Minute


BLOG
SMS
BLOG
SMS
BLOG
LIKE
SMS
BLOG

WORLD ECONOMIC FORUM

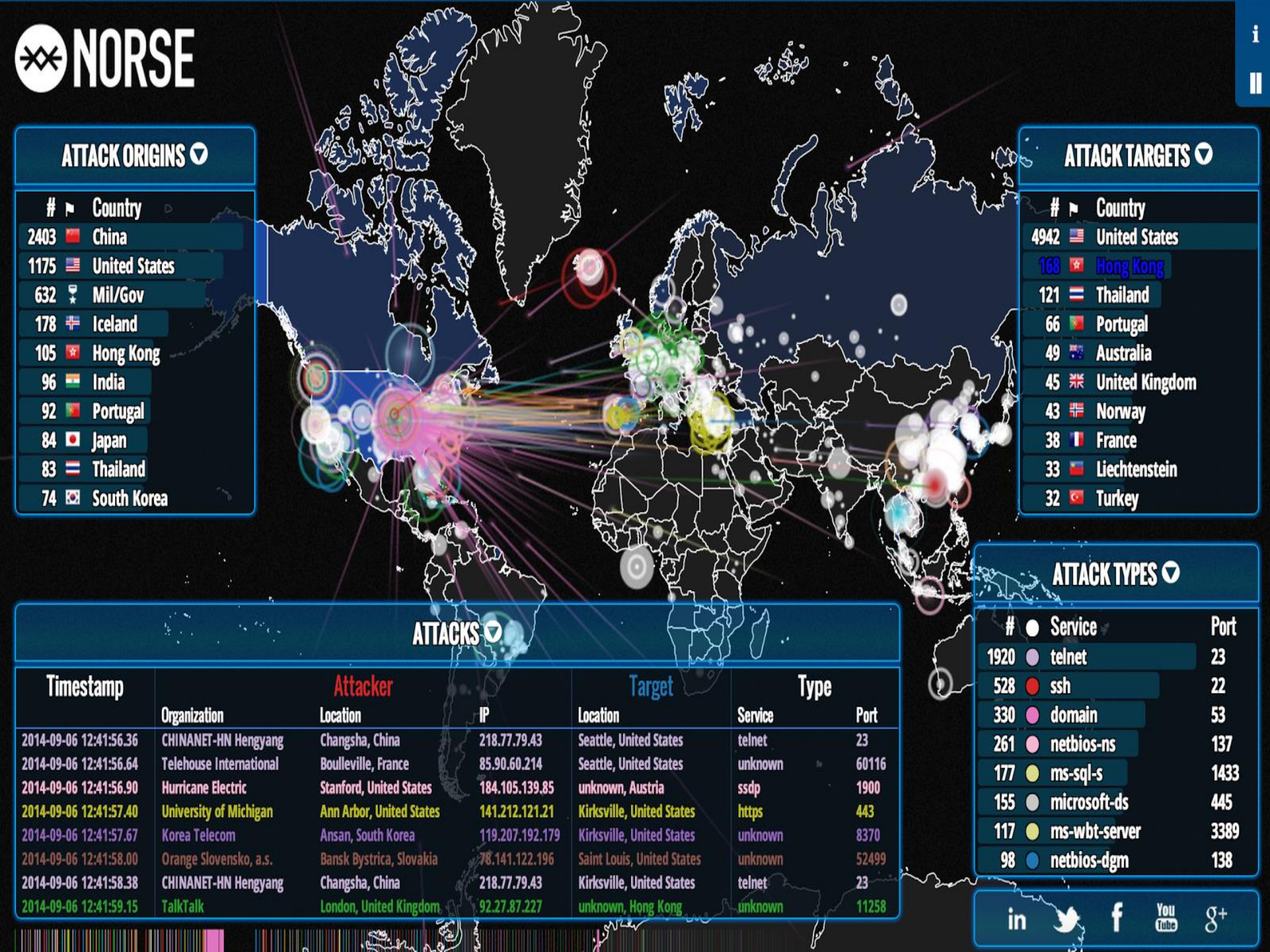


The Global Risks Report 2017

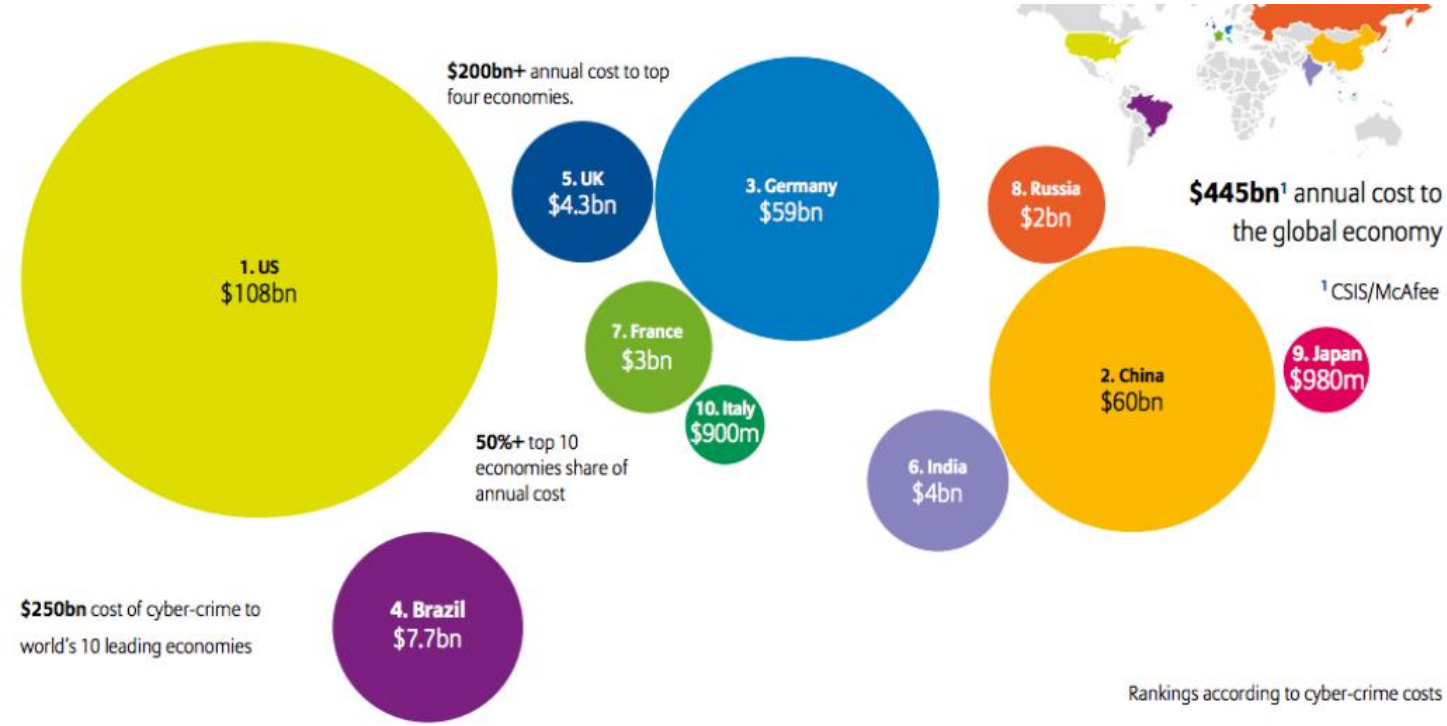


WORLD ECONOMIC FORUM

The Global Risks Interconnections


NORSE
ATTACK ORIGINS
Country
2403 China
1175 United States
632 Mil/Gov
178 Iceland
105 Hong Kong
96 India
92 Portugal
84 Japan
83 Thailand
74 South Korea
ATTACK TARGETS
Country
4942 United States
168 Hong Kong
121 Thailand
66 Portugal
49 Australia
45 United Kingdom
43 Norway
38 France
33 Liechtenstein
32 Turkey
ATTACK TYPES
Service Port
1920 telnet 23
528 ssh 22
330 domain 53
261 netbios-ns 137
177 ms-sql-s 1433
155 microsoft-ds 445
117 ms-wbt-server 3389
98 netbios-dgm 138
ATTACKS
Timestamp | Attacker: Organization, Location, IP | Target: Location | Type: Service, Port
2014-09-06 12:41:56.36 | CHINANET-HN Hengyang | Changsha, China | 218.77.79.43 | Seattle, United States | telnet | 23
2014-09-06 12:41:56.64 | Telehouse International | Boulleville, France | 85.90.60.214 | Seattle, United States | unknown | 60116
2014-09-06 12:41:56.90 | Hurricane Electric | Stanford, United States | 184.105.139.85 | unknown, Austria | ssdp | 1900
2014-09-06 12:41:57.40 | University of Michigan | Ann Arbor, United States | 141.212.121.21 | Kirksville, United States | https | 443
2014-09-06 12:41:57.67 | Korea Telecom | Ansan, South Korea | 119.207.192.179 | Kirksville, United States | unknown | 8370
2014-09-06 12:41:58.00 | Orange Slovensko, a.s. | Bansk Bystrica, Slovakia | 78.141.122.196 | Saint Louis, United States | unknown | 52499
2014-09-06 12:41:58.38 | CHINANET-HN Hengyang | Changsha, China | 218.77.79.43 | Kirksville, United States | telnet | 23
2014-09-06 12:41:59.15 | TalkTalk | London, United Kingdom | 92.27.87.227 | unknown, Hong Kong | unknown | 11258

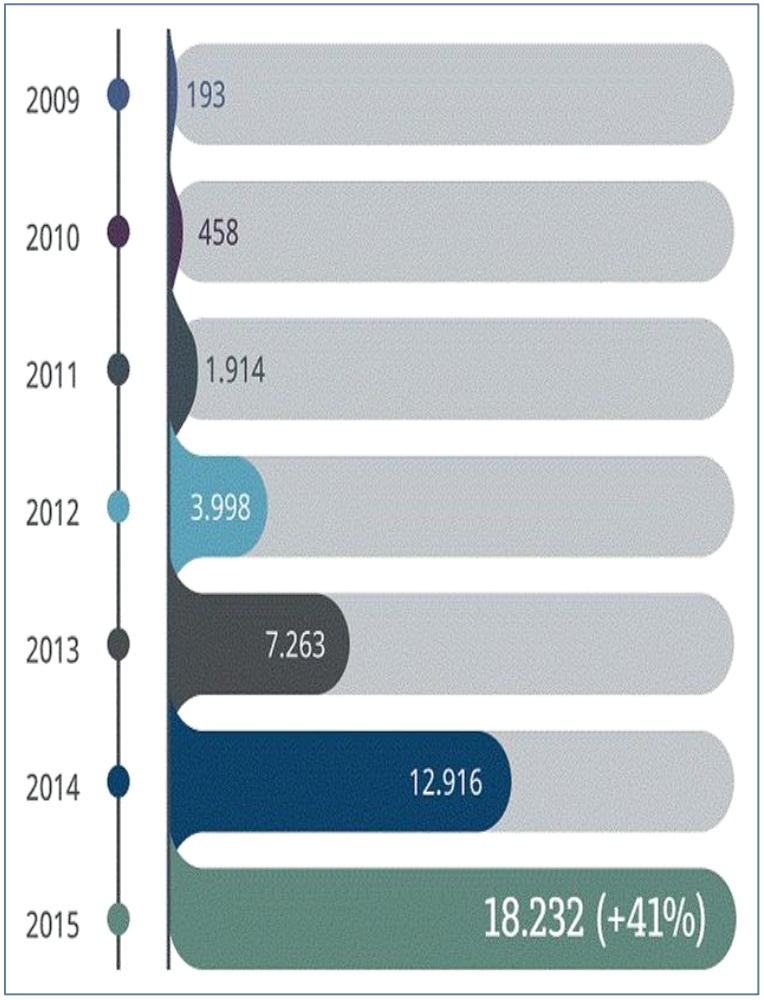
How much does cyber-crime cost the world's leading 10 economies?



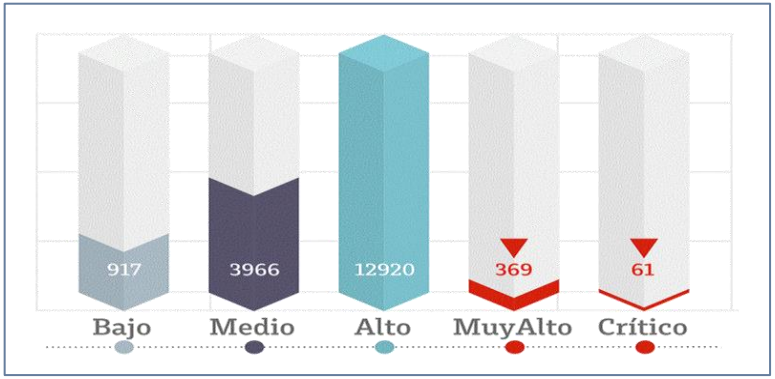
Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]	Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]
1 US	$16.8trn	.64%	$108bn	6 UK	$2.7trn	.16%	$4.3bn
2 China	$9.5trn	.63%	$60bn	7 Brazil	$2.4trn	.32%	$7.7bn
3 Japan	$4.9trn	.02%	$980m	8 Russia	$2.1trn	.10%	$2bn
4 Germany	$3.7trn	1.60%	$59bn	9 Italy	$2.1trn	.04%	$900m
5 France	$2.8trn	.11%	$3bn	10 India	$1.9trn	.21%	$4bn

Source: World Bank, CSIS/McFee Allianz Global Corporate & Speciality.

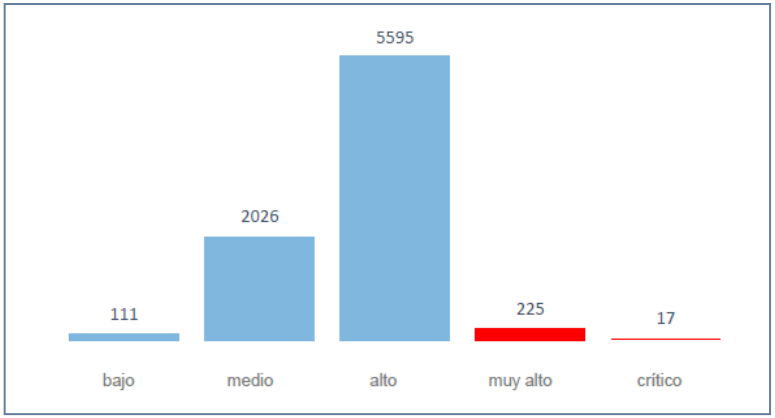
Cyberattacks against public sector in Spain



2015



2016



18 October 2017

Increase of 32 % related to same date 2016

WannaCry

Ransomware Attack

12th May 2017, malware WannaCry, attacking more than 200,000 computers in more than 150 countries


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


NSA Hackers
Shadow Brokers
CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN

Wannacry Impact

United Kingdom 48 hospitals
Russia 70.000 attacks (30% world). 1000 PCs Ministry of Interior, banks, trains, telephone networks
China 4.300 Academic institutions, hospitals, train stations
France Car factories
India Police Andhra Pradesh, ATMs
USA FedEx, health organisations
Germany train stations advertisement systems
Indonesia Hospitals
Republic of Korea Hospitals
Brazil Petrochemical, judicial system, MoFA
Spain (private sector) Telephone companies

Wannacry impact on public sector in Spain

One tablet in one ambulance in La Rioja

Four PCs in Junta de Andalucía

CCN-CERT

Centro Criptológico Nacional

Vaccine NoMoreCry

ccn-cert LORETO

20170513 CCN-CERT NoMoreCry Tool

Nombre

Old Releases

NoMoreCry2000-v0.3.exe

NoMoreCry_mutex

NoMoreCry-v0.1.exe

NoMoreCry-v0.2.exe

NoMoreCry-v0.3.exe

NoMoreCry-Win2000.exe

Only effective vaccine worldwide

CCN-CERT

ccn-cert CERT Gubernamental español

capacidad de respuesta ante incidentes seguridad tic de seguridad de la información

NIVEL DE ALERTA
MUY ALTO

CASTELLANO
ENGLISH
CATALÀ
EUSKARA
GALEGO
VALENCIÀ

CERRAR SESIÓN

ÚLTIMAS VULNERABILIDADES

CCN-CERT-1409-09702
MS14-028 - Importante: Vulnerabilidades en iSCSI p...

CCN-CERT-1409-09701
IBM Security Bulletin: Rational License Key Server...

CCN-CERT-1409-09700
IBM Security Bulletin: Exposed Keystores in IBM Ur...

ver más...

SERIES CCN-STIC

Últimas Guías CCN-STIC
CCN-STIC 455 Seguridad en iPhone (iOS 7.x)

Últimas Guías CCN-STIC Serie 800 (ENS)
CCN-STIC 851B ENS en Windows 7 Server 2008 R2 (servidor independiente)

CCN-STIC
Índice Guias CCN-STIC - Agosto 2014

CCN-STIC 001
Seguridad de las TIC en la Administración

CCN-STIC 401 - Versión julio 2014
Glosario de términos html
Glosario de términos pdf

ver más...

NOTICIAS SEGURIDAD

INFORMES CCN-CERT PÚBLICOS

CCN-CERT IA-02/14 Riesgos de uso de Windows XP tras el fin del soporte -Novedad

CCN-CERT IA-21/13 Riesgos y amenazas del BYOD

ver más...

ÚLTIMOS INFORMES DE SEGURIDAD

CCN-CERT IA-06/14 Recomendaciones generales ante ataques ... El objetivo de este informe es recoger ciertas r...

CCN-CERT ID-17/14 Informe de Código Dañino e IOC de Cri... Critroni es un troyano de tipo Ransomware (bloqueador de si...

CCN-CERT IS-07/14 Resumen ejecutivo
Principales datos extraídos del IS-07/14: incidentes gestionados en el mes de julio ...

ver más...

HERRAMIENTA PILAR

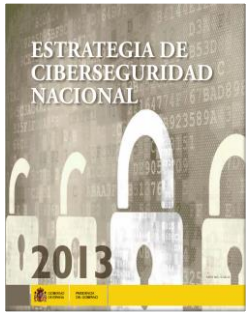
Procedimiento Informático Lógico para el Análisis de Riesgos (última versión)

ver más...

CURSOS CCN-STIC

Cybersecurity Architecture and Crisis Management in Spain

National Security Council



Chair: Prime Minister

Crisis Management Plan

National Cybersecurity Council

National Cybersecurity Action Plan

Branch Plans

Chair: Director National Intelligence

CCN-CERT

National CERT

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

CERT for business & citizens

European Commission

STATE OF THE UNION 2017

CYBERSECURITY

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."

European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017

Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

terrorism in the digital age

Terrorist groups use cyberspace for tasks that do not imply direct commissioning of attacks, but rather radicalising, recruitment, logistics work and propaganda.

terrorism in the digital age

Intelligence

vs

Cyberterrorism

C4I 2017

2nd International Conference on C4I Alliance against Terrorism. Strategies and Capabilities

The Evolving Landscape of Cyber Breaches and Lacking Crisis Management Plan

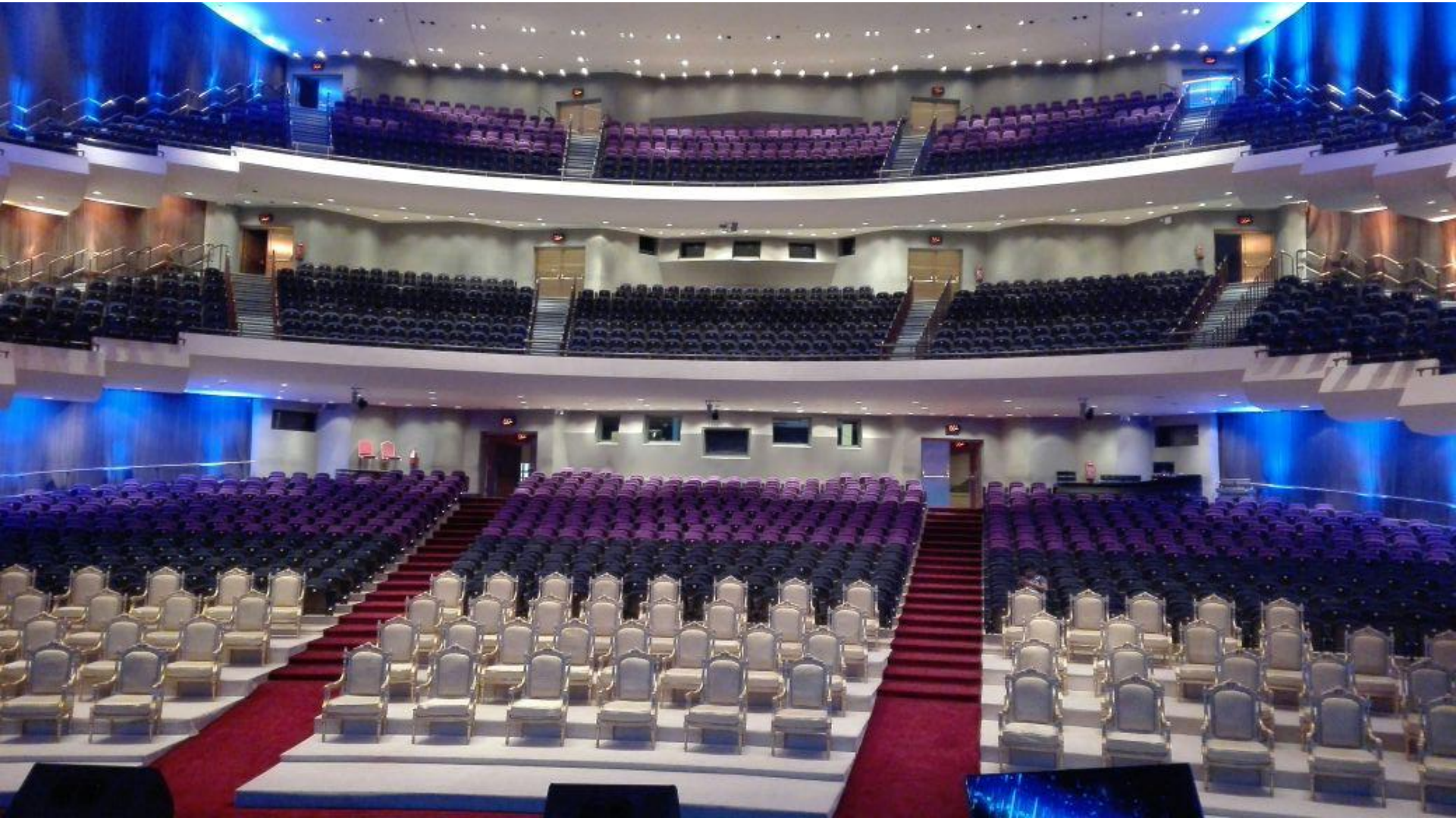
Dr. Anibal Villalba
Senior Adviser to the President of the National Cyber Security Council
Kingdom of Spain

avillalba@oc.mde.es

Riyadh, 19 October 2017

Alert System National CCN-CERT

10 COMPAÑIAS ESTRATÉGICAS



European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive[1] impact on:

75%
our economy

64%
our society

67%
our quality of life

86% of Europeans believe that the risk of becoming a victim of cybercrime is increasing.[2]

Sectors like **transport**, **energy**, **health** and **finance** have become increasingly dependent on network and information systems to run their core businesses.

The **Internet of Things (IoT)** is already a reality. There will be **tens of billions** of connected digital devices in the EU by 2020.[3]

Cyber incidents and attacks are on the rise:

+4,000 ransomware attacks per day in 2016.

In some Member States **50%** of all crimes committed are cybercrimes.

Security incidents across all industries rose by **38%** in 2015 – the biggest increase in the past 12 years.

80% of European companies experienced at least one cybersecurity incident last year.[4]

+150 countries and **+230,000** systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including

hospitals and ambulance services.