El ciberseguridad en el mediterraneo.

Dr. Gustavo Díaz Matey
@gdiazmat

- **Jean-Claude Juncker**, discurso anual sobre el Estado de la Unión (19 de septiembre de 2017) "*Europa sigue sin estar adecuadamente equipada para defenderse de los ciberataques*".
- Julian King, comisario de Seguridad de la UE, añadió el 9 de octubre: "*Hemos subestimado la escala del cibercrimen*".
- Andrus Ansip, vicepresidente responsable del Mercado Único Digital, indicó el mismo 19 de septimbre : "*Ningún país puede hacer frente, por sí solo, a los retos de ciberseguridad. Nuestras iniciativas refuerzan la cooperación de forma que los Estados miembros de la UE puedan acometer juntos estos desafíos*".
- John Arquilla and David F. Ronfeldt, The Advent of Netwar (Santa Monica: RAND, 1996).

RAND CORPORATION

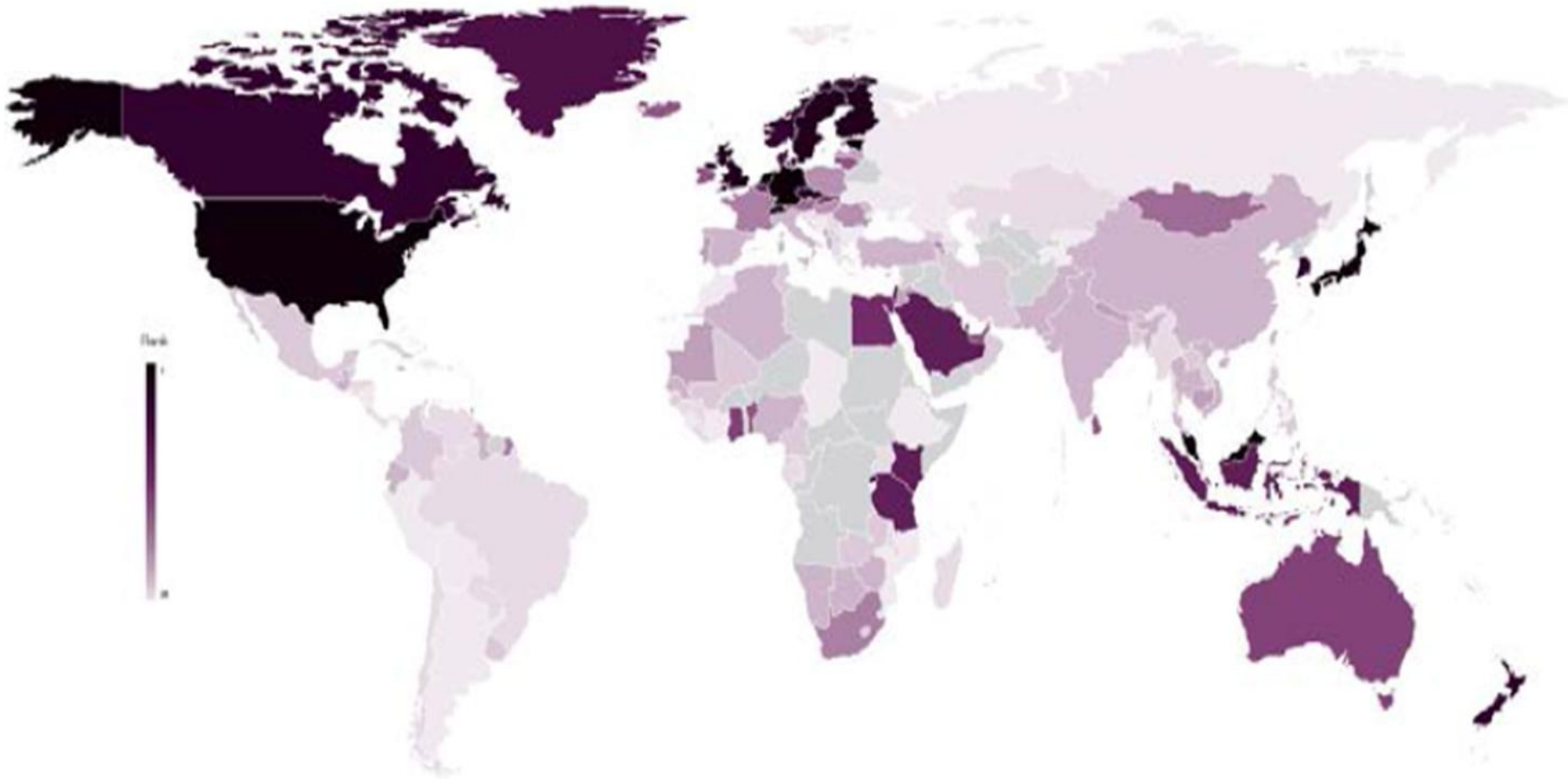

JVC
POLAROID
SONY
Walkman
SPORTS

All this technology is making us antisocial

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2016 - Update						
World Regions	Population (2016 Est.)	Population % of World	Internet Users 30 June 2016	Penetration Rate (% Pop.)	Growth 2000-2016	Table % Users
Asia	4,052,652,889	55.2 %	1,846,212,654	45.6 %	1,515.2%	50.2 %
Europe	832,073,224	11.3 %	614,979,903	73.9 %	485.2%	16.7 %
Latin America / Caribbean	626,119,788	8.5 %	384,751,302	61.5 %	2,029.4%	10.5 %
Africa	1,185,529,578	16.2 %	340,783,342	28.7 %	7,448.8%	9.3 %
North America	359,492,293	4.9 %	320,067,193	89.0 %	196.1%	8.7 %
Middle East	246,700,900	3.4 %	141,489,765	57.4 %	4,207.4%	3.8 %
Oceania / Australia	37,590,820	0.5 %	27,540,654	73.3 %	261.4%	0.8 %
WORLD TOTAL	7,340,159,492	100.0 %	3,675,824,813	50.1 %	918.3%	100.0 %

Todos los datos apuntan a que el número de dispositivos conectados a Internet se triplicará en 2020, pasando de 13.400 millones a 38.500 millones, esperándose que la proporción de productos vendidos vía comercio electrónico aumente más del doble, del 6% en 2014 al 12.8% en 2019.(*World Economic Forum, "Understanding Systemic Cyber Risk", Octubre, 2016.*)

- La figura siguiente muestra el riesgo de ciberataques percibido por distintas regiones mundiales[10].



Top 5 Source Countries for DDoS Attacks, Q1–Q4 2016

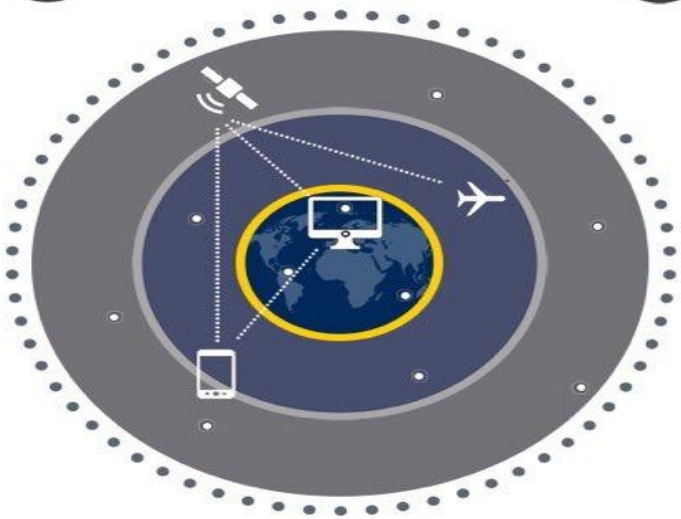
Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
China	16%	China	40%	China	19%	U.S.	24%
	115,478		306,627		81,276		180,652
U.S.	10%	U.S.	12%	U.S.	14%	U.K.	10%
	72,598		95,004		59,350		72,949
Turkey	6%	Taiwan	4%	U.K.	10%	Germany	7%
	43,400		28,546		44,460		49,408
Brazil	5%	Canada	3%	France	6%	China	6%
	36,472		20,601		23,980		46,783
South Korea	4%	Vietnam	3%	Brazil	3%	Russia	4%
	31,692		20,244		13,502		33,211

Ciberespacio como nuevo dominio junto con el espacio terrestre, aéreo, marítimo y espacial.

The Cyber criminal community is evolved from Morris Worm to the ransomware and other organized crime that have high payoff, many countries are working to stop such attacks, but these attacks are contiously changing and affecting brutally to our businesses and nation.

Principales características de los espacios comunes globales

CIBERESPACIO



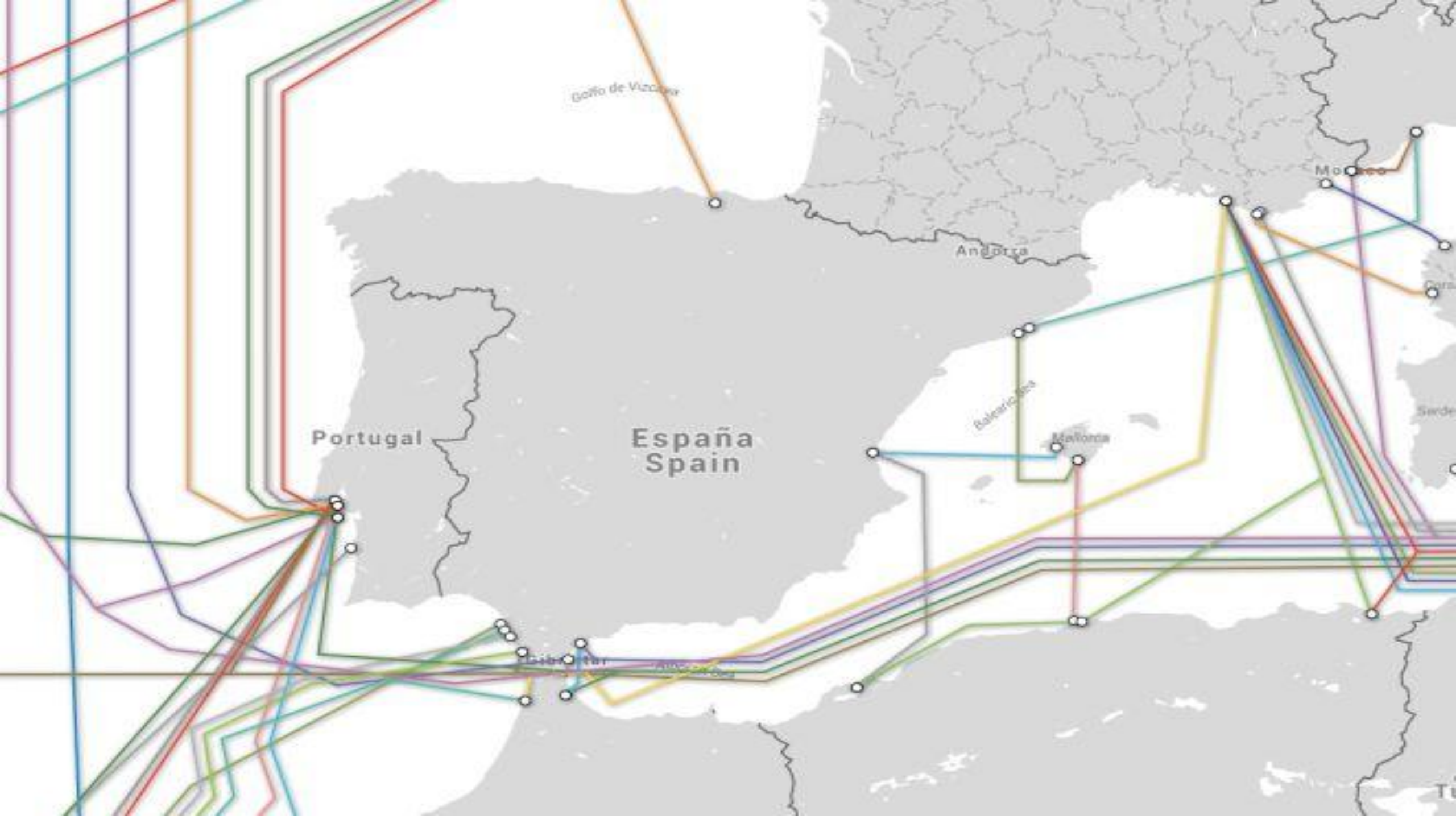
ESPACIO MARÍTIMO

ESPACIO AÉREO Y ULTRATERRESTRE

PRINCIPALES CARACTERÍSTICAS

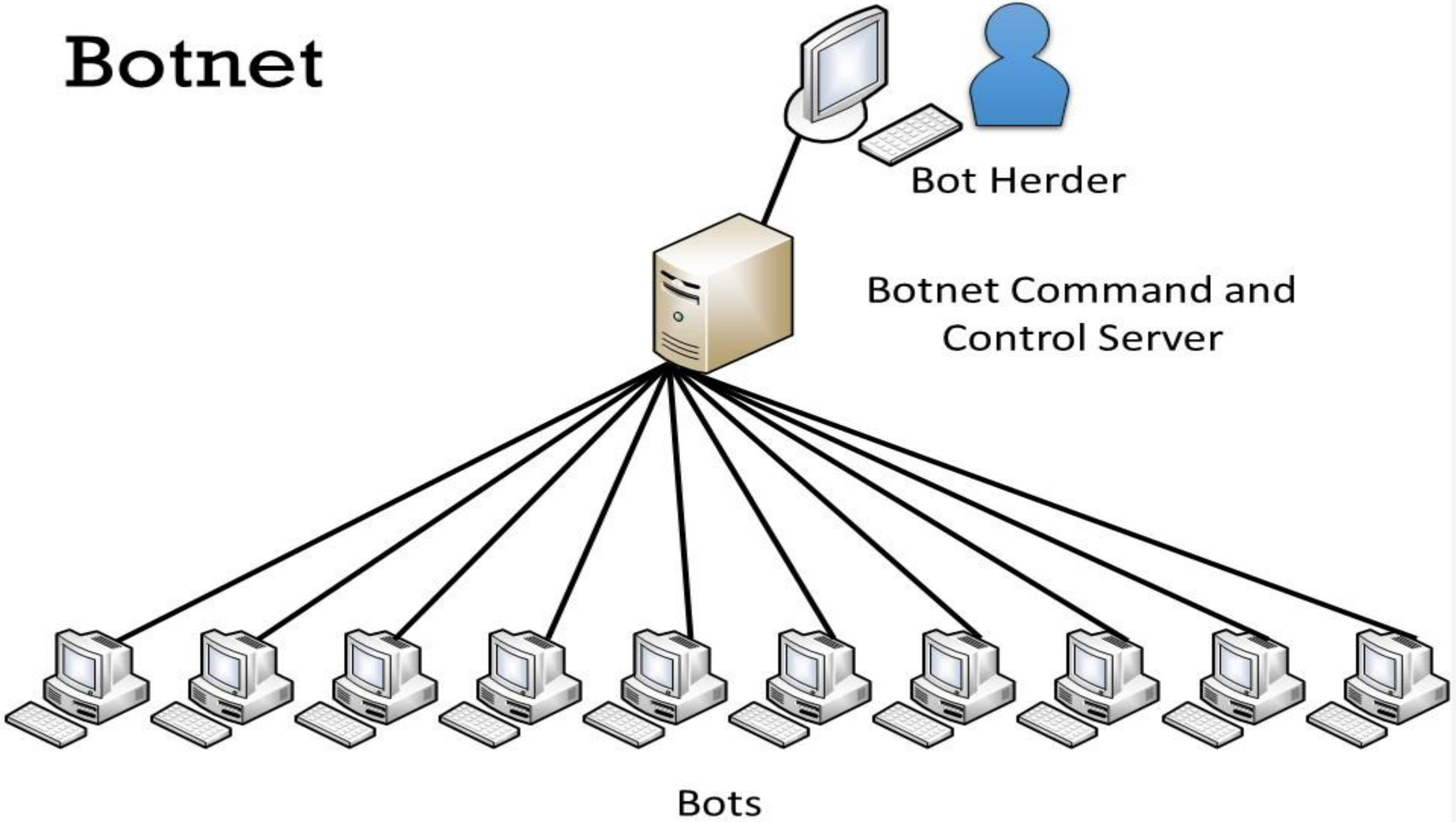
- Apertura geográfica y funcional
- Ausencia de soberanía y jurisdicción por parte de los Estados
- Facilidad de acceso
- Dificultad de atribución de las acciones que en ellos tienen lugar

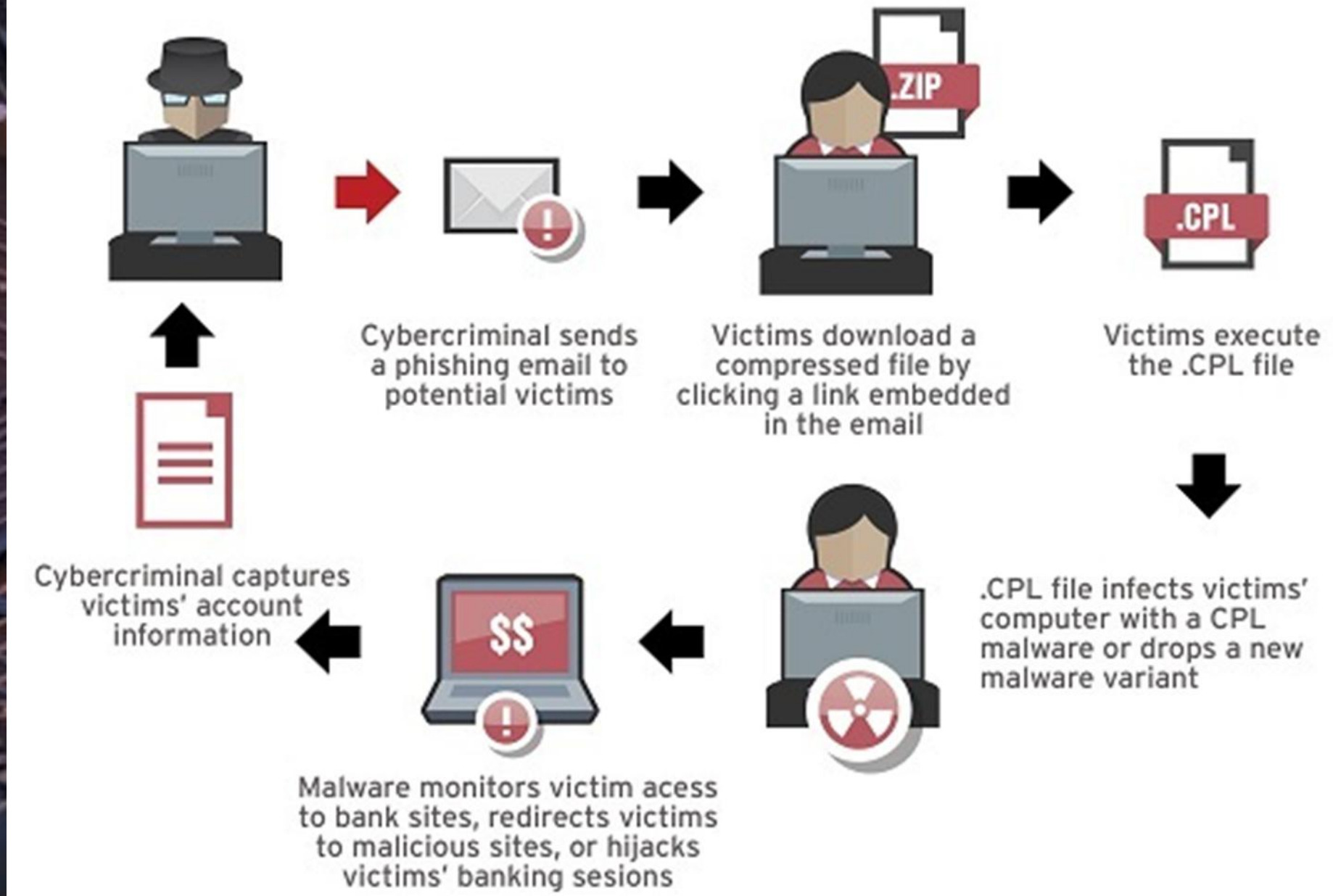

There is
noCloud
just other people's
computers


Golfo de Vizcaya
Andorra
Portugal
España
Spain
Mallorca


malware

Botnet




.ZIP
.CPL
$$
Cybercriminal sends a phishing email to potential victims
Victims download a compressed file by clicking a link embedded in the email
Victims execute the .CPL file
.CPL file infects victims' computer with a CPL malware or drops a new malware variant
Malware monitors victim acess to bank sites, redirects victims to malicious sites, or hijacks victims' banking sesions
Cybercriminal captures victims' account information

Riesgos y Amenazas a la Ciberseguridad Nacional

"On the Internet, nobody knows you're a dog."

Características de los ciberataques

Bajo Coste

- muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un coste muy reducido.

Ubicuidad y fácil ejecución

- la ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.

Efectividad e impacto

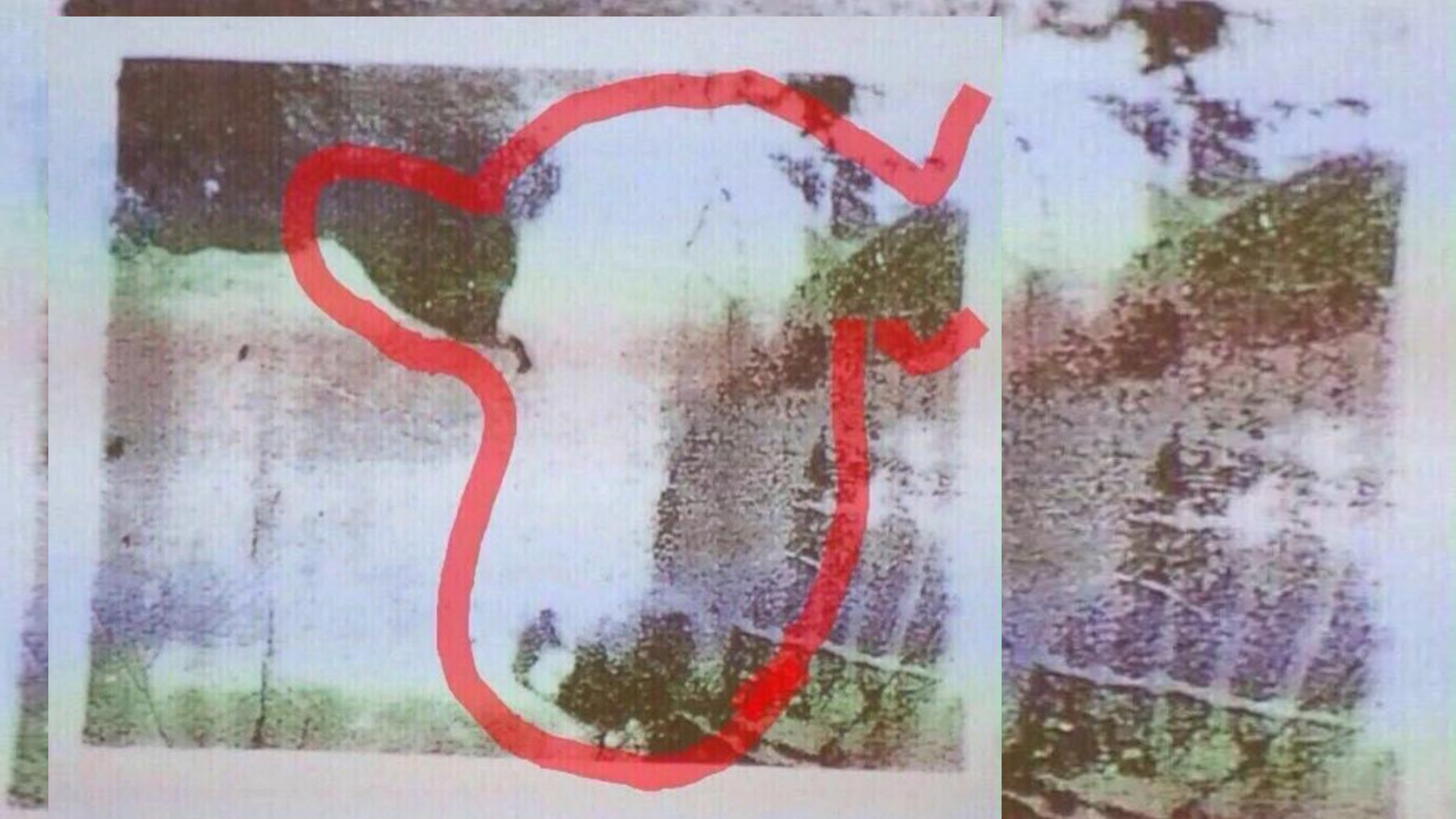
- si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. La ausencia de políticas de ciberseguridad, la insuficiencia de recursos y la falta de sensibilización y formación pueden facilitar este adverso resultado.

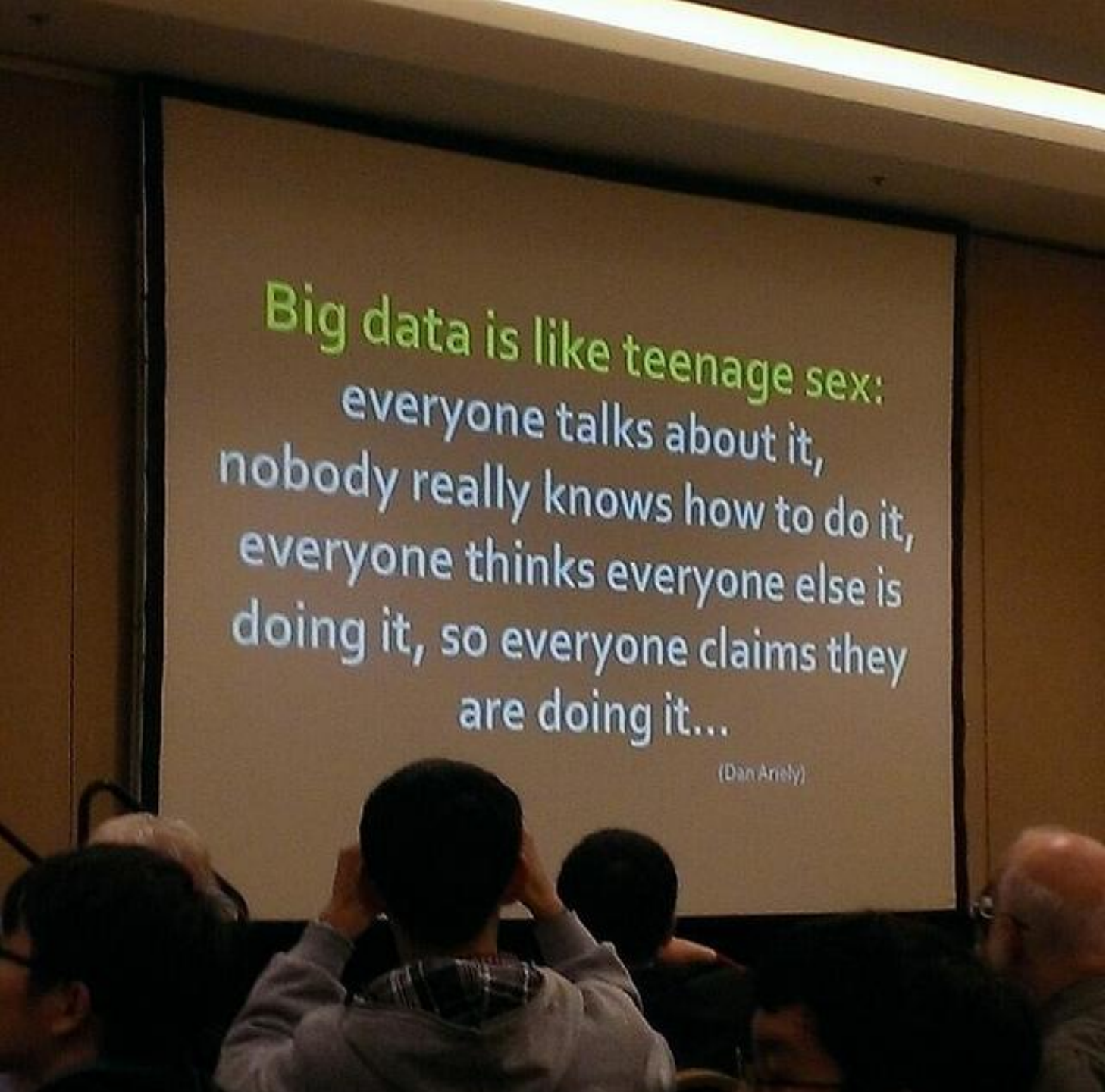
Reducido riesgo para el atacante

- la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificulta la persecución de la acción.

ENISA: The cost of incidents affecting CIIs. Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII) (Agosto, 2016)

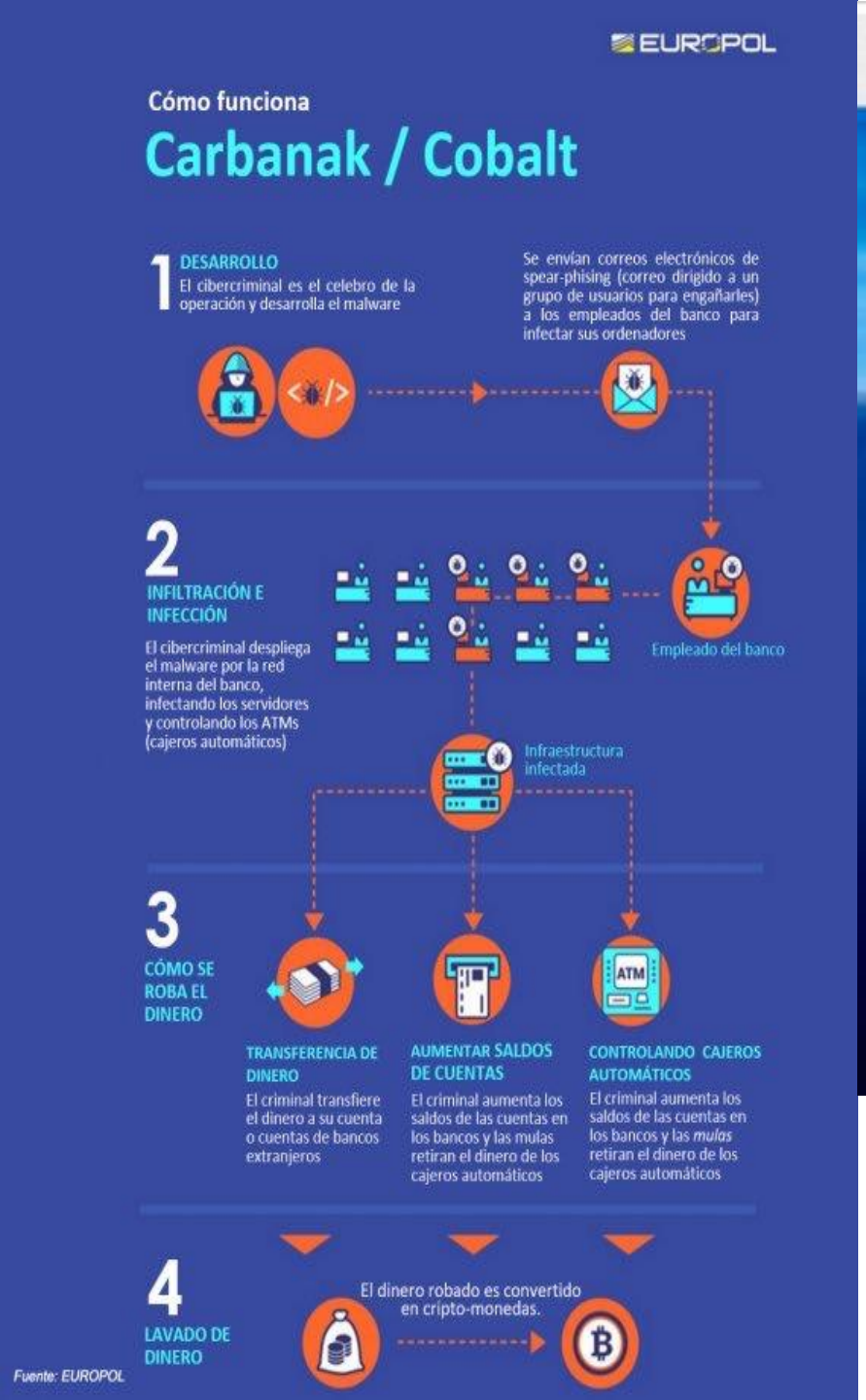
Costes de tiempo de inactividad: Las organizaciones atacadas pueden verse obligadas a cerrar sistemas para hacer frente a la infección. Los clientes, por tanto, se verán afectados. Debido a este tiempo de inactividad, la organización podría experimentar pérdidas económicas y daños reputacionales. En el caso de empresas de servicios públicos, la falta de energía o de agua podría afectar a millones de personas.	**Costes económicos**: Las empresas deben hacer frente a costes derivados de la respuesta a incidentes. Además, las organizaciones atacadas podrían también tener que hacer frente a responsabilidad económica frente a sus clientes e, incluso, al pago de cuantiosas sanciones por motivos legales.
Pérdida de datos: La pérdida de datos debido a que los archivos están cifrados y / o robados puede tener un enorme impacto en las empresas. La pérdida de los registros de la empresa, la información personal identificable de los clientes (PII) o la propiedad intelectual pueden afectar significativamente las finanzas, la marca y la reputación de la organización. Además, los ciberdelincuentes pueden amenazar con publicar datos robados, en un intento de obtener más dinero de la víctima.	**Pérdida de vidas**: En el caso de un hospital u otra organización médica, la vida de los pacientes puede ponerse en riesgo, ya que el equipamiento médico esencial podría verse afectado. Los registros de los pacientes, incluyendo la historia clínica, también pueden quedar inaccesibles, lo que provocaría retrasos en el tratamiento o, incluso, la prescripción de medicamentos incorrectos.



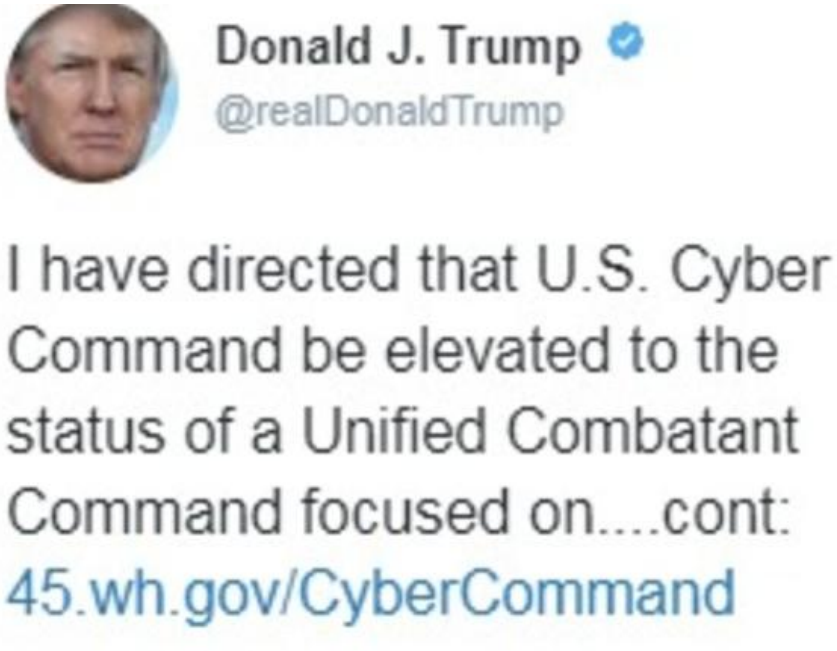

Big data is like teenage sex:
everyone talks about it,
nobody really knows how to do it,
everyone thinks everyone else is
doing it, so everyone claims they
are doing it...
(Dan Ariely)

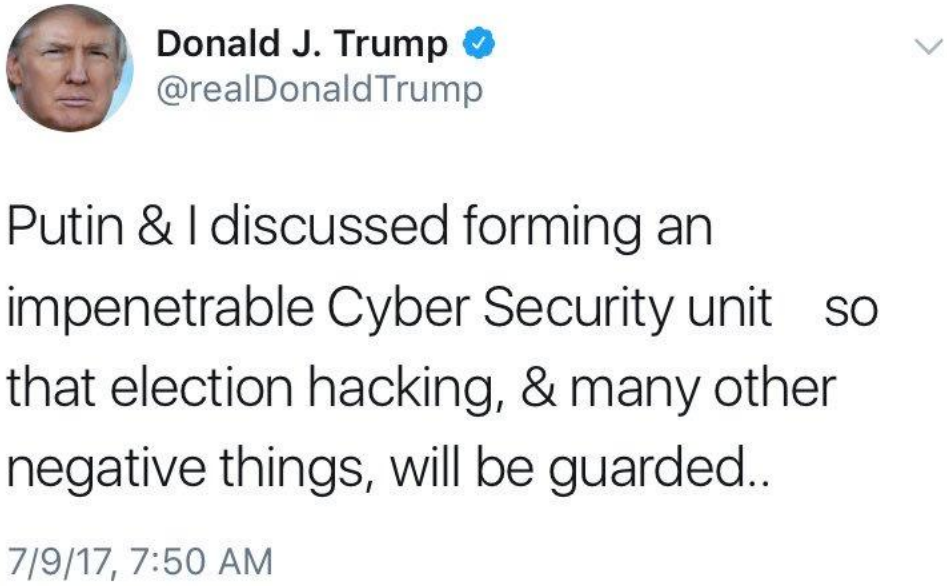
Dan Anely.

- **Estonia** – 26 de abril de 2007. Ataque a las web estatales, caída de
- **Stuxnet** troyano avanzado, que aprovecha la vulnerabilidad MS10- operativos Windows CC, empleados en los sistemas SCADA (Supervisory Control and Data Acquisition) fabricados por Siemens y que se utiliza en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Contra las centrifugadoras en Irán.
- **Crimea /Ucrania** – 23 de diciembre de 2015. Mail de suplantación de identidad en eléctricas Ucranianas para acceder al programa de comandos de control de subestaciones eléctricas.
- **Infomnapal** – Guerra de información contra Rusia publicando información de soldados rusos en la ocupación de Ucrania. RUH8 – Publicación de correos de Bladimir Surco (mano derecha de Putin).
- 2016. Filtración a Wikileaks de correos del partido demócrata.
- 14 mayo de 2017 Virus Wanna Cryt (cifrado de datos).
- **www.cfr.org**



https://cybermap.kaspersky.com/





O), "Improving Critical
inary Cybersecurity Fran

epartamento de Estado
Cyberspace Policy State
el trabajo del Departamento para implementar la President's 2011 International **Strategy for CyberspacePlan**.

- En julio de 2016, se publicó en Estados Unidos la **Presidential Policy Directive (ppd-41): United States Cyber Incident Coordination**. Esta Directiva Presidencial establece los principios que rigen la respuesta del Gobierno Federal a cualquier ciberincidente.
- En diciembre de 2016 la Commission On Enhancing National Cybersecurity publicó el **Report on Securing and Growing the Digital Economy.**
- Executive Order 13800, **Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**, (EO 13800 or EO) 11 DE Mayo de 2017.

- EE.UU. culpó a Corea del Norte del ciberataque "Wannacry", ocurrido en mayo pasado y que bloqueó más de 200.000 computadores de empresas en 150 países. El asesor de Seguridad Nacional Tom Bossert explicó que el Gobierno basa sus acusaciones en "enlaces técnicos a cibermedios, tradecraft (espionaje comercial) e infraestructura operacional de Corea del Norte previamente identificados".

ESTRATEGIA DE **SEGURIDAD NACIONAL**

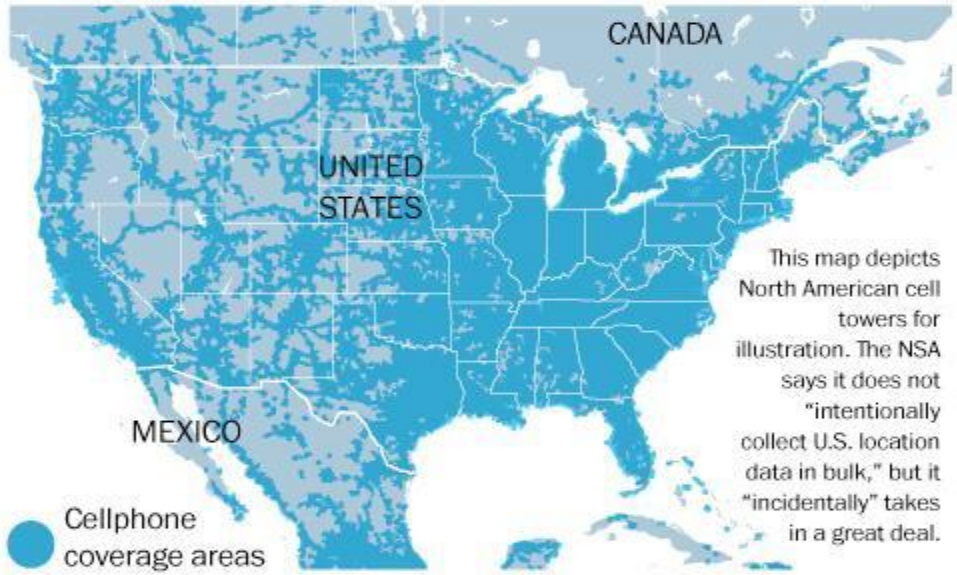
2017

El entorno ha cambiado de forma significativa desde la aprobación de la Estrategia 2013. Nos enfrentamos a una realidad definida por dinámicas a menudo opuestas, a un mundo globalizado, pero a su vez fragmentado y competitivo, un espacio donde la ambigüedad se ha convertido en uno de los mayores retos a la seguridad. Dinámicas como el ritmo acelerado de transformación impulsado por la tecnología, las asimetrías demográficas entre regiones o el cambio climático demandan un esfuerzo para adaptarse y gestionar de forma ágil y flexible los cambios.

El terrorismo transnacional y los ciberataques siguen siendo uno de los principales retos a la Seguridad. Junto a ellos surgen las denominadas amenazas hibridas, una combinación de amenazas convencionales y no convencionales orientadas a la desestabilización de nuestra forma de vida, y cuya identificación y atribución resultan especialmente complicadas.

Cell tower coverage leaves few places to hide

Just by virtue of being "on," a mobile device reveals its location in multiple ways on the basic signaling pathways of the global telephone network. Much of that data crosses U.S. territory, even for foreign-registered phones. NSA collection from those links is known as "UPSTREAM."



This map depicts North American cell towers for illustration. The NSA says it does not "intentionally collect U.S. location data in bulk," but it "incidentally" takes in a great deal.

How the NSA gets locations from mobile devices

When mobile devices connect to a cellular network, they announce their presence on one or more "registers" maintained by telephone providers in order to connect and bill their counterparts for telephone calls. Registration messages often include a device's "coarse" location, at the level of a city or country, or a "finer" position based on distance from a cellular tower.

Many mobile devices and smartphones use WiFi signals as well to fix their locations, relying on databases that map millions of hot spots around the world. These signals can locate a device down to a city block.

Global Positioning Satellite receivers, built into many cellular and satellite telephones, can locate a device within a 100 meter radius or less.

Most mobile operators also track phones precisely by triangulating their distance from multiple towers, for example to provide location-based emergency services.

How the NSA tracks targets to find possible associates

"Co-Traveler Analytics" is one active operational NSA target development method. It draws on

By tracking all phones within a cell tower area along with the target phone, co-travelers can be isolated.

INFLUENCIA
Variables
aumenta
Milgram
mensaje
refiere
atención
tácticas
si
Hoyland
cada
explicar
contexto
conducta
social
nivel
baja
después
producto
funcionan
actos
proclive
eficacia
claves
aceptación
efecto
Táctica
conseguir
diferentes
canal
previamente
clave
fuente
Tácticas
personas
mayor
actitud
debe
influir
depende
teoría
elaboración
produce
técnica
persuasión
decir
conductas
proceso
alguna
misma
heurístico
esfuerzo
cambio
Petty
inicial
primera
autoridad
argumentos
mensajes
influencia
semejantes
persona
audiencia
objeto
compromiso
comprensión
audiovisual
concesión
cara
previos
ser
comunicación
actitudes
racionales
valores
motivación
persuasiva
sustenta
resistencia
implicación
forma
maximiza
technique
reglas
pensamientos
receptor
características
persuasivo
heurística
comunicador
aprendizaje
puede
éxito
peticiones
cognitiva
realizar
procesos
situación
presencia
estrategia
automensajes
aceptar
petición
cognición
cantidad
rechazar
Comunicación
favor
implica
atractivo
coherencia
credibilidad
Modelo
información
Heurístico
postura
rechazo
distracción
argumento
Necesidad
decisión
poca
consiste
receptores
factores
dos
través
tiempo
comportamiento
cambiar
previa

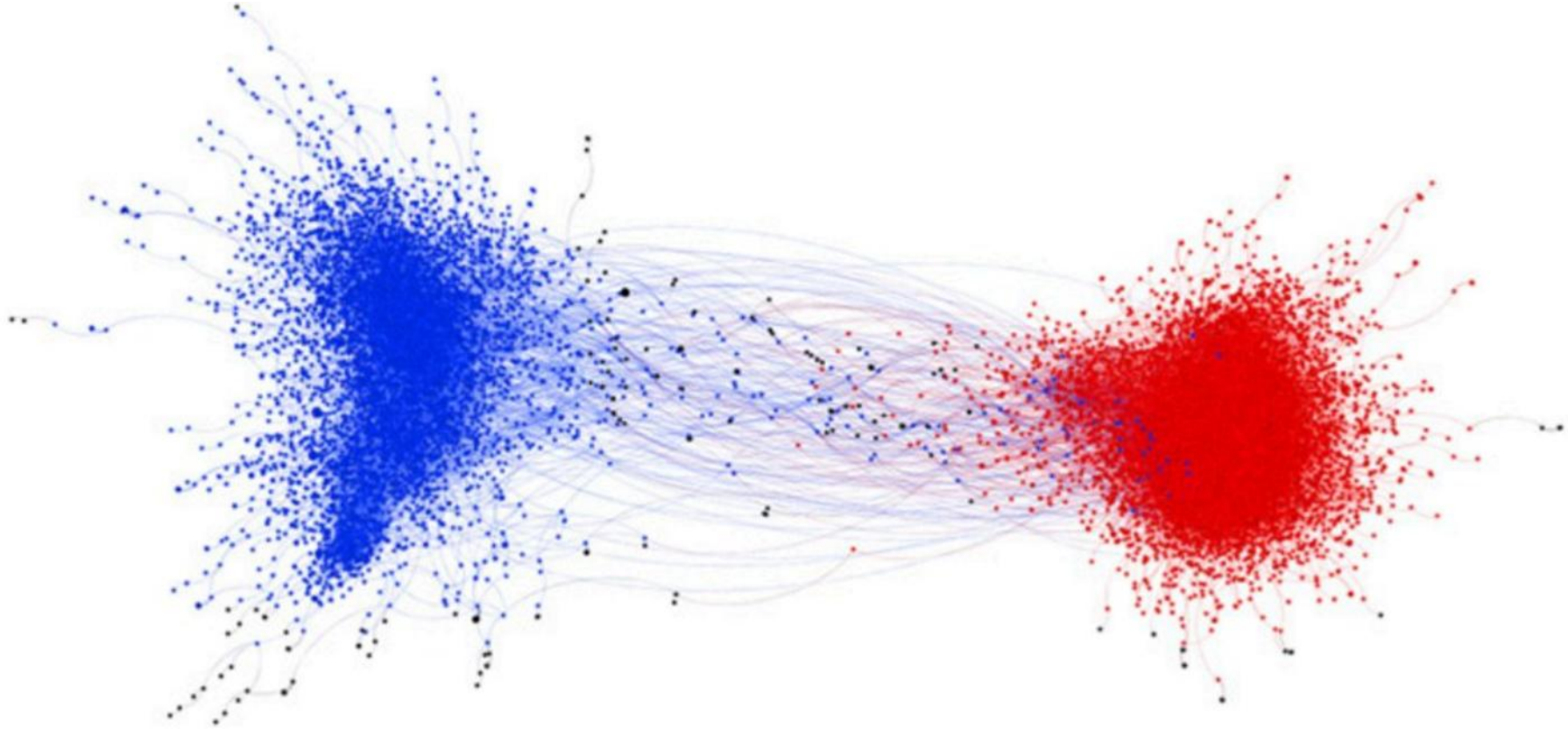


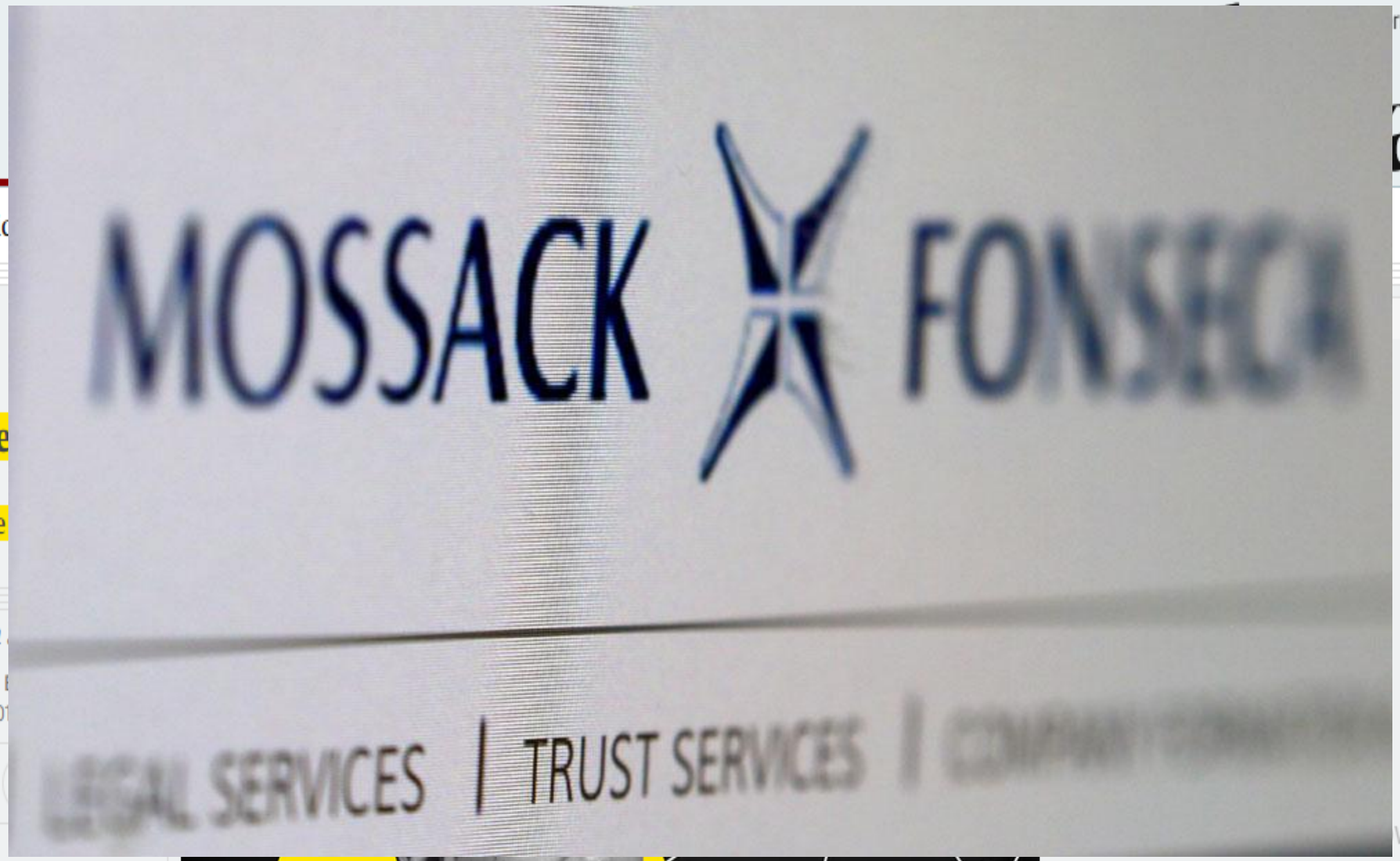
Fig. 3. Network graph of moral contagion shaded by political ideology. The graph represents a depiction of messages containing moral and emotional language, and their retweet activity, across all political topics (gun control, same-sex marriage, climate change). Nodes represent a user who sent a message, and edges (lines) represent a user retweeting another user. The two large communities were shaded based on the mean ideology of each respective community (blue represents a liberal mean, red represents a conservative mean).


A D C B F E C
N I J K L M H
G P O R S T
U U M R Y Z

Support The Guardian

News

UK ▸ UK politic



Cambridge Analytica

The Cambridge Files

Olivia Solon *in*

@oliviasolon

Wed 4 Apr 2018 23.01

2,244

rnational edition

an

WS

Ve a Configuración para activar Window

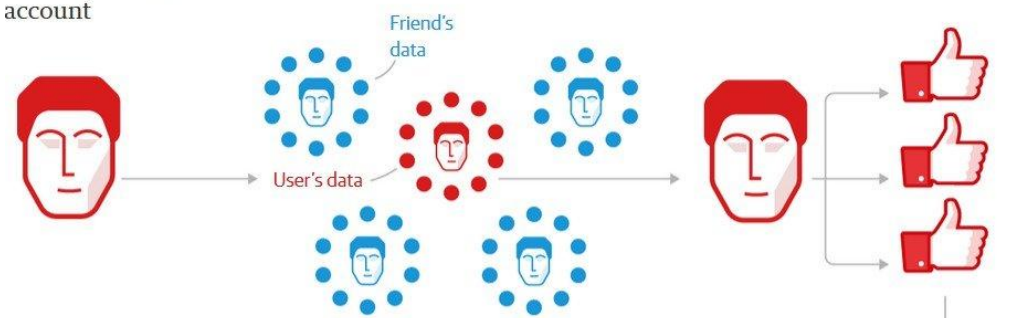

FREEDOM or FREE STUFF
Your Choice.
You Only Get One.

Cambridge Analytica: how 50m Facebook records were hijacked

1
Approx. 32,000 US voters ('seeders') were **paid $2-5 to take a detailed personality/ political test** that required them to log in with their Facebook account

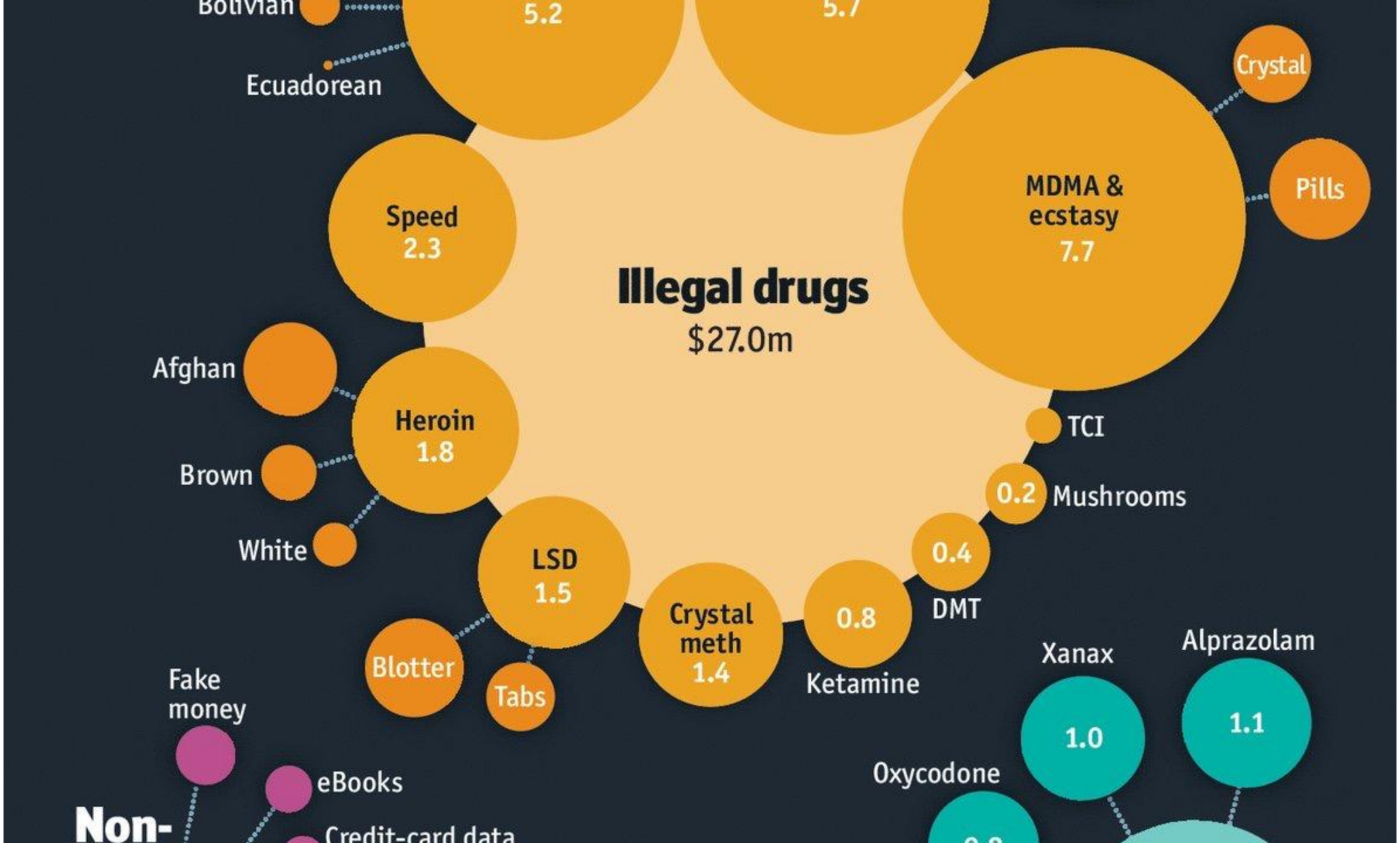
2
The app also **collected data such as likes and personal information** from the test-taker's Facebook account, as well their **friends'** data, amounting to over 50m people's raw Facebook data

3
The **personality quiz results** were paired with their Facebook data - such as **likes** - to seek out psychological patterns



4
Algorithms combined the data with other sources such as voter records to **create a superior set of records (initially 2m people in 11 key states*)**, with hundreds of data points per person.
These individuals could then be targeted with **highly personalised advertising** based on their personality data

Guardian graphic. *Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, West Virginia


Illegal drugs
$27.0m
Speed
2.3
MDMA &
ecstasy
7.7
Crystal
Pills
Heroin
1.8
Afghan
Brown
White
TCI
0.2
Mushrooms
0.4
DMT
0.8
Ketamine
Crystal
meth
1.4
LSD
1.5
Blotter
Tabs
Xanax
1.0
Alprazolam
1.1
Oxycodone
Fake
money
eBooks
Credit-card data
Non-

Diego Moncada
@DiegoMncada

Seguir

People: FACEBOOK FILTRA NUESTRA INFORMACIÓN PRIVADA, MALDITO SEAS MARK ZUCKERBERG.

Also people: "Descubre qué tipo p
eres con solo 20 preguntas" desea
acceso a su información. ¿Acepta
términos y condiciones?

¿Qué raza de perro eres?

Por Maria Gloria Satta

Ver más publicaciones

Google ha cerrado el anuncio

¿Alguna vez te has preguntado qué raza serías si fueses un perro? ¡Haz este quiz y averigualo!

ell people.
n people.

e likes, friend list +

n further.

ne numbers they

onsibility. Not going to

o go into specifics.
ve've solved problems

e FB.

trols.

vith ads.
nission.
ou controls.
elevant.

to MSI.

control.
ave no plans to do so.

- More work to do,

Tim Cook on biz model

- Bezos: "Companies that work hard to charge you more and companies that work hard to charge you less."
- At FB, we try hard to charge you less. In fact, we're free.
- [On data, we're similar. When you install an app on your iPhone, you give it access to some information, just like when you login with FB.
- Lots of stories about apps misusing Apple data, never seen Apple notify people.
- Important you hold everyone to the same standard.]

Disturbing content

- It's very disturbing; and sadly we do see bad things on Facebook.
- Should have no place on our service; community standards prohibit hate, bullying, terror.
- Working to be more proactive; AI, hiring more people e.g. terror, e.g. suicide.
- Will never be perfect; but making huge investments.

Election integrity (Russia)

- Too slow, making progress. France, Germany, Alabama.
- Midterms are important, but not just in the US — Brazil, Mexico, Hungary.
- Just announced committee of academics to commission independent research on social media on democracy.

Diversity

- Silicon Valley has a problem, and Facebook is part of that problem.
- Personally care about making progress; long way to go [3% African American, 5% Hispanics].

Competition

- Consumer choice: consumers have lots of choice over how they spend their time
- Small part of ad market: advertisers have choices too — $650 billion market, we have 6%.
- Break up FB?: US tech companies key asset for America; break up strengthens Chinese companies.

GDPR [Don't say we already do what GDPR requires]

- People deserve good privacy tools and controls wherever they live.
- We build everything to be transparent and give people control. GDPR does a few things:
  - Provides control over data use -- what we've done for a few years.
  - Requires consent -- done a little bit, now doing more in Europe and around the world.
  - Get special consent for sensitive things e.g. facial recognition.
- Support privacy legislation that is practical, puts people in control and allows for innovation.

Dr. Gustavo Díaz Matey
gdiazmat@ucm.es
@gdiazmat

Resumen de estado de riesgo del Ciberespacio

AUTORÍA	OBJETIVOS		
	Gobierno	Sector Privado	Ciudadanos
Ataques patrocinados por Estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	
Ataques patrocinados por Sector Privado	Espionaje	Espionaje	
Terroristas, extremismo político e ideológico	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	
Hacktivistas	Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Robo y publicación de datos personales
Crimen Organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de perfil bajo	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	
Ataques de personal con accesos privilegiados (Insiders)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, infección con malware, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, APT	

Impacto	Alto
	Medio
	Bajo