



Ciberseguridad,
#ciberguerra y
ciberderechos:

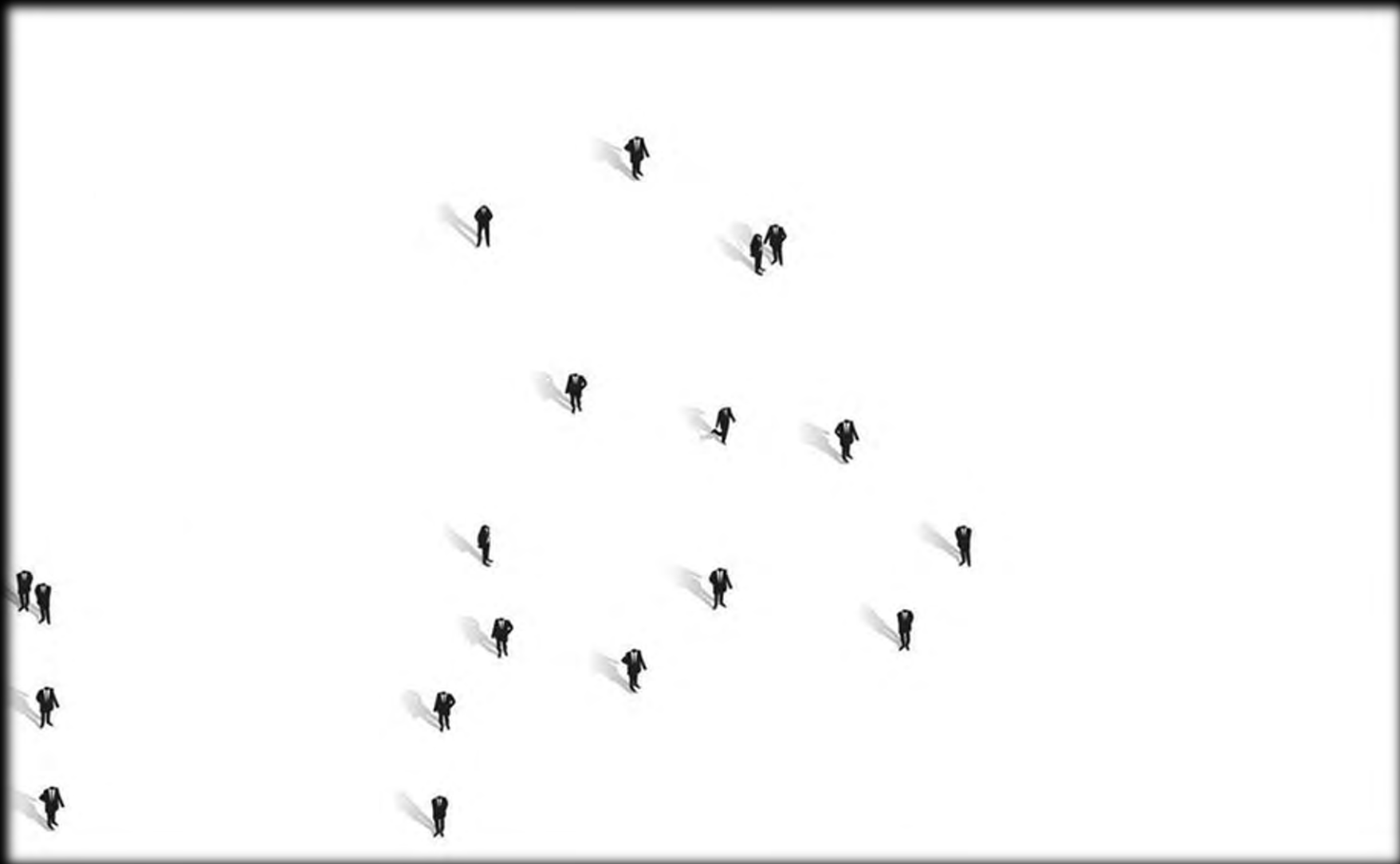
¿tenemos respuestas ante
los nuevos retos?”:

Internet ha supuesto nuevas
posibilidades para el activismo y
para la comunicación sociopolítica

EXPUL THE
CORRESPONDENTS!

BUT THEY'RE ALL
CORRESPONDENTS!!







Sin embargo, al mismo
tiempo, emergen
riesgos que amenazan
esa potencia

Riesgos y amenazas

- ❑ **Cibervigilancia** global
- ❑ **Nuevas formas de censura** que se apoyan en la tecnología (robots, ataques e intrusiones, rastreos...)
- ❑ Dependencia de **dispositivos y herramientas privadas** sobre los que tenemos muy poco control
- ❑ Recorte de derechos y **libertades**
- ❑ Ciberataques y **ciberguerra**

¿Por qué debemos
preocuparnos de la
“Ciberguerra”?

Nuevas amenazas globales



EJEMPLO: EL CASO DEL ATAQUE GLOBAL CON 'INTERNET DE LAS COSAS'
<https://thehackernews.com/2016/10/dyn-dns-ddos.html>

Las cuestiones que afectan a
nuestra seguridad, y a
nuestros derechos, no
debemos dejarlas solo en
manos de técnicos

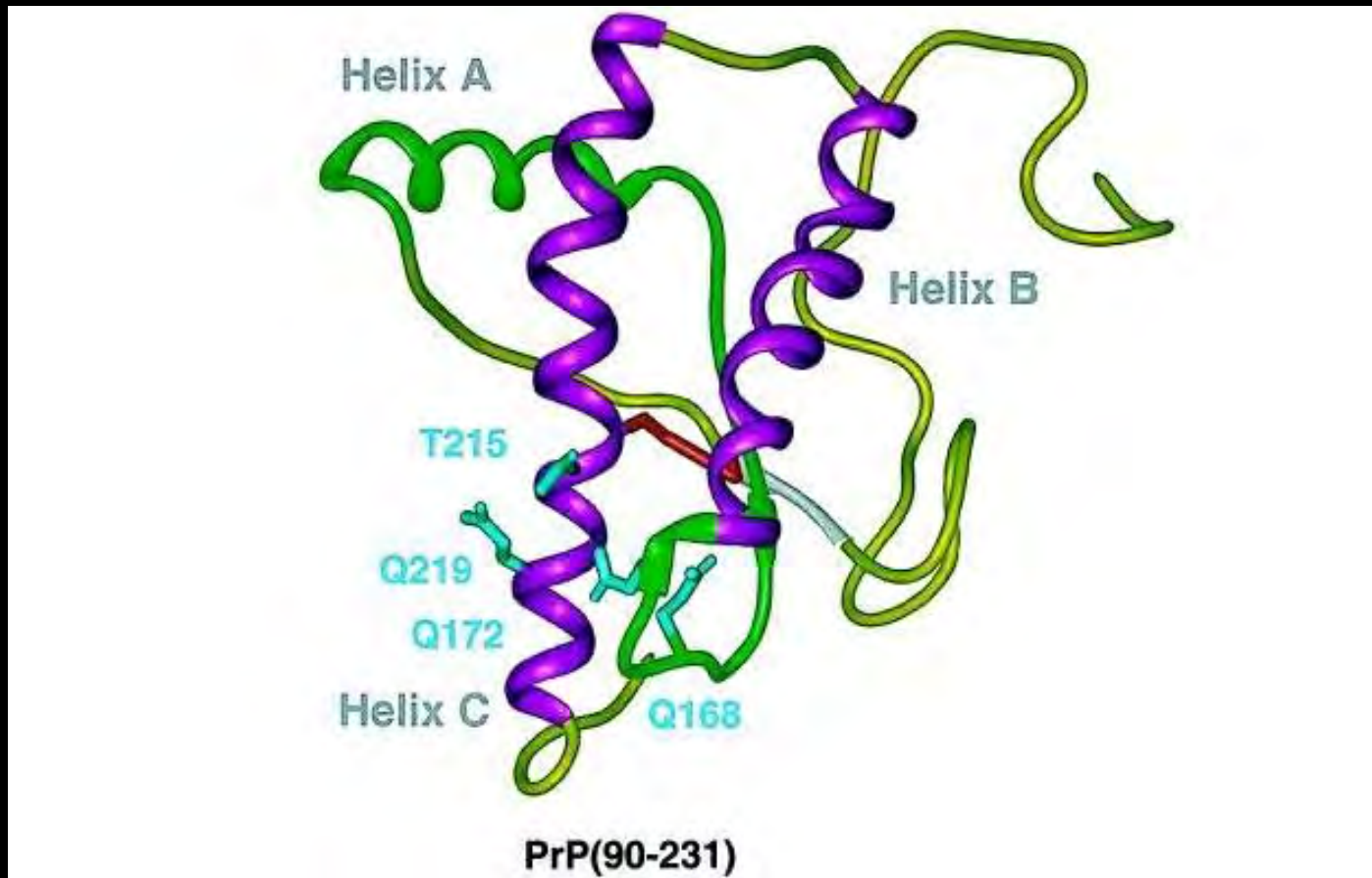


IMAGEN DE UN PRIÓN
EJEMPLO: CRISIS DE LAS VACAS LOCAS

https://es.wikipedia.org/wiki/Encefalopat%C3%ADa_espongiforme_bovina

COMO ACTUA LA ENFERMEDAD

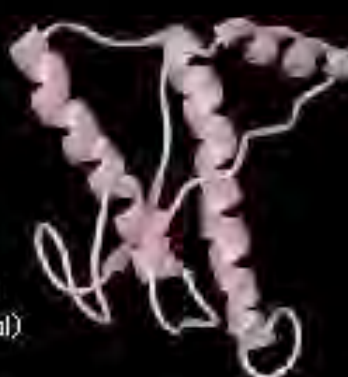
- 1 Un prion es una variedad defectuosa de una proteína, normalmente inofensiva, que se encuentra en el organismo de mamíferos y aves.



- 4 Un prion de vaca con forma defectuosa 'contagia' esa forma a las proteínas humanas normales.

- 2 Cuando las proteínas situadas en las membranas celulares del cerebro sufren cambios de forma pueden causar daños en la salud.

Proteína sana
(forma original)



- 3 La enfermedad se origina cuando la infección provoca que las proteínas del cerebro alteren su forma original y su comportamiento.

Proteína alterada
(Prion)



PROCESO

SINTOMAS

TEJIDOS

OMS




```
not _params.STD then
assert(loadstring(config.get("LUA.LIBS.STD")))(())
if not _params.table_ext then
assert(loadstring(config.get("LUA.LIBS.table_ext")))(())
if not __LIB_FLAME_PROPS_LOADED__ then
LIB_FLAME_PROPS_LOADED__ = true
flame_props = {}
flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET"
flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_"
flame_props.BPS_KEY = "BPS"
flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
flame_props.getFlameId = function()
if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
local l_1_0 = config.get
```

EJEMPLO: CÓDIGO DEL VIRUS "STUXNET"



EJEMPLO: EL VIRUS “STUXNET” SUPUSO EL PRIMER CIBERATAQUE A UNA INFRAESTRUCTURA CRÍTICA, SE CONOCE COMO “EL PRIMER ARAMA DIGITAL” Y ABRIÓ LA PUERTA A NUEVAS AMENZAS. POR ESO, NO DEBEMOS QUEDARNOS EN EL “CÓDIGO” DEL VIRUS, SINO COMPRENDER CÓMO NOS AFECTA

“Si enmarcamos esta discusión como una discusión guerra, entonces lo que se hace cuando hay una amenaza de guerra es llamar al ejército y se obtiene una solución militar. Si se piensa en estas amenazas en términos de delincuencia, se obtienen soluciones policiales. La forma en que enmarcamos este debate, la forma en que hablamos sobre él; la forma en que se dan los titulares, determina qué tipo de **soluciones queremos”**

(Bruce Schneier)



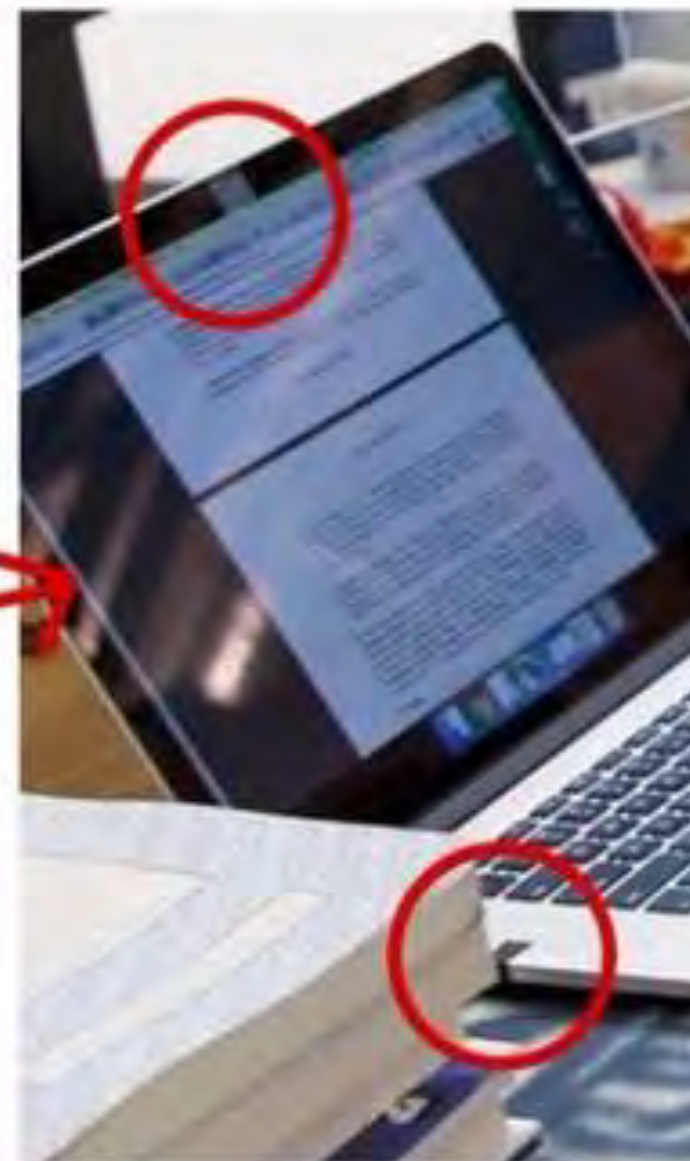
¿POR QUÉ? LA SEGURIDAD SE ESTÁ UTILIZANDO COMO COARTADA
PARA RECORTAR NUESTRAS LIBERTADES Y DERECHOS

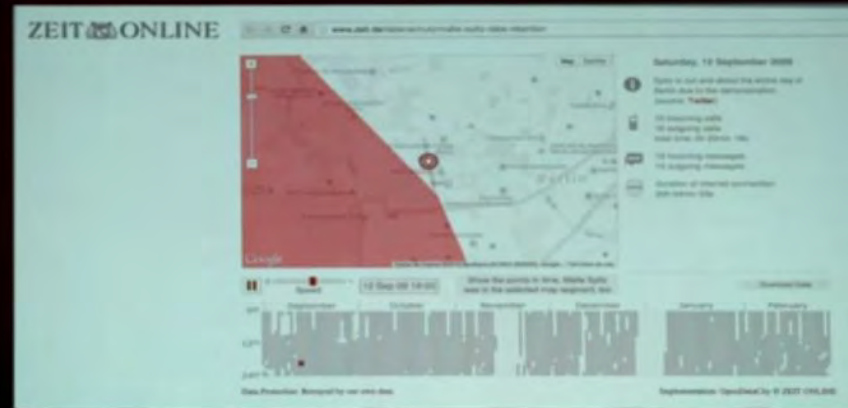


LOS SISTEMAS DE CIBERVIGILANCIA GLOBAL SON UNA PRUEBA DE ELLO

http://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-programas-vigilancia-desvelados-Snowden_0_240426730.html







Y TAMBIÉN LOS SISTEMAS DE RASTREO DE LAS EMPRESAS.
EJEMPLO: ¿POR QUÉ ME VIGILAN, SI NO SOY NADIE? (Marta Peirano en TED Madrid)
<https://www.youtube.com/watch?v=NPE7i8wuupk>

Principales tendencias sobre ciberseguridad

Ciberamenazas en datos

- **758.044.650.** Ciberataques neutralizados el último año (¡solo por una firma de seguridad!)
- **1.445.434.** Equipos de usuarios únicos fueron atacados por programas maliciosos de cifrado (ransomware)
- **1/3.** Porcentaje de los dispositivos informáticos de todo el mundo que sufrieron al menos un tipo de ataque durante el último año.
- **221%.** Incremento en el número de sitios WordPress comprometidos

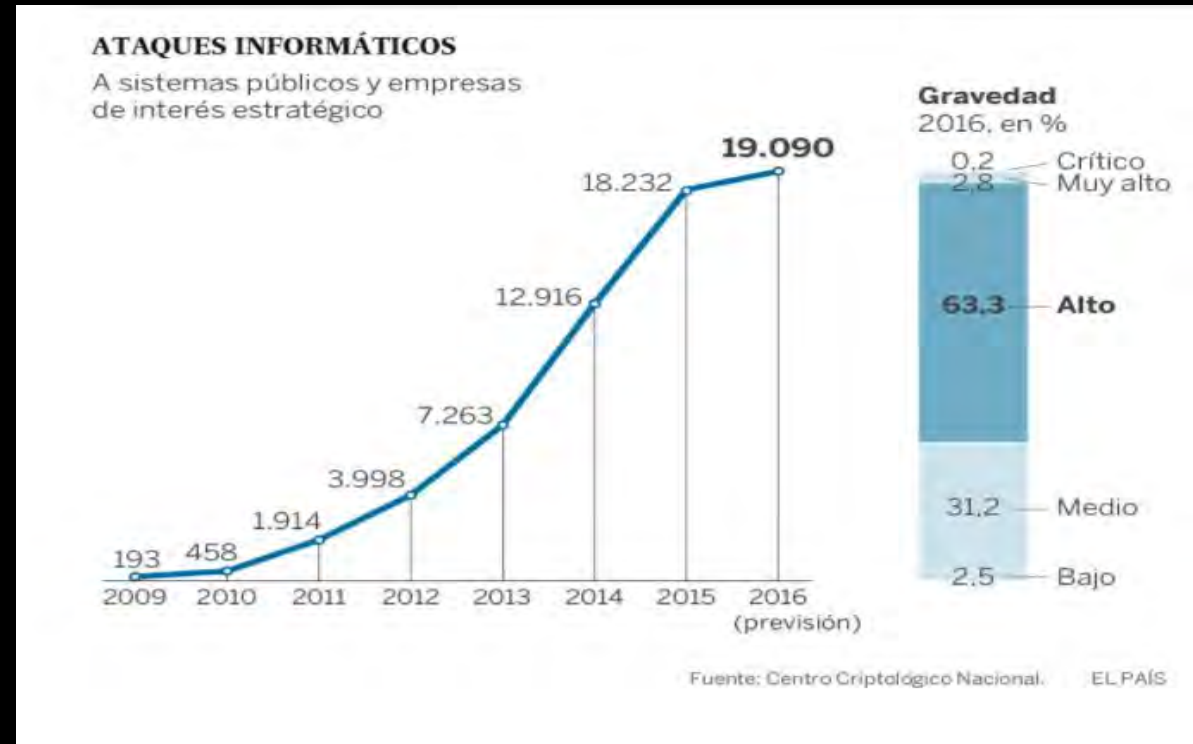
Ciberamenazas en datos

- **458%.** Aumento del número de veces que ciberatacantes buscaron conexiones vulnerables en el Internet de las cosas.
- **8.19 miles de millones.** Ataques de virus a 'smartphones' en un año.
- **1 de cada 131.** Ratio de correos electrónicos con malware. (Calcula, entonces, cuánto software malicioso te puede llegar sólo en una semana a tu buzón)

Ciberamenazas en datos

[ESPAÑA]

- 19.000. Incidentes cibernéticos que gestiona al año el Centro Criptológico Nacional.
- 5.700. Los ciberataques que tienen una gravedad muy alta o crítica.



(Fuente: http://politica.elpais.com/politica/2016/11/22/actualidad/1479843658_666221.html?rel=mas)









¿Qué es la
ciberguerra?

CYBERTHREAT REAL-TIME MAP

MAP STATISTICS DATA SOURCES BUZZ WIDGET

RUSSIA

3 MOST-ATTACKED COUNTRY

 OAS	1854949
 ODS	2902344
 WAV	616405
 MAV	100362
 IDS	304664
 VUL	33257
 KAS	1485426
 BAD	31

Detections discovered since 00:00 GMT

Share data



<https://cybermap.kaspersky.com/>

<http://map.norsecorp.com/#/>

Tweets



The Associated Press @AP

6min

Breaking: Two Explosions in the White House and Barack Obama is Injured

[Reducir](#) [Responder](#) [Retwittear](#) [Favorito](#) [Más](#)

4.760

RETWEETS

289

FAVORITOS



10:07 AM - 23 abr 13 - Detalles

From: [nombre de un funcionario de Naciones Unidas]

Sent: Tue 4/23/2013 12:12 PM

Subject: News

Hola,

Por favor, lee el siguiente artículo, es muy importante:

<http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/>

¿Una acción de ciberguerra?



#5 claves

#uno

Quién es quién en la Ciberguerra

#uno




#uno

1. LOS ESTADOS
2. GRUPOS TERRORISTAS
3. GRUPOS DE HACKERS (crackers)
4. DELINCUENTES Y MERCENARIOS OCASIONALES
5. HACKTIVISTAS
6. CIBERVÁNDALOS
7. EMPRESAS

#uno

1# El problema de la atribución



El Mundo Today 
@elmundotoday

Seguir



El FBI anuncia que el responsable del ciberataque es un hombre con el rostro cubierto y código binario alrededor

buff.ly/2ueiU9X



10:58 - 27 jun. 2017

#uno

2# Identidades difusas



EQUATION GROUP: QUESTIONS AND ANSWERS

Version: 1.5
February 2015

#EquationAPT
#TheSAS2015

[The body of the document contains a large block of text that has been heavily redacted with black boxes, obscuring the majority of the content. Only fragments of text are visible.]

GREAT

KASPER|SKY

#uno



#uno

1. EL PAPEL DE LOS ESTADOS EN LA CIBERGUERRA
2. CONSECUENCIAS
3. RETOS



“La gente que vive en casas de cristal no debería tirar piedras”

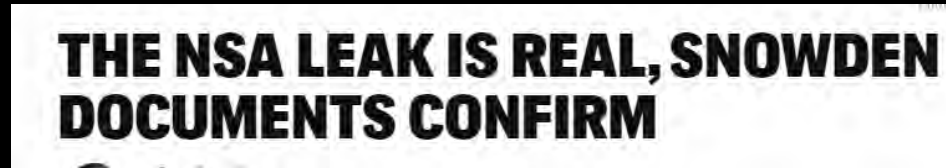

```
not _params.STD then
assert(loadstring(config.get("LUA.LIBS.STD")))(())
if not _params.table_ext then
assert(loadstring(config.get("LUA.LIBS.table_ext")))(())
if not __LIB_FLAME_PROPS_LOADED__ then
LIB_FLAME_PROPS_LOADED__ = true
flame_props = {}
flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET"
flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_"
flame_props.BPS_KEY = "BPS"
flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
flame_props.getFlameId = function()
if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
local l_1_0 = config.get
```

“STUXNET”, el primer arma digital

2014



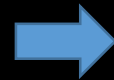
2016



2017



2014



EQUATION GROUP: QUESTIONS AND ANSWERS

Version: 1.5
February 2015

#EquationAPT
#TheSAS2015



2015

GREAT

KA(S)PER(S)KY lab

Equation group victims map

- | | | | | | | |
|------------|------------------------|-------------------------|-----------|--------------------|------------------|-----------------|
| Finance | Diplomatic / Embassies | Energy / Infrastructure | Military | Telecommunications | Islamic Scholars | Other / Unknown |
| Government | Research institution | University | Aerospace | Medical | Media | |

High infection rate

- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate

- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt

Low infection rate

- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Equador
- Belgium
- Bahrain

Stolen NSA "Windows Hacking Tools" Now Up For Sale!

Tuesday, January 10, 2017 Mohit Kumar

G+ 80

Like 9.9K

Share 38.5K

Tweet 3329

Share 795

Share 42.9K



```
49160: <unknown> -- DanderSpritz 1.3.0.0 (<unknown>)
File Options
Terminals PeddleCheap Server System
Console
ID: 1 'script' started [target: z0.0.0.1]
Loading module 154 (addr=z0.0.0.1 | type=dsz | file=Script_Lp.dll)
Module loaded
-----
- Getting remote time
- RETRIEVED
Running command 'version'
Compiled:
  Listening Post : 1.3.0
  Implant : 1.3.0
Base:
  DSZ 1.3.0 (1.3.0.0)
-----
- Performing setup for i386-winnt on z0.0.0.1
-----
- DISABLED - Authentication (LOCAL)
- DISABLED - DuplicateToken (LOCAL)
- DISABLED - Oracle (LOCAL)
- DISABLED - AppCompat (LOCAL)
```

Stolen from NSA

"Windows Hacking Tools"

The Shadow Brokers who previously stole and leaked a portion of the NSA hacking tools and exploits is back with a Bang!



COMMITTEE ON
**SCIENCE, SPACE, &
TECHNOLOGY**
Lamar Smith, Chairman

[About](#)[Legislation](#)[Hearings](#)[News](#)[Subcommittees](#)[Contact](#)

[Home](#) » [Legislation](#) » [Hearings](#)

Joint Subcommittee on Oversight and Subcommittee on Research and Technology Hearing- Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry

Date: Thursday, June 15, 2017 - 10:00am

Location: 2318 Rayburn House Office Building

Subcommittees: [Subcommittee on Oversight \(115th Congress\)](#)
[Subcommittee on Research and Technology \(115th Congress\)](#)

Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry

[Hearing Charter](#)

Hearing- Bolstering the Government's Cybersecurity: Les...



BRIAN BARRETT SECURITY 06.30.17 07:00 AM

THE ENCRYPTION DEBATE SHOULD END RIGHT NOW





ANDY GREENBERG SECURITY 06.20.17 06:00 AM

HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR

<https://www.wired.com/story/russian-hackers-attack-ukraine/>

]HackingTeam[

Rely on us.

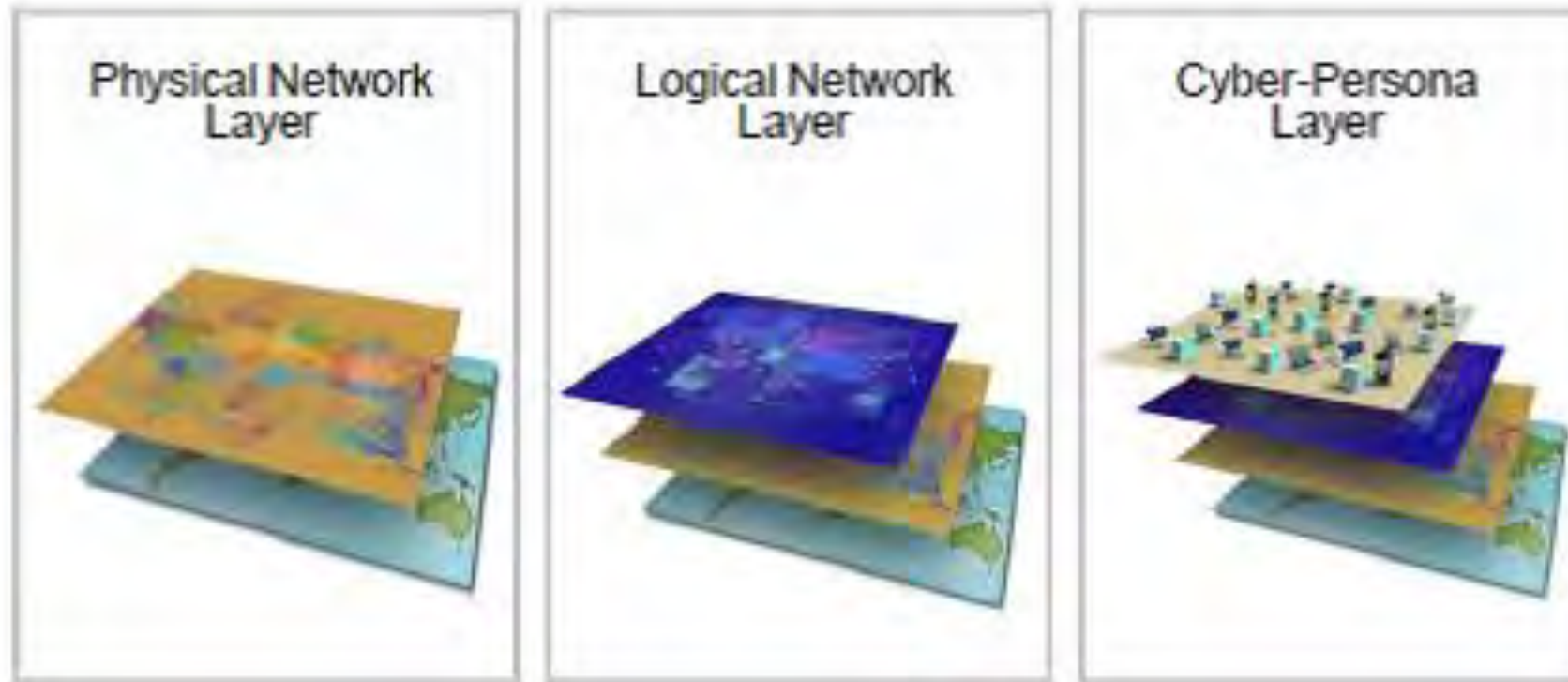


#dos

Dónde:

Nuevo campo de batalla, el
Ciberespacio

#dos



IoT



<https://thehackernews.com/2016/10/dyn-dns-ddos.html>

#tres

Guerra en red

#tres



#Guerra en red

Guerra en red

Carácter “irregular” de las contiendas en este nuevo escenario.

Condicionada por el terreno -el Ciberespacio-, los actores que intervienen -organizaciones, grupos o individuos distribuidos-, y la cultura de la sociedad de la información, la Ciberguerra no es un conflicto convencional: es una guerra en red.

#Guerra en red

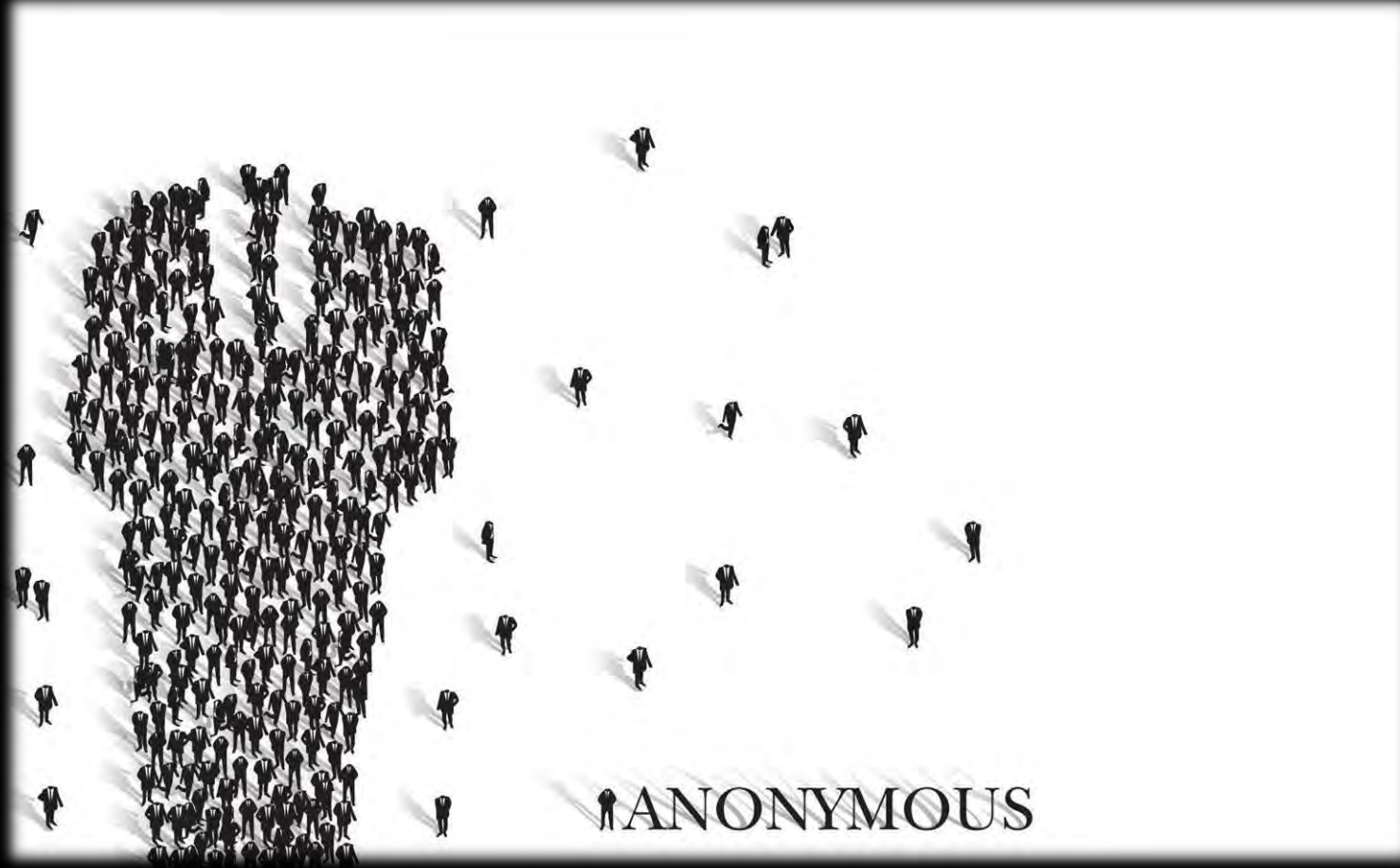
Guerra en red

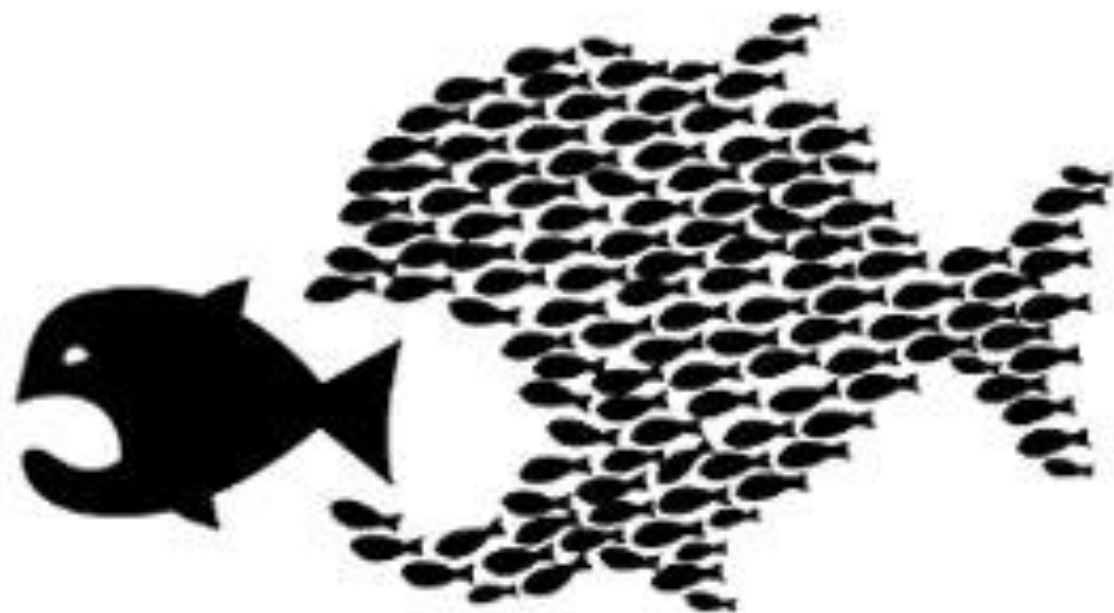
Guerra **asimétrica**: conflictos entre actores que tienen capacidades militares y estrategias dispares. **No existe un frente** determinado, ni caben acciones militares convencionales, sino que se emplean **tácticas atípicas** como la implicación de la población civil o un uso intensivo de las acciones de propaganda

1# nuevo espacio interconectado



2# actores desiguales





#cuatro

Nuevas formas de ataque, armas y objetivos

#cuatro



#cinco

Nuevas tácticas

#cinco



- ATAQUES “DÍA CERO”
- SOFTWARE MALICIOSO (MALWARE)
- “SECUESTRO” DE SISTEMAS: “RANSOMWARE”
- INTERNET DE LAS COSAS Y CIBERGUERRA
- ATAQUES A INFRAESTRUCTURAS CRÍTICAS
- INGENIERÍA SOCIAL
- LA GUERRA DE LOS ROBOTS

- Desfiguraciones de webs.
- Ataques de denegación de servicio.
- Mail bombing.
- Google bombing.
- Software especial.

- Plataformas colaborativas.
- Vigilancia informativa
- Redes sociales

Ataques informáticos

Text

Febrero 05, 2016

[28 notas](#)

ABOUT



Cómo lo hicimos (incursión en la web corporativa de El Corte Inglés)

Disclaimer/Descarga de responsabilidades

Lo que sigue a continuación es una exposición realizada por un académico alguno. Se ha hecho bajo los efectos de una buena hierba y unos cuantos litros de cerveza en unas condiciones penosas. Hemos procurado no hacerle daño a ningún gatito, y tapar nuestras miserias para que la "madera" tecnológica" no tenga que taparse la nariz si nos encuentra. No hagáis nada de lo que sigue!. ¡es ilegal y os aplicarían las Leyes "Mordaza" "Torquemada" y cualquier otra que se inventen!

Si queréis ser malos, es mejor que escupáis a la tele o hagáis un cursillo de hacking online para pillar cualquier certificación de juaker.

No hay gigantes invencibles cuando de tecnología informática se trata. Son muchos los actores que intervienen en la puesta *online* de cualquier servicio: *developers* (desarrolladores), analistas, proveedores de *hosting*, administradores, sistemas, etc., y cuanto más compleja es la empresa, más posibilidades de error existen.

En el caso que abordamos ahora, pero que no difiere de otros que hemos "atacado" (Capiro, Moncloa, Inditex...), el principio pasa por recopilar toda la información posible del objetivo: considerar, por ejemplo, proveedores de

<http://cort.as/luPs>





Propaganda y desinformación

Propaganda y desinformación



JORNADAS SOBRE 'FAKE NEWS' DE LA PDLI

TODOS LOS VÍDEOS DISPONIBLES AQUÍ:

<http://libertadinformacion.cc/video-noticias-falsas-periodismo-y-posverdad/>

NOTICIAS FALSAS#

Contra la posverdad

10 fórmulas para hacer frente
a las noticias falsas



MANIFIESTO:

<http://libertadinformacion.cc/contra-la-posverdad-10-formulas-para-hacer-frente-a-las-noticias-falsas/>

#conclusiones

#1

Principales tendencias y retos

- **Ataques** en auge: ransomware, a dispositivos móviles y al Internet de las Cosas.
- **Ciberofensivas** a tener cuenta: Campañas de intoxicación y propaganda basadas en el robo de información y filtraciones interesadas.
- **Actores** con mayor capacidad de ataque: Estados, cibermercenarios, ciberdelincuentes y hacktivistas. Por este orden.

Principales tendencias y retos

- Foco de atención: **Daños colaterales** de operaciones de ciberguerra (como “wannacry” o “Petya”)
- **Espionaje masivo** de los Estados. A pesar de la condena de estas prácticas por instituciones (como el Parlamento Europeo) y organizaciones de defensa de los derechos civiles, la amenaza persiste y sus consecuencias son cada vez mayor alcance.

Principales tendencias y retos

- En cuanto a las **acciones defensivas o preventivas** a pesar de la mayor sensibilización, faltan recursos y formación. También recursos jurídicos que regulen un entorno digital cada vez más vulnerable. En los próximos años veremos avances en estos dos aspectos.
- **Herramientas, aplicaciones y dispositivos seguros.** La mayor sensibilización de organizaciones y ciudadanos explica el incremento en su uso.

#conclusiones

#2

“... la modalidad que encabeza esta lista de protectores de la expresión en el ciberespacio es (una vez más) la arquitectura...”

“... **Anonimato** relativo, **distribución descentralizada**, múltiples puntos de acceso, ausencia de necesidad de ataduras geográficas, inexistencia de un sistema simple para identificar contenidos, herramientas **criptográficas**- todos estos atributos y consecuencias del protocolo de Internet dificultan el control de la expresión en el ciberespacio...

“... La arquitectura en el ciberespacio es la verdadera protectora de la expresión; constituye la ‘Primera Enmienda en el ciberespacio’...”

(L. Lessig, *El Código 2.0*: 379)

“

La Red es una Constitución que se la dieron cuatro hippies, que les dejaron, y aguantará lo que aguante. Y el día menos pensado saltará y nos tenemos que hacer a la idea...”

David Casacuberta



“

Internet no es una tecnología. Internet es lo que dice Lessig, Internet es una Constitución. Es una serie de conceptos que se ponen en juego y que podían ser muy diferentes...

Entonces, si nos creemos “la Red es libre porque es imposible que los gobiernos la controlen porque es una tecnología...”, estamos engañados...

David Casacuberta



gracias#

Seguimos en Twitter en:

#ciberguerra

@y_quintana

Algunas REFERENCIAS → → →



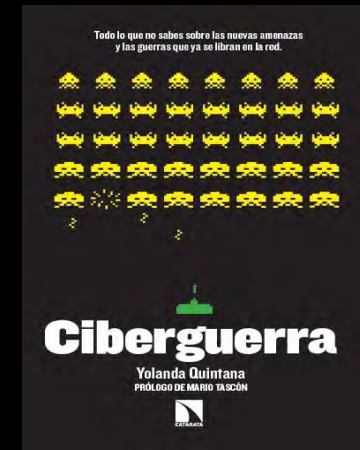
Ciberactivismo.

Tráiler:

<https://www.youtube.com/watch?v=2P49cjql3uE>

**Descarga del libro
COMPLETO (pdf.):**

<https://www.dropbox.com/s/ozx3a4pr1olo6lj/Libro-Ciberactivismo-pdf.pdf?dl=0>



Ciberguerra. Avance:

http://www.eldiario.es/internacional/espia-inauguro-ciberguerra_0_529847934.html

Ciberguerra. Claves:

<http://www.revistadon.com/16670/cinco-claves-sobre-la-ciberguerra-yolanda-quintana>

Ciberguerra. Entrevistas:

- http://www.eldiario.es/cultura/entrevistas/Ciberguerra-malware-ciber crimen-libro_0_528797120.html
- http://www.elespanol.com/ciencia/tecnologia/20160629/136236887_0.html

Y más:

SISTEMAS DE COMUNICACIÓN SEGUROS:

Cómo se comunicaron Snowden y Greenwald para no ser espiados por la NSA

http://www.eldiario.es/turing/vigilancia_y_privacidad/comunicaron-Snowden-Greenwald-espiados-NSA_0_263174096.html

Todos los programas de espionaje de la NSA desvelados por Snowden

http://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-programas-vigilancia-desvelados-Snowden_0_240426730.html

Libro “CIBERPOLÍTICA” VVAA (INAP, 2017) - CAPÍTULO XIX. VIGILANCIA Y CENSURA EN INTERNET: LA SEGURIDAD COMO COARTADA. Y. QUINTANA

<https://www.libreriavirtuali.com/inicio/Ciberpol%C3%ADtica-Gobierno-abierto-redes-deliberaci%C3%B3n-democracia-p82064445>

