

*Posproducción. Viajamos con GoogleEarth hasta Natanz. Aparece la fecha?*

*Instalaciones. Visita de ingenieros.*

**Irán. 2010. Alguien introduce en un ordenador un lapicero de memoria. El virus Stuxnet comienza a trabajar. Es, hasta ese momento, la máquina más perfecta diseñada en ciber guerra. Objetivo: Programa nuclear de Irán.**

Eugene Kaspersky/Consejero delegado Kaspersky Lab

Moscú 1: 21.41.23/21.41.36

Hoy está simplemente destruido con la ayuda de códigos malignos, como virus o troyanos. Infectaron los sistemas en Irán y sencillamente los estropearon. Quedaron físicamente destruidos.

Richard Clarke/Experto en ciber guerra

D16: 2.46/2.56

Creo que Estados Unidos lanzó el ataque de Stuxnet sobre la instalación nuclear iraní. Apoyado por Israel, pero creo que el ataque fue un ciberataque estadounidense.

*Mapa. A Siria. Despegan aviones. Postpro de radar.*

**Siria. Septiembre de 2007. Aviones israelíes sobrevuelan el río Éufrates. Destruyen instalaciones supuestamente destinadas al desarrollo de armas. Falla el recién estrenado sistema de defensa aérea del Ejército sirio. Los radares no detectan nada.**

Richard Clarke/Experto en ciber guerra

D16: 3.31/3.41

Creo que los israelíes cegaron los radares sirios por un ciberataque y lograron que las pantallas de los radares no mostraran aviones en vuelo.

Isaac Ben Israel/Asesor militar israelí

Israel: 1.05.38/1.05.54

Hay cierta confusión entre lo que llamamos ciber guerra, virus y cosas así, y lo que llamamos guerra electrónica. La guerra electrónica es algo diferente.

*Mapa. País tranquilo. Interferencia y sonido.*

Rótulo: Estonia. Año 2007.

No rótulo: Eugene Kaspersky/Consejero delegado Kaspersky Lab

Todo el país quedó desconectado de Internet.

Moscú 1: 21.30.15/21.30.18

*Ordenadores, país informatizado. Al final, disturbios*

**Los sistemas informáticos se vienen abajo. Bancos, líneas aéreas, medios de transporte. Millones de ordenadores de todo el mundo controlados por los agresores multiplican las peticiones de acceso a webs. El sistema se bloquea. Un procedimiento primitivo, pero efectivo.**

**Su origen: el sentimiento de ofensa de la población rusófona por la retirada de una estatua de la era soviética.**

Jamie Shea/Responsable de nuevos desafíos de la OTAN  
OTAN: 1.14.19/1.14.36

No está probado de dónde vino el ataque. Pero el problema es que incluso si sabes que el ataque ha venido de un determinado territorio es muy difícil señalar a ese Gobierno y decir: Tú. Fue en tu territorio. Eres responsable y lo sabemos.

*Mapa. Carros de combate. Guerra tradicional. Entre total cubierto. Luego le descubrimos.*

Isaac Ben Israel/Asesor militar israelí  
Israel: 1.15.48/1.16.23

La guerra entre Rusia y Georgia en 2008 fue una guerra real. Disparando fusiles, carros de combate, bombas, aviones. Una guerra real. Pero estuvo acompañada de una ciberguerra que no atrajo mucha atención... **Pero los rusos paralizaron todas las comunicaciones.**

*Gente y guerra. Pausa para el grito. Después, web de Sakashvili.*

**Cierto. Esa ciberguerra pasa desapercibida, pero no para el Gobierno de Georgia. Es rudimentaria, incluso burda... Llegan a atacar la web del presidente Sakashvili. Como siempre en asuntos de ciberguerra, la atribución de los ataques queda en el aire.**

Eugene Kaspersky/Consejero delegado Kaspersky Lab  
21.32.46/21.32.57

¿Quién estuvo detrás de ese ataque? Simplemente, no lo sé. Sí sé que hubo hackers, quizá un Gobierno... Aunque el Gobierno no me lo contó. Fue muy, muy similar a Estonia.

## AMENAZAcyber

Guión: José Antonio Guardiola  
Realización: Susana Jiménez Pons  
Imagen: Ricardo Vallespín  
Sonido: María Saurín  
Montaje: Javier Mula

*Montaje de Estocolmo. Guerra Fría. Maletines. Metro. Miradas. No desvelamos que estamos en Estocolmo hasta el final. Taxi con puerta...*

**Lo único bueno de la Guerra Fría es que nunca estalló. Durante decenios, el mundo se dividió en dos. Estados Unidos y la Unión Soviética se miraban de reojo. Por las capitales de uno y otro bloque, legiones de espías rastreaban el arma secreta del otro. La literatura y el cine estilizaron una época sucia y traicionera. Hoy, varios especialistas sugieren paralelismos entre aquella Guerra Fría y la actual ciberguerra. Los hay, pero en el fondo la ciberguerra se parece a todas las demás guerras. Los gobiernos temen las armas secretas del enemigo y por eso recurren a los espías, pero en esta ocasión sin maletines. Los métodos cambian... Los escenarios se repiten...**

*Termina de colear el rodaje de Estocolmo. Volamos por GoogleEarth desde el espacio hasta el parque de Estocolmo bajo el que se aloja Pionen.*

Jon Karlung/Presidente de Bahnhof

D9: 44.08/44.21 y 44.26/44.48

Esta instalación se construyó durante la Guerra Fría. Para la protección de Estocolmo, cuando la tensión podía llevar a una guerra en el caso de ataque nuclear.

Después de la Guerra Fría estuvo varios años abandonado, desocupado. En 2007 decidimos ampliar la zona y sacamos otros 40.000 metros cúbicos de roca.

D9: 45.27/45.53 (*Recursos de motores*)

Son motores originales de submarinos alemanes, pero no de la Segunda Guerra Mundial. Son de fechas posteriores. Tenemos una alarma de submarino alemán de la Segunda Guerra Mundial (*y suena*). Sonaba automáticamente en caso de fallo.

*Seguimos con Karlung y sus travesuras. Pionen.*

**Jon Karlung juega divertido en su viejo búnker. En esta nave, a 30 metros bajo tierra, ha sabido combinar la esencia de la Guerra Fría con las nuevas tecnologías. Karlung (y su empresa Bahnhof) son un refugio seguro en el ciberespacio. Sus servidores están blindados ante amenazas de ciberespías o simples delincuentes informáticos. Su cliente más famoso: WikiLeaks.**

*Entramos en la sala con Karlung.*

Jon Karlung/Presidente de Bahnhof

D9: 49.37/49.47

Éste es nuestro centro de operaciones natural, aquí es donde monitorizamos nuestro tráfico y probamos el servicio a nuestros clientes.

D9: 50.23/50.29

Mira, estas no son plantas de plástico. Por supuesto, son reales.

*Seguimos recorrido por sala de mando de Pionen. Le mostramos un punto excéntrico.*

*Al final del párrafo paramos para jugar con los planos del skater. Con música. Arranca el siguiente total de Karlung cubierto por el final de ese montaje.*

**Como otros muchos locos informáticos, a Karlung le apasiona la ciencia ficción y vive con la necesidad de combinar el mundo real con el virtual.**

Jon Karlung/Presidente de Bahnhof

D9: 1.12.14/1.12.34 (*Arranca un poco cubierto con planos skater*)

Estáis sentados en un búnker de la Guerra Fría. Pero la ciberguerra de hoy no es como la Guerra Fría. El búnker fue construido en los viejos tiempos para proteger a Suecia del diablo de la URSS (*sonríe*). Eso ya no es así. La ciberguerra es algo mucho más fragmentado.

*Ojo: Off pegado a total. Más Estocolmo. Trenes. ColdWar. Jruschev. JFK.*

**Y más complejo. Suecia, por su proximidad, fue uno de los países más expuestos a la amenaza soviética durante la Guerra Fría. Pero hoy, en el mundo ciber, las fronteras no existen. Tampoco palabras como lejano o cercano. En todo caso, la gran diferencia entre Guerra Fría y ciberguerra surge del concepto disuasión... Un juego básico en los malabarismos militares y diplomáticos de la posguerra que consistía, básicamente, en que ningún bloque lanzaría un primer ataque porque era consciente de que la respuesta sería devastadora.**

Richard Clarke/Experto en ciberguerra

D16: 7.43/8.14

Con las armas nucleares, sabes que lanzas un misil y tienes un 98% de probabilidades de que alcances el objetivo y lo destruyas. Si vas a lanzar un ciberataque no puedes conocer su efecto hasta que lo lanzas. Y tampoco sabes si quien lo reciba va a sobrevivir y te va a lanzar la represalia. Hay razones por las que la disuasión no funciona. Una de ellas, por supuesto, es que no sabes exactamente quién te ataca.

Jamie Shea/Responsable de nuevos desafíos de la OTAN

OTAN: 1.08.38/1.08.50

Si alguien quiere atacarnos, pero no tiene la certeza sobre cuál va a ser la respuesta de la OTAN o qué capacidad de respuesta tienen los países de la OTAN... Entonces, eso puede ser una buena razón para la disuasión.

*Respira. Paseo del general Roldán. Entramos en el JCISAT. Alarmas. Controles.*

**El principal centro de mando del Ejército español para ciberguerra se encuentra en un sótano a las afueras de Madrid. No muy lejos hay otro exactamente igual. Son espejos. Son espejos. Si falla uno, el otro salta inmediatamente.** *(Pausa, oímos puertas y pitidos)* **Entramos en el búnker con el general al mando, José Manuel Roldán.**

General José Manuel Roldán/Jefe de Sistema Trasmisiones (JCISAT)

D3: 1.01.01/1.01.07

Es el centro en el que se controla toda la plataforma de comunicaciones que dan servicio a todas las Fuerzas Armadas.

D3: 1.05.29/1.05.15

- En este lugar es donde se detectaría un ciberataque contra el Ejército?
- Efectivamente. Desplegado el sistema de información militar, la parte que no vemos representaría las amenazas, las vulnerabilidades y los ataques sobre los distintos sistemas que están en operación.

*Seguimos en la sala. Daremos paso a la conversación.*

**Ninguno de estos ordenadores está conectado a Internet. El Ejército dispone de una red propia, que le blinda ante riesgos y amenazas. Se reciben ataques del exterior, aunque la rutina consiste en desactivar fallos provocados por errores humanos.**

D3: 28.37/29.32 *Cortar.*

Mi sargento, qué es eso? – Mi comandante, hay una alarma en el nodo Delta. –

Compruébala, por favor. – Buenos días. - Le llamamos del centro de incidentes.

Tenemos una incidencia. Un posible acceso no autorizado. – Afirmativo. Un usuario ha introducido varias veces su contraseña y su cuenta se ha bloqueado. –Enterado.

*Búnker. Torrejón aviones. Barco Yibuti.*

**Las nuevas tecnologías han alterado la organización de todos los Ejércitos. A los cuatro ámbitos tradicionales, tierra, mar, aire, y espacio, se suma el mundo cibernético. Invisible, casi inabordable... Y lo peor de todo, barato y accesible.**

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú: 21.35.25/21.35.48

Es muy difícil controlar las ciberarmas porque para desarrollarlas simplemente necesitas una oficina con 10, 20... Quizá 50 ingenieros. Electricidad. Internet. Y ya está. Eso no se puede controlar. No es comparable a las armas nucleares.

*Primera parte del soldado del futuro.*

**Todos somos vulnerables. Por eso, Gobiernos y Ejércitos se centran en desarrollar técnicas de ciberdefensa... Oficialmente, el ciberataque no es propio de la doctrina militar.**

Richard Clarke/Experto en ciberguerra

D16: 14.21/14.37

No todas las guerras necesitan operaciones terrestres. Hay muchos escenarios en los que puedes provocar daños a otro país. Las operaciones sobre el terreno sólo serán necesarias si pretendes ocupar territorio o controlar otro país.

José Manuel Roldán/General de división Ejército de Tierra

D3: 1.16.09/1.16.26

A lo que no renuncian las naciones es si produce un ataque masivo con grado de destrucción elevado y amenaza grande es utilizar otros recursos que no sean de ciberguerra para contrarrestar esa amenaza.

*Ojo: Off pegado a total. USS Cole*

**En otras palabras. Responder a un ciberataque con misiles. Estados Unidos contempla ya esa posibilidad como represalia o simple disuasión. Pero... ¿de qué ciberataque estaríamos hablando? Podría ser contra sistemas utilizados por los Ejércitos o podría ser un ataque global, que afectara a toda la población. Ése es el gran temor y nadie, NADIE, descarta esa amenaza.**

*Arranca total con play. Se suceden los totales a doble pantalla con montaje de infraestructuras críticas. Recuperamos pantalla a total en último testimonio.*

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú 1: 21.44.30/21.44.37

Llegas a tu oficina y aprietas el botón del ascensor... Pero no viene ascensor alguno.

Richard Clarke/Experto en ciberguerra

D16: 13.53/14.03

Destruir infraestructuras. Destruir refinerías, oleoductos... Descarrilar trenes. Provocar confusión en el sistema bancario...

Isaac Ben Israel/Asesor militar israelí

Israel: 1.09.31/1.09.49

Alguien podría penetrar en los ordenadores de la bolsa y sería capaz no sólo de modificar su apariencia sino también de cambiar los precios de las acciones y cosas así.

Jamie Shea/Responsable de nuevos desafíos de la OTAN

OTAN: 1.09.40/1.09.49

Paralizando los sistemas de tráfico aéreo, paralizando la electricidad de toda una ciudad.

Richard Clarke/

D16: 14.06/14.09

Y destruyen generadores y transformadores.

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú 21.44.38/21.44.53

Y vuelves a casa y no hay electricidad. Se ha ido. Intentas llamar por teléfono a los servicios de seguridad y nadie responde porque las líneas de teléfono no funcionan.

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú 21.46.59/

Y el resultado de este ciber Hiroshima sería que el mundo volvería a vivir como hace 200 años. (*Y que sonría*).

*Ojo: Sonría Kaspersky y entra total. Bola del mundo.*

**Y ése es el problema... El mundo ni puede ni quiere vivir sin ordenadores, sin Internet, sin móviles... Como hace apenas unos años. El proceso de informatización es irreversible. La única alternativa es lograr un cibernmundo más seguro.**

*Pausa. GoogleEarth a Fort Meade. Encadenamos con la puerta que entra a...*

*Documentos Pentágono 3.11.*

**Esa puerta nos abre un universo desconocido. Fort Meade es la base del recién creado cibercomando del Ejército de Estados Unidos. Se encuentra en Maryland, no lejos de Washington. En esta sala, y en otras como ésta, se diseñan las armas del futuro. Imposible, siquiera, imaginar su potencial.**

Richard Clarke/Experto en ciberguerra

D16: 11.41/11.51

Estados Unidos tiene una ventaja ofensiva, pero eso no significa que se pueda defender. Es muy bueno en lo ofensivo, pero muy malo en lo defensivo.

Isaac Ben Israel/Asesor militar israelí

Israel: 1.19.37/1.19.54

Sabemos que últimamente los americanos han decidido crear un cibercomando con decenas de miles de personas. Usted puede imaginar qué han podido hacer con decenas de miles de personas...

*Ojo: Off pegado a total. Servidores*

**Un ejemplo: El virus Stuxnet. Un salto cualitativo en el panorama de la ciberguerra. Aún se sabe muy poco de él. Lo que nadie discute es que provocó la parálisis del programa nuclear de Irán. Se especula mucho sobre quién lo diseñó o quién lo distribuyó. Siempre se ha sospechado de Israel, pero Richard Clarke apunta a Estados Unidos.**

Richard Clarke/Experto en ciberguerra

D16: 6.54/7.04

El ataque de Estados Unidos contra las instalaciones nucleares de Irán fue muy sofisticado. Se diseñó para romper cosas. Para que estallaran... Y funcionó.

Isaac Ben Israel/Asesor militar israelí

Israel: 1.04.55/1.05.13

A veces leo declaraciones extrañas de Richard Clarke. Hace sólo una semana dijo que Stuxnet fue diseñado sólo por Estados Unidos. Es divertido...

*Ricardo y teclado. Postpro. La idea de interconexiones, circuitos de luz...*

**Se disputan la autoría de un arma que atemoriza. Es casi perfecta. Inteligente y demoledora. El virus se dedica a rastrear centenares de miles, millones de ordenadores... Y sabe perfectamente lo que busca.**

*Una parte puede ir cubierto con la postpro del gusano.*

Isaac Ben Israel/Asesor militar israelí

Israel: 1.01.20/1.02.04

En el caso de Stuxnet es muy sofisticado. Salta de un ordenador a otro. Y cada vez que alcanza un objetivo, el gusano comprueba. ¿Dónde estoy? Si estoy en un entorno con centrifugadoras de uranio... Eso es una cosa. Y entonces hago cosas con las

centrifugadoras. Pero si estoy en un entorno diferente. Por ejemplo, una planta eléctrica o cosas así... Me voy a dormir.

#### *Monitores*

**El caso Stuxnet no es excepcional. Duqu, Wiper... O Flame, un virus unas 20 veces más potente que Stuxnet y que hace estragos en ordenadores de Oriente Medio. Es capaz de robar millones de datos. Su misión: espionaje industrial. Ésa es la otra guerra que se libra en el ciberespacio.**

Richard Clarke/Experto en ciberguerra

D16: 16.25/16.54

China, por ejemplo, entra en las empresas de todo el mundo... De Europa, de Norteamérica. Roba secretos y pasa esa información a las compañías chinas. Y así pueden competir con más efectividad contra las empresas europeas y americanas. Es una forma de ciberguerra: la inteligencia económica que desarrolla el Gobierno de China para ganar la competición económica global.

#### *Pausa. Repensamos.*

**Es fácil decirlo. Más complicado probarlo. La ciberguerra plantea un serio problema jurídico. No hay forma de atribuir un acto de agresión y eso significa que es difícil asignar un casus belli.**

Jamie Shea/Responsable de nuevos desafíos de la OTAN

OTAN: 1.02.21/1.02.34

Es muy difícil para nosotros, para nuestra defensa, saber de dónde procede el ataque y proteger todos los puntos y saber quién nos está atacando. Es el problema de la atribución.

#### *Los drones del Ejército israelí. Y rodaje del combatiente del futuro.*

**El Ejército israelí exhibe una de las armas más ansiadas por países en desarrollo. Los drones, aviones no tripulados. Provocan serios daños sin causar bajas. En la guerra convencional es habitual mostrar músculo... Presumir de misiles, aviones de combate... En la ciberguerra, la primera lección es la ocultación. Nadie desvela las armas que tiene. Cuando dispones de un arma... la utilizas o la sigues desarrollando, porque si la revelas concedes una pista al enemigo para diseñar su antídoto.**

#### *Rompemos. Pantallas. Accesos a S21sec.*

**Juan Antonio Gómez Bule es el máximo responsable de S21sec. Aún así, es escrupuloso en el cumplimiento del protocolo. Nadie accede al búnker de su empresa sin las debidas acreditaciones.** D1: 21.50 Lo del Banco Sabadell? Dicen que necesitan todo.

**En esta sala blindada, jóvenes informáticos rastrean los peligros a los que se enfrentan a diario las grandes empresas del Ibex35.**

Juan Antonio Gómez Bule/Presidente de S21sec

D1: 10.40/11.02

Afortunadamente, vamos concienciándonos de que los modelos de ciberseguridad o ciberguerra son modelos que están ahí para aprenderlos, para poder tener un escenario



sobre el que trabajar y unas medidas prospectivas que nos permitan protegernos de un escenario del que hace unos años era un futuro y ahora es un terreno diario.

*Empezamos con la multipantalla. Y luego el coleo con las imágenes a total.*

**Los ataques, más o menos sofisticados, son continuos y abrumadores. La empresa de Kaspersky ha dado una cifra: Casi mil millones de ciberataques en todo el mundo sólo en 2011. Son muy similares los ataques y muy parecidos los escenarios en los que se reciben o se intentan mitigar. Grandes pantallas y decenas de dedos ansiosos que acarician teclados.**

Rótulos: PROVISIONAL

S21sec/Rastrea y mitiga ciberamenazas a empresas

JCISAT/Vigila fallos informáticos en Ejército de Tierra

Pionen/Servidores blindados para medios de todo mundo

Metro de Madrid/Vigilancia del tráfico

NASA/Control y seguimiento de satélites

Red Eléctrica Española/Supervisión de la red eléctrica

*Pausa larguita. Puerta del Sol. Kaíto de hacker en calle conectado por ordenador.*

**En nuestra vida todo pasa por el ciberespacio. Y en esto los más expuestos son los países más desarrollados... Los que, como Suecia, trabajan en desarrollar lo que se conoce como gobernanza en internet.**

*Rodaje de totales sobre Avid.*

Helena Lindberg/Directora de Contingencias Civiles de Suecia

D11: 13.33/13.54

Eso nos hace más y más vulnerables. Por ejemplo, hoy en uno de nuestros periódicos leí esta mañana que hemos tenido un ataque contra nuestra agencia fiscal y han podido sacar números de identidad protegidas.

Jamie Shea/Responsable de nuevos desafíos de la OTAN

OTAN:1.01.49/1.02.04

Las empresas informáticas de Estados Unidos que se dedican a dar protección estiman que cada año llegan al mercado 1,6 millones de nuevos ejemplos de malware o virus.

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú 1: 21.51.34/21.51.59

Lo roban todo. Roban cualquier dato disponible. Por supuesto, lo que más les interesa a ellos son las cuentas corrientes, tu información confidencial. Pero también buscan cualquier dato, incluidos los códigos de activación del software, o fotos, o películas.

Anne-Marie Eklund/Directora Seguridad de .se

D11: 23.59/24.20 (*Cortable*)

Si tú clicas y puedes ganar un iPhone, o un iPad, o eres miembro de una lotería o puedes ganar un millón o cualquiera de estas cosas. Tienes que tener claro que eso no es verdad. No hay que confiar en esa información. Hay que ser muy cuidadoso cuando recibes este tipo de mensajes. Sólo piensa un segundo si estás bien protegido.

*D15: 1.43 Se abre la puerta del ascensor. Desfilamos por pasillo. Abrimos puerta. Entramos en sala. Vemos armario y cuando acabe el off entra cubierto el total del guardia civil.*

**La unidad de ciberseguridad de la Guardia Civil no queda lejos del aeropuerto de Barajas. No es fácil encontrar un delito grave en el que no tengan algo que**



**investigar sus especialistas. Las pistas informáticas son cada vez más valiosas. A veces, imprescindibles. Por eso, los agentes siempre están alerta.**

*De los armarios y los maletines pasamos a las clonadoras.*

Total sin rótulo

D15: 10.14/10.36

En este tipo de maletines es donde llevamos el material que utilizamos en las intervenciones. Básicamente, nuestro papel en esas intervenciones es hacer una copia del material original de todos los dispositivos susceptibles de tener información en formato digital. Y hacer una copia exacta. Para ello tenemos este tipo de clonadoras.

D15: 11.24/11.35

En este lado conectaríamos el disco del sospechoso y aquí el disco nuevo y en blanco.

*Pasamos a imágenes de operaciones. Los chalecos negros. De archivo y de las que nos pasa la Guardia Civil.*

*Gente con móviles. Sociedad de la información. Con pausas y muy picado..*

**Hoy, todo deja rastro. Decenas de miles de cámaras nos vigilan. Los correos electrónicos, la navegación en Internet... Incluso apagado nuestro teléfono móvil puede dejar huella. Y nos puede parecer sencillo eliminar datos de nuestros dispositivos electrónicos... Pero no es así.**

*Lo editamos con imágenes del pen drive, la lupa...*

D15: 18.04/18.14

Este pen drive que lo han tirado al fuego lo han destruido físicamente... Da la impresión de que no se podría recuperar información, pero siempre hay una vía para hacerlo.

*Más lab y planos de operaciones de GC.*

**Además de la investigación de delitos ya cometidos, las fuerzas de seguridad trabajan para prevenirlos. Lo más adecuado es actuar con la mente del delincuente. Por eso la mayoría de las empresas y agencias de seguridad contratan a hackers para que prueben, para que jueguen, para que lleven el sistema al límite. Kaspersky nos sitúa en una hipótesis.**

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú 1: 21.36.35/21.36.45

Sólo imagine que alguien va a Madrid y arroja una botella de material biológico. No se puede controlar.

**Suena alarmista, pero es una amenaza real . Lo sabe bien el especialista de la Guardia Civil en ciberterrorismo internacional.**

No rótulo. *Podemos cubrir parte del total con foros varios.*

D15: 51.47/

En los foros, en la parte privada, donde hablo de actividades más comprometidas, uno dice: Quiero envenenar un depósito de agua, qué puedo hacer. Y ahí, en función de la confianza que te tenga, te responden unos *nicks* u otros. Y te van diciendo: Pues mira, podrías hacer esto.

*Imágenes exclusivas de GC. Posproducción del auto.*

**El seguimiento de esos foros resulta vital para detener a este lobo solitario, Albdelatif Aulad Chiba. (Pausa) El auto de la Audiencia Nacional deja claras sus**

**intenciones: Pretendía contaminar depósitos de agua en complejos turísticos del sur de España. Le detuvieron cuando ya tenía muy avanzado el plan. Poco antes de la detención habría escrito, con su seudónimo, este mensaje:**

“Dios mío, concédeme el martirio por tu causa. Que mi cuerpo vuele en pedazos.”

*Lobo solitario de Toulouse. Gerdarmes en sala. Gerdarmes sacan material de casa.*

**La red está inundada de proclamas como ésta. Por eso, después de un gran atentado, como el de este otro lobo solitario de Toulouse, aflora información que – de haber sido bien tratada- quizá habría servido para evitarlo. Pero es inabordable. Ninguna agencia de ningún país del mundo está preparada para cruzar tantos datos.**

*Suena una web yihadista. Suena total de GC. Cubierto con rodaje.*

CGC D15: 46.59/47.36

Estas imágenes corresponden a un foro de internet. Está considerado entre los cinco más destacados de los foros yihadistas. En la parte pública que vemos hay mensajes de líderes terroristas, discursos doctrinales salafistas yihadistas, reivindicaciones de atentados, exaltaciones de mártires y enlaces a otros foros y páginas similares. Existe una parte privada.

D15: 47.51/47.56

Que es donde se llevan a cabo las actividades más comprometidas.

TC Guardia Civil

D7: 38.15/38.40

Los entornos o las células de terrorismo yihadista vienen utilizando Internet como un instrumento. Instrumento tanto para la comunicación como para el adoctrinamiento y la financiación. No tanto como un objetivo de la acción terrorista. Que sería el concepto que consideramos de ciberterrorismo.

*Sala blindada de la Secretaría de Estado de Seguridad.*

**Pero nadie lo descarta. Entramos en la sala de crisis de la Secretaría de Estado de Seguridad en Madrid. Desde esta sala, conectada con los centros de poder, se intentaría desactivar un hipotético ciberataque total. Para prevenirlo, países como España han creado organismos que trabajan para proteger todas las infraestructuras críticas.**

Fernando Sánchez/Presidente Protección Infraestructuras Críticas (CNPIC)

D9: 1.39/1.47

Aquellas que son importantes para que los servicios esenciales fluyan están en torno a 3.700, 3.800.

TCGC. No rótulo

D7: 51.47/51.59

**España tiene un nivel muy alto.** Somos de los países europeos con mayor desarrollo de los procesos preventivos respecto a ciberamenazas.

D7: 52.11/52.34

Y nos estamos tomando desde la Administración Pública el trabajo muy en serio. Pero por otro lado, se da la situación antagónica de que, por definición, los españoles somos

muy dados a transgredir las normas. En nuestros ordenadores personales realmente somos muy anárquicos.

*Edificio de Sol con ventanas. Calles nocturnas y palabras que se forman de luces.*

**La falta de protección informática es muy peligrosa. En la web merodean miles de chicos malos, de bad boys como se les conoce en la jerga, a la caza de cualquier dato. La empresa de Kaspersky dice haber neutralizado casi 300 millones de programas maliciosos. En el mundo virtual también hay desigualdades... Será más vulnerable quien menos dinero se pueda gastar en proteger su ordenador.**

Jamie Shea/Responsable de nuevos desafíos de la OTAN

OTAN: 1.12.29/1.12.46

Tu casa. Si tú sales y dejas las puertas abiertas y te roban... Bueno, asumes una responsabilidad. Pero si proteges tu casa, el ladrón dirá: Ésta es difícil. Me voy a un lugar más fácil.

Isaac Ben Israel

Israel: 1.26.07/1.26.24

Tenemos una idea aproximada de cuántos ataques bloqueamos. Y el número de ataques es de miles de ataques al día. Miles. Un número altísimo.

*Humanos y ordenadores. Robot TVE*

**Internet genera un negocio inimaginable. Y como en el mundo real, hay también un lado oscuro. Desde negocios siempre rentables como el juego o el sexo a mafias que infectan ordenadores personales desde países remotos y los ofrecen al mejor postor para desde ellos lanzar ataques masivos contra webs... Una industria intangible y perversa...**

Eugeni Kaspersky/Consejero delegado Kaspersky Lab

Moscú 1: 21.48.28/21.49.08

Mucha de esta gente gana mucho dinero. Hemos intentado estimar los ingresos de algunos grupos criminales y es sorprendente... Estimamos que los ingresos de estos grupos criminales una vez calculado el número de víctimas y cuánto dinero le roban a cada víctima... Un cibercriminal gana entre 1.000 y 5.000 euros cada día. ¡Cada día! Cada uno. Entre 1.000 y 5.000 euros. Y no pagan impuestos...

*D9: 55.00 Apertura de puerta para servidores en Pionen. Y le seguimos.*

**Jon Karlung introduce su clave secreta para entrar en el templo sagrado de su empresa, bajo las rocas de Estocolmo. En todos estos servidores se alojan miles de webs que eligen Pionen por las garantías que ofrece ante posibles agresiones... Y muy especialmente de periodistas amenazados por grandes grupos o regímenes autoritarios.**

Jon Karlung/Presidente de Bahnhof

D9: 58.33/58.41

Creo que aquí puedes ver... En este hueco estaba ubicado el servidor de Wikileaks.

D9: 1.02.08/1.02.33

**Durante la operación de Wikileaks no hubo un plan de choque del Gobierno sueco. No contactaron con los clientes porque se consideró inconveniente hacerlo. Deben ser razones legales y debemos utilizar todo nuestro poder para proteger a nuestros clientes.**

D9: 1.19.45/1.20.04

No puedo ser muy específico, pero tenemos clientes que hacen lo posible en países como China, Irán, Siria... Que hacen posible el debate y las discusiones sin que el Estado controle lo que estás haciendo.

*M30. Atasco.*

**Es fácil atacar una web o un blog si no cuenta con una buena protección. De hecho, es una nueva forma de cercenar la libertad de expresión. De esto saben mucho en países como Zimbabue o Birmania. Le pedimos a un especialista que simule un ataque a la web de nuestro programa.**

D12: 27.48/28.30

Ahora mismo en esta pantalla estamos viendo el flujo normal de visitas a una web. Cada una de estas líneas sería una persona u ordenador que se está conectando en ese momento a esa página. Lo que vamos a hacer es simular un ataque, por ejemplo, al blog de En Portada. Y vamos a ver qué sucedería. Lo que se ve aquí ahora mismo es que se incrementa la velocidad con la que pasan cada una de estas líneas. Son visitas. Falsas. Activadas desde ordenadores que se coordinan para multiplicar de tal manera la velocidad hasta llegar a bloquear la página. Si ahora quisiéramos visitar En Portada sería imposible acceder a ella y lo que nos saldría es error 503.

*Interferencia. Seguimos un poquito con [www.rtve.es/enportada](http://www.rtve.es/enportada) con la imagen que luego reproducimos a total.*

**Quizá el ordenador en el que posiblemente usted vea este reportaje está contininado. Quizá este mismo reportaje haya quedado anticuado porque el ciber mundo navega a velocidad de vértigo. Quizá alguien controla nuestros movimientos bancarios. O quizá alguien ha logrado inocular un virus que lo convertirá en punta de lanza de un ciberataque a gran escala. Y lo más preocupante es que la inmensa mayoría de los usuarios no tenemos manera de controlar esa amenaza. Es invisible...**

Isaac ben Israel/Asesor militar israelí

Israel: 1.14.30/1.14.49

Un tren es un robot. No hay un verdadero conductor en el tren. Lo conduce un ordenador y eso significa que si eres un Estado moderno eres muy vulnerable. Mucho más que Afganistán o cualquier otro estado del Tercer Mundo.

Eugene Kaspersky/Consejero delegado Kaspersky Lab

Moscú: 21.34.54/21.35.11

Necesitamos que los Gobiernos entiendan que el problema es serio y duro. Que se sienten en una misma mesa y acuerden el control y el no uso de armas digitales.

Moscú: 21.28.20/21.28.39

Temo que en el futuro no sólo vamos a ver más fuerzas patriotas o más hackers desorganizados... Lo que temo es que en el futuro veamos a Gobiernos detrás de estos ataques. Y eso será mucho, mucho peor.

*Agradecimientos*

*Corresponsalías de Washington, Bruselas, Jerusalén y Moscú.*

*Carlos Dias Oliván y Britos.*