El Mundo – 12.03.2017

Jorge Benítez, Josetxu L. Piñeiro

La Tercera Guerra Mundial ya ha estallado y no lo sabes

La ciberguerra destruye infraestructuras críticas, contamina elecciones... y es un jugoso negocio. Espías, 'hackers' y militares desencriptan los secretos de esta contienda

Третя світова війна вже йде, а ви і не знаєте

Кібервійна руйнує критичну інфраструктуру, впливає на хід виборів та, до того ж, це солодка справа. Шпигуни, хакери і військові займаються дешифруванням секретів цього протистояння

Більшість електронних нападів практично нешкідливі і легко відбиваєтьс системами захисту. Проте, є такі, які містять дуже і дуже небезпечне програмне забезпечення (так звані malware, шкідливі програми), розроблене для пошкодження об'єкта або вбудовування в нього. Бої Третьої світової ведуться в штучному світі, створеному електронними засобами. Те, що ще недавно здавалося фантастикою, стало реальністю – Трамп, Китай, Ізраїль, Європа ... 2017 став роком, коли цифрове протиборство з непередбачуваними наслідками починає відчуватися в аналоговому світі. Масштабні диверсії в Україні і США продемонстрували, що боротьба в кіберпросторі перейшла на новий рівень. Сигнали тривоги на Заході замиготіли яскраво-червоним.

http://www.elmundo.es/papel/historias/2017/03/12/58c151f522601dab398b45dc.html

El protocolo de seguridad obliga a dejar en una habitación contigua el móvil y un*pendrive* que uso de llavero. Están prohibidos todos los dispositivos electrónicos. **Entramos en la sala de guerra de la empresa energética más importante de Israel**, a las afueras de Haifa. Una gran pantalla muestra un mapamundi y centenares de luces que caen como cometas desde cualquier punto geográfico sobre un único objetivo: **nosotros**. El mapa recoge en tiempo real todos los incidentes informáticos (miles a la hora) que sufre esta compañía. Un cartel en la pared recuerda que esto no es un videojuego: Como la seguridad no duerme, nosotros no dormimos.

La mayoría de las agresiones electrónicas son prácticamente inocuas y repelidas sin problemas por escudos defensivos. Sin embargo, hay decenas que esconden un *software* significativamente peligroso (llamado *malware*), diseñado para dañar o infiltrarse en el sistema. Esta instalación, responsable del 70% del suministro eléctrico del país, es lo que cualquier Estado consideraría una infraestructura crítica. Su interrupción o destrucción derivaría en **una situación de emergencia nacional**. Israel Electric no desvela si ha soportado una situación límite. Si fuera así tampoco lo admitiría.

El mapa que brilla en la *war room* representa un conflicto que no se decide por tierra, mar, aire o en el espacio: los cuatro escenarios de la guerra de la segunda mitad del siglo XX. **Sus trincheras están en internet**. Bautizado como el quinto dominio por la revista *The Economist*, el campo de batalla de la III Guerra Mundial es un mundo artificial, creado por medios informáticos. Lo que parecía ficción se ha convertido en realidad: Trump, China, Israel, Irán, Europa... 2017 es el año en el que esta lucha digital de consecuencias impredecibles empieza a dejarse notar en el mundo analógico.

La denominación de guerra mundial no es exagerada si atendemos a su definición enciclopédica: «Una contienda a gran escala que involucra a varias naciones de distintos continentes». Eso sí, **la III Guerra Mundial -o I Ciberguerra Mundial**, eso lo decidirán los historiadores- cuenta con unas

características inéditas. Esta lucha **es camuflada, carece de banderas, no ofrece imágenes ni sonidos y en ella impera la ley de silencio**: la única información que sale a la luz proviene de empresas de ciberseguridad o de filtraciones como las protagonizadas por Snowden,Manning oWikiLeaks. El anuncio de la organización activista comandada porJulian Assange esta semana ha supuesto el último terremoto. A lo largo de los próximos días WikiLeaks difundirá documentación relacionada con los programas que utiliza la CIA para espiar desde cualquier dispositivo conectado a la Red. Se esperan sorpresas.

España, como todos los países, también combate. Según fuentes del Centro Criptológico Nacional, organismo adscrito al CNI, el 3% de los ataques informáticos del año pasado contra sistemas públicos y empresas de interés estratégico fueron de gravedad muy alta o crítica (máxima peligrosidad). Se estima que **tres de cada cuatro son patrocinados por otros países**. China y Rusia son los más beligerantes con España. **Su principal objetivo: el robo de información**.

La ciberguerra global presenta una cronología confusa. No hay un detonante claro ni dos bandos identificados como en el mundo físico. Tampoco se ha asesinado a ningún archiduque austrohúngaro en Sarajevo ni un ejército ha invadido Polonia. **Los precedentes históricos han dejado de servir de referencia**. «De cierta forma, esto acaba con la noción de estado tradicional», explica a PAPEL un alto mando de Ciberdefensa de las Fuerzas Armadas de Israel. «De repente, las fronteras son irrelevantes, el Derecho Internacional no impera o tiene muchas interpretaciones... **Sólo rige la ley de la jungla**».

Al contrario que en el fútbol, en el ciberespacio es mucho más difícil defender que atacar. Por eso, gobiernos y empresas han iniciado una carrera armamentística de programadores y herramientas informáticas. «Cuando repeles un ataque sabes que tu enemigo volverá mañana. Tú tienes que ganarle todos los días, mientras que **a él le basta un mal día tuyo para vencer**», explica el español Jose Selvi, investigador de Seguridad Senior de Kaspersky, multinacional rusa especializada en ciberseguridad. El problema es que cada vez hay más posiciones que defender: este año se alcanzarán los 8.400 millones de dispositivos conectados a internet, cifra que **supera el número de habitantes del planeta**. Demasiadas puertas para aquellos que quieren entrar sin llamar.

Kaspersky es un gigante del sector y ejerce de forense en numerosos casos de guerra electrónica. Uno de ellos fue el Stuxnet: para muchos especialistas, **la primera superarma virtual destinada a causar daño físico**. Se trata de un gusano (programa diseñado para copiarse y propagarse por sí mismo) que en 2010 se introdujo en el programa nuclear iraní para sabotearlo.

Las autopsias informáticas tienen algo del *Cluedo*, el popular juego de mesa.**Hay que averiguar quién es el asesino, qué arma usó y dónde se perpetró el crimen**. Ya saben, la señorita Amapola disparó la pistola en el comedor. En internet siempre se deja un rastro que hay que saber seguir. La atribución de un ataque es siempre compleja, incluso localizar la IP del ordenador que lo originó no siempre es suficiente. **Mucha de esa culpa la tiene el frecuente empleo de hackers mercenarios** (patrocinados por Estados, pero que actúan sin bandera), una táctica que difumina al enemigo real y limita sus riesgos. A menudo basta con echar un vistazo a un mapa y ver la lista de rivales comerciales o militares para averiguar quién es tu señorita Amapola.

Y (desafortunadamente) **todos los países tienen su señorita Amapola**.

Stuxnet es descrito por la compañía Kaspersky con una prosa tenebrosa, digna de un cuento gótico: «Es un prototipo funcional y aterrador de un arma cibernética que **conducirá a la creación de una nueva carrera armamentística mundial**». Su sofisticación dejó claro que su diseño escondía un poder tecnológico al alcance de muy pocos. El *New York Times*atribuyó su autoría a Israel con la colaboración de EEUU. Cuando preguntamos sobre el Stuxnet a un representante de la Oficina del Primer Ministro de Israel, su respuesta fue evasiva: «No sé qué es eso».

La negación es otra arma defensiva en la jungla digital, donde no se llevan las declaraciones de guerra a la vieja usanza.

No es una cuestión de modales. Las sociedades, especialmente en Europa, están muy lejos de la efervescencia patriótica que marcaron muchas guerras del pasado y un anuncio así provocaría pánico entre la gente, además de una fuerte contestación. Aunque sobre todo hay un motivo estratégico: **«Si otro país destruye tus infraestructuras críticas y provoca muertes con un ciberataque, podría darse una respuesta militar convencional. Por eso nunca nadie lo reconoce»**, confirma un general de una superpotencia militar.

El contraataque de toda la vida, a sangre y fuego, está justificado en un documento de la OTAN conocido como el *Manual de Tallin*, que recoge una serie de reglas dedicadas a la ciberguerra. Una de las más polémicas es la que **legitima matar a hackers enemigos**, aunque estos sean civiles, si han provocado daños graves.

Esto demuestra la importancia estratégica del *ciberguerrero* en los conflictos del siglo XXI. En muchas circunstancias es mucho más útil que una división acorazada... y más barato. Cuando Estados Unidos lanzó en la II Guerra Mundial dos bombas atómicas sobre Japón, no sólo cumplió con su objetivo militar de forzar la rendición sino que disuadió a cualquier rival de discutirle su liderazgo. Tuvo el monopolio nuclear hasta que los soviéticos fabricaron su bomba en 1949.

En el ciberespacio esto no funciona así. **Un programa como Stuxnet es como una abeja: una vez clavado su aguijón, muere**. Estas armas inician su fin tecnológico cuando son ejecutadas en misiones, porque pueden ser descubiertas y analizadas por el resto de contendientes de la ciberguerra. Cuando esto sucede, se produce un salto en innovación y pronto los demás son capaces de desarrollar más formas de *malware*. Así se alimenta la carrera (ciber)armamentística.

Todo está conectado. Rodeados de amenazas, con criminales que quieren robar nuestro dinero y enemigos que anhelan nuestros secretos, resulta complicado analizar el sosiego de nuestro día a día virtual. Es muy sencillo: **en la ciberguerra no hay muertos**, aunque la población civil empieza a sufrir muchas penalidades. Y las amenazas no dejan de crecer.

ATAQUES MÁS REPRESENTATIVOS DE LA CIBERGUERRA

¿Qué pasaría si se manipularan los semáforos de una ciudad o la torre de control de un aeropuerto? Por desgracia, los acontecimientos recientes desvelan los agujeros de seguridad de muchos sistemas electrónicos que afectan a la ciudadanía. A la denominada guerra económica -muy relacionada con el ciberespionaje industrial y culpable de pérdidas de puestos de trabajo e inversiones- se han unido también agresiones físicas como las registradas en Ucrania.

Dos días antes de la Navidad de 2015, un *malware* bautizado como BlackEnergy se infiltró en una central eléctrica de este país de Europa Oriental. Estaba programado para borrar archivos y sabotear el sistema de esta infraestructura crítica. **Más de 600.000 personas se quedaron sin calefacción en invierno durante unas horas**. Kiev acusó a Rusia de estar detrás del ataque. La ciberguerra ha dejado de ser un asunto exclusivo de espías, militares y empresarios: tres profesiones que conoce muy bien Rami Efrati.

La cita con él es en un restaurante de Tel Aviv. Efrati es un tipo bienhumorado, de edad avanzada y con un inglés con fuerte acento polaco. Durante 28 años sirvió en el ejército en labores de Inteligencia y actualmente dirige su propia empresa de ciberseguridad. Es un ejemplo de la fiebre del oro de una industria multimillonaria que está fichando a los jóvenes más dotados para la física y las matemáticas.

Efrati no ha visto la película sobre Edward Snowden, el ex analista de la NSA que filtró al mundo el espionaje masivo realizado por Estados Unidos. No lo descarta, porque aún se proyecta, dice, en algún cine de la ciudad. Pero no parece que el film de Oliver Stone vaya a hacerle cambiar de opinión:**«Cualquier persona que haya trabajado en una agencia de Inteligencia te dirá que Snowden es un traidor»**, sentencia.

Tiene que haber pocos cartógrafos del cibermundo mejores que Efrati. Conoce hasta las fosas abisales de la Red, ese **mercado negro de coordenadas inaccesibles para el ciudadano corriente donde todo está a la venta:** la *darknet* (literalmente, red oscura). Él la describe de la siguiente

manera: «Un lugar donde se pueden comprar tanto las armas informáticas más sofisticadas como reclutar a programadores de gran nivel. De esa forma la ciberguerra se iguala y los Estados más avanzados no son los únicos actores. Con dinero los grupos terroristas y las mafias criminales se arman como el que más».

Si esas son las tinieblas, la ciberseguridad también tiene su luz. Concretamente, de neón comercial. Cualquiera que haya visitado una feria sectorial (sea de turismo, automóviles o quesos de cabra) sabrá que consiste en pasear por unos pasillos repletos de *stands*. Se ven azafatas, corbatas, folletos y bolígrafos corporativos con colores horteras. El encuentro de CyberTech de Tel Aviv es idéntico, el mismo ambiente, pero allí se reúne lo más granado del negocio de la seguridad. Incluso el Mosad tiene un quiosco con una urna para echar solicitudes de ingreso.

Según previsiones de la agencia de análisis Gartner, l**a ciberseguridad moverá en todo el mundo unos 150.000 millones de euros en 2020**. Es el nuevo El Dorado tecnológico. Razón por la que los emprendedores que triunfan con sus *startup* son las nuevas estrellas del rock: millonarios efervescentes que firman autógrafos y se hacen selfies con *groupies* de la tribu internauta. **«No intentes que tu hijo sea el nuevo Messi, convéncele para que diseñe un antivirus»** es el eslogan tácito que recorre este encuentro global.

Por supuesto, allí veo a Rami Efrati pasear por la moqueta su don de gentes repartiendo tarjetas con dedos ágiles de prestidigitador.

Hasta hace cinco meses, Estados, ciberdelincuentes y terroristas recorrían el ciberespacio con relativa discreción. Todo cambió el pasado mes de octubre, cuando un ejército de hackers de origen desconocido desconectó de internet durante 11 horas a gran parte de la costa Este de Estados Unidos afectando a mil millones de usuarios de todo el planeta. Imagine que trabaja de cajero en un banco, de repente en su ventanilla se planta un millón de clientes y cada uno de ellos quiere ingresar un euro. Eso es lo que se conoce como **un ataque por denegación de servicio (DDoS)**: en este caso el proveedor de internet atacado en manada se asfixió por saturación de tráfico.

Su colapso derivó en interrupciones en webs tan populares como las de Twitter, Amazon, Netflix y *The New York Times*. **Era la primera vez que un ataque masivo se cocía dentro del denominado internet de las cosas** (todos los objetos cotidianos que están conectados a la Red). En este caso, los hackers lanzaron su ataque a través de cámaras de seguridad, decodificadores de televisión y routers domésticos. La originalidad del asalto plantea, según Enrique Ávila, director del Centro Nacional de Excelencia en Ciberseguridad, un problema que tarde o temprano la comunidad internacional tendrá que abordar: los agujeros de seguridad de la cadena de distribución de todo lo que compramos.

«El mundo tecnológico tiene sus fábricas en China porque los costes son muy bajos», dice Ávila. «En ciudades como Shenzhen [con 6.000 fabricantes de la industria] se hacen la mayoría de los dispositivos electrónicos. Estas condiciones impiden que se trate con el rigor necesario la seguridad de unos componentes dotados de un *software* que es susceptible de ser pirateado. **No sabemos ni siquiera si los dispositivos que utilizaron habían sido hackeados antes de su comercialización**».

Ataques como los de Ucrania y Estados Unidos demostraron que en la lucha del ciberespacio se había pasado a otro nivel. Las alertas en Occidente empezaron a brillar en rojo Valentino.

Entonces Trump lo hizo. Se convirtió en el 45º presidente de EEUU.

La injerencia rusa en una campaña presidencial de tal magnitud ha sido un hito crucial en la historia de la I Ciberguerra Mundial. Lo que no había logrado el Ejército Rojo en la Guerra Fría con ojivas nucleares y su presencia en Cuba lo ha conseguido Vladimir Putin a golpe de clic: **influir en la elección del cargo más poderoso de la Tierra**. El 9 de diciembre, el *Washington Post* publicó que la CIA acusaba a fuentes cercanas al Kremlin de filtrar a WikiLeaks los emails pirateados a la campaña de Hillary Clinton con el fin de perjudicarla en la carrera por la Casa Blanca. Sorprendentemente, **se rompía la ley del silencio**. Una superpotencia acusaba a otra de una intromisión política directa y gravísima.

El plan diseñado por los hackers, mercenarios (presuntamente) en nómina de la agencia militar rusa (GRU), se ejecutó gracias al llamado*spear phishing*: un ataque que busca obtener información confidencial mediante el engaño. Su acceso llegó cuando varios miembros de la campaña demócrata abrieron un email trampa y destaparon la caja de Pandora.

Mientras tanto, Europa aguarda incrédula. Su opinión pública se pregunta qué puede pasar después de lo acontecido en la mayor superpotencia mundial. **Es víctima de un pulso psicológico 3.0 y nadie explica muy bien que está sucediendo**. Los mensajes son preocupantes. El gobierno holandés anunciaba en el mes de febrero la retirada del voto electrónico en favor del recuento contado a mano por miedo a que hackers pudieran interferir en sus comicios. La inquietud va más allá del control de un proceso electoral. En plena era de la posverdad, tras el Brexit y la victoria de Trump, la manipulación de datos y la filtración selectiva de información hackeada en las redes sociales podrían ser armas muy efectivas en las elecciones que se van a celebrar en Francia, Alemania e Italia. El auge del populismo y la crisis del proyecto europeo debilitan unas defensas que ya no son sólo informáticas, sino sociales.

¡Es la guerra! diría (Groucho) Marx. Sí. Ahora solamente queda por saber quién la está ganando.