Guerras globales desde un teclado

DAVID CORRAL HERNÁNDEZ

El nacimiento del actual Internet en plena Guerra Fría ofreció a las fuerzas armadas de Estados Unidos una herramienta única y formidable por su superioridad y flexibilidad ante los posibles ataques enemigos o como base para crear redes de comunicaciones o de mando y control (como puedan ser NCW - Network Centric Warfare o NEC - Network Enabled Capability). Hoy, sin embargo, acceder a la Red y sus contenidos es considerado como uno de los mayores avances logrados por la Humanidad, pero también como el Talón de Aquiles de muchas de sus actividades cotidianas por su alta vulnerabilidad al intrusismo de ciberterroristas, ciberdelincuentes, hackers, etc. Los daños que pueden sufrir instalaciones civiles fundamentales y los sistemas de defensa nacionales han convertido a la guerra cibernética en un campo de batalla virtual en el que quedarse atrás es acercase a la derrota.

RED DE REDES

El Departamento de Defensa de Estados Unidos y algunas de las principales universidades del país lograron en 1969 establecer la primera conexión entre ordenadores por medio de líneas telefónicas conmutadas. Los centros enlazados fueron tres universidades de California y una cuarta en Utah y la red, origen y fundamento de Internet, fue llamada ARPANET (Advanced Research Projects Agency

Network). El planteamiento esencial era desarrollar e implementar una red de comunicaciones de alta seguridad, basada en la descentralización, en la fragmentación de los paquetes de datos e información, en la posibilidad de unir a emisores y receptores por caminos diversos y complementarios, que pudiera dar respuesta y solución a los fallos internos y, en su aplicación más militar, que fuera inmune a un supuesto ataque nuclear para asegurar la continua existencia de redes de mando y control y de comunicaciones entre las diferentes unidades. Además de las diferentes aplicaciones civiles que utilizamos habitualmente (como el WWW, correo electrónico, videoconferencias, etc.), esta red primigenia tuvo un progreso militar paralelo a través de redes como DDN (Defense Data Network), nacida como MILNET y empleada internamente por el Departamento de Defensa de EE.UU. desde 1983 a 1995 para unir sus centros con las bases en el extranjero a través de cuatro redes principales: MILNET (para datos sin clasificar), Defense Secure Network One (DSNET 1, para datos secretos), Defense Secure Network Two (DSNET 2, para datos "Top Secret") y, por último, Defense Secure Network Three (DSNET 3, para datos TS/SCI o Top Secret/Sensitive Compartmented Information). En los años noventa MILNET se convirtió en NIPRNET (Nonsecure Internet Protocol Router Network). Según cifras recogidas por la Unión Internacional de Telecomunicaciones, ente dependiente de la ONU, en 2008, con más de 6.000 millones de habitantes en la Tierra, cerca de 1.500 millones de personas tenían conexión a Internet, un 23.8% del total de población mundial, lo que supone un crecimiento del 342.2% respecto al año 2000. Asia, con el 56.3% de habitantes mundiales tiene al 17.4% conectado. Son cifras muy alejadas de las naciones occidentales, pues en Norteamérica están conectados el 74.4% de sus habitantes siendo sólo el 5.0% de población mundial, Oceanía el 60.4% con un 0.5% de habitantes del Globo y Europa un 48.9% para el 12.0% de la población mundial. Por usuarios el número uno es China, con casi 300 millones, lo que representa un 22.4% de penetración y un 18.7% de usuarios. El segundo lugar es para Estados Unidos con algo más de 225 millones de usuarios, un 74.7% de penetración y 14.2% de usuarios. Le siguen en el listado Japón, India, Brasil, Alemania, Reino Unido, Francia, Rusia y Corea del sur. España ocupa el decimotercer puesto con un 70.5% de penetración y un crecimiento del 429,9% para el periodo 2000-2008. Pero la Red tiene su principal éxito y su principal riesgo en sí misma. De instrumento inigualable para la globalización, el comercio, el desarrollo científico, las relaciones sociales, la difusión de la información y la cultura …a caballo de Troya para acceder a datos personales, a los sistemas de gestión como los sanitarios o los del agua corriente, a las redes militares o

financieras, entre muchas otras posibilidades que consideramos como cotidianas y cuya presencia es discreta pero cuya merma o ausencia pueden desembocar en caos muy temidos por los gobiernos.

ARMAS CIBERNÉTICAS, DESTRUCCIÓN REAL

La gran ironía de la Sociedad de la Información de este siglo XXI es que

las mismas tecnologías que nos permiten construir y crear un mundo más grande, mejor y más "conectado" son las mismas que pueden utilizar todos aquellos individuos, grupos u organizaciones que tienen como fin el ataque a estados, sociedades, culturas, etc. Este tipo de agresión desconoce las fronteras, puede lanzarse desde cualquier punto y pasar por miles de ellos hasta que llega a su objetivo final. Los estados como tales pueden no ser autores de estas acciones, lo mismo que tampoco sus ejércitos, aunque puedan instigarlos y apoyarlos. Sus responsables suelen ser, además de evasivos, gente ajena

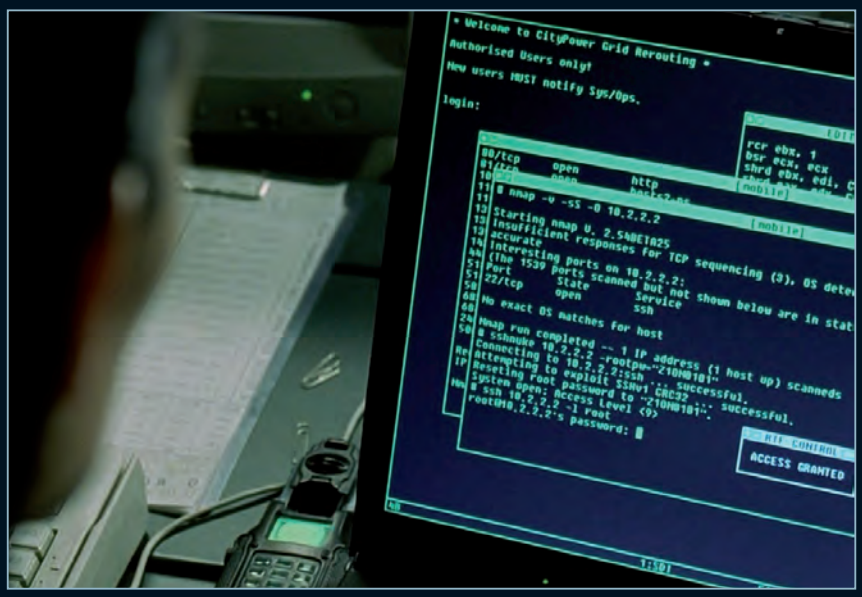
a cualquier institución gubernamental y que difícilmente podrá ser identificada y responsabilizada por investigaciones policiales y judiciales. Incluso si se determina que una nación es autora de los ataques será muy difícil dar una respuesta apropiada y convencional a este conflicto virtual ya que no hay apenas ni legislación ni convenios. En 1988 hizo su aparición el primer gusano informático de Internet, el "Morris Worm". La generación de virus informáticos ha pasado de ser de 40 al día en 2003 a 300.000 al día en 2008 y suman más de 21 millones los virus conocidos. Hoy una de las armas más empleadas para perpetrar un ciberataque es el "Botnet" (o red zombi), un conjunto de ordenadores/servidores infectados de forma remota por un software malicioso que permite al atacante controlar dichas maquinas sin tener acceso físico a ellas y que ejecuta de manera autónoma un virus que va infectando a otros ordenadores/servidores a través de correos electrónicos, páginas web, actualizaciones de software… todo ello sin el conocimiento del propietario. Una vez que el "gusano" ha infectado a miles de máquinas pueden comenzar los ataques de tipo D.D.O.S. (Distributed Denial Of Service) con los que se bloquean los servicios ofrecidos a través de la Red, como las comunicaciones, las redes eléctricas o de suministro de agua, el control del tráfico aéreo, las compras online, las operaciones bursátiles o los servicios de emergencias, entre muchísimas otras. Todas estas cualidades y su bajo coste hacen de él uno de los instrumentos más populares en un ciberconflicto. Decenas de ingenieros y científicos trabajan en virus informáticos y en sistemas de acceso, son armas informáticas para una ciberguerra en la que serían empleadas para observar las capacidades y recursos del adversario, para desmantelar las defensas enemigas antes de un ataque, para sembrar el caos de las comunicaciones o para enviar información falsa con la que generar confusión. El objetivo es entrar y

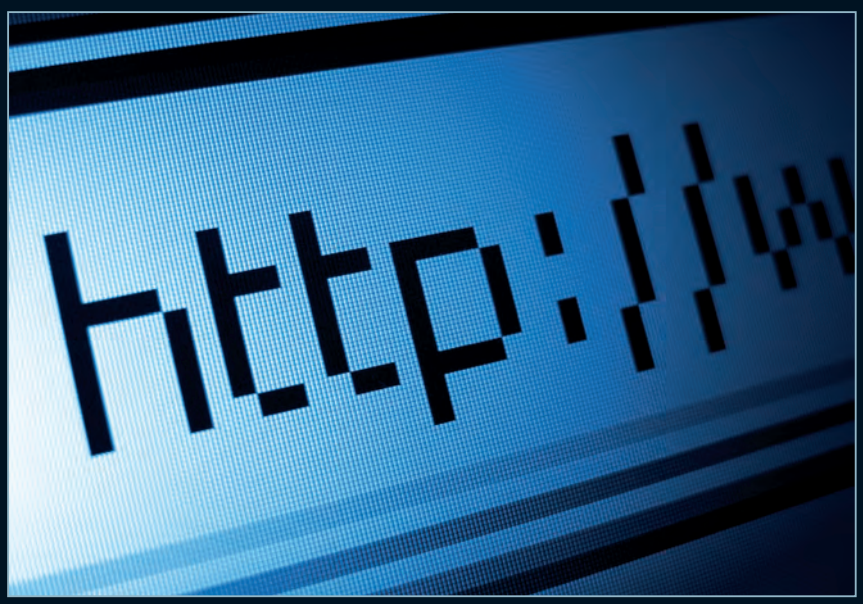
golpear rápidamente la red de datos del enemigo denegando, degradando, inhabilitando, desestabilizando, destruyendo o engañando. En un sector tan altamente tecnificado los efectos sobre los sistemas de control o en los sistemas de armas pueden ser devastadores y cuanto más se dependa de la informática y de las redes mayor será el potencial de recibir daños. A lo largo de las últimas décadas las fuerzas armadas han trabajado mucho para desarrollar redes netcéntricas y C4ISR lo más dinámicas posible, pero el inconveniente es que muchas de ellas siguen dependiendo de su soporte físico, como kilómetros de cables, servidores informáticos, redes de satélites, fibras ópticas, software, … todo ello teóricamente vulnerable a las intrusiones ajenas y a los ataques de bajo coste contra sistemas de avanzada tecnología y elevado precio propios de esta "guerra de las redes" (network warfare). A la cabeza de los "agresores" se encuentran Rusia y China, ambos a la vanguardia de la ciberguerra. Según un informe del Departamento de Defensa estadounidense las fuerzas armadas chinas están invirtiendo ingentes cantidades de dinero en crear contramedidas electrónicas y expresiones como "ataque a una red de ordenadores", "defensa de una red de ordenadores" o "explotación de una red de ordenadores." Según asegura este informe los militares chinos creen que con estas avanzadas técnicas podrán ganar una guerra sin que ésta llegue a comenzar. Desde el Congreso estadounidense, a través de la Comisión de Ciberseguridad, alertan sobre los avances chinos en este campo, haciendo de la ciberseguridad "uno de los desafíos más importantes, junto a los económicos y de seguridad nacional, que Estados Unidos encarará en el siglo XXI". James Mulvenon, director del Centro de Inteligencia e Investigación en Washington, ha afirmado que "los chinos fueron los primeros que usaron los ciberataques para objetivos políticos y militares". Como defensa y para evitar represalias China ha desarrollado un sistema operativo supuestamente invulnerable a la guerra cibernética y a las incursiones de los tres sistemas operativos más populares: Windows, GNU/Linux y Unix. Kylin, que comenzó a desarrollarse en 2001, está siendo instalado desde 2007 en servidores y ordenadores de las fuerzas armadas y de los servicios de inteligencia de la potencia comunista. Junto a este sistema operativo los chinos también han fabricado un microprocesador "invulnerable" que blinda cualquier plataforma frente a los ataques de hackers o software malintencionado. Otro frente muy activo es el ciberterrorismo, con los movimientos radicales islamistas a la cabeza, pues son innume-

rables las ventajas que encuentran para desarrollar estrategias asimétricas, expandir sus discursos y reivindicaciones, intervenir en la política y la sociedad, reclutar y entrenar a sus adeptos, planificar sus acciones y ataques, etc. Las páginas web radicales se han multiplicado por diez del 2007 al 2008 y hay miles de ellas dedicadas al terrorismo en Internet.

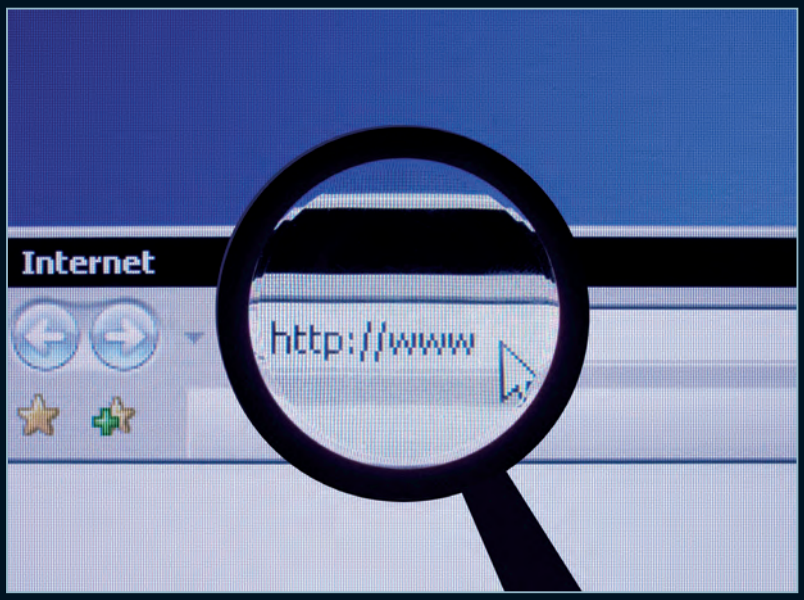
LAS GUERRAS DE LA RED

Los ataques que habitualmente sufren los servidores de los sectores públicos y privados provienen de un heterogéneo conjunto de actores, desde estatales a privados, y las motivaciones son múltiples pues se diluyen las fronteras, las ideologías, las religiones y son muchas las ocasiones en las que el reto personal o el afán de lucro son suficientes para iniciar el asalto. En la Netwar ("Guerra en Red") se podrá llegar a combatir al mismo tiempo en diferentes teatros, niveles y dimensiones (terrestre, naval, aérea, espacial, virtual, etc.) y muchos de los ataques podrán ser acciones combinadas de poder convencional con ideas y tecnologías de la información y la comunicación. El primer caso representativo de ciberguerra, como tal, lo sufrió en 2007 Estonia, seguida por Georgia en 2008 y Kirguizistán en 2009. El país báltico, uno de los que cuenta con mayor número de usuarios de Internet del mundo, recibió durante días ataques masivos que acabaron colapsando las redes informáticas de bancos, instituciones, partidos políticos o medios de comunicación. Fue obra de "hackers" rusos que protestaban por el traslado del Soldado de Bronce de Tallin, un monumento de tiempos soviéticos que conmemoraba la liberación del país de los nazis. El Gobierno estonio acusó entonces a Moscú de haber orquestado esta ofensiva en la que muchos veían la mano de los especialistas del Servicio Federal de Seguridad, el heredero del temible KGB, y de la FAPSI, la organización de comunicaciones gubernamentales e información de Rusia. Fue un ejemplo perfecto de cómo utilizar equipos en terceros países para franquear fronteras "enemigas" sin que las huellas permitan proclamar vínculos o autorías de manera categórica. Para la OTAN estos ataques contra las redes estonias demuestran que el concepto de la defensa ha cambiado profundamente en los últimos años y que ahora es necesario considerar otras posibilidades y nuevos frentes, como el Ciberespacio. Un año después la Alianza creó en Tallin el Centro de Excelencia para la ciberdefensa, un proyecto en el que están involucrados siete países, entre ellos España. Viviane Reding, comisaria europea sobre la Sociedad de la Información, ha sido categórica: "Estonia ha sido una llamada de alerta". Estados Unidos,





que pugna por su hegemonía en el ciberespacio, tampoco es ajeno a estos ataques. En 2008 el número de ciberataques sufridos por las redes del Gobierno aumentó en más de 40 por ciento, según datos obtenidos por el US-CERT (US Computer Emergency Readiness Team), aunque las cifras finales podrían ser superiores ya que sólo un mínimo tanto por ciento de las agencias federales ha desarrollado completamente sistemas de rastreo y la mayoría carecen de los niveles de seguridad adecuados en muchos de sus dispositivos, especialmente los móviles y las PDAs. El Departamento de Defensa de EE.UU. recibió en 2008 cerca de 360 millones de intentos anónimos de intrusión en sus redes. El Pentágono, en 24 horas, llegó a sufrir 6 millones de intentos de acceso cuando antes del 11S la cifra anual más alta no llegaba a superar los 250.000. Sólo en el último semestre el Pentágono se ha gastado 100 millones de dólares en reparar los daños causados por los ataques cibernéticos y ha prohibido a sus empleados el uso de lápices de memoria para evitar infecciones o daños. Pero la brecha más grave parece ser el acceso que obtuvieron unos hackers chinos al programa del avión de combate JSF (Joint Strike Fighter, o F-35), el más caro de la historia militar de Estados Unidos. Pero no es un ejemplo aislado, desde múltiples "posiciones" chinas se ha accedido a muchos ordenadores del Congreso, al sistema de control de la USAF o a la red del suministro eléctrico, entre otros casos. Un informe de McAfee, empresa líder en antivirus, aseguraba que en los tres primeros meses de este 2009 casi 12 millones ordenadores fueron incorporados a las redes de máquinas infectadas con "malware" por los cibercriminales. Además los Estados Unidos han desplazado a China a la cabeza de los países con más ordenadores infectados por "botnet" con el 18% del total mundial frente al 13,4% de China. Ni siquiera el entonces senador Barack Obama se libró durante su campaña presidencial de las incursiones cibernéticas. Su página web sufrió asaltos y algunas bases de datos recibieron la visita de estos ladrones de guante digital. España, que ocupa junto con Francia el puesto 17 en cuanto a páginas web infectadas, lo que supone el 0,7% del total mundial, padeció en 2008 un aumento de un 570% del cibercrimen respecto al año anterior. Los principales casos se deben al robo y secuestro de información industrial, empresarial y financiera y además ha aparecido una nueva modalidad de crimen, el ciber-rescate, por el que los hackers reciben dinero por no desencriptar o publicar la información robada. Vistas las estadísticas nuestro país ha propuesto a la Unión Europea poner en marcha un Plan Estratégico de Seguridad que combata los ataques cibernéticos.



OBAMA.COM

Una de las prioridades de la Administración Obama es, junto a la guerra nuclear o las armas de destrucción masiva, la seguridad nacional frente a los ataques cibernéticos, una amenaza que es cada vez más difícil de prevenir. La Casa Blanca, aconsejada por especialistas, quiere evitar un 11S virtual, un Pearl Harbor digital o un "cybergeddon" (Apocalipsis cibernético). El presidente ha promovido un estudio de 60 días sobre el estado de las infraestructuras de las redes estadounidenses de comunicaciones e información para protegerlas de ataques externos. De él se han obtenido e identificado 250 "necesidades, tareas y recomendaciones" y es que, hasta entonces, sólo la NSA y el DHS (Department of Homeland Security) parecían las únicas grandes agencias encargadas de la seguridad y se hacía necesario definir los objetivos de los diversos servicios de inteligencia y seguridad para asegurar la integridad de las redes empleadas por el Gobierno, muchas de ellas de propiedad y de gestión privada, lo que supone arquitecturas abiertas muy vulnerables y accesibles a los ciberataques. En palabras del presidente Obama los Estados Unidos se preparan para iniciar una nueva guerra, en esta ocasión librada en el ciberespacio, y por ello ha decidido crear una nueva figura, el "Ciberzar", un cargo con asiento en la Casa Blanca y cuya misión es dirigir la ciberseguridad tanto de las redes oficiales como de las privadas. La persona elegida ha sido el teniente general Keith B. Alexander, jefe de la Agencia de Seguridad Nacional (NSA) y director del

JFCCNW (Joint Functional Component Command for Network Warfare), ente responsable de planificar, coordinar y dirigir operaciones ofensivas y defensivas en el ciberespacio. Para él "mantener la libertad de acción en el Ciberespacio en el siglo XXI es tan esencial a los intereses de EE.UU. como lo fueron la libertad de los mares en el siglo XIX y el acceso al aire y el espacio en el siglo XX". Por su parte el secretario de Defensa estadounidense, Robert Gates, ha anunciado la puesta en marcha de un nuevo "Ciber Comando", el primero en la historia militar del país. Desde Fort Meade, en Maryland, su personal estará encargado de proteger las redes informáticas militares estadounidenses contra ataques cibernéticos y deberá desarrollar métodos para atacar los sistemas informáticos ajenos con los que asegurar la "libertad de acción en el ciberespacio". Esta unidad estará adscrita a la NSA mediante US Strategic Command, entidad encargada, entre otras cosas, del arsenal atómico estadounidense, de la defensa espacial e informática, del escudo de misiles y de la detección de armas de destrucción masiva. Un precedente podría ser el AFCYBER, el Cibercomando de la Fuerza Aérea con sede en la Base Barksdale de la USAF y una estructura de mando unificada. Según uno de sus documentos (Air Force Cyber Command, "Strategic Vision"), el entorno estratégico es descrito como "imprevisible y extremadamente peligroso," caracterizado "por la confluencia de globalización, disparidades económicas, y competencia por recursos escasos". También afirman que "poder global es la capacidad de poner en peligro o atacar cualquier objetivo con energía electromagnética y en última instancia asestar efectos cinéticos y no-cinéticos en todos los terrenos. Esas capacidades del ciberespacio nos permitirán asegurar nuestra infraestructura, realizar operaciones militares cuando quiera sean necesarias, y degradar o eliminar las capacidades militares de nuestros adversarios". Son firmes pasos para lograr la Ciberdominancia en unos tiempos en los que los límites del poder cibermilitar y su definición doctrinal están empezando a esbozarse y en los que la Red, además de proporcionarnos múltiples beneficios de manera discreta y cercana, puede suponer una amenaza para la vida cotidiana si los teclados y los bytes explotan sus vulnerabilidades para buscar perjuicios ■