06-07-2007

La guerra de los bits: Cuando las computadoras atacan

John Schwartz
New York Times
Traducido por Francy Pérez y revisado por Mabel Rivas González, del Equipo de Cubadebate y Rebelión

CUALQUIERA que esté al tanto de la tecnología o de los asuntos militares ha venido escuchado las predicciones durante más de una década. La ciberguerra se acerca. Si bien aún no se ha producido el conflicto dirigido por computadoras, tan anunciado y esperado, el pronóstico se torna más siniestro con cada relato: una nación beligerante lanza un ataque, apoyada por sus cerebros y recursos informáticos; quedan destruidos los bancos y otros negocios en los estados enemigos; se paralizan los gobiernos; se desconectan los teléfonos; los muñecos Elmos controlados por microchips serán transformados en máquinas asesinas indetenibles. \n \u003cp\>No, este último artículo no entra en escena, básicamente porque esos \n juguetes controlados por microprocesadores no están conectados a la \n Internet por conducto de las tecnologías industriales de control remoto \n conocidas como sistemas SCADA, o sea, Control \u003cstrong\>de Supervisión y \n Adquisición de Datos.\u003c/strong\> \u003cstrong\>La tecnología permite el monitoreo \n y el control remotos de operaciones como líneas de producción \n manufacturera y proyectos de obras civiles como presas. De modo que los \n expertos en materia de seguridad se imaginan a los terroristas frente a un \n teclado cerrando a distancia las naves de una fábrica, o abriendo las \n compuertas de una presa para devastar las ciudades que se encuentren en \n las partes bajas.\u003c/strong\>\u003c/p\>\n \u003cp\>¿Pero cuán dañina sería realmente una ciberguerra, en especial si se \n compara con una guerra genuina en la que se derrama la sangre y vuelan las \n entrañas? Y por otra parte, ¿existe la posibilidad de que suceda en \n realidad?\u003c/p\>\n \u003cp\>Cualquiera que sea la respuesta, los gobiernos se están preparando para \n la grande. \u003c/p\>\n \u003cp\>\u003cstrong\>Los expertos en seguridad creen que China ha sondeado con \n creces las redes estadounidenses. Según el informe anual de 2007 del \n Departamento de Defensa al Congreso, el ejército chino ha hecho fuertes \n inversiones en contramedidas electrónicas y en defensas contra ataques, y \n en conceptos como "ataque informático, defensa informática y explotación \n informática"\u003c/strong\>. \u003c/p\>\n \u003cp\>Según el informe, el ejército chino calificó las operaciones \n informáticas de "cruciales para lograr □la dominación electromagnética□" \n -que sabe Dios qué significa eso-- desde el principio de un conflicto.\u003c/p\>\n \u003cp\>\u003cstrong\>Los Estados Unidos también se están armando. Robert Elder, \n comandante del Comando del Ciberespacio de la Fuerza Aérea, declaró hace \n poco a periodistas en Washington durante un desayuno que su comando, \n formado recientemente, encargado de defender la información, las \n comunicaciones y las redes de control en la esfera militar, está \n aprendiendo a deshabilitar las redes informáticas del opositor y a hacer \n colapsar sus bases de datos. ",1]); //-->

No, este último artículo no entra en escena, básicamente porque esos juguetes controlados por microprocesadores no están conectados a la Internet por conducto de las tecnologías industriales de control remoto conocidas como sistemas SCADA, o sea, Control de Supervisión y Adquisición de Datos. La tecnología permite el monitoreo y el control remotos de operaciones como líneas de producción manufacturera y proyectos de obras civiles como presas. De modo que los expertos en materia de seguridad se imaginan a los terroristas frente a un teclado cerrando a distancia las naves de una fábrica, o abriendo las compuertas de una presa para devastar las ciudades que se

encuentren en las partes bajas.

¿Pero cuán dañina sería realmente una ciberguerra, en especial si se compara con una guerra genuina en la que se derrama la sangre y vuelan las entrañas? Y por otra parte, ¿existe la posibilidad de que suceda en realidad?

Cualquiera que sea la respuesta, los gobiernos se están preparando para la grande.

Los expertos en seguridad creen que China ha sondeado con creces las redes estadounidenses. Según el informe anual de 2007 del Departamento de Defensa al Congreso, el ejército chino ha hecho fuertes inversiones en contramedidas electrónicas y en defensas contra ataques, y en conceptos como "ataque informático, defensa informática y explotación informática".

Según el informe, el ejército chino calificó las operaciones informáticas de "cruciales para lograr la dominación electromagnética" -que sabe Dios qué significa eso-- desde el principio de un conflicto.

Los Estados Unidos también se están armando. Robert Elder, comandante del Comando del Ciberespacio de la Fuerza Aérea, declaró hace poco a periodistas en Washington durante un desayuno que su comando, formado recientemente, encargado de defender la información, las comunicaciones y las redes de control en la esfera militar, está aprendiendo a deshabilitar las redes informáticas del opositor y a hacer colapsar sus bases de datos. \u003c/p\>\n \u003cp\>Según un reporte que figura en el sitio \u003ca href\u003d\"http://military.com\" target\u003d\"_blank\" onclick\u003d\"return top.js.OpenExtLink(window,event,this)\"\>military.com\u003c/a\>, el comandante \n dijo: \u003cstrong\>"Queremos llegar y noquearlos en el primer asalto". \n \u003c/strong\>\u003c/p\>\n \u003cp\>Danny McPherson, experto de Arbor Netwoks, declaró que una guerra \n cibernética sin cuartel "podría tener enormes impactos". Añadió que el \n haqueo (pirateo, violación) de los sistemas de control industrial podría \n ser "una amenaza muy real". \u003c/p\>\n \u003cp\>Según \u003cstrong\>Paul Kurtz, oficial jefe de operaciones de Safe \n Harbor\u003c/strong\>, consultoría de seguridad, los ataques en la propia \n Internet, digamos, por conducto de lo que conocemos como servidores \n raíces, que son importantes para conectar a los usuarios con los sitios \n web, podría provocar problemas generalizados. Y como son tantas naciones \n que tienen el dedo puesto en el botón digital, evidentemente aumenta la \n posibilidad de un conflicto cibernético ocasionado por un atacante \n equivocadamente identificado, o por un simple problema técnico. \u003c/p\>\n \u003cp\>Así y todo, en lugar de pensar en las repetidas advertencias de la \n industria de un "Pearl Harbor digital" el señor Mcpherson dijo: "Creo que \n la ciberguerra será mucho más sutil," en el sentido de que "algunas partes \n del sistema no funcionarán, o que no podremos confiar en la información \n que tenemos a la vista".\u003c/p\>\n \u003cp\>\u003cstrong\>Independientemente de la forma que adquiera la ciberguerra, la \n mayoría de los expertos han llegado a la conclusión de que lo que sucedió \n en Estonia a principios de este mes no fue un ejemplo de eso. \n\u003c/strong\>\u003c/p\>\n \u003cp\>\u003cstrong\>Los ataques cibernéticos en Estonia al parecer se produjeron \n debido a las tensiones generadas por los planes del país de eliminar los \n monumentos de guerra de la era soviética. Los funcionarios estonios en un \n inicio culparon a Rusia por los ataques al sugerir que sus redes \n informáticas estatales bloquearon los accesos en línea a los bancos y a \n las oficinas

del gobierno.",1]); //-->

Según un reporte que figura en el sitio military.com, el comandante dijo: "Queremos llegar y noquearlos en el primer asalto".

Danny McPherson, experto de Arbor Netwoks, declaró que una guerra cibernética sin cuartel "podría tener enormes impactos". Añadió que el haqueo (pirateo, violación) de los sistemas de control industrial podría ser "una amenaza muy real".

Según Paul Kurtz, oficial jefe de operaciones de Safe Harbor, consultoría de seguridad, los ataques en la propia Internet, digamos, por conducto de lo que conocemos como servidores raíces, que son importantes para conectar a los usuarios con los sitios web, podría provocar problemas generalizados. Y como son tantas naciones que tienen el dedo puesto en el botón digital, evidentemente aumenta la posibilidad de un conflicto cibernético ocasionado por un atacante equivocadamente identificado, o por un simple problema técnico.

Así y todo, en lugar de pensar en las repetidas advertencias de la industria de un "Pearl Harbor digital" el señor Mcpherson dijo: "Creo que la ciberguerra será mucho más sutil," en el sentido de que "algunas partes del sistema no funcionarán, o que no podremos confiar en la información que tenemos a la vista".

Independientemente de la forma que adquiera la ciberguerra, la mayoría de los expertos han llegado a la conclusión de que lo que sucedió en Estonia a principios de este mes no fue un ejemplo de eso.

Los ataques cibernéticos en Estonia al parecer se produjeron debido a las tensiones generadas por los planes del país de eliminar los monumentos de guerra de la era soviética. Los funcionarios estonios en un inicio culparon a Rusia por los ataques al sugerir que sus redes informáticas estatales bloquearon los accesos en línea a los bancos y a las oficinas del gobierno. \u003c/p\>\n \u003cp\>El Kremlin negó las acusaciones, y los funcionarios estonios finalmente \n aceptaron la idea de que quizás dicho ataque fue obra de activistas \n entendidos en la tecnología o "hactivistas", quienes han estado preparando \n ataques similares contra casi todo el mundo desde hace varios años. \u003c/p\>\n \u003cp\>Aun así, muchos en la comunidad de seguridad y los medios noticiosos \n ien un inicio calificaron los ataques digitales contra las redes \n informáticas de Estonia como la llegada de un nuevo capítulo vaticinado \n desde hacía tiempo en la historia de los conflictos, cuando, en realidad, \n las tecnologías y las técnicas utilizadas en los ataques no eran \n desconocidas; ni eran del tipo de cosas que sólo un gobierno poderoso \n tendría en su parafernalia digital. \u003c/p\>\n \u003cp\>El ataque parece haber venido de ejércitos de computadoras "zombie" \n infectadas con software que las hacen presas fáciles para ser manipuladas \n y dirigidas a distancia.\u003cstrong\> Andrew Lewis, director del Programa de \n Política Pública y Tecnológica del Centro para Estudios Estratégicos e \n Internacionales, dijo que estos botnets se utilizan más comúnmente \n para actividades ilícitas, como cometer fraude en línea y enviar spams \n (basura informática o correo chatarra).\u003c/strong\>\u003c/p\>\n

\u003cp\>El método principal de ataque en Estonia, por conducto de lo que se \n conoce como una negación digital de servicio, no inhabilita las \n computadoras desde dentro, sino que sencillamente amontona tantos \n deshechos en la entrada, que los visitantes legítimos, como los clientes \n de bancos, no pueden entrar.\u003c/p\>\n \u003cp\>\u003cstrong\>El señor Lewis enfatizó que no es lo mismo inhabilitar una \n computadora desde dentro, y añadió: "El hecho de que Estonia haya quedado \n paralizada debe servirnos de experiencia para poner los pies sobre la \n tierra".\u003c/strong\>\u003c/p\>\n \u003cp\>Es más, según Ross Stapleton-Gray, asesor de seguridad en Berkely, \n California, el ataque habría acarreado riesgos reales para Rusia, o para \n cualquier nación agresora. "La consecuencia negativa de ser descubierto \n haciendo algo más, muy bien podría ser una escalada militar", añadió.",1]); //-->

El Kremlin negó las acusaciones, y los funcionarios estonios finalmente aceptaron la idea de que quizás dicho ataque fue obra de activistas entendidos en la tecnología o "hactivistas", quienes han estado preparando ataques similares contra casi todo el mundo desde hace varios años.

Aun así, muchos en la comunidad de seguridad y los medios noticiosos ien un inicio calificaron los ataques digitales contra las redes informáticas de Estonia como la llegada de un nuevo capítulo vaticinado desde hacía tiempo en la historia de los conflictos, cuando, en realidad, las tecnologías y las técnicas utilizadas en los ataques no eran desconocidas; ni eran del tipo de cosas que sólo un gobierno poderoso tendría en su parafernalia digital.

El ataque parece haber venido de ejércitos de computadoras "zombie" infectadas con software que las hacen presas fáciles para ser manipuladas y dirigidas a distancia. Andrew Lewis, director del Programa de Política Pública y Tecnológica del Centro para Estudios Estratégicos e Internacionales, dijo que estos botnets se utilizan más comúnmente para actividades ilícitas, como cometer fraude en línea y enviar spams (basura informática o correo chatarra).

El método principal de ataque en Estonia, por conducto de lo que se conoce como una negación digital de servicio, no inhabilita las computadoras desde dentro, sino que sencillamente amontona tantos deshechos en la entrada, que los visitantes legítimos, como los clientes de bancos, no pueden entrar.

El señor Lewis enfatizó que no es lo mismo inhabilitar una computadora desde dentro, y añadió: "El hecho de que Estonia haya quedado paralizada debe servirnos de experiencia para poner los pies sobre la tierra".

Es más, según Ross Stapleton-Gray, asesor de seguridad en Berkely, California, el ataque habría acarreado riesgos reales para Rusia, o para cualquier nación agresora. "La consecuencia negativa de ser descubierto haciendo algo más, muy bien podría ser una escalada militar", añadió. \n \u003cp\>Según el señor Lewis, querer involucrarse en lo equivale a ser un acoso \n de alta tecnología es un riesgo demasiado grande para un gobierno. "Los \n rusos no son tontos", dijo. \u003c/p\>\n \u003cp\>Por su parte Andrew MacPherson, profesor asistente de investigación en \n estudios judiciales en la Universidad de New Hamshire, declaró que, \n incluso si llegara a

desatarse un conflicto por conducto de la Internet y \n los microchips beligerantes cumplieran sus peores cometidos, causarían un \n efecto muy diferente al de una lucha de verdad. \u003cstrong\>"Si uno tiene un \n jarrón de porcelana y lo tira al suelo, es muy difícil volverlo a armar", \n dijo. "Un ataque cibernético es tal vez más bien como una sábana que puede \n romperse en pedazos y luego volver a coserse". \u003c/strong\>\u003c/p\>\n \u003cp\>Es por eso que Kevin Poulsen, escritor de Wired News especializado en \n temas de seguridad, dijo que le resultaba dificil imaginar la amenaza que \n otros sí ven de un ataque desde el exterior con electrones y fotones \n solamente. "¿Acaso desatan sus virus mortales y luego aterrizan en \n nuestras playas y arrasan con nuestro país sin ninguna resistencia porque \n nosotros estamos reiniciando nuestras computadoras?", preguntó.\u003c/p\>\n \u003cp\>En realidad, los Estados Unidos se han preparado para los ataques \n cibernéticos, por ejemplo, mediante nuestra exposición diaria a fallas, \n problemas técnicos, distintos tipos de virus y saturaciones. Hay muy pocos \n lugares en que una computadora es tan fundamental que todo se viene abajo \n si la máquina se descompone. \u003c/p\>\n \u003cp\>Los ingenieros espaciales rusos se esforzaron por arreglar las \n computadoras que se descomponían a bordo de la Estación Espacial \n Internacional que ayudan a mantener al laboratorio orbital correctamente \n orientado en el espacio; y si no las hubiesen logrado reparar, la estación \n habría tenido que ser abandonada, al menos temporalmente. \u003c/p\>\n ",1]); //-->

Según el señor Lewis, querer involucrarse en lo equivale a ser un acoso de alta tecnología es un riesgo demasiado grande para un gobierno. "Los rusos no son tontos", dijo.

Por su parte Andrew MacPherson, profesor asistente de investigación en estudios judiciales en la Universidad de New Hamshire, declaró que, incluso si llegara a desatarse un conflicto por conducto de la Internet y los microchips beligerantes cumplieran sus peores cometidos, causarían un efecto muy diferente al de una lucha de verdad. "Si uno tiene un jarrón de porcelana y lo tira al suelo, es muy difícil volverlo a armar", dijo. "Un ataque cibernético es tal vez más bien como una sábana que puede romperse en pedazos y luego volver a coserse".

Es por eso que Kevin Poulsen, escritor de Wired News especializado en temas de seguridad, dijo que le resultaba dificil imaginar la amenaza que otros sí ven de un ataque desde el exterior con electrones y fotones solamente. "¿Acaso desatan sus virus mortales y luego aterrizan en nuestras playas y arrasan con nuestro país sin ninguna resistencia porque nosotros estamos reiniciando nuestras computadoras?", preguntó.

En realidad, los Estados Unidos se han preparado para los ataques cibernéticos, por ejemplo, mediante nuestra exposición diaria a fallas, problemas técnicos, distintos tipos de virus y saturaciones. Hay muy pocos lugares en que una computadora es tan fundamental que todo se viene abajo si la máquina se descompone.

Los ingenieros espaciales rusos se esforzaron por arreglar las computadoras que se descomponían a bordo de la Estación Espacial Internacional que ayudan a mantener al laboratorio orbital correctamente orientado en el espacio; y si no las hubiesen logrado reparar, la estación habría tenido que ser abandonada, al menos temporalmente.

En cambio, aquí en la tierra, este corresponsal se encontraba cerca del \n Centro Espacial Kennedy en una tienda mixta, sin dinero en efectivo y cuya \n red de tarjetas de crédito no estaba funcionado. "No hay conexión con el \n satélite", dijo el dependiente. "Es a causa de la lluvia". Por lo tanto, \n la compra de tasajo y soda tuvo que esperar. En el complejo de visitantes \n del centro, un vendedor tuvo el mismo problema al sacar los comprobantes \n de venta. \u003c/p\>\n \u003cp\>Después de todo, las personas no son computadoras. Cuando algo sale \n mal, no nos venimos abajo; sino que, Por el contrario, buscamos otra \n solución: Improvisamos y arreglamos las cosas. Sacamos los \n comprobantes.\u003cbr\>\u003c/p\>\u003c/span\>\u003c/td\>\u003c/tr\>\u003c/tbody\>\u003c/table\>\u003c/p\>\u003c/font\>\u003c/div\>\u003c/div\>\n",0]); D(["ce"]); //-->

En cambio, aquí en la tierra, este corresponsal se encontraba cerca del Centro Espacial Kennedy en una tienda mixta, sin dinero en efectivo y cuya red de tarjetas de crédito no estaba funcionado. "No hay conexión con el satélite", dijo el dependiente. "Es a causa de la lluvia". Por lo tanto, la compra de tasajo y soda tuvo que esperar. En el complejo de visitantes del centro, un vendedor tuvo el mismo problema al sacar los comprobantes de venta.

Después de todo, las personas no son computadoras. Cuando algo sale mal, no nos venimos abajo; sino que, Por el contrario, buscamos otra solución: Improvisamos y arreglamos las cosas. Sacamos los comprobantes.