Depende: ciberguerra

Thomas Rid

No hay que temer al* hombre del saco *digital. Un conflicto virtual es todavía más palabrería que realidad.

“La ciberguerra ya está aquí”

Ni hablar. “¡Llega la ciberguerra!”, predijeron John Arquilla y David Ronfeldt en un famoso informe Rand en 1993. Desde entonces, parece que ya ha llegado, por lo menos según el aparato militar de Estados Unidos. En enero, el Departamento de Defensa estadounidense se comprometió a equipar a las Fuerzas Armadas para “llevar a cabo una campaña combinada en todos los terrenos, tierra, aire, mar, espacio y ciberespacio”. Mientras tanto, cada vez más libros y artículos exploran las amenazas de la ciberguerra y el ciberterrorismo y cómo sobrevivir a ellas.

Pero seamos serios: la ciberguerra todavía es más palabrería que realidad. Pensemos en la definición de lo que es un acto de guerra: tiene que ser posiblemente violento, tener un propósito claro y ser político. Los ataques cibernéticos que hemos visto hasta ahora, desde los de Estonia hasta el virus Stuxnet, no cumplen esos criterios.

Un ejemplo es el dudoso caso de la explosión de un gaseoducto soviético en 1982, que los verdaderos creyentes en la ciberguerra mencionan con frecuencia y consideran el ciberataque más destructivo de la historia. Según cuentan, en junio de 1982, un gaseoducto en Siberia que la CIA tenía prácticamente lleno de trampas explosivas, con un dispositivo denominado “bomba lógica”, explotó en una tremenda bola de fuego que pudo verse desde el espacio. La Fuerza Aérea estadounidense calculó que había sido una explosión de 3 kilotones, equivalente a una pequeña bomba nuclear. La operación, dirigida contra un gaseoducto soviético que unía los yacimientos de gas de Siberia con los mercados europeos, saboteó los sistemas de control de la línea gracias a un programa creado por una empresa canadiense y en el que la CIA había

incluido un código malicioso. No murió nadie, según Thomas Reed, asesor del Consejo de Seguridad Nacional estadounidense en aquella época, que reveló el incidente en su libro de 2004 *At the Abyss*; el único daño lo sufrió la economía soviética.

¿Ocurrió de verdad ese incidente? Cuando se publicó el relato de Reed, Vasily Pchelintsev, exjefe del KGB en la región de Tyumen, donde se supone que se produjo la explosión, negó la historia. Tampoco existen informaciones de prensa que confirmaran la explosión en 1982, pese a que, a comienzo de los 80, era frecuente ver noticias de accidentes y explosiones en los oleoductos y gaseoductos de la URSS. Es probable que sucediera algo, pero el libro de Reed es la única mención pública del caso, y su relato solo se apoya en un documento. Las pruebas existentes sobre el suceso son tan endebles que no puede utilizarse como caso demostrado de ciberataque.

La mayoría de los demás casos de guerra cibernética que suelen mencionarse son todavía menos destacados. Por ejemplo, los ataques producidos en Estonia en abril de 2007, como respuesta al polémico traslado de un monumento soviético a la guerra, el *Soldado de bronce*. Estonia, muy bien interconectada, fue objeto de un ataque masivo de denegación de servicio procedente de hasta 85.000 ordenadores pirateados y que duró tres semanas. El punto culminante se alcanzó el 9 de mayo, cuando atacaron 58 páginas web estonias al mismo tiempo y se cayeron los servicios del mayor banco del país. “¿Qué diferencia hay entre el bloqueo de puertos y aeropuertos de unos Estados soberanos y el bloqueo de páginas web de instituciones oficiales y periódicos?”, preguntó el primer ministro, Andrus Ansip.

Pese a sus analogías, el ataque no fue un acto de guerra. Fue, sin duda, una molestia y un golpe emocional al país, pero ni siquiera penetraron de verdad en la red del banco; solo estuvo caída durante 90 minutos un día y dos horas el siguiente. El ataque no fue violento ni pretendía alterar la forma de comportarse de Estonia, y no lo reivindicó ninguna entidad política. Lo mismo ocurre con la enorme mayoría de los ciberataques que se conocen.

No se sabe de ningún ataque cibernético que haya causado la pérdida de vidas humanas. Ningún delito informático ha herido jamás a una persona ni ha provocado daños en un edificio. Y, si un acto no tiene al menos la posibilidad de ser violento, no es un acto de guerra. Separar la guerra de la violencia física la convierte en un concepto metafórico; significaría que no hay manera de distinguir, por ejemplo, entre la Segunda Guerra Mundial y las *guerras* contra la obesidad y el cáncer. Sin embargo, estos últimos son males que, a diferencia de los ejemplos de *guerra* cibernética, sí matan a las personas.

“Los ciberataques son cada vez más fáciles”

Todo lo contrario. El director de los Servicios de Inteligencia de Estados Unidos, James R. Clapper, advirtió el año pasado que el volumen de *software* malicioso en las redes estadounidenses se había multiplicado por más de 3 desde 2009, y que todos los días se descubren más de 60.000 muestras de programas maliciosos. EE UU, dijo, está experimentando “un fenómeno conocido como ‘convergencia’, que aumenta la posibilidad de ciberataques, incluso contra infraestructuras físicas”. (La “convergencia digital” es un término muy elegante para designar algo muy sencillo: cada vez hay más dispositivos capaces de comunicarse entre sí, y sectores y actividades que antes estaban separados pueden trabajar cada vez más juntos).

Sin embargo, el que haya más programas maliciosos no significa que los ataques sean más fáciles. De hecho, debería ser más difícil realizar ataques con capacidad de ser perjudiciales o verdaderamente peligrosos. ¿Por qué? Los sistemas más delicados suelen tener incorporados sistemas de redundancia y seguridad, de modo que el objetivo más probable de un atacante no será cerrar el sistema, porque el mero hecho de obligar a cerrar un sistema de control, por ejemplo una central eléctrica, puede desencadenar un atasco y que los operadores empiecen a buscar el problema. Para ser un arma eficaz, los programas maliciosos deben poder influir en un proceso activo, pero no interrumpirlo por completo. Si la actividad maliciosa se prolonga demasiado, tiene que ser sigilosa. Y eso es más difícil que apretar el botón de apagado virtual.

Por ejemplo, Stuxnet, el gusano que saboteó el programa nuclear de Irán en 2010. No se limitó a cerrar las centrifugadoras de la planta nuclear de Natanz; lo que hizo fue manipular sutilmente el sistema. Stuxnet se infiltró en las redes de la central y luego saltó a los sistemas de control protegidos, interceptó los valores que transmitían los sensores, grabó esos datos y dio al código legítimo de control unas señales falsas grabadas con anterioridad, según los investigadores que han estudiado el caso. Su objetivo no era solo engañar a los operadores en una sala de control, sino sortear la seguridad digital y vigilar los sistemas para poder manipular de forma secreta los procesos.

Para construir y desplegar Stuxnet fue necesario conocer con gran detalle los sistemas que debía intervenir, y lo mismo ocurrirá con otros armas cibernéticas verdaderamente peligrosas. Es cierto que la “convergencia”, la normalización y la defensa chapucera de los sistemas de control *podrían* aumentar el riesgo de ataques en general, pero también han hecho que las defensas de los objetivos más codiciados estén mejorando sin cesar y que la reprogramación de instalaciones muy específicas con sistemas antiguos sea cada vez más compleja.

“Las armas cibernéticas pueden causar inmensos daños colaterales”

No parece probable. Cuando se conocieron las noticias sobre Stuxnet, *The New York Times* dijo que lo más impresionante de la nueva arma era el “daño colateral” que causaba. El programa malicioso había “salpicado miles de sistemas informáticos en todo el mundo, y muchos de sus efectos los sufrieron esos sistemas, en vez de lo que se suponía que era su objetivo, los equipamientos iraníes”, **explicó***The New York Times*. Estas palabras reafirman la opinión de que los virus informáticos son como virus biológicos muy contagiosos que, una vez salidos del laboratorio, se vuelven en contra de todos los sistemas vulnerables, no solo sus supuestos blancos.

Pero esta metáfora tiene muchos fallos. A medida que crece la capacidad destructora de un arma cibernética, disminuye la probabilidad de que pueda dañar un gran número de sistemas a distancia. Stuxnet infectó más de 100.000 ordenadores, sobre todo en Irán, Indonesia e India, aunque también en Europa y Estados Unidos. Pero estaba programado con una meta tan concreta que no causó ningún daño en todas esas máquinas, sino solo en las centrifugadoras iraníes de Natanz. La agresiva estrategia de infección del gusano pretendía aumentar al máximo sus probabilidades de alcanzar el objetivo propuesto. Como dicho objetivo no estaba

en Red, “toda la funcionalidad necesaria para sabotear un sistema estaba directamente incrustada en el ejecutable de Stuxnet”, observó Symantec, la empresa de *software* de seguridad, al analizar el código del gusano. Es decir, Stuxnet sí *salpicó* muchos sistemas, pero no soltó su carga dañina más que en el sitio para el que estaba destinada.

La infección colateral, en resumen, no tiene por qué ser un daño colateral. Un programa malicioso complejo puede infectar numerosos sistemas, pero, si existe un objetivo concreto, lo más probable es que la infección tenga una carga específica que será inocua para la mayoría de los ordenadores. La imagen de los daños colaterales involuntarios, sobre todo en el contexto de las armas cibernéticas más sofisticadas, no se sostiene. Es más como un virus de la gripe que solo afecta a una familia.

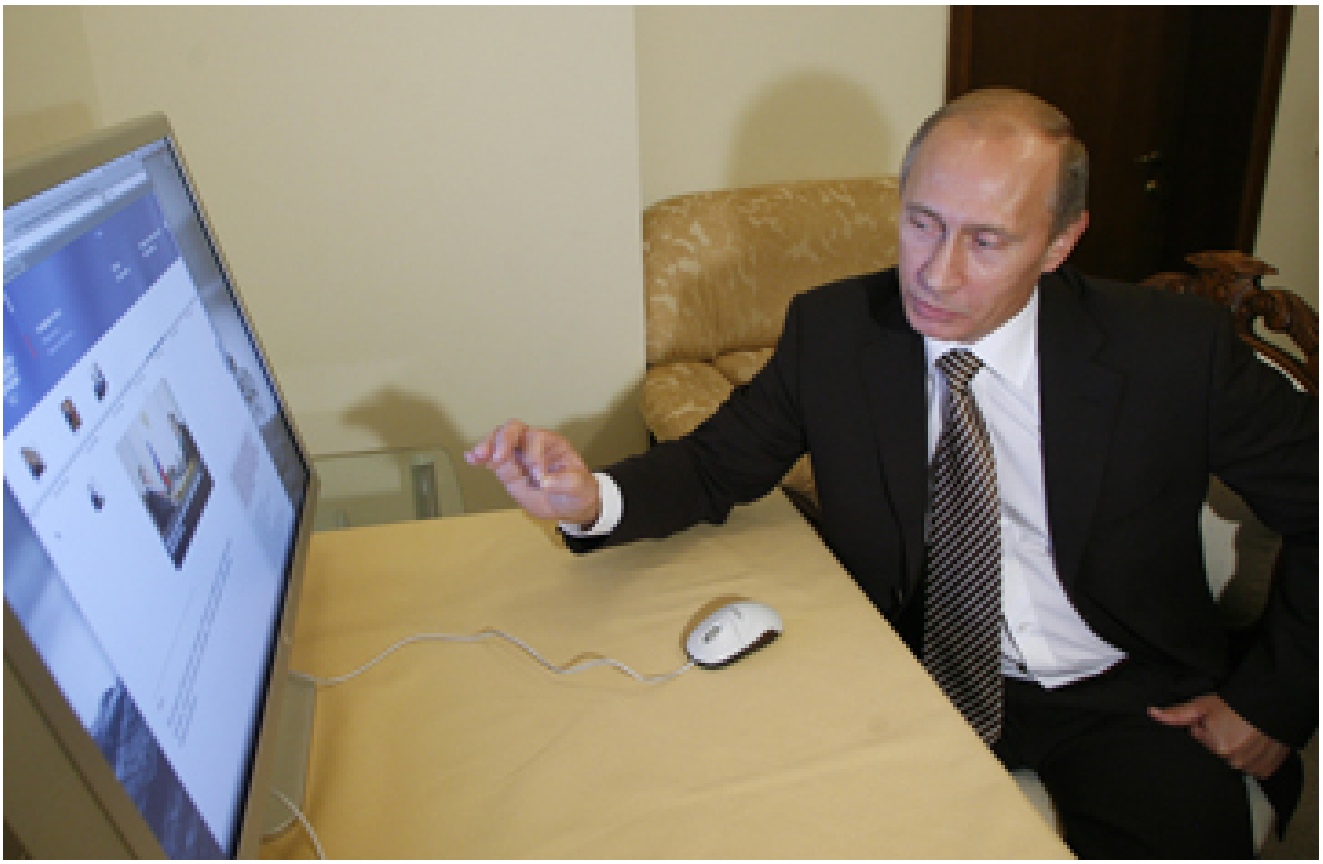
“En el ciberespacio, el ataque domina a la defensa”

Tampoco esto es cierto. Un informe del Pentágono de 2011 sobre el ciberespacio subrayaba “la ventaja de la que disfruta en la actualidad la política de ataque en la ciberguerra”. Los servicios de inteligencia pusieron énfasis en lo mismo en su informe anual de amenazas presentado al Congreso estadounidense el año pasado, en el que decían que las tácticas de ataque –conocidas como descubrimiento y explotación de las vulnerabilidades– están evolucionando a gran velocidad y el Gobierno de EE UU y la industria no son capaces de adaptar sus mejores instrumentos de defensa con la rapidez suficiente. La conclusión parecía clara: los atacantes informáticos tienen ventaja sobre los defensores, “y la tendencia, seguramente, se acentuará durante los próximos cinco años”.

Sin embargo, si se examina la situación con más detalle, salen a la luz tres factores que suponen una desventaja para el ataque. El primero es el elevado coste de desarrollar un ciberarma, en tiempo, talento e información sobre los objetivos. Los expertos calculan que, para desarrollar Stuxnet fueron necesarios un equipo soberbio y mucho tiempo. En segundo lugar, las posibilidades de construir armas de ataque genéricas son menores de lo que se supone por los mismos motivos, y las inversiones importantes en programas de ataque muy específicos solo se pueden hacer contra unos objetivos muy limitados. Tercero, lo más probable es que una herramienta de ataque, una vez desarrollada, tenga una vida media mucho más corta que las medidas defensivas instaladas contra ella. Peor aún, un arma puede ser capaz de golpear una sola vez; cuando se descubre lo que hace un programa malicioso especializado, lo normal es que de inmediato se reparen y protejan los sistemas más delicados. Y un arma, por poderosa que sea, no es gran cosa si no puede repetir el ataque. Cualquier amenaza política depende de la amenaza creíble de que se puede atacar o repetir un ataque. Si se duda de eso, el poder de

coacción del ciberataque se vería drásticamente reducido.

“Necesitamos un acuerdo de control de armas cibernéticas”



No. Los alarmistas de la ciberguerra quieren que Estados Unidos se plantee la seguridad informática como un nuevo reto geopolítico. Creen que el ciberespacio está empezando a ser un nuevo ámbito de rivalidad militar con adversarios como Rusia y China, y que son necesarios nuevos acuerdos de limitación de armas cibernéticas que lo eviten. Se oye hablar sobre la instauración de normas internacionales al respecto: el Gobierno británico convocó una reunión en Londres, a finales de 2011, que pretendía hacer de Internet un lugar más seguro mediante la aprobación de nuevas normas de circulación, y Moscú y Pekín propusieron en la Asamblea General de la ONU del pasado septiembre el establecimiento de un “código de conducta internacional en materia de seguridad informática”. Ahora, los diplomáticos están debatiendo si Naciones Unidas debería intentar elaborar el equivalente a control de las armas nucleares en el ciberespacio.¿Debería? La respuesta es no. Los intentos de limitar las armas cibernéticas mediante acuerdos internacionales tienen tres principales inconvenientes. El primer es la dificultad de trazar el límite entre el delito informático y la posible actividad política en el ciberespacio. Por ejemplo, en enero, un *pirata* saudí robó alrededor de 20.000 números de

tarjetas de crédito israelíes de una página de venta por Internet y filtró los datos al público. En represalia, un grupo de *piratas* israelíes entró en páginas saudíes y amenazó con hacer públicos datos privados de las tarjetas de crédito.¿Dónde está la línea divisoria? Aunque fuera posible distinguir la actividad delictiva de la actividad política y patrocinada por un Estado, muchas veces utilizan los mismos medios. Y existe otro problema de tipo práctico: la comprobación sería imposible. Contar con exactitud la dimensión de los arsenales nucleares y vigilar los programas de enriquecimiento de uranio ya son actividades muy difíciles; instalar cámaras para captar a programadores y *comprobar* que no están diseñando programas maliciosos es totalmente iluso.El tercer problema es político y todavía más fundamental: los agresores cibernéticos pueden actuar por motivos políticos, pero, al contrario de lo que ocurre con la guerra, suelen estar muy interesados en *evitar* la reivindicación. Los actos subversivos siempre han prosperado en el ciberespacio porque conservar el anonimato es más fácil que atribuir un acto de forma inequívoca. Ese es el origen del problema político: creer que unos cuantos Estados van a ponerse de acuerdo en limitar las armas cibernéticas es tan realista como pensar en un tratado que prohíba el espionaje y tan práctico como declarar ilegal la subversión general del orden establecido.

“Occidente está quedándose atrás respecto a Rusia y China”Sí, pero no en el sentido que piensan. Rusia y China dedican grandes esfuerzos a afilar sus armas cibernéticas y ya están muy acostumbradas a utilizarlas. El Ejército ruso actuó de forma clandestina para dañar la economía estonia en 2007 y el Gobierno y los bancos de Georgia en 2008. Los numerosos *ciberguerreros* del Ejército Popular de Liberación chino llevan mucho tiempo insertando *bombas lógicas* y *trampas* en infraestructuras fundamentales de Estados Unidos, unos dispositivos que duermen hasta que llegue el momento de hacer estragos en la Red y el bolsillo del país, en caso de crisis. China y Rusia tienen acceso a la tecnología, el dinero y el talento necesarios, y tienen más margen para llevar a cabo maniobras maliciosas que los Estados democráticos de derecho de Occidente, que tienen que librar la ciberguerra con una mano atada a la espalda.Eso es lo que nos dicen los alarmistas. La realidad es muy distinta. Stuxnet, el ciberataque más sofisticado, con gran diferencia, que se conoce, fue probablemente una operación de Estados Unidos e Israel. Es verdad que Rusia y China han mostrado grandes aptitudes para el espionaje informático, pero estoy prácticamente seguro de que ni la ferocidad de los *ciberguerreros* orientales ni su armamento codificado son tan terribles como se dice. A la hora de realizar ataques ofensivos de tipo militar, Estados Unidos e Israel parecen llevar una enorme ventaja.Lo irónico es que quizá Moscú y Pekín estén más preocupados por otro tipo distinto de ciberseguridad. ¿Por qué esos países han sugerido que Naciones Unidas establezca un “código internacional de conducta” para la seguridad informática? En la redacción del convenio se ignoró con gran elegancia el ciberespionaje, cosa lógica porque las irrupciones virtuales en el Pentágono y Google siguen siendo dos de los pasatiempos oficiales y

corporativos favoritos de ambos países. En cambio, lo que para las democracias occidentales es libertad de expresión en el ciberespacio, protegida en las constituciones, para Moscú y Pekín es una nueva amenaza a su capacidad de controlar a los ciudadanos. La seguridad informática tiene un sentido más amplio en los Estados que no son democracias: para ellos, lo peor que puede pasar no es que se vengan abajo unas centrales eléctricas, sino que se venga abajo su poder político.La Primavera Árabe y el impulso que recibió en los medios sociales han suministrado a los dictadores un ejemplo de la necesidad de patrullar el ciberespecio, no solo en busca de códigos subversivos, sino también de ideas subversivas. La caída de Hosni Mubarak en Egipto y Muamar el Gadafi en Libia debió de dar escalofríos a las autoridades de Rusia y China. No es extraño que los dos países pidieran un código de conducta que ayude a combatir las actividades que utilizan las tecnologías de la información –"incluidas las redes" (es decir, las redes sociales)– para minar "la estabilidad política, económica y social".En resumen, Rusia y China van por delante de Estados Unidos, pero sobre todo en la definición de la ciberseguridad como la lucha contra el comportamiento subversivo. Esa es la verdadera ciberguerra que están librando.

Artículos relacionados

- El oscuro arte de la ciberguerra. ***Alastair Gee***
- El ejército 'pirata' de China. ***Mara Hvistendahl***
- El Ejército virtual del Kremlin. ***Evgeny Morozov***
- Luchas en la Red: Putin ataca Estonia.
- El comienzo de las *ciberguerras.*

Fecha de creación
6 marzo, 2012