>> Jorge Dávila

Ciberdefensa, violencia y civilización

Un aderezo habitual de los medios de comunicación generalistas son los incidentes informáticos, los hackers, los grandes golpes que alimentan el morbo de muchos, pero lo que se está fraguando (intencionadamente en algunos casos) es una sensación de "indefensión digital" que algunos aprovechan para invocar la autodefensa activa y la legalización de un mercado de capacidades ofensivas civiles. Algunos quieren llevar la violencia legal a Internet y eso es algo que requiere más de una reflexión.

La violencia, un concepto complejo

"Es el uso de la fuerza para conseguir un fin, especialmente para dominar a alguien o imponer algo. Es el tipo de interacción entre sujetos que se manifiesta en aquellas conductas o situaciones que, de forma deliberada, aprendida o imitada, provocan o amenazan con hacer daño o sometimiento grave a un individuo o a una colectividad; o los afectan de tal manera que limitan sus potencialidades presentes o las futuras. Puede producirse a través de acciones y lenguajes, pero también de silencios e inacciones" [1].

Se trata de la **violencia**; un concepto complejo que algunas veces va acompañado de matizaciones interesadas dependiendo del punto de vista desde el que se considere. La violencia está asociada a la idea de la fuerza física y el poder. El latín llama **vis** [2], **vires** [3] a esa fuerza que hace que la voluntad de uno se imponga sobre la de otro. En el Código de Justiniano se habla incluso de una *"fuerza mayor, que no se puede resistir"* (*vis magna cui resisti non potest*). Esa raíz latina dio lugar al adjetivo ***violentus*** del que viene ***violare*** en el sentido de agredir con violencia, maltratar, arruinar, dañar.

Al tratarse de un concepto tan antiguo como el propio lenguaje, no es de extrañar que esté permeando en la nueva realidad del siglo XXI que llamamos ciberespacio [4]. Desde la toma de consciencia de los riesgos que corremos al utilizar (a ciegas) Internet, desde la asunción del término ciberdefensa o ciberguerra en el manualillo de tertulianos y comentaristas de todo tipo, la violencia ha entrado en esa dimensión no física que llamamos Internet.

De hecho, habría que remontarse al final del siglo pasado para encontrar los que, posiblemente, eran los primeros actos de violencia cibernética. Me refiero a la aparición de los hoy denominados ataques distribuidos de denegación de servicio [5] (DDoS)

Los primeros ejemplos de ataques en la red fueron los implementados por la **red Strano** [6], un colectivo italiano que protestó en 1995 contra la arrogante política nuclear del gobierno francés. En ese caso los ataques eran complicados procesos manuales que requerían una atención constante y no podían durar mucho porque la conexión telefónica a la red era cara.

El siguiente hito fue orquestado por el grupo **Electronic Disturbance Theater** [7] (EDT) que a finales de los años noventa consiguió la atención de los medios mediante ataques DDoS. En esa ocasión, los ataques se presentaron como una forma de *"protesta virtual"* y en ellas se utilizaron herramientas desarrolladas exprofeso por ellos mismos, lo que permitía a cualquiera unirse a la manifestación. La herramienta utilizada se llamaba **FloodNet** [8] y dirigía el tráfico de los usuarios hacia un blanco predeterminado por el EDT y que en

En la guerra del Ciberespacio no se puede atribuir de forma cierta la autoría de los hechos en general y de los ataques en particular y, por tanto, no se puede identificar un culpable o culpables a los que legítimamente sancionar. Cualquier reacción, incluso las de autodefensa, podrían ser ataques injustificados a otras entidades del todo inocentes que justificarían subsecuentes reacciones en cadena.

[1] Ver https://es.wikipedia.org/wiki/Violencia

[2] El vocablo latino *vis* proviene de la raíz prehistórica indoeuropea *wei-*, que se refiere a la "fuerza vital".

[3] *Vis* (fuerza) femenino. Nominativo *vis*, *vires*; Vocativo *vis*, *vires*; Acusativo *vim*, *vires*; Genitivo -, *virium*; Dativo -, *viribus*; y Ablativo *vi*, *viribus*.

[4] Ver https://en.wikipedia.org/wiki/Cyberspace

[5] Ver https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack

[6] Ver https://es.wikipedia.org/wiki/Hacktivismo#Notables eventos de hacktivistmo

[7] Ver https://en.wikipedia.org/wiki/Electronic_Disturbance_Theater

[8] Ver https://en.wikipedia.org/wiki/Electronic_Disturbance_Theater#floodnet

su momento fueron sitios web de políticos mejicanos y de la Casa Blanca en Washington.

Posteriormente, el colectivo de *hackers* **Anonymous**[9] maduró esta forma de activismo y popularizó el uso de "*botnets*[10] *voluntarios*". En este caso la herramienta utilizada era el **Low Orbit Ion Cannon**[11] (LOIC), mediante el cual los participantes conectaban sus ordenadores a una red y donaban sus recursos computacionales y de red al ataque.

Por su desarrollo, un ataque DDoS debería verse como una forma de protesta y ser reconocido como discurso político, que habría de estar protegido del mismo modo que lo está la libertad de expresión. Este fue el argumento principal esgrimido por la defensa en el proceso a **los 14 de Paypal**[12]; un grupo de simpatizantes de WikiLeaks[13] involucrados en ataques a sitios de comercio electrónico en diciembre de 2010.

Sin embargo, lo que se aplicó en ese caso fue el **Computer Fraud and Abuse Act**[14] aprobado por el congreso de los EEUU en 1986 como enmienda a la ley de fraudes electrónicos contenida dentro del **Comprehensive Crime Control Act**[15] de 1984. Al final, diez de los acusados se declararon culpables de dañar un ordenador protegido y del delito de conspiración, otras tres personas se declararon culpables de un delito menor[16] y todo quedó en el pago de una multa.

En este ejemplo, tanto los atacantes a PayPal como el propio PayPal utilizaron lo que ahora muchos consideran **ciberviolencia** con fines políticos. En origen de ese caso estuvo en el cierre, por parte de PayPal, de las cuentas de donativos a favor de Wikileaks con el fin de ahogar económicamente a esa organización y castigarla por su filtrado de las imágenes de la matanza en Bagdad[17] el 12 de julio de 2007 por parte de dos helicópteros Apache del ejército norteamericano.

La situación se complica cuando algunos presionan para que aparezca el vocablo **ciberterrorismo**[18] en los medios de difusión de masas. Los apóstoles del término lo definen como el uso de medios y tecnologías de comunicación e informáticas con el propósito de generar miedo o terror en la población, en la clase dirigente o en el gobierno, causando con ello una violación de la libre voluntad de las personas. Dentro de él se consideran los actos deliberados de disrupción en redes telemáticas y en ordenadores personales conectados a Internet, mediante herramientas como son los virus y el *malware* en general.

Eugene Kaspersky, cuya empresa de antivirus dio a conocer, junto con el Laboratorio de Criptografía de la Universidad de Budapest, la existencia del virus **Flame**[19], dijo[20] que no era simplemente un virus más, sino que era "*tan sofisticado que representa un nuevo nivel de ciberamenaza, uno que podría ser el principio del fin del mundo [interconectado] tal y como lo conocemos*".

Para Kaspersky, el término **ciberguerra**[21] tiene sentido cuando dos enemigos conocidos y de fuerzas similares se enfrentan en el Ciberespacio, pero el caso de Flamey otras ciberarmas, ésta no es posible porque "*en los ataques actuales, estas sin pruebas sobre quién lo hizo o cuándo lo volverá a hacer de nuevo. No es una ciberguerra, sino ciberterrorismo.*"

Lo que descarta la guerra del Ciberespacio es que no se puede atribuir de forma cierta la autoría de los hechos en general y de los ataques en particular y, por tanto, no se puede identificar un culpable o culpables a los que legíti-

La imposibilidad de atribución puede servir como elemento de disuasión para todos aquellos que hoy claman venganza pero no querrían enfrentarse a una hecatombe en la que todos atacan a todos y, encima, "en legítima defensa". Las consecuencias económicas y sociales de tales comportamientos podrían ir mucho más allá de lo que la población usuaria del Ciberespacio podría estar dispuesta a tolerar.

Al igual que La 9ª Columna de Anonymous no es quién para ir de justiciera por Internet, tampoco lo son cualesquiera empresas que estén acariciando codiciosamente el sueño del mercenariado digital.

[9] Ver https://en.wikipedia.org/wiki/Anonymous_(group)
[10] Ver https://en.wikipedia.org/wiki/Botnet
[11] Ver https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon
[12] Ver https://en.wikipedia.org/wiki/PayPal_14
[13] Ver https://en.wikipedia.org/wiki/WikiLeaks
[14] Ver https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act
[15] Ver https://en.wikipedia.org/wiki/Comprehensive_Crime_Control_Act_of_1984
[16] Ver http://www.cnet.com/news/anonymous-hackers-plead-guilty-to-2010-paypal-cyberattack/
[17] Ver https://en.wikipedia.org/wiki/July_12,_2007_Baghdad_airstrike
[18] Ver https://en.wikipedia.org/wiki/Cyberterrorism
[19] Ver https://en.wikipedia.org/wiki/Flame_(malware)
[20] Ver http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/
[21] Ver https://en.wikipedia.org/wiki/Cyberwarfare

mamente sancionar. Cualquier reacción, incluso las de autodefensa, podrían ser ataques injustificados a otras entidades del todo inocentes que justificarían subsecuentes reacciones en cadena.

Esta imposibilidad de atribución puede servir como elemento de disuasión para todos aquellos que hoy claman venganza pero no querrían enfrentarse a una hecatombe en la que todos atacan a todos y, encima, "*en legítima defensa*". Las consecuencias económicas y sociales de tales comportamientos podrían ir mucho más allá de lo que la población usuaria del Ciberespacio podría estar dispuesta a tolerar.

RootedCON, los 'francotiradores' y la autodefensa

En la conferencia **RootedCON**[22] de este año se celebró una mesa redonda en la que se planteaba la conveniencia de desarrollar "*capacidades ofensivas en el mundo civil*", e incluso se llegó a preguntar sobre de dónde saldrían y quién entrenaría los "*ciber francotiradores*" que deberían responder a los ataques. El tema es importante y conviene cogerlo con perspectiva.

En 1754 **Jean-Jaques Rousseau**[23] publicó "*El Contrato Social o los Principios del Derecho Político*"[24] y con ello inspiró reformas políticas y revoluciones en toda Europa y especialmente en Francia. Ese ensayo va contra la idea de que los monarcas sean los elegidos por dios para escribir las leyes. Rousseau fue el primero en entregar al pueblo toda la soberanía y todo el derecho para escribir las leyes.

El **Contrato Social** es un modelo teórico originado en el periodo de la Ilustración europea, que afronta cuestiones como el origen de la sociedad y la legitimidad de la autoridad del estado sobre los individuos. El argumento principal es que los individuos consienten, de forma explícita o tácitamente, en renunciar a algunas de sus libertades individuales (derechos naturales) para entregárselas a una autoridad o subordinarlas a la decisión de la mayoría, a cambio de la automática protección del resto de sus derechos (derechos legales).

Uno de esos derechos naturales es de la **autodefensa**, y hay que verlo como el derecho que tienen todas las personas para, utilizando una fuerza razonable en cada caso, y siempre en respuesta a un ataque previo, defender sus vidas y las de otros, incluyendo en algunos casos el uso de fuerzas letales que puedan causar una gran lesión o la muerte al atacante.

Las teorías más antiguas no distinguían entre la defensa de la persona y la defensa de la propiedad, y que se plasma en el concepto romano de "***dominium***". Por este principio, el ataque a los miembros de la familia o a sus propiedades era un ataque personal y directo al "***pater familias***"[25], hombre y único propietario de su hacienda que está autorizado por la ley a disponer libremente de todos sus descendientes, sin atender a su edad. Ese primitivo principio de autodefensa se entendía como "*vim vi repellere licet*" (*es lícito repeler la fuerza con la fuerza*) tal y como aparece en el Digesto de Justiniano[26] publicado en el siglo sexto de nuestra era.

Por otra parte, en el **Leviathan**[27] (1651) Thomas Hobbes[28] propone que la teoría política distinga entre el "estado de la naturaleza" en el que no hay autoridad y los individuos no tienen obligación de obedecer a nadie, pero que podrán ser juzgados según lo indique el derecho natural[29], y el "estado moderno". Hobbes argumenta que aunque algunos puedan ser suficientemente fuertes o más inteligentes que los demás en su estado natural, nadie es suficientemente fuerte como para no temer una muerte violenta, y ello justifica la auto-defensa como la más alta necesidad del ser humano.

En su **Segundo Tratado de Gobierno Civil**[30], John Locke[31] explica por qué un ciudadano debe abandonar su autonomía. En él se describe el "estado natural" como algo más estable que la versión hobbiana de una "*guerra de todos contra todos*", y argumenta que todos los hombres son creados iguales por dios. Desde ese estado original intenta explicar la aparición de la propiedad y la civilización, e indica que sólo son gobiernos legítimos los que cuentan con el consentimiento de los gobernados, y quien dé órdenes sin el consentimiento del pueblo puede ser derrocado.

Lo último que necesitamos los ciudadanos del ciberespacio es una Internet llena de mercenarios, gorilas, guardaespaldas, troles de alquiler, esbirros, secuaces, francotiradores, gánsteres, hampones, perdonavidas, balandrones, gallitos, matasietes, cazarecompensas, salvapatrias, matones, sicarios y tragahombres, por decir unos cuantos.

[22] Ver http://www.rootedcon.es/
[23] Ver https://en.wikipedia.org/wiki/Jean-Jacques_Rousseau
[24] Jean-Jacques Rousseau: "*Du contrat social ou Principes du droit politique*", 1762.
[25] Ver https://en.wikipedia.org/wiki/Pater_familias
[26] Ver https://es.wikipedia.org/wiki/Digesto
[27] Ver https://en.wikipedia.org/wiki/Leviathan_(book)
[28] Ver https://en.wikipedia.org/wiki/Thomas_Hobbes
[29] Ver https://en.wikipedia.org/wiki/Natural_law
[30] Ver https://en.wikipedia.org/wiki/Two_Treatises_of_Government
[31] Ver https://en.wikipedia.org/wiki/John_Locke

Un ciberespacio llamado a ser civilizado

No hay ninguna razón por la que el advenimiento del ciberespacio deba cambiar los logros que se han conseguido después de tantos años y generaciones de gente, al menos tan lista como nosotros. Si el ciberespacio está llamado a ser civilizado, los cibernautas deberán depositar en las mismas fuerzas que otorgan el mundo físico, los encargos de defender sus derechos. El carácter civilizado elimina la posibilidad de que el individuo civil o cualquier reunión de éstos puedan ejercer y ejerzan capacidades ofensivas de ningún tipo. Para eso están las fuerzas de seguridad de los diferentes estados.

Al igual que La 9ª Columna de Anonymous no es quién para ir de justiciera por Internet, tampoco lo son cualesquiera empresas que estén acariciando codiciosamente el sueño del mercenariado digital. Sólo tenemos que echar un vistazo a la denominada Guerra de Irak[32] para ver qué se consigue privatizando la guerra. Además de multitud de muertos y miles de delitos de guerra, la administración Bush trajo el mayor despilfarro posible[33] a la economía de los EE.UU. para favorecer económicamente a compañías de mercenarios como **Blackwater**, después conocida como **Xe Services**, y ahora como **Academi**[34].

No hay duda, lo último que necesitamos los ciudadanos del ciberespacio es una Internet llena de mercenarios, gorilas, guardaespaldas, troles de alquiler, esbirros, secuaces, francotiradores, gánsteres, hampones, perdonavidas, balandrones, gallitos, matasietes, cazarecompensas, salvapatrias, matones, sicarios y tragahombres, por decir unos cuantos; resulta que **las represalias no son posibles en el ciberespacio**. Dado que es muy muy difícil, si no imposible, establecer la autoría de un ataque, lo más probable es que la víctima de cualquier respuesta o represalia sea tan inocente como la víctima anterior que se auto defiende.

Hay algo que se denomina **back scattering** en física y explica por qué nos ciega la niebla si encendemos los faros del coche, y también se da en la seguridad de las redes, y es un efecto colateral de cualquier ataque de denegación de servicio mediante *spoofing*[35]. En esos ataques se falsifica la dirección IP del remitente en todos los paquetes que se envían a la víctima. En general, la máquina atacada no puede distinguir los paquetes falsificados de los auténticos, por lo que responde como si todos fuesen auténticos. Estas respuestas llegan a sitios en Internet que nada tienen que ver con el que ha realizado el ataque, por lo que el contrataque termina afectando a terceros que incluso pueden ser realmente las víctimas buscadas como es el caso de los ataques de falsa bandera[36].

La autodefensa en Internet consiste en estar atentos y vigilantes, en minimizar la exposición, anonimizarlo todo, compartimentar, prepararse para reponerse con agilidad y no contar con más derecho que aquel que uno sepa defender de forma eficaz.

Las autoridades que nos defienden en el mundo físico, deben intentar hacerlo también en Internet, pero quizá no puedan llegar al mismo nivel de calidad de servicio que dan en la realidad física; sin embargo, seguro que necesitan de nuestra parte sistemas ciber más robustos.

Guerras sin ganador

No tiene sentido empezar guerras que no se pueden ganar. Las únicas soluciones que hay frente a los ataques en el Ciberespacio son esencialmente defensivas. La calidad del software empleado, la racionalidad de las infraestructuras, de los procesos, de los datos recopilados y procesados son la única vía para construir infraestructuras robustas y seguras. El ciberespacio es un medio nuevo e intangible, en el que no podemos aplicar las mismas recetas que en el mundo físico.

La autodefensa en Internet consiste en estar atentos y vigilantes, en minimizar la exposición, anonimizarlo todo, compartimentar, prepararse para reponerse con agilidad y no contar con más derecho que aquel que uno sepa defender de forma eficaz. Las autoridades que nos defienden en el mundo físico, deben intentar hacerlo también en Internet, pero quizás no puedan llegar al mismo nivel de calidad de servicio que dan en la realidad física; sin embargo, seguro que necesitan de nuestra parte sistemas ciber más robustos. ■

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[32]Ver https://en.wikipedia.org/wiki/2003_invasion_of_Iraq

[33]Jeremy Scahill: "*Blackwater: The Rise of the World's Most Powerful Mercenary Army*" Nation Books. Avalon Publishing Group Inc., 560 páginas, 2007. ISBN-13: 978-1568583945

[34]Ver https://es.wikipedia.org/wiki/Academi

[35]Ver https://en.wikipedia.org/wiki/Spoofing_attack

[36]Ver https://en.wikipedia.org/wiki/False_flag