ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

57/2013 19 junio de 2013

*Ángel Gómez de Ágreda**

CIBERDESPACIO

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

CIBERDESPACIO

Resumen:

El ciberespacio es un entorno dinámico y activo por naturaleza. La protección de los recursos que gestionamos en él debería ser sólo una de nuestras prioridades. Esta defensa no puede ni debe basarse en una actitud pasiva. Es fundamental mantener un equilibrio entre el concepto de "necesidad de conocer", que implica restricciones al acceso a la información, y el de "necesidad de compartir", que permite un mayor aprovechamiento de todas las posibilidades de la red. La seguridad en internet tiene que basarse en una combinación de medidas de protección y en una incesante innovación e influencia sobre el entorno.

Abstract:

Cyberspace is a dynamic environment by its own nature. Protection of the resources that we manage in it should only be one of our priorities. This defense cannot and should not be based on a passive attitude. It is of paramount importance to keep a balance between the "need to know" and "need to share" concepts. The former implies curtailing access to information while the latter allows for a better use of the web's possibilities. Internet security needs to be based in a combination of protective measures and a neverending process of innovation and influence over the environment.

Palabras clave:

Ciberespacio, Ciberdefensa, Internet, Medidas de protección.

Keywords:

Cyberspace, Cyber, Internet, Protection Measures.

*NOTA: Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

No, no se trata de una errata. Desde luego se trata, cuanto menos, de una paradoja. Todo lo "ciber" es incompatible con la lentitud, la parsimonia, la apatía,... He escrito ciber-despacio con la tranquilidad de saber que, en cualquier caso, casi todas las ciber-palabras que utilizamos a diario, no están en el diccionario.

Sin embargo, en algunos momentos parece que estuviéramos viviendo en una versión analógica del siglo XXI. Como queriendo dar la espalda a una realidad que se impone por sí misma y que no nos permite, en realidad, resolver los problemas que nos plantea su versión digital con las unidades ni con los ejes de coordenadas de hace sólo unos años.

Hace unos días escuché una frase que me llamó poderosamente la atención: "Es que el correo electrónico... es tan siglo XX". (Creo que la entonación va implícita.) Pues bien, parece que muchos se empeñan en mantenerse en su esfera de confort, en espacio conocido, en terreno conquistado donde, a pesar de no entender realmente las preguntas que se les hacen, encuentran soluciones con las que se quedan satisfechos.

Lo que viene a continuación es fruto de una reflexión muy personal después de bastantes contactos con personas del sector digital dentro y fuera de España. Supongo que una buena parte de ellas no comparte mis conclusiones.

Volvamos al principio. Le decía que, de todas las palabras con el prefijo "ciber", el español solo admite "ciberespacio". Nuestra lengua, a pesar de la excelente labor que desarrollan desde la Academia y desde otras fundaciones, todavía no recoge la definición de "ciberseguridad" ni de "ciberdefensa". Ni, obviamente, la diferencia entre ambas.

Quizás asuma (como hace el Manual de Tallin respecto de la validez del Derecho Internacional en el ciberespacio[1]) que todas las actividades humanas, una vez "ciberizadas", pueden recibir el tratamiento equivalente al de antes de serlo. De esta manera, la ciberseguridad sería la seguridad del –o en el– ciberespacio y la ciberdefensa, la defensa del – o en el– ciberespacio.

Otra posibilidad es que no existan ni la ciberseguridad, ni la ciberdefensa. O que no exista la diferencia entre ambos conceptos y los académicos –muy precavidos ellos– estén esperando a que los términos estén bien definidos para incorporarlos a los diccionarios físicos y digitales.

---

[1] ***"The Tallinn Manual on the International Law Applicable to Cyber Warfare"*** (http://www.ccdcoe.org/249.html) es una publicación del *NATO Cooperative Cyber Defence Centre of Excellence*, un centro asociado de la OTAN ubicado en Tallin, Estonia, dedicado a la reflexión sobre temas de ciberdefensa. El manual explora la aplicabilidad del Derecho Internacional Público al entorno digital.

Tampoco parece que estén contentos todavía con la diferenciación que hay entre ciber-gamberradas, ciber-activismo, ciber-hacktivismo, ciber-crimen, ciber-terrorismo y ciber-guerra. Ninguna de estas acepciones, con o sin guión, ha encontrado todavía acomodo entre las páginas de nuestros lexicones y tesauros.

Se me ocurre pensar que, lejos de culpar a nuestros académicos de falta de diligencia, quizás no sea tan importante definir cada una de estas categorías. En sesudas reuniones, mesas redondas, foros, seminarios, conferencias y jornadas he tenido ocasión de comprobar el gusto del ser humano por etiquetar absolutamente todo. Podemos no entender algo bien, pero si lo tenemos clasificado, nos resulta menos hostil.

Sin embargo, mientras que en el mundo físico y tangible es importante la diferencia entre determinados comportamientos porque responden a realidades distintas, el *modus operandi* que se sigue en muchas de las actividades enumeradas dos párrafos más arriba es prácticamente el mismo. De hecho, llama la atención cómo la Estrategia de Ciberdefensa (término que no sé si existe en holandés) de los Países Bajos[2] no se pierde en disquisiciones sobre si los atacantes son galgos o podencos. Los holandeses advierten que no van a perder el tiempo en averiguar si el ataque que están recibiendo proviene de actores privados o estatales, si es en el contexto de un conflicto o en las vacaciones de verano. Simplemente, si nos atacas y te pillamos, iremos a por ti.

Podría ser que los neerlandeses sean unos simples, o unos vagos que no quieren tomarse la molestia de discriminar entre un adolescente que les roba los planos de su última fragata para divertirse y una potencia enemiga que les roba los planos de su última fragata para copiársela. Mi impresión es que no son ni simples ni vagos sino que lo importante es si te han robado los planos de una fragata que, además del valor económico que puedan tener, pueden servir para afectar al equilibrio geopolítico, económico e industrial en un modo no deseado.

En este asunto de las clasificaciones me gusta emplear el ejemplo de un hacker saudí que se dedicó a sustraer datos de tarjetas de crédito y a regalarlos a cualquiera que le diera un propósito para el dinero que iba a obtener fraudulentamente. No tenía que ser algo como pagar la operación de una madre enferma o evitar un desahucio de una familia numerosa con todos sus miembros en paro. Si querías comprarte una maqueta de un tren o la última versión de un juego de la PlayStation, podías pedirle un par de números de tarjeta y sus contraseñas para comprártelos on-line[3].

---

[2] La Estrategia de Ciberdefensa de los Países Bajos (disponible on-line en http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf) es un documento derivado de su Estrategia Nacional de Ciberseguridad y de aplicación al ámbito de la Defensa Nacional.

[3] http://www.haaretz.com/news/diplomacy-defense/saudi-hacker-publishes-details-of-another-200-israeli-

Se trata de un caso "de libro" de fraude, por mucho que él apenas se lucrase con las tarjetas sustraídas y que, generosamente, se pudiera decir que se trataba de una gamberrada cibernética.

Sin embargo, este joven saudí sólo robaba tarjetas de crédito de víctimas israelíes. Detrás de la actividad fraudulenta, había también una intencionalidad política. Arabia Saudí e Israel no mantienen unas relaciones como las que puedan tener los Estados Unidos y Canadá, por ejemplo. De hecho, al cabo de un tiempo, hackers israelíes comenzaron a tomarse la revancha con tarjetas de crédito saudíes.

A mí, personalmente, en este caso me cuesta bastante establecer diferencias claras entre las distintas categorías que nos empeñamos en definir. No sabría muy bien definir dónde acaba la gamberrada y empieza la falta, o el delito, o la xenofobia, o el acto terrorista.

Otro caso parecido sería el del hacker que se introdujo en la cuenta de Twitter de la agencia de noticias Asociated Press. El rumor –avalado por el prestigio de AP– de que se habían producido unas explosiones en la Casa Blanca y que el presidente Obama estaba herido hizo que los índices bursátiles de Wall Street perdiesen varios puntos porcentuales de su valor (es decir, muchos millones de dólares) para recuperarse poco después cuando se confirmó la falsedad del tuit.

Doctores tiene la Santa Iglesia y seguro que se puede llegar a definir dónde empieza la gamberrada, dónde la apropiación de identidad, dónde la manipulación de información y, finalmente, hasta qué punto las pérdidas y ganancias bursátiles que se hayan podido obtener, son lícitas o no. Es posible que esta taxonomía sea necesaria a efectos procesales, pero no nos va a ayudar a solucionar el problema de la seguridad.

Curiosamente, este hecho es el resultado de la utilización de algoritmos financieros que se emplean para invertir en bolsa de forma automática. Y, en este caso, se trata de un producto informático perfectamente legal. Estos algoritmos detectan palabras clave en los despachos de las agencias de noticias e intentan anticipar la reacción del mercado en cada caso.

Así pues, me permito dudar de la necesidad de establecer ciber-nombres distintos para actividades cuyos efectos son muy parecidos. En cualquier caso, no creo que debamos hacer de ello una prioridad.

---

credit-cards-1.406853

De hecho, poner muchos nombres tiene un problema muy parecido al de poner muchos CERT[4], puedes dejar huecos entre lo que significan –o protegen– cada uno de ellos.

Uno de los problemas fundamentales que tenemos cuando nos enfrentamos al ciberespacio es que en él (un conocido me lo comentaba hace poco) la física cuántica tiene una aplicación mucho mayor. Especialmente, el principio de incertidumbre. Y tenemos pocos expertos en física cuántica.

Me temo que, por lo que me han explicado, la ciencia informática forense (que existe, y es la que se encarga de determinar, por ejemplo, quién ha causado un efecto, cómo y desde dónde) está todavía en un estado bastante incipiente. Para un hacker avezado resulta relativamente sencillo complicar el trabajo de los investigadores –los e-CSI, por así decir– y esconder sus huellas en las infinitas conexiones de internet. Por el momento estamos condenados a luchar contra esos efectos. Tenemos que actuar sobre lo conocido para protegerlo o para controlarlo.

A pesar de todo, las empresas siguen empeñadas en vender soluciones de seguridad que garantizan nuestra protección.

Hace muchos años me explicaron que la seguridad (tenía que ser la física, porque no existía internet) es siempre cara y nunca es total[5]. A lo máximo que podemos aspirar es a gestionar los riesgos a los que nos enfrentamos de tal manera que el daño que nos inflijan sea el menor posible. En el ámbito cibernético –y, cada vez más, en todos– se emplea el término "resiliencia" (que también me subraya el procesador de textos). En su día lo quise traducir como "resistencia adaptativa". Se trata de resistir las agresiones sin que el sistema llegue a romperse completamente y luego ser capaces de reconstruirlo en el menor tiempo posible y, ya puestos, de un modo más resistente frente a ataques similares al sufrido.

Está claro que una muralla se puede rebasar por encima, por debajo, o a través de ella. El mundo de internet es algo más complejo porque se caracteriza por las conexiones que se establecen. Las rutas que llegan a la muralla son muchas y muy diversas. Uno no puede pretender ser capaz de repeler todas las agresiones. Ni se puede uno anticipar a los ataques; al menos, no fácilmente.

---

[4] *Computer Emergency Response Team.*

[5] El *World Economic Forum*, en publicación *Global Risks 2012. Seventh Edition.* (disponible en internet en: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf) establece como axiomas del ciberespacio que:
- Cualquier dispositivo con un comportamiento definido por software puede ser alterado para que lleve a cabo acciones para las cuales no estaba diseñado.
- Cualquier dispositivo conectado a una red de cualquier tipo, sea como sea esta conexión, puede ser comprometido por un agente externo. (pág. 27).

Cada día se crean más de 70.000 nuevas piezas de *malware* (programas dañinos como virus, gusanos, troyanos,...). Resulta comprensible que incluso el mejor antivirus no haya "oído hablar" de alguna de las amenazas que se encuentra a diario.

Lo que sería lamentable es que permitiésemos que la misma arma pudiese ser empleada varias veces sin que se hubieran puesto los medios para combatirla.

Una adecuada gestión de la información y una capacidad de procesado y distribución ágil deberían permitir minimizar los riesgos derivados de "rebotes ofensivos" (empleando terminología baloncestística) que permiten segundas oportunidades al adversario.

Se puede decir que, para cada ataque, tenemos que diseñar una respuesta personalizada en mayor o menor medida y que, por lo tanto, estamos condenados a ser básicamente reactivos cuando nos colocamos en una actitud pasiva. Claro es que no debemos colocarnos en una actitud pasiva.

En el ciberespacio, la mejor defensa no es un ataque. No se puede detener cualquier agresión con otra. Fundamentalmente porque, según la teoría de la "primera batalla", un ataque lo suficientemente potente puede anular tu capacidad para operar y, por lo tanto, para contraatacar.

Esto no significa que tengamos que permanecer pasivos. Quizás la mejor técnica defensiva que podemos adoptar (sin dejar por ello de reforzar nuestros instrumentos tradicionales) es una actitud activa –que no necesariamente agresiva– en varios frentes. Para ello conviene recordar que los actores que participan en la actividad cibernética somos seres humanos. Las máquinas todavía no han "tomado conciencia" de sí mismas como el *Skynet* de Terminator. Encima de cada ratón y cada teclado hay una mano que lo mueve.

Por lo tanto, podemos volver a los clásicos. Sun-Tzu nos decía que el general que se conoce a sí mismo pero no conoce al adversario (o el que conoce al adversario, pero no se conoce a sí mismo) ganarán unas batallas pero perderán otras. Sólo aquel que se conoce a sí mismo y conoce a su enemigo puede alcanzar siempre la victoria.

En la red podemos aplicar esa misma máxima. Tenemos que conocer a nuestro adversario tomando una postura activa de vigilancia de hechos y –muy importante– de tendencias. Una gran amenaza es como un gran meteorito, si estás mirando en la dirección correcta con los medios adecuados, deberías poder verla venir.

La otra parte es conocerse a sí mismo. Y conocer el propio entorno. En el ciberespacio, hombre y máquina se convierten en un único sistema. Las vulnerabilidades de uno y de otro son igualmente importantes; aunque su protección pueda ser muy distinta. Una vulnerabilidad sin parchear en una máquina es una herida abierta por la que puede infectarse el conjunto.

Desgraciadamente, no existen parches para la estupidez humana[6]. Este axioma ya es un clásico en la comunidad cibernética.

El entorno digital no puede, igual que el físico, llegar a ser absolutamente seguro. Como dicen en las películas: "puedes correr, pero no esconderte". Todo sistema terminará por desvelar sus vulnerabilidades, aunque sólo sea por el hecho de ser artificial y, por lo tanto, sujeto a las imperfecciones de su diseñador.

Por lo tanto, si no cabe esconderse y si la mejor defensa es correr, corramos. Seamos más rápidos, más efectivos, más productivos. El mismo ciberespacio nos proporciona las herramientas para hacerlo. Diseñemos nuestra estrategia desde un punto de vista distinto. No se trata de proteger lo que tenemos porque lo que tenemos es cosa del pasado. No, no vamos a regalarlo, pero vamos a invertir en su protección el esfuerzo que merezca y vamos a no hacer de la seguridad un fin en sí misma, sino el medio que es para llegar a algún sitio, para construir algo.

La globalización y el ciberespacio llevan asociados cambios que parece que no acaban de ser entendidos, ni siquiera por parte de muchos de los que están plenamente implicados en su construcción. No es extraño, el fontanero que contribuye a la construcción de una vivienda no tiene porqué hacerse una idea de su conjunto para hacer su trabajo. Sin embargo, probablemente, su aportación al resultado final podría ser mucho mayor si fuese capaz de ver más allá de grifos y tuberías.

Es muy llamativo, en un campo tan técnico como el de la seguridad informática, comprobar que una parte importante de aquellos que están diseñando las herramientas con las que se construye el siglo XXI siguen viviendo anclados en las estructuras lógicas, psicológicas, sociológicas y organizacionales del XX.

[6] No, me temo que el arrepentimiento puede, a lo sumo, tener aplicación en el campo de la ética. En internet, cada *click* del ratón tiene consecuencias muchas veces indelebles. Sobre Ética y Derecho es interesante el artículo de DUNLAP Jr., Charles, "Cyber Lawfare?", disponible en ISN http://www.isn.ethz.ch/isn/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=163103&tabid=1454266499&contextid774=163103&contextid775=163100

De este modo, muchos pretenden vivir, en un mundo en el que los individuos vienen definidos por las relaciones que mantienen dentro de una estructura reticular muy poco jerarquizada, manteniendo organizaciones piramidales y *stovepipes* (en su equivalente militar, el conducto reglamentario).

Esas mismas personas suelen enfrentarse a la evolución de los acontecimientos con una parsimonia propia de la época victoriana. En el mundo digital no sólo cambian las unidades de medida, sino que, aquellas que siguen existiendo ven alterado su orden de magnitud. Así, claro, no dejan de sorprenderse cuando los acontecimientos les sobrepasan, cuando las innovaciones se producen en saltos revolucionarios más que en rampas evolutivas. Muchas veces, cuando oigo algunos comentarios de esta gente, no puedo menos que recordar el sonido que hacía mi modem telefónico allá en los años 80.

El principal problema del elemento humano en el ciberespacio es que tiene más de dos mil millones de usuarios en todo el mundo... y creciendo. Y todos estamos conectados. No en igualdad de condiciones, claro está, pero conectados. La seguridad de una muralla no se mide por su tramo más alto y robusto, sino por el más bajo y vulnerable. De poco sirve disponer de grandes especialistas si el nivel general de conciencia del riesgo y de las amenazas no responde a unos mínimos. Quizás deberíamos crear una "e-ducación para la e-ciudadanía" que beneficiase al conjunto.

¿Tienen nuestros líderes –aquellos con capacidad de decisión a todos los niveles y en todos los sectores– una formación suficiente como para comprender el alcance del ciberespacio en la sociedad en su conjunto y en el individuo en particular? Me temo que, en el mejor de los casos –y salvo excepciones–, cada cual tiende a ver internet y el ciberespacio en general desde el punto de vista que mejor se acomoda a sus prejuicios y a su formación y experiencia.

Por internet se mueve información, datos. Igual que el mar es el medio más rentable para el transporte de mercancías, el ciberespacio lo es para la difusión de ideas. La diferencia es que yo no puedo comprarme un petrolero, pero sí puedo acceder a las redes sociales y ser un actor relevante en ellas.

El ciberespacio rompe, de alguna manera, el monopolio estatal sobre la violencia. Digo de alguna manera, porque la sociedad –así, en abstracto– sí se va acomodando al significado de la globalización, por mucho que los Estados no lo hagan. Y la sociedad ya ha incorporado formas de violencia asimétrica que generan un impacto mucho más relevante del que corresponde a su potencia.

En el ciberespacio, este acercamiento entre los efectos que puede provocar un individuo y los que puede conseguir un Estado se hace cada vez mayor. La inacción por parte de los colectivos les convierte en rehenes de los individuos con mayor iniciativa. Ese es, en mi opinión, el mayor riesgo que nos acecha en internet: la pérdida de la iniciativa por parte de las instituciones y organizaciones públicas y privadas y un cambio sustancial del modelo de sociedad en el que vivimos (o la sobrerreacción de los Estados, como alternativa).

La Orden Ejecutiva del Presidente Obama parece entender la importancia de compartir la información no como una opción contrapuesta a la de protegerla, sino como la mejor forma de apoyar esta defensa. Estaría bien que esta claridad de ideas no fuera exclusiva del Ejecutivo norteamericano sino que hubiera sido compartida y estado apoyada también por el legislativo. Parece evidente que, para dar pasos en la buena dirección, lo primero es saber hacia dónde se quiere ir.

Estamos viviendo el equivalente a la Línea Maginot tras la guerra de posiciones de la Primera Guerra Mundial casi cien años después de que ésta ocurriese. Los que no entiendan el dinamismo que se requiere en este nuevo escenario, los que pretendan defender lo que tienen parapetándose detrás de alambres de e-spino, los que cedan la iniciativa y sean incapaces de controlar la punta de lanza del conocimiento en lugar de intentar proteger la lanza completa, todos esos acabarán perdidos en el Ciberdespacio.

[i]

*Ángel Gómez de Ágreda**
TCOL.EA.DEM

NOTA: Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.