>> Jorge Dávila

Autodefensa analógica para un destino digital

Hay gente que ve el ciberespacio como una mera traslación de su realidad analógica, y cree que lo que funciona en este universo llamado "realidad", también funciona en el otro universo llamado "virtual". Esa estrategia da ciertos éxitos cuando se aplica a los riesgos (fraude y ciberfraude se parecen muchísimo), pero cuando se aplica a posibles soluciones, los fallos de traslación y la disparidad de resultados abundan. En estos día se habla de cibervoluntariado y ciberreservas construidas sobre el patriotismo ciudadano, pero no está claro que esos modelos de este universo analógico sean realmente solución a los problemas planteados en el otro digital y, sin embargo, bien podrían ser otra cosa.

La autodefensa es el derecho que tienen las personas a utilizar una fuerza razonable con el fin de defender su propia vida o la de otros incluyendo, en ciertas circunstancias, el uso de la fuerza letal. Si un defensor utiliza fuerza defensiva por estar amenazado por un ataque mortal o que le inflija un daño grave a sí mismo o a otra persona, o si tiene una percepción razonable de esa amenaza, en ese caso, el defensor tiene como justificación la autodefensa. Lo que es así para los individuos, también puede elevarse a las sociedades o comunidades de individuos.

En general son tres los grandes modelos para conseguir esa protección defensiva. Por una parte están, por ejemplo, los **Grupos de Autodefensa** o **Guardias Comunitarias** de México, que están compuestos por civiles que toman las armas para defender sus comunidades de los ataques de los cárteles de la droga. Este movimiento aparece en México a principios del 2013 y aún continúa, y su propósito es el de enfrentarse a las bandas de delincuentes que campaban por sus respetos en los estados de Michoacán, Guerrero y Jalisco.

Otro ejemplo de defensa colectiva podría ser el de Rick Grimes [1], personaje ficticio que, al despertar de un estado de coma, encuentra un mundo plagado de zombis y, tras encontrar a su familia, se une a un grupo de supervivientes de los que se hace su jefe. La ficción conocida como "*The Walking Dead*" narra las vivencias de ese grupo y de cómo se enfrenta tanto a los caminantes muertos, como a otros grupos de personas vivas, y lo hace disparando y masacrando a todo lo que no son ellos, a todo lo que es diferente a ellos.

Ejemplos reales de este modelo de gangsterismo [2] los podríamos encontrar, si les dejaran, en los 165 grupos de supremacistas blancos [3] que visten uniformes de combate, portan armas militares y dicen ser "extremadamente patrióticos"; de hecho, ellos se consideran el "ala armada" del movimiento patriótico norteamericano que consta de 623 grupos diferentes.

Por otra parte tenemos la opción de profesionalizar la defensa y contratar a alguien para que se encargue de luchar por nosotros. El ejemplo más reciente y descarado de ese proceder lo podemos encontrar en la denominada **Guerra de Irak** o **Segunda Guerra del Golfo**, que comenzó el 20 de marzo de 2003 y continuó hasta diciembre de 2011. Podemos decir que en este caso se trata del **modelo Bush** [4]**–Cheney** [5]**–Rumsfeld** [6], de una guerra artificial e injustificada en la que los contribuyentes norteamericanos ponían los millones de dólares, la población iraquí los muertos, heridos y torturados, y las compañías privadas paramilitares como **Blackwater Worldwide** [7] se llevaban todos los beneficios; todo ello con la colaboración de un iluminado neoliberal [8] llamado Erik Dean Prince [9] amigo de los Bush. Este modelo consiste en recurrir a **ejércitos de mercenarios** como son los **Gurkhas** británicos o la **Legión Extranjera** [11] francesa, cuyas únicas lealtades son al dinero y a los beneficios personales.

El tercer modelo se conoce como **leva**, y consiste en el reclutamiento forzoso de la población para servir en el ejército si así lo requiere el que

El objetivo último de las Fuerzas de Reserva militar en general es que una nación pueda reducir sus gastos militares permanentes al tiempo que se mantiene una fuerza preparada para la guerra; en pocas palabras, es una solución propia de naciones pobres. Quizás esas propuestas de ciberreservismos sean el reconocimiento de que nuestro país no se piensa gastarse ni un duro en su defensa en el ciberespacio.

[1] https://es.wikipedia.org/wiki/Rick_Grimes
[2] https://en.wikipedia.org/wiki/Gang
[3] http://www.bbc.com/mundo/noticias-internacional-42314419
[4] https://es.wikipedia.org/wiki/George_W._Bush
[5] https://es.wikipedia.org/wiki/Dick_Cheney
[6] https://es.wikipedia.org/wiki/Donald_Rumsfeld
[7] https://es.wikipedia.org/wiki/Academi
[8] Simons, Suzanne: "Master of War: Blackwater USA's Erik Prince and the Business of War". Nueva York: Harper. p. 253 (2009). ISBN 978-0-06-165135-9.
[9] https://es.wikipedia.org/wiki/Erik_Prince
[10] https://es.wikipedia.org/wiki/Gurkha
[11] https://es.wikipedia.org/wiki/Legi%C3%B3n_Extranjera_Francesa
[12] https://es.wikipedia.org/wiki/Alfredo_el_Grande

manda o la **Seguridad Nacional**. Ya el rey inglés **Alfredo el Grande**[12] en el Siglo IX tenía a sus súbditos divididos en dos, una mitad estaba trabajando en el campo y la otra mitad reclutada para servir en el ejército. Con el tiempo, la población rotaba entre las tareas militares y las de ganadero o agricultor. De este modo el Rey Alfredo logró defender las islas británicas de los Vikingos[13].

La leva es el modelo dominante en el sistema feudal, donde los campesinos se utilizaban para cubrir las necesidades de los hombres de armas en funciones secundarias como zapadores, exploradores, herreros, leñadores, etc., pero no como guerreros. Sin embargo, ninguna de esas levas medievales tuvo la magnitud de las que se hicieron durante la **Revolución Francesa**.

Levas en masa

La primera manifestación de levas en masa en la historia de la humanidad, se dio en el periodo de los **Reinos Combatientes** de la historia China. En ese momento, se enfrentaban diferentes escuelas filosóficas y una de ellas, la filosofía legalista, proponía que las leyes fueran reforzadas mediante castigos y recompensas según marcasen esas mismas leyes, estableciendo así una meritocracia. Sin embargo, los legalistas también pensaban que el aspecto más importante del gobierno era hacer fuerte al Estado y por ende la creación de ejércitos fuertes.

El legalista más importante fue **Gongsun Yang**[14], señor de Shang y primer ministro del estado de **Qin**[15] desde 361 a 338 a C. Yan creía que toda la ciudadanía de un estado debía ser dividida entre agricultores y militares y, de ese modo, el estado resultante sería invencible. Su objetivo era el de transformar la nación en un arma y que cada ciudadano pusiera su parte alícuota para apoyar a la milicia. El estado de Qin movilizó todos sus recursos para subyugar a sus vecinos y unificar China, lo cual terminó ocurriendo en el 221 a C. Al empezar las contiendas, su ejército era de casi un millón de soldados sobre de una población de sólo cinco millones de habitantes. Probablemente, este sea el mayor porcentaje de personal alistado en un ejército de toda la historia de la humanidad, y es un magnífico ejemplo del concepto de **leva en masa**.

De los tres modelos, el más civilizado, el menos peligroso para la población civil, es el de las levas utilizadas durante la **Revolución Francesa**. En el modelo de movilización voluntaria o forzosa[16], **la soberanía y el poder no dejan de estar en manos de los ciudadanos**. En los modelos pretorianos de contratar mercenarios o permitir grupúsculos anárquicos de autodefensa, lo que realmente se está haciendo es fomentar un cáncer social que pronto se volverá contra los que lo permitieron y terminarán siendo esclavizados bajo alguna forma de autocracia o plutocracia.

En el escenario Ciber, la potencia no se mide por el número de hombres/combatientes que se tiene, ni siquiera por la potencia energética o las habilidades logísticas de los ejércitos, sino por el talento de sus usualmente pocos integrantes y la muy cuidadosa preparación de las operaciones. El mundo Ciber tiene poco de improvisación, tanto en ataque como en defensa, y por ello el modelo de Fuerzas de Reserva no es aplicable.

La traslación de la mentalidad analógica militar al ciberespacio

La llegada del ciberespacio[17], pronto hizo que se ampliase la cosmogonía militar y se hablase del **Quinto Dominio** como una metáfora en la que volcar años de experiencia militar analógica. De ahí se acuñaron rápidamente términos como **Ciberguerra**, **Ciberoperaciones** (ofensivas), **Ciberdefensa**, **Ciberinteligencia militar**[18], etc. Sin embargo, no está claro que ninguna de ellas sea tan real, prominente y dañina para la sociedad en general como lo es la **Ciberdelincuencia**[19]. Estos términos tan castrenses y que tanto gustan a periodistas sensacionalistas, conferenciantes alarmistas, contertulios populistas y algún que otro diputado[20], realmente no dan cuenta de lo que pasa en una sociedad que se encuentra en medio de la muy cacareada **Transformación Digital**[21].

Lo que afecta a la sociedad real a través del ciberespacio se podría resumir en lo que se denomina **Ciberseguridad**, y que sería el ámbito

Las ciberarmas, al igual que el resto de las armas analógicas, físicas o cinemáticas, las producen y las deben producir empresas especializadas que están y deben estar bajo un férreo control del estado para asegurar la calidad y la misma existencia de esas armas. El control férreo debe impedir que esos artefactos de destrucción no caigan en manos de personal no autorizado, ni se puedan usar de forma ilegal a la luz de los acuerdos internacionales. Para fabricar ciberarmas tampoco sirve el modelo de Fuerzas de Reserva, la creación de armas no es algo puntual, sino una actividad industrial (para algunos) como otra cualquiera.

[13] https://en.wikipedia.org/wiki/Great_Heathen_Army
[14] https://en.wikipedia.org/wiki/Shang_Yang
[15] https://en.wikipedia.org/wiki/Qin_(state)
[16] https://es.wikipedia.org/wiki/Servicio_militar
[17] https://en.wikipedia.org/wiki/Internet_metaphors
[18] http://www.asint360.com/que-es-la-ciberinteligencia-la-inteligencia-en-materia-de-ciberseguridad/
[19] http://www.elmundo.es/economia/2017/01/08/586fc1d222601d6f4b8b4584.html
[20] https://www.eldiario.es/cultura/tecnologia/PP-confundir-mezclando-ciberguerra-desinformacion_0_749626059.html
[21] https://es.wikipedia.org/wiki/Transformación_digital

en el que se reúnen las tecnologías, procesos y controles que son diseñados específicamente para proteger sistemas, redes, datos y procesos vitales de cualesquiera ataques. Una ciberseguridad de éxito **reduciría el riesgo de ciberataques**, no su número pero sí sus efectos finales, y protegería las organizaciones y los individuos de la explotación no autorizada y dañina de sus sistemas, redes, tecnologías y datos.

Siguiendo con la traslación de la mentalidad analógica militar[22] al ciberespacio, desde hace tiempo algunas voces[23] proponen el establecimiento de un sistema de **Ciberreserva Militar**. En ella civiles voluntarios, en momentos de crisis, se pondrían a las órdenes de autoridades militares para contribuir con su talento y saber hacer, a la defensa de la seguridad nacional en el ciberespacio.

En realidad, el objetivo último de las **Fuerzas de Reserva militar** en general es que una nación pueda reducir sus gastos militares permanentes al tiempo que se mantiene una fuerza preparada para la guerra; en pocas palabras, es una solución propia de naciones pobres. Quizás esas propuestas de ciberreservismos sean el reconocimiento de que nuestro país no tiene mucho para gastar en su defensa en el ciberespacio.

Las Fuerzas de Reserva tienen sentido cuando lo que se necesita es poder disponer de ciudadanos/soldados que puedan incorporarse rápidamente a un escenario bélico; cuanto más haya y mejor entrenados estén, mejor papel harán en la contienda. Sin embargo, en el escenario Ciber, la potencia no se mide por el número de hombres/combatientes que se tiene, ni siquiera por la potencia energética o las habilidades logísticas de los ejércitos, sino por el talento de sus usualmente pocos integrantes y la muy cuidadosa preparación de las operaciones. **El mundo Ciber tiene poco de improvisación, tanto en ataque como en defensa**, y por ello el modelo de Fuerzas de Reserva no es aplicable.

La Ciberdefensa debe ser una estrategia plurianual que prepare a todos nuestros sistemas para detectar, resistir, gestionar y recuperarse de los ataques más arriesgados que puedan darse. La ciberseguridad es esencialmente proactiva y no reactiva, por lo que el modelo de entrenamiento periódico y movilizaciones puntuales propio de la Fuerzas de Reserva militar tampoco le va bien a la Ciberdefensa.

Se habla de los muchos puestos de trabajo en ciberseguridad que hay en la parte de la demanda y la absoluta escasez de profesionales para cubrirla. ¿Cuánto dinero han invertido esos demandantes de ciberexpertos para formar a esos futuros trabajadores? ¿Cuántos buenos programas universitarios en Ciberseguridad están financiados por el estado o por las empresas? ¿Qué interés real han puesto las instituciones académicas en atender a esa demanda de una profesión transversal que no encaja con sus reinos de taifas? La respuesta sincera a todas estas preguntas es, insignificante.

Ciberatacar (operaciones ofensivas)

Si hablamos de ciberatacar (operaciones ofensivas), lo que salta a la palestra es el tema de las **ciberarmas**, que es el término correcto para el uso militar del *malware* que es habitual en el mundo de la ciberdelincuencia y el fraude digital. En nuestra sociedad capitalista occidental, las ciberarmas, al igual que el resto de las armas analógicas, físicas o cinemáticas, las producen y las deben producir **empresas especializadas** (**complejo industrial-militar**[24]) que están y deben estar **bajo un férreo control del estado** para asegurar la calidad y la misma existencia de esas armas. El control férreo debe impedir que esos artefactos de destrucción no caigan en manos de personal no autorizado, ni se puedan utilizar de forma ilegal a la luz de los acuerdos internacionales. Para fabricar ciberarmas tampoco sirve el modelo de Fuerzas de Reserva, la creación de armas no es algo puntual, sino una actividad industrial (para algunos) como otra cualquiera.

Si hablamos de tener una sociedad más cibersegura, eso significa que todos los sistemas digitales sobre los que se apoya nuestra sociedad deben ser más seguros. En este escenario no se puede hablar de contingencias puntuales de crisis, sino de una continua, bien pensada y suficientemente financiada actividad permanente. La Ciberdefensa debe ser una estrategia plurianual que prepare a todos nuestros sistemas para detectar, resistir, gestionar y recuperarse de los ataques más arriesgados que puedan darse. **La ciberseguridad es esencialmente proactiva y no reactiva**, por lo que el modelo de entrenamiento periódico y movilizaciones puntuales propio de la Fuerzas de Reserva militar tampoco le va bien a la Ciberdefensa.

Escasez crónica en España

El valor estratégico del ciberespacio está bastante aceptado por casi todos, sin embargo, España sufre una escasez crónica en cuanto a recursos en materia de ciberseguridad. Esto es claramente así en el sector público, pero que no canten victoria en el sector privado porque todavía les queda muchísimo que hacer y hacerlo bien. También está muy en boga achacar nuestra **"ciberpenu-**

[22] https://en.wikipedia.org/wiki/Military_reserve_force
[23] http://www.abc.es/espana/abci-primera-linea-defensa-espana-ciberdefensa-201801150227_noticia.html
[24] https://en.wikipedia.org/wiki/Military-industrial_complex

ria" generalizada a la **falta de talento** o, mejor dicho, a la incapacidad de reunir, captar y fidelizar el talento al estilo **Mr. Robot** que hay en nuestro país.

Se habla de los muchos puestos de trabajo en ciberseguridad que hay en la parte de la demanda y la **absoluta escasez de profesionales** para cubrirla. ¿Cuánto dinero han invertido esos demandantes de ciberexpertos para formar a esos futuros trabajadores? ¿Cuántos buenos programas universitarios en Ciberseguridad están financiados por el estado o por las empresas? ¿Qué interés real han puesto las instituciones académicas en atender a esa demanda de una profesión transversal que no encaja con sus reinos de taifas? La respuesta sincera a todas estas preguntas es, insignificante.

El modelo de Mr. Robot queda muy bien en la pantalla pero es un desastre en un escenario real de Ciberdefensa. Este quinto dominio no es una palestra en la que luchan campeones que determinan con sus proezas el resultado de la contienda. No es hora de reclutar a los Agamenón, Héctor, Aquiles o Paris de la comunidad hacker española, sino de establecer estructuras defensivas realmente bien pensadas, bien ejecutadas y bien gestionadas por un número bastante significativo de profesionales que nada tienen de héroes. Esos muchos profesionales que faltan, solos no se van a formar y nadie los está formando.

No es hora de reclutar a los Agamenon, Hector, Aquiles o Paris de la comunidad hacker española, sino de establecer estructuras defensivas realmente bien pensadas, bien ejecutadas y bien gestionadas por un número bastante significativo de profesionales que nada tienen de héroes. Esos muchos profesionales que faltan, solos no se van a formar y nadie los está formando.

Una alternativa: la Academia Ciber

Dejémonos de Fuerzas de Reserva y voluntariados mal entendidos y montemos una especie de Academia Ciber, que sea eminentemente civil, nada Universitaria pero sí avanzada, y con una importante financiación pública equiparada a la privada. Mediante un proceso continuo de selección, esta entidad daría a los ciudadanos mejor capacitados de las diferentes disciplinas que confluyen en la Ciberdefensa, la formación y oportunidad que una sociedad democrática y segura necesita.

Los costes del proceso también se sufragarían, en parte, por esos mismos estudiantes mediante préstamos personales que se les conceden, y que deberán devolver. Para ello contará con los ingresos obtenidos en un puesto de trabajo bien remunerado en el que tendrá que trabajar durante unos años después de terminada su formación. Con este tipo de esquemas de inversión estratégica a medio plazo, se generaría de forma continua el talento necesario (no buscándolo debajo de las piedras) y colocarlo en los lugares que sean necesarios dentro de una sociedad que desea ser segura.

Montemos una especie de Academia Ciber, que sea eminentemente civil, nada Universitaria pero sí avanzada, y con una importante financiación pública equiparada a la privada. Mediante un proceso continuo de selección, esta entidad daría a los ciudadanos mejor capacitados de las diferentes disciplinas que confluyen en la Ciberdefensa, la formación y oportunidad que una sociedad democrática y segura necesita.

Por último resta decir que la solución a nuestros problemas en el ciberespacio no puede ser, como algunos han propuesto, simplemente una lista o censo de personas [25] y sus ciber-cualidades a las que llamar cuando llegue el crujir de dientes [26]. Eso de hacer una lista me recuerda al **Registro de Mutantes** [27] del Universo Marvel, y **la infausta iniciativa de una futura Ley de Seguridad Privada** [28], promovida por el Gobierno del PP, en la que se crearía un registro que incluyese a todas aquellas empresas o personas con capacidades ciber, y que puedan utilizar "instrumentos" que pudiesen tener utilidad en un ataques cibernético.

Casi en ninguna ocasión es bueno aparecer en una lista [29], por lo que la mera propuesta de ese tipo de "*censos*" preocupa y trae a la memoria las tristes **listas negras** [30] **del Macartismo** [31]. Las listas pueden ser elaboradas con aparente buena intención, pero luego pueden ser utilizadas para cualquier otra cosa. La comunidad *hacker* española no da credibilidad [32] a esta iniciativa del Gobierno de Rajoy pero, sin duda, el tema de la Ciberreserva cumple sus funciones de distracción o narcosis [33], y consigue que no se hable de otra cosa mientras no se soluciona nada. ■

[25] https://youtu.be/npNop24AmCE
[26] http://bibliaparalela.com/luke/13-28.htm
[27] http://www.enciclopediamarvel.com/card/3334
[28] https://redminerva.org/reglamento-de-seguridad-privada-2017/
[29] https://15mpedia.org/wiki/Lista_de_represaliados_en_el_Franquismo
[30] https://en.wikipedia.org/wiki/Blacklisting
[31] https://en.wikipedia.org/wiki/McCarthyism
[32] https://www.elconfidencial.com/tecnologia/2017-06-05/hackers-espana-ciberreserva-rajoy-pp-seguridad-informatica_1392824/
[33] http://www.wordreference.com/definicion/narcosis

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