Casar Corredera, José Ramón (dir.), *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012.

El trabajo coordinado por el profesor José Ramón Casar Corredera, contribuye de manera interesante a un tema que durante estos últimos años ha cobrado una relevancia jamás pensada y menos en el plano internacional. Surge como parte de la evolución tecnológica, por la convergencia entre la informática y la modernidad de las armas, dando origen a los fenómenos nunca concebidos como la *ciberguerra* y la *ciberdefensa*.

La historia, ahora será un testigo de un nuevo campo de batalla de los tradicionales y los ya conocidos como la tierra, el mar y el aire. Con el auge de las tecnologías de la información y la comunicación (TIC) el ciberespacio se ha convertido en un escenario más de confrontación, en el que se despliegan amenazas nunca antes vistas y con consecuencias tampoco pensadas. En este contexto surge esta publicación titulada *El ciberespacio. Nuevo escenario de confrontación*.

Es un trabajo fresco e innovador que ofrece reflexión sobre el estado actual de los conflictos en el ciberespacio, plantea desde la visión española estrategias de actuación ante las posibles amenazas, bajo un esquema militar enfocado en la *ciberdefensa*. Sin embargo por los análisis históricos, doctrinales, jurídicos y tecnológicos que en él se aprecian, permite desprender algo más que fórmulas militares, la amplitud del tema y las múltiples esferas relacionadas al tema reconocen y hacen necesario atender intereses de los individuos y sus comunidades.

La publicación comienza con una introducción de Ramón Casar, el coordinador de la obra, la cual se encuentra dividida en seis capítulos cada uno de ellos muestra independencia y autonomía del autor, en el que con un estilo propio y la rigidez académica que un trabajo de esta

magnitud requiere ilustran con reflexiones muy interesantes y propositivas. Es Luis Feliu Ortega quien comienza el primer apartado sobre "la Ciberseguridad y la Ciberdefensa".

Con claridad, Feliu, teniente general del Ejército de Tierra Español, hace un recuento histórico del concepto de conflicto armado, pasando por los Convenios de Ginebra (1899-1907) y la Paz de Westfalia (1648) e incluso refiriéndose a grandes pensadores como Vitoria, San Agustín y Santo Tomas. Establece los elementos que componen los conceptos de defensa y seguridad y de la mano se aproxima a los fenómenos tecnológicos y jurídicos que son el ciberespacio, la ciberseguridad, la ciberdefensa y el ciberconflicto; de esa manera logra plantear estrategias de seguridad nacional y dedica un apartado al caso de España. En el que propone la creación de un órgano único de ciberseguridad al más alto nivel del gobierno.

Es muy contundente el teniente Feliu Ortega al afirmar que "cuanto más desarrollado un país, más elementos vulnerables que afecten su seguridad poseerá y por tanto deberá garantizarla" (p. 43), por esta razón el autor se centra en los ciberataques a infraestructuras críticas, reflexiona sobre las ciberarmas y la complejidad que existe para la atribución del ataque.

Finalmente hace una reflexión muy interesante sobre la actividad y estrategias de la Unión Europea y de la OTAN, el jefe de ciberseguridad de este último organismo pone clara la trascendencia del tema cuando menciona que los ciberataques y el ciberterrorismo suponen la misma amenaza para la Seguridad Nacional que un misil (p. 52).

El segundo capítulo titulado "Estrategias Internacionales para el Ciberespacio" está a cargo del comandante de Ejército en Tierra Carlos Enríquez González. El estudio describe una perspectiva internacional del tema de ciberseguridad, contemplando las violaciones a delitos de alta gravedad e incorporando una visión política militar.

El teniente Enríquez dice "Internet la red, una tela de araña que supera los esquemas del viejo mundo westfaliano, que no conoce fronteras, Estados ni naciones y sobre la que no existen ni cuerpo legal ni gendarmerias" (p. 74); el autor se cuestiona sobre la viabilidad de la regulación o no de Internet, y debate las dos posiciones. La primera, es la línea de Nicolas Sarkozy, quien pugna por una regulación que mantenga

la seguridad de los usuarios y la red; la otra es la de Mark Zuckerberg (presidente de Facebook), quien promueve un Internet sin límites en favor de la innovación tecnológica y la capacidad de emprendimiento, es decir, propone la autorregulación (p. 75).

Desarrolla el tema la ciberseguridad desde una perspectiva internacional y estudia el actuar de la ONU, la OTAN, la OCDE, la UIT y la UE, particularmente las normativas al respecto. El autor sella su participación bajo la idea que existe una fragmentación ocasionada por el objeto de cada organismo internacional, situación de índole natural ocasionada por cumplir y satisfacer los fines para lo que fue creada, razón por la que no existe una integridad en temas de ciberseguridad. Evidentemente el gran reto que tiene ante sí el derecho internacional es fomentar la uniformidad de las normas.

El tercer apartado denominado "La evolución del conflicto hacia un nuevo escenario bélico" es responsabilidad de Javier López de Turiso y Sánchez, en el que explica la evolución del concepto de conflicto hasta llegar a su forma más acabada y violenta que es la guerra. Asume una posición interesante, "el conflicto es necesario, hace evolucionar al hombre con nuevas ideas y pensamientos" (p. 122). Describe las características de los distintos escenarios bélicos (marítimo, terrestre, aéreo y espacial), y contrasta las similitudes y diferencias que existen con el ciberespacio.

El desarrollo informático de las redes se ha enfocado en robustecer y desarrollar mejores sistemas en el Internet, sin hacer prevalecer el tema de la seguridad, así lo entiende el autor de este tercer capítulo. Parte de la premisa que siempre existirán vulnerabilidades que serán aprovechadas por el enemigo y revisa las ventajas de la ofensiva en el ciberespacio junto con el tipo de armas que permiten enfrentar a dichos agresores. El autor concluye en proponer un cuerpo permanente, de dedicación exclusiva y especializado en la ciberdefensa que goce de independencia y autonomía.

Finalmente hacer un comentario que se desprende de este tercer capítulo, el subsecretario del Departamento de Defensa de Estados Unidos, William Lynn, declaró "que si se considera un ataque informático peligroso para la vida de civiles o la Seguridad Nacional, el presidente podrá responder con los medios que tenga a su alcance, incluyendo el

militar" (p. 144). Esta aseveración, debe ser considerada a la luz del derecho internacional, por las consecuencias jurídicas que ello refieren. ¿Será entonces posible que un Estado haga uso de la fuerza armada por recibir un ataque cibernético? ¿Esto se encuentra regulado por el derecho internacional? ¿Es aplicable la legítima defensa? Este es un tema que al autor preocupa y aunque no se ocupa del tema de fondo, deja ver entre luces la gran incógnita que ello supone.

El cuarto capítulo es una genialidad de Ángel Gómez de Ágreda, en su aportación define al ciberespacio como un elemento igualador de capacidades y reductor de asimetrías, su naturaleza artificial y diseño por el hombre lo dota de imperfecciones (p. 171). El autor identifica sus tres capas, la sintáctica, semántica y la física, todas ellas vulnerables y motivación para los *hackers* e intrusos, que en su búsqueda de penetrar a los sistemas ajenos intentarán obtener información o incluso manejarlos con fines maliciosos.

Para el Teniente Gómez, Coronel del Ejército del Aire, el ciberespacio es parte de la globalización y ambos permanecen unidos en el mundo moderno, este nuevo escenario plantea constantes amenazas y reflexiona sobre los objetivos de los hackers, quienes persiguen distintos fines, desde probar su capacidad como un mero aficionado, hasta obtener información clasificada o beneficios económicos directos. El autor hace una remembranza de casos emblemáticos de ciberataques, estos son los de Georgia y Estonia, donde los sistemas informáticos de ambos países se colapsaron, a tal grado que Estonia solicitó a la OTAN activar el artículo V del Tratado de Washington que establece el principio de defensa mutua. Ataques que quedaron impunes, en razón de que los Estados no tuvieron la capacidad de atribuir la autoría de dichos actos.

Finalmente el teniente Ángel Gómez, cuestiona si en el ciberespacio debe prevalecer la libertad sobre la seguridad, ya que el 80% de los sistemas críticos de una nación están en manos privadas y la protección de los gobiernos es sólo parcial (p. 193). Propone una visión integral basada en un conjunto coherente en el que participen las estructuras privadas, públicas, civiles, militares y empresariales, para garantizar el eterno compromiso entre libertad y seguridad.

En el quinto capítulo Óscar Pastor Acosta contribuye con el tema "Capacidades para la defensa en el ciberespacio", dedica la reflexión a la ciberdefensa como el subconjunto más operativo que se desarrolla para garantizar la Seguridad Nacional. Clasifica las capacidades de ciberdefensa de la siguiente manera: la defensa de prevención, detección, reacción y la de recuperación. En este contexto define la ciberdefensa como el conjunto de sistemas, infraestructuras, personas, medios de apoyo y procedimientos doctrinales, que permiten cumplir con la misión de defender el ciberespacio.

Pastor Acosta demuestra que la sofisticación de la amenaza cibernética evoluciona con rapidez y es necesario hacer frente con medidas más contundentes que pongan fin a ellas. Considera que las preventivas, las de detección y reacción son importantes pero no suficientes, implementar acciones que neutralicen el origen de las amenazas con capacidades de ciberejército será fundamental para garantizar la seguridad. Finalmente mencionar que el autor pone en la mesa una realidad a la que se enfrenta el derecho internacional, que es la ausencia de regulación jurídica durante enfrentamientos cibernéticos, hoy en día estos carecen de normas, apreciación interesante sobre la que valdría la pena plantear algunas nuevas ideas.

Para cerrar con broche de oro, Manuel Pérez Cortés escribe sobre "Tecnologías para la defensa en el ciberespacio". Comienza con un elemento básico que es conceptualizar el ciberespacio, en el mismo apartado se encarga de la seguridad de los Sistemas de Armas en Red y los Sistemas de Información Militar contra los posibles intrusos (p. 259). En un epígrafe siguiente analiza los ataques y las amenazas cibernéticas, recordando el robo de más de 90 000 direcciones y contraseñas militares que sustrajo el grupo terrorista AntiSec, alusión que ejemplifica la trascendencia de la ciberdefensa.

De manera técnica describe los ataques a las infraestructuras críticas, las cuales son contra dos capas: uno, la física, esto es anula el material de redes y ordenadores para imposibilitar su funcionamiento y segundo, la manipulación de software o sistemas operativos.

El autor hace una descripción de las fases que se desarrollan durante un ataque cibernético, con variaciones que dependen de la capacidad intelectual y tecnológica del agresor. De forma general se puede decir

que se originan desde la recopilación de información hasta una ciberguerra o una denegación del servicio como lo ocurrido con Estonia. (pp. 264 y 265).

Así Manuel Pérez analiza cerca de 25 tipos de amenazas que ocurren en el ciberespacio, destacando entre las más comunes: los Botnets, Troyanos, Gusanos, Abuso de Privilegios de Acceso, los de Hardware y Denegación de Servicio. Propone con qué clase de tecnologías y servicios se coadyuva a la detección, respuesta y asistencia en las amenazas cibernéticas. Finalmente se ocupa de las herramientas y la metodología que se aplica en la seguridad del ciberespacio.

Concluye el autor con una serie de ideas para evitar que las amenazas antes mencionadas provoquen daños a las estructuras críticas, sus recomendaciones son proteger los datos con confidencialidad e integridad; la detección rápida de intrusos; la capacidad de adaptación y recuperación de los sistemas y la necesidad de atribuir los ciberataques.

Una amplia felicitación para todos los que contribuyeron a la realización de este magnífico libro, ya que dejan en manos de los lectores un interesante avance desde el punto de vista tecnológico y militar del ciberespacio como un nuevo escenario de conflicto, en el que se plantean desafíos y retos muy interesantes para el derecho internacional.

Merece hacer algunas consideraciones finales que se desprenden de la lectura general del libro y de la que se destacarán tres puntos a reflexionar, aspectos que también son coincidentes en la mayoría de los autores: primero, la necesidad de crear elementos jurídicos y tecnológicos que permitan atribuir la autoría de los ciberataques; segundo, la ausencia de normas que regulan los enfrentamientos cibernéticos; tercero, el conflicto que existe entre regular o no Internet, ponderando entre la seguridad y la libertad.

Fernando **Navarrete Saavedra**