Revista de Pensamiento Estratégico y Seguridad CISDE

Recibido: 17-05-2016 / Revisado: 23-05-2016
Aceptado: 23-05-2016 / Publicado: 31-05-2016

CISDE Journal, 1(1), 2016

La ciberguerra como realidad posible contemplada desde la prospectiva

Cyberwarfare as a possible reality considered from the perspective of future studies

José Domínguez León[1,2]

[1] UNED – Centro Asociado de Sevilla, España
[2] Academia Iberoamericana de La Rábida

josedominguezl@hotmail.com

RESUMEN. A lo largo de los últimos años ha tomado cuerpo la idea de una posible guerra en la que participen algunas de las potencias mundiales. Este gran conflicto se presupone en los diferentes marcos convencionales y, además, en el ciberespacio. Cada vez se da mayor valor a la ciberguerra, mediante la cual es factible atacar estructuras de diversas naturalezas, infraestructuras críticas y ocasionar daños que pueden poner en jaque a toda una sociedad. Se habla de una guerra latente y próxima. Esto genera una notable preocupación en los países desarrollados, que cuentan con extensas y sólidas estructuras e infraestructuras, posibles objetivos de una guerra convencional y de una guerra en el ciberespacio. Los Estados han de adoptar medidas y constituir organismos para la defensa ante ciberataques. En algunos casos, esta pasa por contar con capacidad para atacar. La comunidad internacional ha de plantearse una ética que rija en este campo.

ABSTRACT. In the recent years, the idea of a possible war involving some of the global powers is taking shape. This large-scale conflict is assumed in all different conventional contexts as well as in cyberspace. Cyberwar has been gradually valued as a way of actually attacking various types of networks and critical infrastructures and causing damage that may put a whole society in check. The topic of a latent, coming war is often talked about. This is generating significant concern in the developed countries, which own large and solid networks and infrastructures, possible targets of both a conventional war and a war on cyberspace. The nations must take the necessary steps and create organizations for their own defense against cyberattacks. In some cases this defense would also imply a strike capability. The international community need to find the ethics that would govern this field.

PALABRAS CLAVE: Ciberguerra, Ciberespacio, Potencias mundiales, Ciberterrorismo, Ciberdefensa, Ciberataques, Guerras mundiales, Prospectiva.

KEYWORDS: Cyberwar, Cyberspace, World powers, Global powers, Cyberterrorism, Cyberdefense, Cyberdefence, Cyberattack, World wars, Future studies.

1. Introducción

Resulta complejo establecer unas líneas nítidas a través de las cuales se pueda tratar de sintetizar un entramado amplio y con múltiples ramificaciones, como es el relativo a la ciberguerra. Al abordar esta temática es inevitable referirse también a una serie de conceptos, campos y problemas que constituyen todo un mundo de diatribas, afrontadas por distintas disciplinas científicas y no pocos saberes técnicos. La humildad de los investigadores lleva a veces a verse desbordados por la inmensidad de los terrenos y los elementos que componen esta temática. Este reconocimiento de la propia limitación no ha de ser obstáculo para proseguir investigando, sobre todo porque desde los logros que se alcancen serán viables unas aportaciones a la paz mundial, construida poco a poco y por medio de muchos esfuerzos (Monografías del CESEDEN, 2012).

Durante los últimos años se ha desarrollado en el campo del análisis de Seguridad, de Geopolítica y Geoestrategia toda una línea de actuación y de investigación en el sentido de poner sobre la mesas de las cancillerías y de los estados mayores de los ejércitos la difícil situación en el entramado de las relaciones entre grandes potencias. Si se realiza un barrido para el análisis de fuentes abiertas en la Red acerca de las posibilidades de conflictos entre esas grandes potencias, es común hallar informes, noticias, publicaciones, documentación de muy variado corte que enlaza con la traída y llevada tercera guerra mundial. Visto así, se ha de resaltar que la humanidad ha estado en más de un momento al borde de contemplar un serio conflicto entre países antagónicos que pudo haber derivado en un conflicto a gran escala, en lo que se entendía como una guerra mundial.

La diplomacia y el sentido común parece que han dominado los escenarios pasados, y aunque se han producido conflictos de toda clase, en muy diferentes zonas del mundo, nunca se ha llegado a uno declarado que conllevase el calificativo de mundial o generalizado. Precisamente se ha de contar con que el horror al empleo de armas convencionales de alto poder destructivo, o a no convencionales de destrucción masiva, era un freno que ponía sobre las espaldas de los dirigentes políticos y estadistas la difícil decisión sobre su empleo. La cordura manifestada durante décadas no ha impedido que, a pesar de los tratados de no proliferación de armas nucleares, varios países accedieran a contar con estas. Algunos de estos casos son llamativos, como India y Pakistán, vecinos y enfrentados. En ciertos casos la razón del investigador se puede topar con algún país que recibe ayudas exteriores de organizaciones de corte humanitario, para contribuir a su desarrollo, cuando sus gobiernos han empleado importantes recursos en armamento nuclear. Es un sinsentido recibir ayudas para respaldar a la población más empobrecida, y a la vez dedicar grandes sumas para contar con todo un programa nuclear que incluye armas de destrucción masiva.

En este panorama empiezan a emerger voces que tratan sobre hipotéticas futuras confrontaciones entre grandes potencias, o entre estas y otras emergentes. Se tilda como algo posible un enfrentamiento entre Estados Unidos y China, o entre el primero y Rusia, o entre el primero y los otros a la vez. Se enfatiza que India puede desencadenar un serio conflicto, o que Israel puede apostar en un momento dado por pasar de las estrategias mantenidas hasta el momento a otras de diferente calado y consecuencias. De los países europeos pertenecientes a la Unión Europea no suele insistirse en sus posibles derivas hacia este terreno, aunque se les dibuja como un bloque que tendría que hacer frente a amenazas de muy variado cuño, procedentes de oriente, del mundo islámico, y de hipotéticos nuevos colosos militares.

2. Sentido y concepto de ciberguerra

Como una especie de cúspide que representaría la culminación de un proceso de poder, de hegemonía, y a la vez de operatividad en el hecho de causar a un hipotético enemigo un gran daño sin efectuar ataques convencionales, se sitúa la ciberguerra, es decir, la situación caracterizada por ataques de tipo cibernético contra objetivos que tienen un determinado valor. En esta parcela cabe ubicar todo tipo de estructuras e infraestructuras, no solo las críticas. Cualquier estructura que sea dañada y devenga en no operativa puede significar un serio daño al país o la sociedad atacados. Una inviabilidad de obtención de servicios esenciales puede deparar, incluso, la pérdida de vidas humanas. Esto implica que la ciberguerra puede llegar a ser tan devastadora como lo que hasta hace poco tiempo se entendía como guerra convencional (López, 2006).

En algunos ambientes, incluso de personas con alto nivel cultural o educativo, existe una acusada ignorancia acerca de los riesgos que puede conllevar la ciberguerra. Es común que se entienda como tal un conjunto de ataques a estructuras como las financieras, las empresariales, etc. Cuando se analiza esa marcada lejanía ciudadana respecto de un riesgo tan serio, y que se puede concretar en resultados tan materiales como las víctimas humanas, cambia el talante de quienes solo ven las pérdidas de carácter económico. Apenas se cuenta con un conocimiento científico ni siquiera aproximativo sobre lo que es la ciberguerra y qué consecuencias puede acarrear a la sociedad. En el momento en que las personas comienzan a entender y a visualizar ciertas consecuencias de un conflicto de este corte, cambian sus percepciones sobre el mismo.

Se trata, en esencia, de eso, de percepción del riesgo, de categorización de amenazas, de sentido de la realidad que sobrepasa. Si se comparase este riesgo, y todas las amenazas que lleva aparejadas, o a la inversa, es decir, amenazas y riesgos, por este orden, suele captarse en los sectores más sensibilizados de las sociedades occidentales que las amenazas vienen de otro baluarte. Se habla de la amenaza islamista extremista, que concluye en terrorismo, y este se enseñorea en un constante ejercicio de golpes perpetrados contra intereses occidentales, desde personas hasta bienes. Otro temido tejido de miedos y amenazas proviene de la desazón que provoca la inseguridad en cuanto a futuros, o sea, preocupaciones ante el desempleo, la precarizad de las futuras pensiones o del estado del bienestar, si no se ponen remedios oportunos, etc. Los miedos, cabe considerar que en aumento, podrían convertirse en verdaderas pesadillas al modo de urdirse una trama a base de los mismos, de tal manera que un gran miedo se agregue a otros y, entre varios, terminen por atenazar a sociedades en su conjunto. En cierta medida, los diferentes tipos de terrorismo pretenden acaparar monopolios de pánico para dominar a las sociedades que se convierten en sus principales objetivos y víctimas a la vez.

Al mismo tiempo, se trata de un proceso muy estudiado desde los centros neurálgicos de decisiones que desencadenan ataques contra determinados objetivos, particularmente en occidente, aunque ese terrorismo perpetra, igualmente, constantes ataques contra sus enemigos cercanos. Algunos países y poblaciones viven en continuo estado de alarma, tensión, y hasta desesperación. No hay que extrañarse de que masas de población considerables, millones de personas, huyan ante el empuje del terror, y esto genere fenómenos migratorios no regulados, de tipo caótico. Muchas personas mueren en el intento de lograr acceder a un espacio de paz y seguridad.

De hecho, esta situación no es muy diferente a otras que se han vivido a lo largo de la historia. La presión de unos pueblos y de millones de desplazados determinaría, en distintos momentos históricos, incluso la caída de imperios.

El terror y el terrorismo son conducidos en los últimos años hacia la extensa parcela de lo cibernético, de la Red, de los sistemas de control a través de la Red de múltiples estructuras hoy imprescindibles para la vida en comunidad. Ahí están los servicios básicos, sin los cuales no se podría desarrollar la existencia humana tal como hoy la concebimos. Los daños que un potencial enemigo acarrearía a través de la Red pueden ser incalculables desde un punto de vista cuantitativo, pero más aún en lo referente a lo social, a lo humano.

En numerosas fuentes y en diferentes ámbitos políticos, económicos, técnicos y militares se traduce una clara inquietud en torno a una posible confrontación mundial, de acuerdo con distintos factores que caracterizan las relaciones entre las grandes potencias. Parece que el sentido común se suele imponer o, al menos, es lo que ha venido sucediendo a lo largo de décadas, en cuanto a poner los medios necesarios para evitar conflictos que pudieran tener consecuencias irreparables para la humanidad. El contexto de una posible confrontación no es únicamente el que se puede considerar convencional, es decir, el que tradicionalmente ha acompañado a las guerras, a las grandes guerras, con empleo de armamento, tácticas y estrategias marcadamente convencionales. En la actualidad, y desde hace décadas, se cierne sobre el mundo la amenaza de una gran guerra que podría conllevar unos tintes muy diferentes a las hasta ahora conocidas. La novedad consiste, en esencia, en que el ciberespacio podría contemplar un serio enfrentamiento. Se estaría ante la ciberguerra.

No se trata solo de esa colisión entre opuestos sino, también, de un marcado y enconado esfuerzo por parte de las potencias más determinantes en el mundo por controlar el ciberespacio. De hecho, la ciberguerra no debería ser considerada solo como una situación de abierta hostilidad y declarado choque entre países o coaliciones, sino igualmente como la pugna entre estos, que llevaría a un forcejeo y una toma de posiciones tendente a dominar el ciberespacio. El concepto se refiere al ciberespacio convencional, conocido, y paralelamente a cualquier estructura o espacio cibernético que pudiera derivarse de la aplicación de las recientes tecnologías de la comunicación. Redes poco conocidas, e incluso otras que pudieran estructurarse en el futuro, inmediato, próximo o remoto, cobran valores excepcionales si se tiene en cuenta el papel que pueden llegar a desempeñar en una hipotética relación entre países, bloques o grupos de interés. En este aspecto es preciso hacer notar que la Prospectiva no se refiere únicamente a escenarios posibles en un ciberespacio hoy concebido sino, por extensión de la aplicación de nuevas tecnologías y procedimientos, a un concepto de ciberespacio como pudiera ser entendido y materializado en los plazos de décadas, de acuerdo con las concepciones cibernéticas actuales.

3. Visiones sobre la ciberguerra en el presente y para el futuro, desde la Prospectiva

Algunos analistas han resaltado la emergencia de problemáticas en torno a este entramado cibernético. El profesor Paul Rexton Kan ha puesto de manifiesto en reiteradas ocasiones, y a través de publicaciones, que los términos ciberguerra y wikiguerra son bastante más que determinantes en el mundo actual. Cualquier intrusión en un sistema informático de cierto calado puede resultar fatal para el vulnerado, sea administración, empresa, ejército... Esto supone un conjunto de riesgos y amenazas, es decir, potenciales y reales situaciones dibujadas sobre el tablero de la planificación, pero que en muchas ocasiones se han visto materializados. Junto a la ciberguerra se establece todo un panel de amenazas cibernéticas que hacen plausible, viable, y hasta objetivamente muy posible, un Pearl Harbor cibernético. Esto viene a situar a la humanidad ante el constante riesgo que tiene como origen no se sabe qué país u organización. De lo que no cabe la menor duda es de que el riesgo es real, y que, como ocurriera en su día en forma de ataque aéreo, pueda trasladarse a otro tipo de ataque, por sorpresa, con toda la intención de producir daños, a la realidad (Rexton Kan, 2014).

La sociedad actual ha de hacerse a la idea de que es imprescindible contar con medios adecuados para detener, contrarrestar, minimizar, repeler… estos ataques cibernéticos, y máxime cuando se traten de golpes contra las infraestructuras críticas de uno o varios países, a las que hay que agregar las de carácter militar o de defensa en general. Se han concebido las infraestructuras críticas como un conjunto de elementos que permiten los servicios elementales a la sociedad. Es momento de que se trate, igualmente, el conjunto de infraestructuras militares en el mismo campo, dado que una grieta en alguno de los sectores vitales de la defensa de uno o varios países puede llevar a un auténtico desastre. Aquí puede obrar la defensa como un hecho transversal, sin posibilidad de aislarla de las comunicaciones, los servicios sanitarios, el abastecimiento de alimentos o agua, el sistema energético, etc. Todo se interrelaciona. Todo se interconecta. Una falta de fluido eléctrico puede llevar a algo más que un apagón transitorio. Un desabastecimiento de agua o alimentos básicos puede conllevar una caída de otras estructuras. Una inviabilidad de transportes puede paralizar toda una sociedad, todo un país. En paralelo, un ataque cibernético que opere sobre centrales eléctricas, sistemas de transportes, comunicaciones, es un ataque en toda regla a una comunidad. El ciberespacio es un ámbito que hoy posibilita el control de muchas y muy variadas infraestructuras, críticas y convencionales, de defensa y de capacidades operativas para repeler posibles ataques. No se puede bajar la guardia en ningún punto de este extensísimo tejido. Solo una fisura, detectada por un potencial enemigo, puede dar lugar a sufrir un ataque de imprevisibles consecuencias.

Desde el terreno de la Criminalística se ofrecen modelos de actuación que deben estar basados en el modo de pensar ante los posibles agresores, atacantes, también en el amplio campo de lo cibernético. Esto equivale a plantear que se ha de pensar con mente criminal, o sea, revisar los posibles modelos de operar de hipotéticos atacantes, y señalar cuáles son los flancos que estos atacarían. Se ha de pensar con la mente criminal con que ellos actuarían. De lo contrario, se estaría en una dinámica de reacción. Ante esa dinámica reactiva es

imprescindible proponer otras de carácter proactivo, es decir, de anticipación, de organizarse para no tener que sufrir las consecuencias de este tipo de ataques en la Red y otros colaterales.

Algunas visiones acerca de la ciberguerra son bastante explícitas en cuanto a considerar dentro de este ámbito gran parte de las agresiones, intrusiones y hechos que se perpetran en la Red. En esa línea se encuentra Richad Clarke quien, a través de distintas publicaciones, deja patente el peligroso marco de la denominada ciberguerra, en la que incluye muchas de las manifestaciones de ciberataques. Se contarían aquí diversas modalidades de ciberataques, aislados, sistemáticos, persistentes, selectivos. Clarke resalta una clara inquietud en torno al papel de los Estados Unidos, subrayando su honda preocupación en el sentido de que se vaya quedando rezagada en este campo. Para ello compara la situación en ciberdefensa y capacidad de ciberataque de este país respecto de otros posibles oponentes, como es el caso de China o Rusia. Esta inquietud, puesta de relieve por Clarke desde hace años, se ha visto corroborada por la realidad, en tanto los ciberataques dirigidos contra Estados Unidos en los últimos años han dejado constancia de que sus ciberdefensas son realmente vulnerables, y de ello son buenas muestras los ciberataques que han logrado obtener datos de funcionarios, por ejemplo (Clarke y Knake, 2010).

De otra parte, Thomas Rid apunta que la ciberguerra no llegará a producirse, y argumenta a favor de una serie de factores que ponen frenos y remedios a tan terrible perspectiva. Al menos es lo que planteaba en su libro publicado en 2013, y en otras publicaciones que tienen como escenario un mundo en el que determinados mecanismos impedirían ese desenlace. No obstante, las más recientes situaciones producidas en el ciberespacio en cuanto a intrusiones, ataques o robos masivos de información, ponen en tela de juicio una visión no catastrofista del asunto. El profesor Rid, no obstante, ha fundamentado muy bien sus aseveraciones, razón por la cual deben ser tenidas muy en cuenta (Rid, 2012, 2013).

En una orilla muy distinta, y con las miras puestas en una Red más abierta y en una constantemente esgrimida transparencia en la misma, se sitúa la obra de Julian Assange y otros autores colaboradores Cypherpunks: Freedon and the Future of Internet. Con independencia del calado relativo a su puesta fuera de la legalidad y su reclusión diplomática, se ha de destacar que alrededor de la Red existen infinidad de posiciones que hacen valer la opción de evitar que esta se convierta en un campo de batalla, a la vez que conseguir una fluidez en la información abierta que haga inviable a los sectores más poderosos que hoy controlan sus flujos llevar a cabo sus deseos (Assange et al., 2014). No es cuestión aquí, ni en este trabajo, de entrar en ninguna polémica. Es preciso ahondar en las relaciones que existen entre los grandes centros de poder político, económico, militar, etc, y los derroteros que han ido marcándose en la evolución de las posiciones ante la Red en los inicios del siglo XXI. Las opiniones y tendencias que desde la investigación se pueden hallar son múltiples, poliédricas, con demasiadas aristas, como para comprenderlas en una simple percepción de las mismas. Es más, en ciertos casos apenas se pueden percibir algunas de estas opciones o visiones, en tanto se encuentran soterradas para el común de quienes se acercan a investigar el tejido difuso conectado con la Red y la ciberguerra. A veces, el investigador llega a conclusiones que le señalan que no es lo aparente a primera vista el camino acertado. Hay demasiadas contradicciones al respecto.

Aparte de la aludida tendencia en el ciberespacio a desplegar una ciberguerra consistente en el ataque a infraestructuras críticas y de defensa, se barrunta una especie de teoría sobre hacia dónde se encaminan las posibles modalidades de ciberataque. Desde una visión prospectiva simple destacan las nociones alrededor de la preparación de ciberbombas, tal vez denominadas así y de otras formas similares porque penetran en el corazón del oponente, y el agresor no se preocupa del daño que causarán. Es casi una premisa de este proceder que las ciberarmas llegarían a alcanzar un estado de dominio tal que podrían ser capaces de atacar desde su propia ingeniería, preparada, como una especie de código que se ha impreso en las mismas. Esta preparación se podría centrar en preparar ciberarmas inteligentes que el atacante incluso no pudiera controlar en toda su extensión y profundidad. Bastaría con dotarlas de capacidad para acumular datos relativos al objetivo y, a través de la persistencia en el ataque, lograr determinados objetivos. No cabe duda de lo que ello podría significar. Primero en cuanto a las grandes inversiones que esto requeriría. Segundo, a lo que ello implicaría en lo relativo a avanzar en transferencia científica, pues no es solo cuestión de invertir en

Investigación, Desarrollo e innovación. Es imprescindible pasar al otro lado de la barrera que implica la ejecución de transferencias rápidas de lo conseguido en términos científicos y experimentales. De esta guisa, habría que reelaborar, en gran medida, una buena parte de la doctrina inherente a la Ciberdefensa y la Ciberseguridad.

Este tipo de armas puede ocasionar serios y enormes daños a un potencial oponente, aun cuando en el entramado de especialistas, analistas, ciberdefensores y ciberatacantes, hackers –en el sentido no negativo del término y de su significado-, etc, se baraja de continuo que, por muy desconocida que sea una de estas ciberarmas, terminará siendo descubierta y asmilada por los atacados y neutralizada. De lo cual parece deducirse que el futuro puede acarrear una elevada dosis de investigación para lograr modelos de ciberarmas cuyos entresijos sean difícilmente descifrables. Cuanto más tiempo tarde el oponente atacado en descubrir sus mecanismos de proceso, tanto más eficaces serán, puesto que ese tiempo dedicado a tal tarea obra en perjuicio propio.

De alguna manera esto ubica uno de los principales papeles de los ciberanalistas, en lo concerniente a obtener una preparación tal que les permita enfrentarse en tiempos verdaderamente cortos a las ciberarmas del oponente, para poder neutralizarlas antes de que el daño causado sea irreparable.

No hay que olvidar que los ciberatacantes estarán, de la misma manera, preparados para recibir las correspondientes réplicas por parte de los atacados, en cuanto estos tengan la capacidad operativa suficiente para ello. Una deducción lógica es que los ciberatacantes deben estar también preparados para neutralizar las respuestas de los atacados. Luego, cabe pensar que cualquier gran operación de ciberataque puede conllevar importantes riesgos para quien las desencadena.

Llevado esto al terreno de la doctrina, señala Klimburg la aparente obviedad de que la defensa en el ámbito del ciberespacio se puede topar con la disyuntiva de alcanzar una capacidad operativa adecuada sobre la base de aceptar ciertas prácticas no siempre deseables. Lograr capacidad de defensa puede incluso conllevar la aceptación de algunas formas no claramente aceptables (Klimburg, 2011).

En este apartado se halla en controvertido aspecto la doctrina concerniente a lograr la adecuada capacidad de disuasión, inherente a todo modelo de carácter militar, y es preciso subrayar que este trabajo se refiere a la ciberguerra, y que esta es inevitable que se encuentre ligada a las operaciones o acciones que se esté dispuesto a efectuar. Castigo, respuesta, represalia, reacción: se pueden aportar términos que en este quehacer significan casi lo mismo, aunque ello no cambia que el fondo de la cuestión tal vez radique en la capacidad operativa lograda y, a la vez, en la firme decisión de ejecutar operaciones de clara respuesta ante el oponente ciberatacante.

Diferente es el aspecto de que la disuasión puede ser muy evidente cuando se manejan armas convencionales. El hecho de una demostración de fuerza –en el sentido militar adjudicado al contingente humano–, o de armamento, sitúa a un determinado ejército o país en un público escaparate que permite a sus oponentes calibrar el potencial de que se trate, en mayor o menor medida. Aparte se emplean los elementos clave de la Información y la Inteligencia, dando forma a todo un conocimiento sobre el poder militar efectivo, real. Sin embargo, en el campo de la ciberguerra es altamente complicado hacer notar la fuerza propia a un oponente. Tal vez la única alternativa para hacerse notar, para hacer visible esa fuerza propia, sea poniendo en juego algo de la misma, mediante ciberataques que no siempre tienen una intencionalidad clara y manifiesta de ocasionar serios daños, sino más bien de mostrar y demostrar una hipotética superioridad. El problema radica, sin rodeos, en que un ciberataque que no sea demoledor puede que no muestre el verdadero poder que se posee, a la vez que origina una senda de respuestas que no son deseable y, probablemente, imprevisibles en algunos casos. Hacer daño solo para ejercer acciones que sean denotativas del ciberpoder puede llegar a ser radicalmente descabellado, aparte de que esto se desvincula de cualquier moral que se conecte con los derechos humanos y con el Derecho Internacional aplicable en las relaciones entre Estados. La polémica estaría servida y hace falta una profunda reflexión al respecto (Libicki, 2007, 2009, 2011).

Algunos investigadores adoptan posiciones que pretenden ser equidistantes, sobre todo porque poco a poco se está urdiendo una doctrina que, una vez compilada puede dar como resultado que un posicionamiento de hoy signifique un mañana en uno u otro sentido. La reflexión implica, o puede llevar aparejado, un determinado nivel de disquisición y hasta de dilema (Torres, 2011).

Tras los estudios que desde la Prospectiva cabe realizar en este campo de la ciberguerra, es imprescindible entender que si el futuro dibujado, a partir de las diferentes metodologías prospectivas, no es agradable, se han de disponer los medios para que no se produzca de esa forma en que se nos ha descrito. Es siempre mucho mejor que, empleando términos colectivos y conjugando verbos en plural, nos preparemos para lograr un futuro que se considere adecuado, y no dejar que otros vertebren ese futuro por nosotros. Esto equivaldría a tomar las riendas del futuro, de cada comunidad, sea país, organización, etc.

4. A quién creer sobre las posibilidades de materialización de la ciberguerra

Alejados de una literatura científica se puede correr el riesgo de perderse en un frondoso bosque en el que predominan opiniones. Desde una perspectiva científica han de pesar algunas de esas opiniones, siempre que procedan de especialistas, aunque no estén contenidas en trabajos editados en publicaciones de carácter estrictamente científico. Cabe realizar esta apreciación para llegar a entender que en algunos casos resulta extremadamente difícil penetrar en un armazón que pueda ser considerado verosímil alrededor de las muchas posturas que se advierten sobre la ciberguerra.

En Prospectiva se han de tener muy en cuenta las valoraciones de especialistas, aunque estas no se encuentren demasiado perfiladas. A veces es necesario partir de apreciaciones, conjeturas, posicionamientos no definitivamente elaborados, si bien esto puede hacer zozobrar la propuesta o teoría que se reelabore. De momento, se constata que personas del ámbito de la informática avanzada, con una gran proyección en el marco de la confrontación cibernética, han puesto el énfasis de su voz en afirmar que:

- La ciberguerra existe, no es una invención y muchos países se aprestan a poseer estructuras de ciberdefensa y ciberataque, como algo consustancial a la propia dinámica de la tensión y el enfrentamiento, lo cual ha pasado de un plano extraordinario y poco común a otro totalmente cotidiano.
- La ciberguerra no es una cuestión de un futuro más o menos próximo, sino que está aquí y que los Estados y los países la viven de muy diferentes formas.
- Los daños que puede ocasionar serían hoy día tal vez incalculables.
- Los países desarrollados han de apresurarse a poner al día sus mecanismos de ciberdefensa e igualmente de ciberataque, en un modelo en el que la disuasión será fundamental.
- Junto a las agencias y organismos nacionales y supranacionales de ciberdefensa y ciberataque existe toda una infinidad de grupos, organizaciones y personas empeñados en constituirse en garantes de la ciberseguridad y dispuestos a ser reclutados por el mayor postor, sea Estado, ejército, empresa o institución situada en el lado de la legalidad.
- Estos organismos legales se ampararán en los hackers, quienes muestran su saber y su eficacia para librar auténticas batallas en el ciberespacio. Algunos de estos parece que persiguen ser contratados por quienes defienden el bien, el Estado de derecho, las libertades y los derechos humanos
- Junto a éstos se sitúan, enfrente, toda clase de organismos oficiales, grupos, técnicos, personas, etc, de la misma manera dispuestos a perpetrar ciberataques con determinados fines, enclavándose en el lado no legal. De similar manera pueden pretender ser reclutados por instituciones, Estados, empresas, etc, cuyos objetivos están fuera de la ley y del sentido ciudadano más elemental.
- El fenómeno del ciberterrorismo es emergente y se consolida a pasos agigantados. Se ha de distinguir este ciberterrorismo en estado puro, caracterizado por agresiones contra objetivos concretos en unos casos y algo difusos en otros.
- Junto a este ciberterrorismo, se alinea el empleo de la Red para todas las labores de captación, adiestramiento, comunicaciones, etc, por parte de organizaciones de carácter terrorista. Esto le confiere a otros tipos de terrorismo una especie de plus, al valerse de las estructuras específicas que la Red le ofrece, de tal

forma que avanzan muy rápidamente en la consecución de sus fines (Betz y Stevens, 2011; Kramer, Starr y Wentz, 2009; Rattray, 2001; Caro Bejarano, 2012; Miró, 2012).

De acuerdo con este breve y sintético recorrido por la reciente investigación al respecto, cuesta poco creer que la ciberguerra es una realidad actual, que parece ir en crecimiento, lo cual la haría salir de acciones u operaciones selectivas y muy concretas a otro amplio terreno de actuación. La ampliación de su proyección puede llevar a acciones entre:

- Dos países entre si.
- Más de dos países entre si.
- Un país o más de uno contra una empresa o institución o más de una.
- Uno o más países, instituciones o grupos contra una coalición (por ejemplo, la OTAN).
- Coaliciones entre si.
- …

Las posibilidades pueden verse multiplicadas hasta un extremo, en tanto actualmente se produce un claro desarrollo institucional y corporativo con intereses en la Red o a través de ella. Cuanto más evoluciona la Red y sus usuarios, mayor es el riesgo de que sea empleada para cometer algún tipo de cibercrimen. Si se lleva esto a las relaciones y marco de intereses de Estados y grandes instituciones, primando lo macro-corporativo, las posibilidades de que se perpetren ciberataques de gran calado aumentan.

Una deducción a primera vista, tras un análisis de los estudios elaborados y publicados lleva a entender que la ciberguerra, en sus diferentes acepciones, irá en aumento. Se presupone que las estadísticas que son accesibles al usuario medio de la Red sobre intrusiones y ciberataques son ciertas. La forma de percibir este riesgo posiblemente vaya más allá de su contemplación en tiempo real, cuando los analistas comprueban el nivel de saturación o de disminución de tales ciberataques. Es aconsejable captar estos detalles por diferentes medios en la Red, en cuanto que unos y otros pueden diferir en la cuantificación del fenómeno. A la mano de los internautas estaban los mapas de ciberataques en tiempo real que elaboraban Norse y también Kaspersky, lo cual ha ayudado a muchas organizaciones a monitorizar, constantemente, la situación mundial en este aspecto.

La Red contiene, además, sobradas noticias, producidas en diferentes momentos en el último lustro, sobre la ciberguerra emergente, así como acerca de quiénes y cuáles serían sus principales actores. Basta con una revisión en la Red, en fuentes abiertas, de los comunidados, conferencias, entrevistas, etc, protagonizados por personajes como John McAfee y Eugene Kaspersky, quienes hacen hincapié en el creciente peso de las actividades de ataques en la Red. En alguna medida incluso se llega a valorar la importancia adquirida, así como su poder de ciberataque, de grupos como Daesh, en tanto se apunta que su grado de dominio de técnicas y de procedimientos para empleo de la Red en pro de sus propios fines, así como de efectuar acciones de ciberterrorismo es muy sólida. Al lado de este tipo de afirmaciones se ha puesto en duda la capacidad defensiva de países occidentales en tal ámbito, como es el caso de Estados Unidos.

Desde un punto de vista del análisis de inteligencia, no se ha de descartar que algunas de las apreciaciones emitidas que ponen énfasis en afirmar la falta de preparación integral de algunos países occidentales y de sus agencias de seguridad y ciberseguridad, pueden ser simples estelas conducentes a poner de relieve la imperiosa necesidad de apoyarlas con más medios, técnicos y humanos, para desequilibrar una balanza que cada vez se escora más hacia el lado no deseado por las democracias occidentales y los países democráticos en general. Reconocer las propias limitaciones y estrecheces presupuestarias al respecto es una forma nítida de acercarse a declarar que es preciso potenciar las agencias de ciberseguridad, tal vez confinadas a contar con presupuestos muy limitados y con un personal altamente cualificado, aunque notablemente escaso.

Sin entrar en ninguna apreciación sobre debilidades y vulnerabilidades en dicho terreno, un factor muy importante de la disuasión consistiría en mostrar una parte neta de las fuerzas y recursos con que se cuenta,

así como ofrecer muestras evidentes de un poder de neutralización de ciberataques y de repeler los mismos. Todo esto sin que quede atrás la capacidad operativa –no teórica- de efectuar ciberataques en los casos en que se estimase necesario. Como se ha indicado, los factores preventivo, disuasor, reactivo y proactivo han de estar suficientemente claros como para no ofrecer dudas a hipotéticos ciberatacantes.

5. Necesidad de regulación del ciberespacio a partir del Manual de Tallín

Sobre la necesidad de regular el ciberespacio se ha debatido en muy diferentes foros y desde distintos enfoques. Se constata desde la visión puramente geoestratégica, con aditamentos de carácter militar, a la constituida por aspectos económicos y políticos. El mundo del Derecho ha venido insistiendo en que la utilización del ciberespacio es algo que debe ser regulado y trasladado a acuerdos, tratados, códigos, etc. Ha de existir una ciberética que haga posible las actuaciones dentro de un conjunto de intervenciones consideradas válidas, legales y proporcionadas. Mientras, esa misma ética debe poner de manifiesto qué se considera como contrario a un recto proceder y, por tanto, situarlo al margen de la ley. No obstante, las leyes que regulen el ciberespacio y las actuaciones en el mismo podrían ser consideras con tal laxitud que una interpretación y otra pudieran ser diametralmente opuestas. Por ello es fundamental que las grandes potencias, que a su vez pueden ser los más sólidos poderes en el ámbito hipotético en que se desarrollase la ciberguerra, han de ponerse de acuerdo y no transgredir las normas de que ellas mismas se hayan dotado.

Por todo esto, la OTAN elaboró el denominado Manual de Tallín, hecho público en 2013, que venía a describir las líneas más destacadas alrededor de esta ética que la situación reclamaba y que era imprescindible por escrito. Cabe preguntarse si esto se puso en marcha solo como un hecho formal, es decir, sin muchas intenciones de llevar a la práctica unas reglas que pongan coto a las posibles acciones a desarrollar o, por el contrario, en todo esto se debería contemplar una rotunda convicción de evitar grandes desastres (Klimburg, 2012; Schmitt, 2013).

Desde una perspectiva meramente humanitaria, parece claro que la regulación que se alude es absolutamente necesaria, y que esto, llevado a la materialidad debe dar como resultado un impacto y redundar en buenas prácticas, unidas al marco de la Ciberseguridad y la Ciberdefensa.

La OTAN ha querido dejar patente cómo y cuál sería su respuesta en caso de verse atacada en y desde el ciberespacio, entendiendo que tal ataque podría ser de carácter preventivo. Desde luego, a los ojos de quienes están fuera o al margen de las estructuras defensivas de la OTAN, tal vez fuese extremadamente complicado, y hasta difuso, establecer las líneas divisorias de lo que constituyera dicho ataque preventivo (Ganuza Artiles, 2011; Mazo, 2013).

Aunque las Convenciones de Ginebra, sobre la guerra convencional, fueron capaces de poner de acuerdo a diferentes naciones, ello no implicó que todas cumplieran con sus dictados. La guerra ha dado pie a la elaboración de documentos y normas que, ratificados por los gobiernos de diferentes Estados, han contribuido a reducir los efectos más terribles de las contiendas, aunque no han impedido que estas se produzcan.

Si se traslada una estructura normativa al marco de la regulación del ciberespacio y de las actuaciones a través del mismo, se sabe que lo logrado, inicialmente, puede ser mejorado, ampliado, matizado, puesto al día conforme aparezcan nuevas amenazas en la Red, etc. Aunque todo esto es muy probable que no evite confrontaciones. Al menos existirá un modelo para encajar dentro del mismo las actuaciones correctas y fuera las que se lleven a cabo lejos de sus parámetros. Por tanto, cabe esperar que este tipo de reglamentaciones tenga un futuro de largo recorrido, y que se vayan ampliando y perfilando de la mejor manera posible.

Alrededor de estas cuestiones parece que se ha ido imponiendo un criterio regulador, es decir, que debían imponerse unas normas, unas reglas, unos parámetros por los cuales regirse, orientándose a minimizar los daños que pudieran producirse. Hasta hace pocos años se venía argumentando que un enfrentamiento en la Red no tenía por qué adquirir unos tintes excesivamente dramáticos.

Sin embargo, en el momento actual, no se duda al respecto de que un conflicto que tuviese como escenario la Red puede resultar fatal para quien lo sufra. Se ha argumentado que ello con tendría que conllevar la pérdida de vidas humanas, aunque cabe pensar que la paralización de ciertas infraestructuras críticas podría implicar esa catástrofe.

Si se tiene en cuenta la larga relación de realidades constatadas en los ciberataques, y muy especialmente las que se han estudiado con mayor detenimiento, esto lleva a considerar que se podría pasar, en unos casos, de un colapso en cuanto a no operatividad de servicios básicos para una comunidad, para una sociedad, e incluso para todo un país, a otras situaciones en las que la no operatividad de determinados servicios básicos conectados con determinadas infraestructuras críticas, podría implicar un desastre de carácter humanitario, y que de ello se podría alcanzar una situación de verdadero riesgo vital para las personas.

A partir de aquí, estas ciberamenazas se han llegado a particularizar en distintos centros de interés, desde las infraestructuras críticas de un país o zona concretos, hasta la denegación de servicio con lo que esto implica en cuanto imposibilidad de ejecutar cualquier tipo de operación necesaria para los ámbitos de transportes, económicos, financieros, suministros de agua o electricidad, etc, en lo que se puede entender como aspectos palmarios de la vida cotidiana.

Desde una perspectiva teórica sobre lo que podría suponer este nuevo modelo de guerra, la cibernética, hay que pensar que como todo, incluidas aquí las guerras convencionales, ha de someterse a una regulación que tenga presente unas normas básicas.

La cuestión inherente a estos planteamientos radica en qué ocurriría si, a pesar de la regulación mediante este tipo de normas, no se produce el previsto y conveniente acatamiento de las mismas. De hecho, la ciberguerra, tal como en estos momentos puede ser concebida y ejercida, puede llegar a convertirse en un espacio en el que no existan, o no estén suficientemente nítidos, los parámetros de acatamiento de lo que sea considerado como un mínimo exigible en el modelo de una sociedad democrática, que se caracterice por el respeto a los derechos humanos. No hay que dudar que la realidad hoy imaginable de la ciberguerra, caracterizada por ciberataques de gran envergadura, puede violar los derechos más elementales de las personas a disfrutar de determinados bienes. En cierto modo, a través de estas acciones, se producirían violaciones de los derechos de las personas.

Por otro lado, la conciencia sobre la ciberguerra, en occidente y países democráticos, abunda en el pensamiento de que no parece claro que en los países con menos recursos, y con menos estándares de calidad democrática y de derechos humanos se esté muy por la labor de someterse a unas normas sobre el uso del ciberespacio. Se sabe que un país con un nivel de escaso desarrollo puede, no obstante, elaborar toda una estructura que le permita llevar a cabo determinados tipos de ataques en la Red. Además, esto se conectaría con una falta de acatamiento de las normas establecidas por la comunidad internacional, o por algunos de los miembros más destacados de la misma.

Si se agrega a este supuesto que estos países se hallen distantes del respeto a los derechos humanos, y del Derecho Internacional Humanitario, en general, estaríamos ante un perfil muy claro de quién no respetaría esas hipotéticas normas para el ciberespacio. Sus reglas y las de países democráticos distan mucho. Incluso cabría considerar las proximidades que existen entre los factores definitorios de la ciberguerra y algunos de la ciberdelincuencia. Esto debe inducir a la comunidad internacional a dotarse de unas reglas al respecto.

Abundando en estos aspectos, e ilustrando esta dinámica, se constata la propuesta de Eugene Kaspersky, realizada en junio de 2012, en torno a que se lleve a cabo un acuerdo o pacto internacional que regule lo que se ha denominado "ciberarmas". Como cabe extraer, no contó con los convenientes respaldos, ni siquiera por parte de las que hoy se consideran potencias mundiales, algunas de las cuales argumentan y esgrimen de continuo su talante democrático y conciliador, en aras de la paz.

En el marco estrictamente normativo parece que se reconoce la ciberguerra como un elemento de gran peligrosidad para la humanidad. Se reconoce, al mismo tiempo, que los efectos de un ciberataque pueden ser materialmente tan nocivos y letales como los generados en el ámbito de las guerras consideradas estrictamente convencionales. Se ha puesto de modelo, a modo de ejemplo y en repetidas ocasiones, un ciberataque a una central nuclear, o bien a estructuras marcadamente sensibles, como transportes de variada tipología, dentro del campo de las infraestructuras críticas. Se trata, en un sentido similar, de ciberataques a instalaciones industriales complejas que implican sustancias nucleares, químicas, biológicas, etc. Las consecuencias podrían llegar a ser devastadoras y hasta letales.

En diferentes medios de comunicación se ha recogido, y trasladado a través de variadas fuentes, que voces altamente autorizadas como la de Eugene Kaspersky alertan y ponen énfasis sobre una especie de carrera de armamentos en el marco de lo cibernético, es decir, una carrera ciberarmamentista, y ello conlleva, inevitablemente, una imperiosa necesidad de regulación (Segura y Gordo, 2013).

Contemplado desde esta orientación, es imprescindible poner orden en unas cuestiones catalogadas como de alta peligrosidad. El Manual de Tallín es algo más que una intención para poner en funcionamiento mecanismos que regulen la actividad en el ciberespacio. Por muy contestado que fuese en el momento de su edición, nadie puede negar la necesidad de un instrumento de su naturaleza y categoría. Otra cuestión muy diferente es que haya que mejorarlo o completarlo.

En términos muy concretos, y como especie de pautas compiladas, el Manual de Tallín aborda aquello que la Alianza Atlántica ha considerado que puede estar permitido y aquello que debe estar prohibido en el ámbito de la ciberguerra.

Un factor que puede ser relevante de la ética aparentemente impresa en el Manual de Tallín es que se propone deben excluirse de los ciberataques las instalaciones dedicadas a la producción de energía eléctrica para usos civiles, o aquellas destinadas al mantenimiento de la vida y la salud de las personas, o sea, algunas de las infraestructuras críticas que pueden devenir en algo marcadamente vital (Ahijado, 2013).

Otro factor de enorme importancia radica en la propuesta de que las respuestas sean proporcionales a los ciberataques, y nunca fuera del espacio en que se intenta responder. Esto, de forma transparente, implica un freno a las posibles respuestas ante los ciberataques.

La respuesta de algunos países, como el caso de Rusia, se plasmaron en afirmar que la OTAN había realizado un movimiento que suponía legitimar la ciberguerra, en tanto subrayaba determinados aspectos acerca de la aplicación de pautas y normas derivadas del Derecho Internacional, aplicándolas al ámbito de la ciberguerra. Esto, se afirmaba, podría resultar altamente complejo y hasta peligroso. La polémica estaba servida, aunque, aparte de esta aparente propuesta rusa, no se llegó a realizar una aportación que mejorase sólidamente la elaborada por la OTAN. Naturalmente, esto no quiere decir que no sea posible efectuarla.

Si se tiene en cuenta este planteamiento de las autoridades rusas, cabe apuntar que se realizaba bajo la afirmación de que Rusia se encontraba efectuando notables esfuerzos a favor de evitar o impedir que el ciberespacio se convirtiese en un campo definido y orientado hacia la militarización a ultranza. Visto con la perspectiva que hoy se tiene desde su edición, en cierta forma esta formulación venía a significar un rotundo rechazo a lo que entonces provenía de la Alianza Atlántica. A la vez, se podía entender como una llamada de atención a la realidad de que Rusia y otros países, algunos de ellos potencias mundiales, deberían haber sido tenidas en cuenta para elaborar documentos tan cruciales como los que regulen el ciberespacio, tal vez como única forma de conducirles hacia el acatamiento de las limitaciones que se proponen al respecto en el uso del ciberespacio.

Partiendo de lo abordado en el enfoque y el contenido del Manual de Tallín, en cuanto al Derecho Internacional Humanitario, se traduce que las víctimas o las autoridades competentes, podrían acusar a quienes

cometiesen determinados ciberataques (Reguera Sánchez, 2015).

Al mismo tiempo, se concibe que quien padece el ciberataque puede recurrir a contramedidas o actuaciones proporcionadas en el ciberespacio. Cabe resaltar lo de proporcionadas. Quedarían, por tanto, excluidas las contramedidas que supusieran un avance en el grado de concepción, extensión y profundidad, así como en los daños que pudieran provocar.

Si desea poner un ejemplo que no presente lugar a dudas en cuanto a definición de qué es un acto de fuerza en el ciberespacio, lo fijaron los autores del Manual de Tallín en el ataque perpetrado con el virus Stuxnet contra Irán en 2009, aunque no se explicitaba el origen del mismo. Los medios de comunicación de diferentes países señalaban que este provenía de Estados Unidos e Israel.

La dirección de la elaboración del Manual de Tallín recayó en Michael D. Schmitt, profesor de la Escuela de Guerra Naval de Newport (Estados Unidos).

Los principales objetivos del Manual de Tallín se concretan en:

• Cubrir un amplio espacio vacío, o sea, una laguna en el marco de la Ciberseguridad y la Ciberdefensa, recogiendo los principales logros en materia de Derecho Internacional aplicado al ciberespacio y la Red.

• Redefinir e interpretar aquello que había alcanzado hasta el momento de su publicación sobre las normas relativas a los ciberataques.

• Vincular, de una manera adecuada el contexto de la Ciberseguridad y la Ciberdefensa con el marco legal subyacente a lo que se conoce como ciberguerra.

• Lograr un consenso entre los países para un entendimiento sobre la aplicación de los recursos en el marco de la Ciberdefensa y la Ciberseguridad.

• Definir límites dentro del terreno del consenso ético en este campo.

• Marcar los límites de lo que se ha entendido en este ámbito como ciberguerra, agresión armada y empleo de la fuerza.

• Rellenar un espacio legal desde el consenso, en la dirección de anticiparse a las posibles acciones en la Red en cuanto a Ciberseguridad y Ciberdefensa.

• Ofrecer una adecuada herramienta para quienes se encuentran en el campo jurídico, de cara a alcanzar una visión general sobre los principales problemas en la ciberguerra y la Ciberdefensa.

• Matizar con claridad los acuerdos y los principales desacuerdos entre los especialistas en esta área de conocimiento.

• Dejar patente que no era un documento oficial que recogiese o reflejase la doctrina oficial de la Alianza Atlántica, como tampoco lo era de los países miembros de la misma, sino más bien que recogía la visión y la opinión de un Grupo Internacional de Expertos (GIE).

• El denominado Manual de Tallín lo integran 95 reglas, agrupadas en dos partes: La Seguridad del ciberespacio en el Derecho Internacional, y El Derecho Internacional de los conflictos cibernéticos. Esto se articula a lo largo de siete capítulos. Desde un punto de vista formal, diversos especialistas han destacado que algunas de las reglas del Manual reflejan elementos o artículos ya insertos en convenios internacionales sobre la materia. En otros casos se realiza una especie de adaptación de normas previamente existentes a la situación del ciberespacio. Se agregan comentarios que sirven para orientar la asimilación de cada propuesta, así como las principales fuentes empleadas, todo ello matizado desde la perspectiva del Derecho Internacional Humanitario.

• Los núcleos principales que se tratan en el Manual llevan a diferentes especialistas en la materia a agruparlos en los siguientes enunciados, que obran en el sentido de articular las distintas áreas que se han tratado, entre ellos:

• El sentido de ciberataque y las contradicciones y conflictos que se pueden derivar desde la interpretación a partir del Derecho Internacional Humanitario.

• Los conceptos de responsabilidad y de soberanía de cada una de las partes que intervienen.

• El concepto y el sentido de uso de la fuerza, partiendo de indicios que ayudan a entender o valorar si

una determinada acción en el ciberespacio constituye o no uso de la fuerza: la gravedad; la inmediatez; la intrusión y el grado de penetración o alcance de las operaciones.

- El concepto y el sentido de ataque armado.
- El concepto y el sentido de la legítima defensa y su relación con la inminencia y la inmediatez.
- El principio de necesidad y de proporcionalidad.
- La participación directa en las acciones u hostilidades.

6. La regulación de la ciberguerra desde la perspectiva del Derecho Internacional Humanitario y el Manual de Tallín

A partir de la edición del Manual de Tallín se pueden efectuar algunas acotaciones sobre sus contenidos y los valores que en el mismo se recogen, entre estos:

• El Manual de Tallín se inscribe en una Política de Seguridad que parte de la ética aplicada al ciberespacio. Suponiendo que la Red sea un espacio de libertades y de amplísimas opciones para personas e instituciones, es preciso aplicar unos criterios éticos que hagan posible que esta no se emplee desde perspectivas contrarias a una ética elemental. Esto no quiere decir que en la Red solo se vayan a constatar actitudes y comportamientos acordes con las leyes ni con la ética consensuada. Habrá de todo, aunque los Estados de la Alianza deben comprometerse a seguir los pasos de un modelo ético imperante en occidente y en el marco de la democracia.

• Como una derivación de lo anterior, la libertad en el ciberespacio ha de encontrar determinadas barreras, acotaciones, límites, impedimentos, etc. Algunas de estas cuestiones pueden estar muy claras, si tenemos en cuenta la propia esencia de la Seguridad, es decir, no transgredir los límites a partir de los cuales se podría poner en juego la propia libertad y la seguridad.

• El binomio libertad-seguridad ha de estar presente en las acciones y operaciones en el ámbito del ciberespacio, de una manera extensa y precisa a la vez. Habría que lograr no perder en ninguna de las dos direcciones de este binomio, dentro de los cauces establecidos por el Derecho Internacional.

• Resulta imprescindible saber delimitar las posiciones que se ocupan en cuanto a presencia y tareas o acciones en la Red, valorando que aparecen fenómenos como el cibercrimen. En este campo encontramos las variantes de los ataques informáticos que más abundan en la Red, como el phising, los troyanos y los malware. Si en los primeros casos se hacen los delincuentes con contraseñas para acceder a información determinada, el último avanza en la Red de forma alarmante, bajo la forma de virus, troyanos, puertas traseras, programas espías, gusanos, etc. En este ámbito del cibercrimen parece que algunos países sufren mayores ataques que otros, cuestión relacionada con aquello que los ciberdelincuentes pretenden obtener. Se constata en algunas publicaciones que países como Rusia, China, Sudáfrica o Estados Unidos se llevan una parte considerable de los ciberataques, aunque no quedan atrás Israel y España, junto con otros países europeos o algunos emergentes de otros continentes. Esta somera relación puede ir evolucionando en los próximos años, dado el potencial que algunos países emergentes constituyen en el ciberespacio, así como el interés que los contenidos de que disponen y sus infraestructuras críticas, industriales, etc, pueden ocupar (Urueña Centeno, 2015).

• Como un ámbito muy específico, el ciberterrorismo se percibe marcadamente al alza en esta situación de la Red. No parece que se halle conectado directamente, en todos los casos, con intencionalidades económicas, sino más bien políticas, al procurar despertar el miedo en el atacado. Desde la perspectiva de las amenazas conectadas con factores ideológico-religiosos, ha tenido en los últimos años un importante auge esta modalidad de ciberdelincuencia, en tanto se mueven a sus anchas quienes llevan a cabo prácticas de reclutamiento, adoctrinamiento, propaganda, comunicaciones, financiación, etc. Es factible conectar esto con la importancia creciente en determinados conflictos, muy ideologizados o con profundo matiz religioso, de la Red para ser empleada en todos estos territorios, y en otros muchos más. En el marco de las guerras actuales se puede entender que la supremacía en los terrenos aludidos viene a ser determinante en el desarrollo de las contiendas entabladas. En caso de no existir ninguna regulación se puede caer en el extremo de que sean permitidas las acciones claramente contrarias a la ética y a las normas de que se han dotado los Estados democráticos.

• Muy en conexión con lo anterior se encuentra la denominada ciberguerra que, como se ha señalado, es un concepto más que una realidad, aunque se constaten materializaciones que la corroboran. En puridad, esta ciberguerra puede ser coyuntural o permanente. Puede afectar a estructuras de comunicación sensibles o

menos sensibles. De lo que no podemos dudar es del enorme daño que se puede llegar a producir a partir de las acciones de un hipotético oponente o un enemigo. Algunos especialistas apuntan a que los países desarrollados se aprestan a poner en pie verdaderos ejércitos de expertos en esta ciberguerra, así como contar con medios materiales que les permitan afrontar las situaciones previsibles dentro del marco de aquella. Una cuestión muy diferente es que un Estado, o la propia Alianza Atlántica, se encontrase en un futuro ante situaciones que no pudieran contrarrestar porque los ciberataques fuesen de tal envergadura, o de una selectividad tal que resultase imposible neutralizarlos. Claro está que a los países democráticos se les exigirá que el combate se ciña a unas reglas, y que se utilicen unos medios proporcionales. Por tanto, queda en el aire la duda acerca de si los atacantes, con mayor o menor preparación, pericia y medios se comportarían con ética y cierto sentido de no alcanzar un daño extremo en el atacado. Verdaderamente, quien ataca parece que está dispuesto a llegar a las consecuencias que sea posible alcanzar. Algunos de dichos ciberataques se cometerán por mera cuestión de prestigio, o de oportunidad, o persiguiendo un logro que sitúe a sus autores en el parnaso de los técnicos que se disputaría cualquier agencia de Seguridad de los países desarrollados. No hay que olvidar que se empleen ciberataques con un matiz preventivo, disuasorio o con el cariz de que se acompañen, precisamente para mostrar al oponente la fuerza con la que se cuenta (Barat-Ginies, 2013).

7. Conclusiones

Dada la naturaleza de la temática tratada las conclusiones solo pueden ser provisionales, en función de que se está ante algo en constante evolución.

La ciberguerra es presente y es futuro. No cabe duda que los países desarrollados tienden hoy y pueden tender, igualmente, en un futuro inmediato, a construir todo un sistema de medios que les permitan repeler posibles agresiones en el ámbito del ciberespacio, y lo mismo cabe señalar en cuanto a su capacidad de ataque. Esto último se encauza, en un sistema democrático avanzado, a mostrar la cualificación tal que pueda ser empleada como medio de disuasión ante oponentes cibernéticos.

Como se ha indicado, el Manual de Tallín ha sido contestado desde determinadas perspectivas que pueden estar interesadas en la no regulación del ciberespacio en sentido estricto y partiendo del Derecho Internacional Humanitario. Esta regulación resulta imprescindible.

Desde la pura lógica, cabe pensar que los países en los que brilla por su ausencia este Derecho, o se ha constatado que a lo largo de años, de décadas, han contribuido a la desestabilización de sistemas políticos y económicos, o que han participado directa o indirectamente en conflictos desde una óptica claramente expansionista, anexionista, etc, pueden estar en el marco de quienes no aboguen por una regulación del ciberespacio, precisamente para actuar a sus anchas.

Puede representar un cierto valor el que países como Rusia reclamen que se les tenga en cuenta a la hora de la elaboración de un documento tan crucial como el Manual de Tallín. Se trata de una aspiración legítima el que se desee estar presente en el foro en el cual se pone de relieve la tan traída y llevada necesidad de regulación del ciberespacio.

No obstante, los intereses no deben ir únicamente dirigidos a estar presente en la regulación de la denominada ciberguerra. En puridad se debería acometer, internacionalmente, la labor de poner claridad acerca de todo lo referente a la regulación del ciberespacio, incluyendo, por supuesto, los aspectos relativos a la ciberguerra.

La revisión de notas de prensa emanadas de distintos países ajenos a la Alianza pone de manifiesto y en candelero que se hace precisa una pronta restauración de las confianzas mutuas entre Estados, sean o no pertenecientes a la OTAN. De lo que se trata es de que se alcance un consenso mundial sobre la materia del ciberespacio, y la ciberguerra, en particular partiendo de los conceptos básicos y consensuados de Ciberseguridad y Ciberdefensa. Si no se tiene en consideración a todos, o a una inmensa mayoría, referida a

países, organizaciones internacionales, personalidades relevantes del ámbito de la ciencia y de la técnica y, en general, a los principales actores actuales del escenario del ciberespacio, difícilmente se podrá alcanzar un acuerdo sólido y duradero, es decir, el consenso que es preciso.

Cómo citar este artículo / How to cite this paper

Domínguez, J. (2016). La ciberguerra como realidad posible contemplada desde la prospectiva. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 1(1), 18-32. (www.cisdejournal.com)

Referencias

Ahijado, C. (2013). El primer manual de ciberguerra por encargo de la OTAN. ALTICNATIVA. (http://www.lahuelladigital.com/alticnativa/el-primer-manual-de-ciberguerra-por-encargo-de-la-otan/)

Assange, J.; Appelbaum, J.; Müller-Maguhn, A.; Zimmermann, J. (2014). Cypherpunks: Freedon and the Future of Internet. OR Books, New York-London.

Barat-Ginies, O. (2013). Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a 22 de noviembre de 2012, trad. Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra, Madrid, traducción número 13-0623.

Betz, D.; Stevens, T. (2011). Cyberspace and the State: Toward a strategy for cyber-power. Adelphi Series, 51(424).

Caro Bejarano, M. J. (2012). Ciberdefensa. Equipos de Respuesta Inmediata de la OTAN. Documento Informativo 16/2012, Instituto Español de Estudios Estratégicos.

Clarke, R. A.; Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins Publishers, New York.

Ganuza Artiles, N. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN, en Ciberseguridad, retos y amenazas a la Seguridad Nacional en el Ciberespacio, Cuadernos de Estrategia 149. Instituto Español de Estudios Estratégicos (Ministerio de Defensa) – Instituto Universitario General Gutiérrez Mellado, Madrid, 166-214.

Klimburg, A. (2011). Mobilising Cyber Power. Survival, 53(1), 41-60.

Klimburg, A. (2012). National Cyber Security Framework Manual. NATO CCD COE Publication, NATO Cooperative Cyber Defence Centre of Excellence. Tallinn.

Kramer, F. D.; Starr, H.; Wentz, L. (eds.) (2009). Cyberpower and National Security. Potomac Books Inc, Washington DC.

Libicki, M. (2007). Conquest in Cyberspace. National Security and Information Warfare. Cambridge University Press, Cambridge.

Libicki, M. (2009). Cyberdeterrence and cyberwar. Rand Corporation, Santa Monica.

Libicki, M. (2011). Cyberwar as a Confidence Game. Strategic Studies Quarterly, 5(1), 132-146.

López, P. (2006). El Ciberespacio y su Ordenación. Grupo Difusión: Difusión Jurídica y Temas de Actualidad, Madrid.

Mazo, A. (2013). La Ciberseguridad en el contexto de la OTAN y la UE. Ponencia del XXVI Curso de verano - Universidad Complutense Madrid (julio de 2013) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. (http://www.ieee.es/Galerias/fichero/cursosverano/ElEscorial2013/Ciber_Escorial_Mazo.pdf)

Miró, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons, Madrid. (https://www.marcialpons.es/static/pdf/9788415664185.pdf)

Monografías del CESEDEN (2012). Los Ámbitos no Terrestres en la Guerra Futura: Espacio. Ministerio de Defensa.

Rattray, G. J. (2001). Strategic Warfare in Cyberspace. MIT Press, Boston.

Reguera Sánchez, J. (2015). Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario, en Grupo de Estudios en Seguridad Internacional. Universidad de Granada, Análisis GESI 7/2015.

Rexton Kan, P. (2014). Cómo analizar la guerra en Wi-Fi. De ciberguerra a Wikiguerra: la lucha por el ciberespacio. Military Review, Septiembre-Diciembre, 30-36.

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.

Rid, T. (2013). Cyber War Will Not Take Place. C. Hurst & Co.

Segura, A.; Gordo, F. (coords.) (2013). Cibereseguridad Global. Universidad de Granada, Granada.

Torres Soriano, M. R. (2011). Los dilemas estratégicos de la ciber-guerra. Ejército, LXXII(839), 14-19.

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, New York.

Urueña Centeno, F. J. (2015). Ciberataques, la mayor amenaza actual. Documento de Opinión 9/2015, 16 de enero de 2015, Instituto Español de Estudios Estratégicos.