La 'ciberguerra' se puede evitar

Henning Wegener

El concepto de *ciberguerra* está de moda en todo el mundo. Con él se relaciona una vaga sensación de creciente amenaza de un enemigo invisible, en el que no se distingue entre WikiLeaks, *cibercrimen* profesional, *hackers* o la utilización militar de tecnología digital. La idea de estos nuevos peligros alude a pronósticos apocalípticos, una amenaza existencial al individuo y a la economía, al Estado, a la sociedad, a meros fallos o averías en sectores. En cualquier caso, la ciberguerra se percibe como algo terrible. Razón suficiente para un nuevo análisis de los riesgos, y también para una definición más precisa. La especificidad del uso militar, la amenaza para la *ciberestabilidad* mundial, solo pueden ser abarcados si se contempla en su totalidad la evolución del espacio digital.

En el número 80 de *Política Exterior* (2001) publiqué "La guerra cibernética", el primero y hasta ahora único artículo sobre esta cuestión, en el que analizaba los nuevos peligros y amenazas. Las advertencias que entonces se hicieron sirven también para hoy, ya que la estructura básica de Internet y sus características técnicas se mantienen inalterables. Las nuevas tecnologías de la información siguen ejerciendo su potencial como transmisor y

Henning Wegener ha sido embajador de Alemania en España (1995-99).

El espacio digital aparece como el quinto escenario bélico, junto a la tierra, el mar, el aire y el espacio exterior. Hoy el ciberespacio es indispensable para cualquier planificación estratégica y exige un nuevo tipo de 'ciberdiplomacia' y una legislación internacional.

factor de crecimiento del conocimiento global, como estimulador de sociedades más abiertas y participativas, como globalizador del mercado y mensajero de valores universales. Pero también el abuso y las probabilidades de ataque y sus graves consecuencias crecen.

Un espacio transformado

¡Pero, qué aluvión de nuevos y exponenciales desarrollos desde entonces, a pesar de que los fundamentos permanezcan invariables! No es exagerado hablar de la pasada década como una segunda revolución digital, una revolución de enorme dinamismo y de resultados aún desconocidos que continúa avanzando. Al menos ocho características esenciales del espacio digital se han transformado radicalmente y deben ser analizadas.

1. En nuestro análisis de 2001 había en el mundo unos 500 millones de ordenadores con conexión a Internet, un Internet que operaba esencialmente como único soporte de la comunicación digital. Hoy, poco más de una década más tarde, hay 2.000 millones de ordenadores con capacidad de conexión a estructuras de redes con bandas mucho más anchas y que disponen de una capacidad de almacenamiento de tamaño inmenso. Todavía mayor es el número de aparatos móviles, como los teléfonos con conexión a Internet, ordenadores de bolsillo, tabletas y demás aparatos sin

cable. La separación entre las diferentes plataformas digitales va desapareciendo. Los aparatos móviles y fijos convergen, telefonía y televisión digital funcionan por Internet, y todo ello produce un universo digital entrelazado. Es posible que en esta década se alcancen los 20.000 millones de soportes digitales, casi tres veces la población mundial.

2. Pero no solo los ordenadores y procesadores pertenecen a la categoría de equipos conectados susceptibles de ser atacados y manipulados desde fuera. Tenemos que incluir cada microprocesador, como por ejemplo los miles de millones de sistemas incorporados (*embedded systems)* en productos tecnológicos, los sensores con chip activos y pasivos, los también miles de millones de RFID (más comunmente llamado Radio Frecuencia, es la forma que tiene de comunicarse los objetos modernos) con cada vez más capacidad. Asimismo hay que incluir el "Internet de los objetos": cada vez más máquinas y objetos de uso diario están conectados y pueden ser manipulados desde fuera. Calefacciones, aires acondicionados, lavadoras, aparatos médicos que recogen datos y dan indicaciones, son en esencia tan vulnerables como los ordenadores u otros aparatos con conexión a Internet. Más aún, los desarrollos tecnológicos etiquetados como *next generation* indican hacia dónde nos lleva cuantitativamente este viaje: ultraminiaturización de circuitos digitales, instalación masiva de procesadores con múltiples centros, aumento de las aplicaciones de fibra de vidrio, rápido crecimiento de los transportes de datos móviles, el desarrollo de nuevos y potentes aparatos *smart* (inteligentes), ubicuidad de nuevos elementos de computación cada más miniaturizados, que también configurarán nuevas y variadas estructuras y mecanismos de redes digitales (entre otras las llamadas *artificial neural nets* o redes neurales artificiales), la biometría, minicomputadores cosidos a los vestidos o instalados en gafas, la construcción de ordenadores minúsculos que se organizan autónomamente, comunicándose con otros aparatos digitales… Todas estas mejoras llevan un aumento explosivo del número de dispositivos digitales y una curva exponencial de conectividades, y con ello también un aumento de nuevas posibilidades de manipulación. El número de soportes en este grandioso mundo de redes podría pronto alcanzar los 50.000 millones.

3. En los Estados más técnicamente desarrollados se incluyen en esta red, en la total penetración de la economía y de la sociedad, las infraestructuras públicas, sobre todo el suministro eléctrico, el sistema bancario y el sanitario, el tráfico aéreo y ferroviario, la red de agua, los embalses y la defensa. Todos ellos son gestionados de forma creciente a distancia, por Internet,

donde no se prevé un regreso a la utilización manual. En este mundo altamente industrializado e interconectado aparece una dependencia intensa. Con el crecimiento exponencial de las conectividades aumenta también exponencialmente la fragilidad. Las víctimas potenciales de los ciberataques son los nervios centrales de nuestra civilización.

4. Se ha producido un cambio realmente revolucionario respecto a los autores de la *ciberdelincuencia*. En lugar del autor solitario, a menudo jóvenes *hackers* con ganas de divertirse, aparecen hoy enormes organizaciones criminales profesionales y con medios técnicos y financieros ilimitados. Esta criminalidad organizada se concentra en pocos y conocidos países, y canaliza sus ataques anónimamente (*station hopping*) a través de otros países (principalmente Estados Unidos), utilizando por ejemplo a individuos en la red para blanquear el dinero. Estas organizaciones disponen de ficheros de direcciones de correo electrónico que pueden inundar con *spam*. Los correos *spam* no son solo una molestia para el usuario, sino un vehículo de transmisión de virus y otros programas dañinos (*malware*). Hace 10 años se contaban unas 40.000 variantes de virus, ya en 2008 la empresa de antivirus Panda fijaba su número en 13 millones. Se estima que cada dos segundos aparece en Internet un nuevo agente *malware*. Frente a estos, los programas de protección solo tienen eficacia contra las versiones conocidas. Estos nuevos agresores desarrollan tantas variantes, con capacidades técnicas mejoradas y tan rápidamente, que los sistemas de protección tienen que estar eliminando constantemente nuevas vulnerabilidades.

> En la pasada década cambió drásticamente la matriz entre ataque y defensa, y esto es una gran amenaza para la 'ciberestatalidad'

En la pasada década, a pesar de los avances en la industria de la seguridad, se ha cambiado drásticamente la matriz entre ataque y defensa, y esto es una mayor amenaza para la ciberestabilidad. El desarrollo más peligroso viene de los llamados *botnet*. El término se refiere a que el usuario no sabe que está infectado por un virus, que permanece dormido, hasta que el agresor en cualquier momento decida despertarlo (troyano). Los ordenadores se convierten en zombies, en robots, y permiten al cerebro criminal (*bot herder o bot master*) realizar en cualquier momento numerosas opera-

ciones. Los grandes *botnet* están rígidamente organizados. El número de ordenadores infectados por troyanos desconocidos en algunos países alcanza el 60 por cien. Algunas variantes del *software botnet* consiguen por sí mismas reclutar nuevos ordenadores para la red. Los *botnet* pueden al mismo tiempo movilizar un gran numero de ordenadores saturando las direcciones de e-mail de receptor, bloqueándolos o causando daños permanentes (*distributed denial of service*, DDoS), una forma de ataque ya practicado antes de 2001, pero ahora en una nueva dimensión).

Con ello no solo se pueden paralizar sectores enteros de la economía, sino atacar infraestructuras esenciales y las mismas estructuras de la red, dejándolas fuera de servicio con graves daños. Lo mismo sirve, y todavía más grave, para instalaciones del sector de la defensa. Estos *botnet* pueden alquilarse, previo pago, por otros criminales o Estados. Las tres posibilidades de uso de los *botnet* para el espionaje de datos, especialmente industrial y entre Estados, bombas lógicas y DDoS, son sencillamente aterradoras. En 2009, por ejemplo, apareció en 122 países el *botnet Conficker*, que con los medios de entonces no era atacable y que afectó a entre cinco y ocho millones de dispositivos.

5. Sin embargo, no se trata solo de cambios cuantitativos. Junto a la omnipresencia de las siempre nuevas variantes de *malware* y sus crecientes niveles de sofisticación, los agresores pueden usar la complejidad de los *software* comerciales, que en gran medida son utilizados también por los ministerios de Defensa. En los modelos de Microsoft 2001 los códigos tenían pocos millones de líneas, hoy Windows Vista posee más de 80 millones de líneas, sin que la seguridad inherente haya aumentado suficientemente. En consecuencia, el número de lagunas de seguridad, las puertas abiertas para ataques e instalación de bombas lógicas y troyanos han crecido. El desarrollo en el diseño de *software* más seguro, desde un punto de vista de la política de defensa, es una tarea ineludible.

6. Desde las funciones originales principales de la era digital –comunicación, información, operaciones de cálculo– hemos vivido en los últimos años una migración espectacular al almacenaje de datos en unas dimensiones sin precedentes. No solo es que cualquier aparato digital, incluyendo el *smartphone*, dispone hoy de una capacidad de almacenaje hasta ahora desconocida, sino que los datos de empresas, gobiernos e individuos son almacenados y administrados en grandes centros de datos externos ("en la nube", *the cloud*), donde la unidad de medida es el *petabyte* (1PB= 1.015 bytes), centros cuya localización y procesos internos apenas son conocidos,

cuyo procedimiento de gestión y almacenaje para el usuario individual es totalmente opaco y convierten a los tradicionales cortafuegos en inútiles. La cantidad de datos –que anualmente se duplican o triplican– pueden alcanzar fácilmente en un año o dos la totalidad de los datos de la historia de la humanidad. Las cuestiones de seguridad de tal masa de datos o de su suministro de electricidad no están resueltos de forma satisfactoria. Físicamente pero también virtual son claros objetivos de ataque.

7. Hay un salto cualitativo en el potencial de los daños por ataques digitales. Esto supone una verdadera amenaza a la economía. A pesar de que las cifras son oscuras, los expertos hablan de unas pérdidas anuales de al menos un billón de dólares. Es un cambio de la cantidad a la calidad, una amenaza sistémica, que muestra las dimensiones que puede tener una ciberguerra.

La tecnología de la información ofrece un enorme fortalecimiento de las fuerzas de combate a través de mejores comunicaciones

8. Un cambio decisivo desde 2001 es que más de 100 Estados han creado una capacidad cibermilitar nacional, en algunos de ellos con auténticos cibercomandos que, junto a las misiones de reconocimiento y del pilotaje del propio sistema de defensa están orientados hacia un dispositivo militar ofensivo *network-centric*. Su crecimiento parece imparable. Estos desarrollos pueden desprenderse en gran parte de la literatura abierta al público. Apoyarse de este modo en la moderna tecnología de la información supone un enorme fortalecimiento de las fuerzas de combate a través de la mejora de la comunicación, el rápido tramite de datos, la aceleración en las decisiones en el campo de batalla, el uso más efectivo de armas y un mejor control de escalada. Al mismo tiempo, los ataques digitales dirigidos pueden dañar al enemigo mediante ataques a sus infraestructuras de información críticas, tanto civiles como militares.

El armamento cibernético no es ningún privilegio de las grandes potencias, si bien unos 20 ocupan el primer plano. También los Estados más pequeños pueden sacar provecho del efecto asimétrico de la tecnología digital y construir con medios relativamente limitados un potencial ofensivo notable. Hay que llamar la atención sobre el hecho de que se emplea mayor creatividad y recursos para técnicas de ataque y la preparación de acciones

ofensivas que para la prevención de la guerra y la defensa. El espacio digital aparece como el quinto escenario bélico, junto a la tierra, mar, aire y el espacio exterior, y resulta, por tanto, parte indispensable de cualquier planificación estratégica.

Escenarios del 'ciberconflicto'

A la luz de estos cambios podemos concretar el concepto de ciberguerra. Los fenómenos señalados anteriormente nos indican la cantidad de recursos a disposición de los Estados para el supuesto de un *ciberconflicto*. La ciberguerra gana actualidad debido al gran rearme digital y a las nuevas posibilidades técnicas; las tendencias muestran también que muchas actividades civiles y militares en un mundo virtual y conectado van unidas, como pueden ir unidas en un conflicto, a ataques virtuales y reales, cinéticas. El aprovechamiento militar de la tecnología de la información, aparte de la elaboración de un *software* de ataque específico, funciona con la misma tecnología y las mismas técnicas de ataque, pero también con la misma vulnerabilidad que los civiles.

Empezaremos con cuatro escenarios arquetípicos de conflicto. A todos les falta un marco jurídico internacional, y todos comparten la difícil identificación del autor del ataque y la imputación del ataque a alguien, que el autor con intenciones de agresión además intenta esconder.

• *El primer escenario es el de la masiva ciberinteligencia.* Un número medio de Estados y de actores no gubernamentales se introduce ya en tiempos de "paz" en el sistema de información del enemigo, obteniendo con ello informaciones sobre planes militares y capacidades en tiempo real, creando así un permanente estado de tensión, pero también un trampolín para un conflicto futuro; por ejemplo, mediante troyanos y bombas lógicas preimplantadas sin que el enemigo se dé cuenta. Tal invasión digital puede, en caso de conflicto abierto, falsear inmediatamente la información de campo, dañar o hacer inoperativos los sistemas de defensa y provocar un caos militar, con las consecuencias de extenderse a la sociedad civil. ¡La ciberinteligencia, el ciberespionaje es casi un estado de normalidad!

•*El segundo escenario se orienta a un ataque masivo a redes privadas y públicas.* El efecto relámpago y paralizante de los ataques digitales sobre la totalidad de un Estado y sus infraestructuras se pudo observar en Estonia en 2007. Durante semanas las páginas del gobierno, partidos políticos, empresas, bancos, operadoras de telefonía móvil y periódicos fueron

bloqueadas por determinados Denial of Service Attacks. Algunos sospecharon de Rusia, pero finalmente los autores del ataque no se conocieron. ¿Hasta qué punto estos autores habían sido reclutados en un Estado vecino o en consorcios criminales internacionales con su potencial de *botnet* (cibermercenarios)?

• El ataque a Estonia es un ejemplo del *tercer escenario* y ha servido como una llamada de alarma para el debate internacional sobre el potencial de la ciberguerra. Sin embargo, este ataque fue solo virtual. En el conflicto de Rusia con Georgia (y las provincias del entorno) en agosto de 2008 aparecieron graves ataques virtuales a las infraestructuras del gobierno de Georgia que facilitaron al mismo tiempo ataques cinéticos dirigidos. Las comunicaciones del gobierno de Georgia fueron silenciadas por secuencias de ataques DDoS. Estados amigos, como en el caso de Estonia, prestaron ayuda técnica a Georgia, pudiendo crear complejos problemas de Derecho Internacional y de neutralidad.

El ciberataque ofrece numerosas ventajas porque es barato, efectivo y puede estar listo en segundos sin causar pérdidas humanas

• *El cuarto y comparativamente más grave escenario* aparecería con los siguientes elementos: un Estado, o una combinación de propietarios de *botnet* y gobiernos, atacan, a la vez y en segundos, estructuras clave de la economía, infraestructuras esenciales y sistemas de defensa. Una agresión así puede provocar el colapso total de un Estado. A estas alturas sería irrelevante si esta ofensiva viene acompañada por un tradicional ataque cinético. Un asalto digital y general como este provocaría enormes destrozos y un número incalculable de vidas humanas.

Hay que reconocer que el aspecto militar de la cibertecnología, desde el punto de vista del armamento, posee un enorme potencial y se presenta como una amenaza latente incalculable. ¿Qué decir sobre la posibilidad de un ciberconflicto?

Para un agresor, un ciberataque ofrece numerosas ventajas, porque su uso es relativamente barato, efectivo y puede estar listo en segundos, sin necesidad de preparativos visibles, sin pérdidas humanas del agresor y fácilmente potenciado a través de mercenarios. La atribución de la autoría del ataque es, conforme a la situación técnica actual, complicada y poco fiable,

se trata de un desafío forense, bajo la presión del tiempo, sobre todo cuando el agresor enmascara sus ataques. La ciberguerra es en gran parte asimétrica y no supone ningún equilibrio de fuerzas.

Por otro lado, los ciberataques masivos son difíciles de medir, sus consecuencias pueden ser incalculables. Desde el punto de vista del grado de interconexión del mundo digital, los efectos en cascada son incalculables. Los efectos se pueden extender a través de redes nacionales e internacionales que inutilizarían o deteriorarían. Junto a los daños directos se generaría una ola de pánico, alterando equilibrios de poder y la geoestabilidad de nuestro dependiente mundo digital. Un agresor digital debe tener en cuenta sobre todo sus propias dependencias. Entre ellas, que el enemigo atacado puede pasar espontáneamente a un gran conflicto cinético o que el agresor sufra un cibercontraataque masivo en sus vitales infraestructuras de red. Aquí nos encontramos con la paradoja de que justo los Estados dotados de grandes capacidades técnicas y con mayor potencial ofensivo –debido a la interconexión en red de todos sus sistemas– son extraordinariamente vulnerables. Richard Clarke y Robert Knake (*Cyberwar*, Nueva York, 2010) han establecido una matriz en la que evalúan las ciberfuerzas ofensivas, el grado de dependencia del sistema y la eficacia de su dispositivo digital de defensa. Para potencias muy fuertes digitalmente como EE UU, ellos fijan un *ciber war gap*, que no puede subsanar con un aumento de fuerzas ofensivas y que determina el cálculo de seguridad en mayor medida. Por el equilibrio entre las ventajas y los propios peligros de un ciberataque, numerosos analistas dudan también sobre la posibilidad de una ciberguerra total. Si bien es indiferente hacia qué pronósticos inclinarse, sí es importante valorar la amenaza latente de un ciberarsenal y reflexionar sobre lo que significaría un aumento sin freno del mismo, sin un marco claro de Derecho Internacional acompañado de restricciones definidas.

En el cálculo de los pros y contras de una ciberguerra hay que tener en cuenta dos hechos esenciales. En primer lugar, al contrario de lo que ocurre en la guerra convencional, en la que el sistema de armamento o las posiciones estratégicas del enemigo deben ser eliminadas, en la ciberguerra, desde el punto de vista de la imponderabilidad de la limitación de las consecuencias, entra en juego la integridad y el funcionamiento de las estructuras de red mundiales, cuya inutilización no afecta solo al enemigo elegido, sino al nervio vital del propio agresor y de muchos otros. Las redes digitales son un bien público, un *common good*, digno de protección en interés de todos. El segundo es la trampa terminológica. La militarización de la planificación

para una ciberguerra conduce a la militarización del pensamiento operativo (*war fighting doctrine*), lo que puede llevar a analogías erróneas y peligrosas. Incluso al concepto de ciberguerra hay que ponerle reparos, ya que estimula esquemas de pensamiento militar. Por ello, es más apropiado hablar de ciberconflicto. Quien piensa respecto a medios digitales en categorías militares, no ha pensado en conceptos como *ciberweapons*, disuasión (*deterrence*) –que en el sentido tradicional militar prácticamente no funciona en el ciberespacio–, contragolpe final, represalias (*retaliation*) reglas de gestión, y la especificidad técnica de una ciberguerra. También aparecen problemas en el empleo de analogías con el Derecho Internacional bélico (la limitación de los objetivos humanitarios, la definición de Estado de combate). Demasiado pronto para que el ciberataque se tipifique y se considere como un ataque armado en el sentido del pacto de la OTAN y de la Carta de las Naciones Unidas, y se resuelvan los problemas de la imputación con respuestas militares incluyendo armas cinéticas. La solución no puede ser esta.

Estrategias preventivas

Bajo estas circunstancias, parece positivo perfilar en la actualidad un frente amplio en el cambio de paradigmas. En lugar de más capacidad ofensiva y dudosas doctrinas de *war fighting*, debe apostarse por doctrinas de estrategias preventivas, colaboración internacional y autorrecuperación (*resilence*): es decir, por una actitud principalmente defensiva y unas ciberestructuras más robustas y resistentes a ataques. Algunas voces vienen incluso de EE UU, donde la Estrategia de Operación en el Ciberespacio aprobada en julio de 2011 empuja hacia la defensa, la estrecha coordinación entre el gobierno, entre el gobierno y la industria y la colaboración internacional, pero sin excluir acciones ofensivas. La cumbre de la OTAN de Lisboa del 20 de noviembre de 2010 fijó el centro de gravedad en la ciberprotección y en la construcción de una ciberdefensa colectiva, sobre unas posibilidades de colaboración nacionales e internacionales (apartado 40). La OTAN evita expresamente subsumir los ciberataques automáticamente como ataques armados del artículo 5 del Tratado de Washington, y se apoya en el mecanismo de consulta del artículo 4.

Desde la posibilidad de una ciberguerra en las listas de preocupaciones internacionales, uno de los temores siempre ha sido la debilidad jurídica del espacio digital –cuando no libre de derechos– lo que hace posible cualquier forma de ciberataque sin limitación. Es bueno, por tanto, reforzar ahora el

desarrollo de un marco de Derecho. Existe un creciente consenso en cuanto a que la gestión de la ciberguerra trae consigo daños y pérdidas, consecuencias comparables a las de una guerra cinética y que, por tanto, se pueden aplicar analógicamente las reglas sobre ataque armado de la Carta de la ONU o del Tratado de la OTAN y, por ello, sus subsiguientes consecuencias jurídicas. También se perfila un consenso sobre las convenciones de Ginebra en cuanto a que la protección de instalaciones e infraestructuras sanitarias sean extensivas a los ciberataques.

En 2012 tanto EE UU como la OTAN trabajarán sobre las fronteras del Derecho Internacional en lo relativo a los ciberataques. Aquí se muestra el potencial de desarrollo evolutivo del Derecho Internacional al frente de las nuevas amenazas. Ya en 2001 hicimos hincapié en la creación de un Derecho penal internacional para la ciberdelincuencia (basado en la Convención sobre el Cibercrimen del Consejo de Europa). Entre tanto, continúan los esfuerzos para la armonización de las reglas sobre Derecho penal y policial internacional, todavía con demasiada lentitud y sin proporción a la magnitud de la amenaza.

En el sentido de estos nuevos paradigmas en 2001 se fundó el Permanent Monitoring Panel on Information Security de la Federación Mundial de Científicos, para la gestión de los ciberconflictos. Su trabajo se centra en los conceptos de ciberestabilidad y ciberpaz (recomiendo el libro *The Quest for Cyber Peace,* La búsqueda de la paz en el ciberespacio, elaborado en 2011 por un grupo de expertos encabezado por Hamadoun Touré (secretario general de la Unión Internacional de Telecomunicaciones, UIT).

La ciberpaz intenta fijar en la antinomia de guerra-paz la perspectiva de un orden de paz digital, que garantice la continuidad de las redes de información transnacional (que no se debe sacrificar a un cálculo militar). La idea esencial es deslegitimar tanto como sea posible la ciberguerra, y dejar libre de ataques el espacio digital, promover un balance (armonización) de bienes, la autoprotección, la ciberdefensa, y dar prioridad a la contención sobre el ataque.

La ciberpaz exige una nueva forma de ciberdiplomacia. A esta pertenece sobre todo un consenso internacional sobre reglas de Derecho y de comportamiento en el espacio digital, un código sometido también a la presión del tiempo. Muchas voces llaman hoy a un *Global Cyber Treaty* (cibertratado global), que bajo el Derecho Internacional vinculante, limite y sancione el uso militar del espacio digital. El hecho es que para este marco legal es necesario un cuerpo obligatorio de Derecho Internacional. Sin embargo, la idea

de un tratado detallado, aunque el objetivo sea claro, hace surgir dudas. Para la adaptación y la nueva interpretación del Derecho Internacional existente, incluyendo el Derecho Internacional de guerra y el Derecho Humanitario, es preferible una evolución pragmática del mismo. La preparación, aceptación y ratificación de un tratado mundial que transforme las reglas necesarias de comportamiento para los Estados y otros actores digitales directamente en Derecho Internacional, sería una tarea demasiado larga en el tiempo, incierta y, quizá, incluso, irreal.

El debate se dirige cada vez más a la idea de crear un paquete de medidas de confianza y un código de conducta, que no excluyan acuerdos parciales pero permitan un tratamiento del problema más dinámico y promueva la construcción evolutiva de un amplio consenso. El código debe describir normas para el comportamiento en el espacio digital tanto en tiempos de paz como en tiempos de guerra y vincular a todos los actores, también industrias tecnológicas, servidores y organizaciones internacionales. Un buen ejemplo: la Asamblea General de la ONU, a través de la resolución A/66/24 de 13 de diciembre de 2011, ha creado un grupo de expertos para elaborar unos principios a seguir por los Estados y unas medidas de confianza. Siguiendo la idea de un código de conducta, y desde las diferentes discusiones, se puede compilar una lista indicativa de las necesidades de regulación y los determinados puntos que tal código debe desarrollar. Una lista sin duda ambiciosa, pero con un sentido como punto de salida:

> Es preciso crear medidas de confianza y un código de conducta internacional para el comportamiento en el espacio digital

– Establecimiento del principio de que un ataque contra un Estado, directamente o a través de agentes interpuestos, es una lesión al Derecho Internacional público.

– Obligación de cada Estado a no realizar ningún uso de ciberarmas contra otro Estado, en tanto no haya sido atacado con armas convencionales.

– Los Estados se obligarán en un marco nacional e internacional para asegurar una política de prevención de ciberconflictos con prioridad de la defensa cibernética y asegurar junto con la industria sus sistemas y redes a través de una máxima robustez, defensa y capacidad de resistencia a los ataques, segmentación de redes, ciberhigiene, gestión eficiente, etcétera.

– Los Estados se orientarán en el caso de un ciberataque o de un grave daño en las estructuras de la red, hacia una restauración, tan pronto como sea posible, de las redes y de un sistema eficiente, estable y pacífico de comunicación.

– Los Estados estarían obligados a proteger en su territorio las infraestructuras críticas, entre ellas el suministro de energía, el sistema bancario y sanitario, y otras instalaciones humanitarias. La red de estructura digital transnacional sería inviolable. El ataque a estas infraestructuras estaría prohibido.

– Obligación para todos los Estados de aunar intereses en la creación de un Derecho Internacional armonizado y la creación de un Derecho Penal para la persecución de los ciberdelitos, sea mediante la adopción de la Convención sobre Cibercrimen del Consejo Europeo o a través de normas similares, así como una colaboración internacional policial y jurídica eficiente.

– Obligación de cada Estado a proteger a sus ciudadanos en el espacio digital.

– Todos los Estados están obligados a perseguir legalmente a los ciberterroristas o ciberdelincuentes que operen en su territorio. Asimismo, en el marco de sus posibilidades técnicas (por ejemplo, mediante *deep packet inspection* de las principales arterias de fibra de vidrio de sus suministradores de servicio, ISP) los países evitarán la utilización de su territorio por ciberdelincuentes.

– La introducción de *botnet* y otros elementos ciberbélicos debe prohibirse y los Estados están obligados a velar por esta prohibición en sus territorios.

– La neutralidad está vigente en la era digital, y no pueden dirigirse ataques cibernéticos a través de las redes de países neutrales.

– Los países deben prestarse apoyo recíproco en la investigación de ciberdelitos, especialmente de los que partan de su territorio.

– Los Estados se asocian a los sistemas de información internacional y los sistemas de alerta temprana (acuerdos 24/7, mantenimiento de puntos de contacto, redes internacionales multidisciplinarios como las de CERT, seguridad de la información).

– Además de los convenios multilaterales, los Estados fomentarán acuerdos bilaterales, con compromisos recíprocos de no agresión, de defensa común ante un ciberataque y apoyo mutuo en caso de daños.

Este tipo de reglas aumentarían la transparencia y elevarían la confianza en la integridad y la capacidad de funcionamiento del sistema y de las estructuras de red. Este criterio decisivo en la sociedad de la información sería un ingrediente importante en la ciberpaz.

Respecto a dónde podría tener lugar este proceso de negociación multilateral, hay varias opciones. Se podría pensar en una conferencia de Estados que, después de la negociación, crearán un observatorio para los países firmantes que controlara las infracciones contra el código. La participación sería voluntaria, y junto a los Estados podrían participar otros actores. Esta conferencia no estaría sometida a la obligación del consenso universal o a las normas de votación de la ONU. De este modo, los Estados participantes serían libres a la hora de declarar vinculante para ellos parte del código. El objetivo es fomentar un consenso dinámico.

Una alternativa sería elegir como foro de trabajo a una de las grandes organizaciones internacionales como la UIT, encargada internacionalmente de las cuestiones de telecomunicaciones y de seguridad de la información, o la Conferencia de Desarme de Ginebra, con reconocida experiencia en acuerdos de seguridad internacional. Pero estas son cuestiones de orden práctico que van más allá del planteamiento de este artículo.