XXVI CURSOS DE VERANO - UNIVERSIDAD COMPLUTENSE
EL ESCORIAL, DEL 1 AL 5 DE JULIO DE 2013

CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

Ponencia del Teniente General (EA) D. Ángel Mazo da Pena. 02 de julio.
La Ciberseguridad en el contexto de la OTAN y la UE

INTRODUCCIÓN.

La evolución tecnológica en el mundo de la información y las comunicaciones ha causado un notable cambio de paradigmas en nuestras sociedades. Cada vez es menos necesario insistir en la creciente importancia que todo lo concerniente al ciberespacio va cobrando en nuestras vidas, y cuanto veíamos hasta no hace mucho tiempo en ciertas películas de ciencia ficción forma ya parte integral de nuestra rutina diaria y es visto con la mayor naturalidad, se ha incrementado enormemente nuestra dependencia de los sistemas de información en los campos más diversos y la ciberguerra ha irrumpido con fuerza en la historia. La actividad cibernética, como toda actividad humana, presenta sus pros y sus contras; así ha ocurrido con todos los avances que han visto los tiempos: por un lado, la correcta utilización de las facilidades que nos proporcionan las nuevas tecnologías –con la consecuencia lógica de un nuevo e innegable progreso para la humanidad- y, por otro, la explotación de la capacidad de daño que también encierran –con la consiguiente necesidad que experimenta el hombre de defenderse nuevamente del propio hombre-.

Centrándonos sin más preámbulo en los aspectos de la defensa, diré que la historia militar ha visto cómo, en menos de un siglo, se incorporaban a los ámbitos tradicionales de la tierra y la mar otros dominios físicos: el aire y el espacio (anteayer), y uno global y artificial (en realidad, físico también): el del ciberespacio (ayer). Hoy sentimos el vértigo que nos produce constatar que es cada vez más tarde para tomar ciertas decisiones porque los acontecimientos muestran claramente que se marcha en una sola dirección. Del mismo modo que la entrada del hombre en la tercera dimensión acabó provocando, pocos años después, la creación de fuerzas aéreas porque sin el dominio del aire las operaciones de superficie quedaban en entredicho, la entrada del hombre en el ciberespacio acabará provocando la creación

de un nuevo ejército (el cibernético) cuya acción habrá que conjuntar con la de los demás, o quedaremos sorprendidos cuando las operaciones en que nos empeñemos se vean afectadas e incluso impedidas. Es más, con la aceleración general del tiempo, de que también somos testigos, no hay sino que esperar que este proceso dure mucho menos.

Aunque eso se ve aún muy lejos, efectivamente ése es el futuro, falta tan sólo una "circunstancia catalizadora" para que se haga realidad, y no resulta arriesgado afirmar que, tristemente, se tratará de un inesperado y fatídico ataque de catastróficas consecuencias (de hecho, ataques de ninguna, escasas o aún desconocidas consecuencias ya se producen a diario…) Si somos capaces de anticiparnos y reaccionar a tiempo, las consecuencias serán mínimas; si no nos organizamos antes, tarde o temprano habremos de sufrir recorriendo precipitadamente el mismo camino, pero envueltos en lamentos como hacemos cuando invertimos en blindar puertas y ventanas de nuestro hogar… dos días después de que nos hayan robado una cantidad muy superior a tal inversión.

Las dificultades y resistencias previsibles ante la decisión de crear un nuevo ejército son evidentes, el momento económico no es el más propicio, pero aún así se puede hacer mucho y, afortunadamente, ya hemos comenzado.

Nuestra visión, además, trasciende el mundo militar y el del Ministerio de Defensa; la ciberdefensa es una necesidad nacional que requiere dirección unificada -a muy alto nivel- de la acción; no sólo de la contribución de las Fuerzas Armadas y aun de las Fuerzas y Cuerpos de Seguridad del Estado, sino de todos los sectores incluidos en la Ley 8/2011 sobre medidas de protección de infraestructuras críticas.

El ciberespacio es un tema muy particular: de entrada, es transnacional, combina amenazas producidas por actores estatales y no estatales, afecta a vulnerabilidades civiles y militares, requiere respuestas también civiles y militares, por un lado, y públicas y privadas, por otro; bordea o vulnera la legalidad establecida, las políticas reinantes y la doctrina militar. Es el actual "talón de Aquiles" de nuestras sociedades.

CONCEPTOS.

Conviene que distingamos entre ciberseguridad y ciberdefensa porque entre ambos términos hay una frontera muy difusa, se entremezclan y es que, en ocasiones, son sinónimos.

Ciberseguridad es más genérico, quien lo usa se refiere –generalmente- a la seguridad de la información de individuos concretos: usurpaciones de identidad, robos de propiedad intelectual; también denegaciones de servicios varios y ataques a infraestructuras no críticas (redundantes) o privadas.

En Ciberdefensa interviene el Estado como tal, sus Fuerzas Armadas, sus infraestructuras críticas, está implicada la protección de los derechos humanos en general (no de individuos), no hablamos de delincuentes sino de enemigos, no de ataques aislados y furtivos con finalidad económica de beneficio personal del delincuente, sino de ataques masivos y abiertos con finalidades de orden estratégico. Por cierto, dos reflexiones a tener en cuenta: 1) el mundo cibernético se desarrolla con bastantes paralelismos al mundo nuclear pero mucho más rápidamente, y 2) las consecuencias de un ataque cibernético masivo pueden ser tan serias como las de una bomba nuclear.

La protección contra la acción con fines terroristas pueden considerarse como ciberseguridad, pero yo la veo más en el ámbito de la ciberdefensa ya que el terrorista produce daño a individuos y propiedades, pero el efecto pretendido (sembrar el terror) es siempre estratégico.

Más fácil es el salto del concepto de ciberdefensa (en paz y en guerra) al de ciberguerra (en guerra ya abierta, declarada o no).

Si me permiten una simplificación extrema como la que voy a decir por bien de la necesaria finalidad didáctica de esta exposición, hay que asociar la UE (soft power) a la ciberseguridad y la OTAN (hard power) a ciberdefensa; como todas las simplificaciones, esta asociación es errónea y en un momento demostraré por qué, pero se comprueba con facilidad que cada una de las dos organizaciones se preocupa más directamente del concepto al que le he asociado y emplea muchísimo más a menudo el término correspondiente.

Parte del ciberespacio de control estatal está asignado a las FAs, es el que podemos denominar como ciberespacio militar.
El viernes, cubrirá el Jefe del nuevo Mando Conjunto de Ciberdefensa información (yo no voy a entrar en ella hoy) sobre las redes de área extensa y local de nuestro ministerio, las responsabilidades de las distintas autoridades, los centros de respuesta existentes, los distintos documentos en vigor y sus contenidos.
Me contentaré con expresar mi satisfacción porque, en un plazo mucho menor del

que yo esperaba, se van tomando las decisiones que he estado predicando en el pasado, como la creación de este Mando...

VACÍO LEGAL.

Pasado mañana se tratarán aspectos legales de ciberseguridad; yo voy a introducir todos pero haciendo hincapié en los correspondientes a ciberdefensa, ya que se espera de mí que hable desde la perspectiva militar.

Cuando se legisla es para regular la interacción social en cualquier ámbito en que ésta se produzca, creando un marco que permita la convivencia y el respeto a los derechos humanos. El ciberespacio permite esta interacción… luego exige su regulación… Pero existe un gran vacío porque dificultan la regulación ciertos aspectos de la naturaleza (virtual) del ciberespacio: desaparición de fronteras, dificultades de atribución de acciones a individuos concretos, rapidez en la difusión de la información o inmediatez de efectos dañinos… acceso fácil y barato a HW y SW en el mercado…, etc.

Es un espacio "muy paralelo" al mundo físico; de hecho, ésa es la conclusión de un grupo internacional de expertos legales del que hablaré suficientemente más tarde (el paralelismo nos facilita su comprensión y la necesaria reacción), pero hay matices intrínsecos muy relevantes que no permiten un paralelismo total.

Si hablamos de ciberseguridad, podemos preguntarnos si el uso del ciberespacio es un derecho y cómo debe protegerse, hasta dónde puede intervenir el Estado; considerar el equilibrio entre el derecho a la intimidad y la necesaria identificación de los delincuentes o la obtención de evidencias de los delitos, una cuestión de naturaleza política clásica (viejo conflicto libertad-seguridad), la división de lo liberal frente a lo conservador, pero también cuestión política internacional puesto que 1) unos gobiernos creen en la libertad más que en la seguridad y en otros es al revés, y 2) conflicto soberanía-seguridad colectiva (paralelismo de la libertad de los individuos y la soberanía de los estados, organizaciones supranacionales, etc…).

La desaparición de fronteras acerca las personas unas a otras, pero también acerca a delincuentes y víctimas, a explotadores y explotados, a violadores y violados, dadas las dificultades de atribución de los delitos a quienes los han cometido.
La rapidez en la difusión de la información permite la consulta urgente de un dato necesario para completar un conocimiento o incluso para salvar vidas, pero permite también difundir –incontrolable e irreparablemente- un dato manipulado, una

mentira, una calumnia…

Las nuevas tecnologías permiten dar la orden de conectar la calefacción de nuestros hogares desde fuera de ellos con la antelación que queramos, pero también la orden de paralizar una central eléctrica sirviendo a millones de personas, o una red de cajeros automáticos.

El acceso fácil y barato es muy interesante para todos y, en particular, para la población juvenil, pero también para los llamados "hackers".

Yendo ya a la ciberdefensa, podemos preguntarnos si un ordenador puede ser considerado como un arma o usarse como tal, o cómo definir un acto de fuerza en el ciberespacio, qué se considera y qué no como una "amenaza", qué es y qué no un "acto hostil", y qué es o no un "ataque armado". Cómo aplicar las leyes y usos de la guerra en vigor, los Convenios internacionales (de Ginebra, La Haya), si precisamos de leyes como las del Mar y del Espacio Exterior, los principios de necesidad y proporcionalidad en el empleo legítimo de la fuerza por el Estado en la respuesta ante un ataque, por ejemplo: aplicabilidad del art. 51 de la Carta de Naciones Unidas sobre autodefensa, o art. V del Tratado de Washington de la OTAN, la defensa individual y colectiva, cómo arbitrar Reglas de Enfrentamiento en el ciberespacio… Los derechos de los combatientes, los prisioneros de guerra, los que no tienen los mercenarios… la protección de civiles, de neutrales y de no beligerantes…

Hasta ahora, el ámbito de jurisdicción de un país coincidía siempre con sus límites territoriales pero ya no; es más, ante una acción en internet, pueden coincidir varias jurisdicciones a la vez con consecuencias legales distintas en cada una…

En definitiva, cómo aplicar al ciberespacio el progreso logrado en el "ius ad bellum" (o derecho internacional que regula el recurso a la fuerza por parte de los Estados) y el "ius in bello" (o derecho de la guerra, o derecho humanitario internacional, que regula el comportamiento durante el uso de la fuerza en un conflicto o guerra abierta). Y cómo aplicarlo a pesar de que el derecho internacional pierde poder con el aumento del número de actores que lo ignoran totalmente y el hecho de que, por su propia naturaleza, son ocultas las acciones de ciberguerra.

Ámbito (legal) internacional.

ONU:

- 4 resoluciones desde 2000 sobre aspectos concretos pero ningún acuerdo

global; por ejemplo, en 2010 faltó consenso para aprobar una propuesta contra cibercrimen…

CONSEJO DE EUROPA:

- Convenio sobre Ciberdelincuencia (Budapest, 2001), aspectos de jurisdicción, extradición, coordinación, asistencia mutua.

UNIÓN EUROPEA:

- 2010: la Comisión Europea presentó un plan con iniciativas legislativas para ella misma y los Estados Miembros.

PARLAMENTO EUROPEO:

- Resolución general de 2012.

ESPAÑA:

- Hay artículos del Código Penal que son trasladables al ciberespacio.
- En 2010 se introdujeron dos nuevos delitos exclusivos (informáticos).

OTAN:

- Es de destacar el Manual legal del CoE de Tallinn, que es uno de los llamados Centros de Excelencia de la OTAN (aproximadamente 20) en los que se llevan a cabo labores de investigación y enseñanza en áreas diversas.

RESUMEN DEL MANUAL DE TALLINN

Bajo los auspicios del Center of Excellence on Cyberdefense, de Tallinn (Estonia), un grupo internacional de expertos legales ha elaborado un manual que, pese a no ser un documento aprobado por ningún país, ni constituir doctrina OTAN sino simplemente la opinión de ese grupo de expertos (incluso se muestran algunas discrepancias internas en algún aspecto concreto), constituye a mi modo de ver el avance más notable que se ha registrado a este respecto.

El manual identifica cuanto les parece aplicable del derecho internacional, que no es poco, y establece hasta un total de 95 interesantísimas reglas que versan sobre conceptos como soberanía y responsabilidad de los Estados, posibilidades y limitaciones del uso de la fuerza, autodefensa legítima y sus condiciones, iniciación y conducción de hostilidades, medios y métodos de ciberguerra, ataques y precauciones, perfidia y espionaje, protección de personas (médicos, religiosos,

detenidos, periodistas, niños…), instalaciones y propiedades culturales, archivos, medioambiente, ayuda humanitaria, territorios ocupados, Estados neutrales y no beligerantes…, etc.

IMPORTANCIA DADA A LA CIBERDEFENSA EN LO INTERNACIONAL.

La ciberdefensa está declarada como una de las primeras prioridades para OTAN y UE (incluida la EDA). También para USA (como esta misma mañana nos contará un representante de ese gran país muchas cosas, entre ellas que han creado un Mando de Ciberdefensa que tiene del orden de 9.000 personas trabajando…). Palabras parecidas podrían pronunciar representantes de UK, FR, GER, etc. Todos los países occidentales están atareadísimos definiendo conceptos, adaptando o creando organizaciones: mandos y unidades militares a niveles estratégico, operacional y táctico. En cuanto a otros, como China, Irán y Corea del Norte, se cree que están preparando ciberejércitos en toda regla de cibernautas.

La OTAN: Además del desarrollo de una capacidad de respuesta incidentes con el NCIRC (NATO Computer Incident Response Capability) y de la creación del CoE mencionado, en 2010 el nuevo Concepto Estratégico subrayó las amenazas y necesidad urgente de protegerse contra ellas, por lo que encargó al NAC para que desarrollase una política de ciberdefensa; en 2011 se hizo un Concepto y esa fue la base de la NATO policy adoptada el mismo año por los Ministros de Defensa.

La UE tiene una Estrategia Europea de Seguridad, de 2008, que identifica ya ciberamenazas como posibles y probables, y establece la urgente necesidad de colaboración internacional en materia de ciberseguridad.

ESPAÑA: nuestra Estrategia Española de Seguridad de 2011 ya lo recogía también e identificó el vacío legal como un factor principal. Ahora, de nuevo, forma parte importante de la Estrategia Nacional de Seguridad, aprobada el mes pasado. A la espera de una estrategia específica de ciberseguridad que, finalmente, ha coordinado el CNI (EECS Estrategia Española de Ciberseguridad), se han ido desarrollando iniciativas parciales como la creación de diversos CERT: CCN-CNI, CNPIC (M. Interior), INTECO (M. Industria), COSDEF (M. Defensa), Comunidades Autónomas y bancos.

TÉCNICAS MILITARES Y OTRAS CONSIDERACIONES.

Tras la evolución de la guerra electrónica (consistente, básicamente, en impedir o perturbar la telecomunicaciones enemigas y preservar las propias, mediante el dominio de otro espacio singular como es el del espectro electromagnético), ahora es posible hacer eso, y mucho más, sin presencia física o cercana (sin, siquiera, aviones) y permanente (sin barcos, por ejemplo); y sin otras limitaciones como la necesidad de equipos especializados sofisticados y costosos…

Un ciberatacante, ¡un terrorista! por ejemplo (no digamos un grupo de ellos, o un ejército de cibernautas), con un portátil y cierto SW, sólo necesita conocimiento de vulnerabilidades y ya puede atacar (dañar o tomar control) de aquellos sistemas de información que él haya decidido convertir en sus objetivos, atacar la red eléctrica de un país, paralizar sus FAs (actualmente, los aviones –sobre todo: UAVs- y sistemas C2 son muy dependientes de su HW y SW), etc.

Cuanto más desarrollado es un país, más dependiente es de los sistemas informáticos (lo mismo ocurre con las FAs), lo que nos lleva a un concepto ya bien conocido hoy que es el de "guerra asimétrica". Pero también la ciberguerra es atractiva para los poderosos… que pueden atacar sin tener que asumir costes de vidas humanas y eludir con mayor facilidad las acusaciones de "daños colaterales".

Dentro del mundo de las capacidades militares en materia de ciberdefensa se distingue entre las de:

- defensa (protección de las redes y sistemas propios 24/7, como la defensa aérea),
- explotación (inteligencia de las del enemigo, de sus medios e intenciones de ataque, etc.),
- respuesta (ante un ataque cibernético con otro, cibernético o no)

La defensa y la explotación, rebosan coherencia con los principios de nuestra Constitución y con las guías políticas de OTAN y UE. Y el ataque también, si es la legítima respuesta a un ataque enemigo en ejercicio del derecho de autodefensa (art. 51 de la Carta ONU); el problema, como señalo, en este caso se traslada a la elección del tipo de respuesta. El criterio podría basarse en la escala y en las consecuencias del ataque: si las ha habido en el mundo real, una respuesta real podría ser adecuada (en OTAN, además, si son tan suficientemente malas como para invocar el artículo V, será legítimo responder de forma adecuada con todos los medios y de todas las formas a mano).

Estamos, desde luego, ante un instrumento de poder militar; desde luego, técnica y tácticamente distinto de los demás instrumentos del poder militar, pero que –claramente- no escapa a la estrategia. Se está empezando a militarizar el ciberespacio porque hay oportunidades para la acción estratégica que son mucho menos caras que la de las armas convencionales y nucleares, pero que pueden ser igual de efectivas que aquellas y, tal vez, que éstas.

Aunque empecemos ya a legislar y evitemos la ciberanarquía, hay asuntos como el ciberespionaje, que está ya ahí, y la militarización del ciberespacio, que está por llegar. Necesitamos una respuesta común, porque los problemas y las amenazas son comunes. Como vemos, a los elementos defensivo, ofensivo y de inteligencia que acabo de mencionar, hay que añadir los de cooperación nacional e internacional, y el de multidisciplinar.

Durante la Guerra Fría, estuvimos al borde del holocausto nuclear con la estrategia de la Destrucción Mutua Asegurada, pero USA y URSS se contuvieron y convinieron reducir y limitar sus armas. Pronto necesitaremos algo similar si queremos impedir una caótica militarización del ciberespacio y la proliferación de armas estratégicas ciberespaciales.

Pronto hablaremos de medidas de transparencia y confianza mutua para evitar el riesgo de escalada sin las que los estados atacantes podrían eludir responsabilidades culpando a atacantes privados... hace falta, por tanto, un debate sobre las responsabilidades de los estados en los ataques lanzados desde su propio territorio. De momento, el ciberespacio sigue siendo un poco “tierra de nadie”.

Los instrumentos tradicionales de control de armas y desarme no son prácticamente aplicables al ciberespacio. Todavía no es posible verificar la actividad cibernética, en buena parte porque no se ha llegado a una definición de armas cibernéticas. Las capacidades en el ciberespacio no pueden ser clasificadas de modo tradicional en civiles y militares, y no pueden ser fácilmente limitadas, ni pueden imponerse restricciones de capacidades técnicas a los estados…

Algunas medidas de confianza podrían ser:

- Mecanismos de alerta temprana (CERTS Computer Emergency Response Teams).
- Intercambio de información y mejores prácticas sobre estrategias nacionales de ciberseguridad.

- Cooperación en el impulso al desarrollo de recomendaciones técnicas para tener infraestructuras robustas y seguras.
- Establecimiento y notificación de puntos focales nacionales.
- Establecimiento de canales de comunicación de emergencia para uso en caso de ciberincidentes.
- Apoyo para la construcción de capacidades en ciberseguridad en países en desarrollo.
- Establecimiento de programas de formación e instrucción.

No hay un código internacionalmente aceptado de conducta en el ciberespacio. Habría que hacer uno (y suficientemente antes de que sea necesario aplicarlo) que, como el Manual de Tallinn, incluyera los principios derivados de la Carta de ONU y el derecho humanitario internacional. No es fácil: por ejemplo, el recurso a la autodefensa militar (art. 51 de la UN Charter) requiere la existencia de un ataque armado, por lo que ya decía antes que se precisa definir muy bien las características que deben reunir los efectuados con medios cibernéticos para cumplir tal condición.

Por otra parte, la defensa de todas las redes y todas las posibilidades de ataque es muy difícil y nunca posible al 100%; por el contrario, es facilísimo el ataque dado lo barato y poco complejo de hacerse con los medios que requiere (por cierto, que pueden reclutarse cibermercenarios también, ¿por qué no?) y luego es difícil atribuir legalmente del ataque a un presunto atacante que no habrá precisado siquiera acercarse geográficamente al estado víctima.

LA OTAN.

De manera muy resumida, puede decirse que la política de ciberdefensa (vs. ciberseguridad) de la OTAN consiste en:

- Integrarla en sus estructuras y procesos de planeamiento (NDPP targets) para desarrollar dos de sus tres tareas principales (según el Concepto Estratégico en vigor, el de Lisboa): defensa colectiva y gestión de crisis (la otra es cooperación internacional).
- Centrarse en prevención, resistencia y defensa de los medios críticos cibernéticos, suyos y de las naciones miembro.
- Desarrollar capacidades y proteger las redes propias y nacionales conectadas, apoyando a los aliados en lo posible.
- Relacionarse con socios (esto tiene algunas dificultades, sin embargo),

organismos internacionales, así como con el sector privado y el académico.

Los principios, por tanto, son los de:
- prevención (de la ocurrencia de ataques).
- resistencia (ante los ataques que puedan ocurrir).

Como consta en el Tratado de Washington y en el Concepto Estratégico vigente, la OTAN defenderá su territorio, poblaciones e intereses, contra cualquier ataque, incluyendo los derivados de los retos de seguridad emergentes como, por ejemplo, los ciberataques (art. IV y V). Cualquier respuesta será sometida a la decisión del NAC y, mientras, mantendrá una ambigüedad estratégica y oportuna flexibilidad sobre cómo responderá a crisis que contengan un componente cibernético.

Se está debatiendo cómo proporcionar asistencia a cualquier país aliado que sea atacado y lo requiera, porque la ciberdefensa es, básicamente, una responsabilidad nacional (paralelismo con el debate "arcaico" de defensa nacional en general, parece que es inevitable…). Para facilitar todo ello, la OTAN (NCDMA y B: NATO Cyber Defence Management Authority y Board) ha firmado un Acuerdo Marco (MOU) con las autoridades máximas nacionales en esta materia (22 de 28 naciones miembro, en el caso de España, con el CNI, cuyo Secretario de Estado Director estará aquí pasado mañana).
Para responder a incidentes, ha desarrollado una capacidad de respuesta que se materializa en el NCIRC (NATO Computer Incident Response Capability), ya mencionado (IOC en 2006 y FOC en OCT 2013). RRTs para redes propias y, si se aprueba en oct, apoyo a naciones aliadas).

Hay en marcha un Plan de Acción, que es un documento vivo (revisado constantemente) para asegurarse de que está "a la última" de los desarrollos en el ciberespacio y mantiene la necesaria flexibilidad para hacer frente a los retos que se produzcan. Si la Policy indica el "qué", el Plan de Acción indica el "cómo" y, así, se indican asuntos como:
- requisitos mínimos de los sistemas de información y comunicaciones
- requisitos de autenticación
- prioridades diversas
- nivel mínimo de protección de infraestructuras
- formas de apoyo mutuo entre aliados
- integración de la ciberdefensa en el planeamiento general de la defensa
- responsabilidades de distintas autoridades de la estructura de mando y de las fuerzas desplegadas en teatros de operaciones

- requisitos paralelos de las fuerzas que co-operan en esos teatros pero que pertenecen a otras naciones asociadas a OTAN pero no miembros
- procesos de adquisición de sistemas de alerta cibernética temprana, conciencia situacional y de herramientas de análisis
- formación y adiestramiento, en general y en relación con el CoE de Tallinn.

NDPP: 75% de targets de ciberdefensa aceptados. Explicar esto (alto/bajo porcentaje).
Socios: 1) con empresas y academias, OK; 2) con naciones (caso por caso).

LA UNIÓN EUROPEA.

La Estrategia Europea de Ciberseguridad (vs. ciberdefensa) representa la visión de conjunto de la UE sobre cómo prevenir y resolver las perturbaciones de la red y los ciberataques. Se trata de impulsar los valores europeos de libertad y democracia, y velar por un crecimiento seguro de la economía digital. Se prevé una serie de medidas específicas para reforzar la ciberresistencia de los sistemas y reducir la ciberdelincuencia; además, desarrollar capacidades en el ámbito de la CSDP o Política Común de Seguridad y Defensa (operaciones militares -como EUTM Mali- y misiones civiles -como EUCAP Néstor-), los recursos tecnológicos industriales correspondientes y la colaboración en el establecimiento de una política internacional adecuada.
Se han logrado importantes avances como crear un Centro Europeo de Ciberdelincuencia y una alianza mundial contra abusos sexuales a menores en internet.

Pero también se preocupa la UE de la ciberdefensa como capacidad militar e integra su desarrollo en el planeamiento propio de defensa (CDP), con:
- definiciones,
- características,
- principios,
- niveles,
- responsabilidades,
- cooperación (Comisión Europea, Centro UE Cibercrimen, NATO/ACT, CoE Tallinn…)…

…así como dentro del trabajo de la EDA (Agencia Europea de Defensa), que identificó la ciberdefensa como una de las diez prioridades principales en el desarrollo de capacidades militares (iniciativa Pooling & Sharing comprende dos proyectos de cyber).

CONCLUSIÓN.

La llegada del hombre al ciberespacio es un hito en la historia de la humanidad cuya relevancia todavía no terminamos de asumir en su verdadera dimensión. Supone un avance innegable pero ofrece tantas posibilidades de un uso nefasto por el propio hombre como han supuesto otros grandes hitos anteriores.

Las ciberamenazas existen verdaderamente, puede que se disponga de poca información por los recelos a compartirla en esta materia, pero se da ya un enorme número de ciberataques diariamente (los más conocidos son los masivos efectuados contra Estonia en 2007 y contra Georgia en 2008, o de los puntuales contra instalaciones nucleares iraníes en 2010 con el Stuxnet, y otros).

Se precisa una legislación específica tanto a nivel nacional como internacional, si bien el grupo de Tallinn ha demostrado buena parte de la aplicabilidad del derecho humanitario existente.

La UE y la OTAN tienen un rol esencial y están bien preparadas para hacer frente a todos los retos: desde la producción de legislación relevante hasta las acciones de respuesta adecuadas, ya sean judiciales, policiales, militares o de otros órdenes. La UE y la OTAN se concentran en la ciberseguridad y ciberdefensa, para las cuales están, respectivamente, mejor dotadas.

Aún así, queda mucho camino por andar para absorber adecuadamente los nuevos conceptos cibernéticos en el pensamiento estratégico y desarrollar las correspondientes nuevas capacidades a fin de estar en condiciones de defendernos de ciberataques y gestionar ciberemergencias.

Con todo, el ciberespacio ha producido muchas más oportunidades que amenazas, es por eso por lo que la gente percibe más aquéllas que éstas, y es responsabilidad de las administraciones la de ocuparse de unas y otras. En cualquier caso, no quiero dejar en el aire una sensación pesimista y preocupante, ¡el ciberespacio es un nuevo y maravilloso cosmos para la Humanidad!.

Muchas gracias por su atención.