# EL CIBERESPACIO EN EL CONTEXTO DE LA OTAN Y LA UE

2014

DIVDOC

DIVISIÓN DOCTRINA

30

Envíe sus comentarios y opiniones directamente a la División Doctrina (DIVDOC), por Intranet al correo institucional J023.

**Editor responsable**
División Doctrina

**Valenzuela Llanos 623, La Reina**
**(56 - 2) 2290 74 60**

**PRIMERA EDICIÓN**
**2014**

# EL CIBERESPACIO EN EL CONTEXTO DE LA OTAN Y UE

## A. INTRODUCCIÓN.


- La evolución de las tecnologías de información y comunicaciones (TICs) han causado un notable cambio de paradigmas en nuestra sociedad. Cada vez, es menos necesario insistir en la importancia que va asumiendo en nuestra vida personal y profesional el ciberespacio, lo que es visto con la mayor naturalidad. Este paradigma ha incrementado enormemente nuestra dependencia a los sistemas de información en los campos más diversos, incluyendo el campo militar.

- La actividad del ciberespacio, como toda actividad humana, presenta sus ventajas y desventajas; por un lado, la correcta utilización de las facilidades que nos proporcionan las nuevas tecnologías y comunicaciones, 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.

- Es importante indicar desde un principio que el concepto "ciber", que parece ser muy moderno, no lo es en absoluto, ya que este proviene de la palabra cibernética, etimológicamente nos llega del francés (cibernétique), que a su vez lo tomo del inglés (cybernetics), aunque originalmente viene del griego **kyberneees,** donde se hace referencia al arte de gobernar una nave, cabe señalar que el término representa divergencias en el concierto internacional, su definición depende de los intereses de quien lo emplee.

- Es así como a principios de los años 80, el escritor William Gibson[1] estableció el término ciberespacio, para describir una red ficticia de computadoras que contenía enormes cantidades de información que podrían explotarse, con el fin de adquirir riqueza y poder.

- Por otro lado, se estima que el ciberespacio es el conjunto de un dominio global dentro del entorno de la información, dado por el uso de las "Tecnologías de Información y Comunicación" (TICs) para almacenar, modificar y explotar información a través de redes y plataformas computacionales[2]

- Esta definición es tan buena como otras muchas que hay del nuevo espacio, conformado por la combinación de la capacidad de computación de la informática y la transmisión de datos de las nuevas tecnologías de comunicación. Igual que la mayoría de ellas, sin embargo, plantea un exceso tecnológico en su descripción. Nos expone de forma clara y concreta en qué consiste el espacio cibernético y enumera sus posibles usos, pero dista mucho de introducirnos en las aplicaciones y amenazas que tiene su mera existencia para el ámbito militar y estructuras críticas de un estado.

- El ciberespacio es mucho más que el conjunto de máquinas que nos permiten la explotación del espectro electromagnético para comunicarnos; incluso, más que la información que se mueve por él, lo que hemos construido va más allá de un nuevo espacio de confrontación, como lo es posiblemente el emergente campo de batalla virtual (Guerra de Redes).

- En el espacio virtual estamos forjando nuevas personalidades, nuevas identidades y nuevas formas de gestión comunicacional (Mando y Control), que replican como si fuera un universo paralelo las actividades que llevamos a cabo en el mundo físico. Ponemos eso sí, mucha atención en la fortaleza de nuestros sistemas de información y de comunicaciones, en lo que se refiere a proteger nuestros equipos militares con antivirus e invertimos tiempo y dedicación en la generación de complicados sistemas de acceso, restringido en un esfuerzo asimétrico que no tiene en cuenta el principio de que toda cadena se rompe por el eslabón más débil.

- A la proliferación de dispositivos informáticos móviles como laptops, smartphones, tablets y sistemas de ordenadores digitales, que aprovechan la tecnología inalámbrica para transmitir la comunicación e información militar, se añade una nueva brecha a la muralla de nuestra seguridad informática, los dispositivos forman parte del ciberespacio, generando vulnerabilidades al existir la oportunidad de introducirse en un sistema informático de defensa y el hecho de que no exista conexión física entre los terminales, no supone protección alguna, **la amenaza existe, aunque el sistema no esté conectado a internet**.

- Los ataques e intrusiones de terceros (hacker, hackativismo, piratas informáticos, agencias de inteligencia, organizaciones cibercriminales y otros), han pasado a ser una seria amenaza para las instituciones, organizaciones públicas y privadas, al tener la capacidad de operar desde cualquier parte del mundo con el único requisito de tener acceso al ciberespacio, (de hecho, ataques de ninguna, escasas o aun desconocidas consecuencias, ya se producen a diario…).

- El ciberespacio requiere la gestión de ciberseguridad desde el más alto nivel del estado, para asumir los retos y amenazas a la seguridad nacional, en función de la necesidad de protección de las estructuras críticas del país y por extensión, disponer un organismo conjunto para generar una integración de esfuerzos de las instituciones fundamentales del estado, en lo que se viene llamando la **"Aproximación del conjunto del Estado" (Whole of State Approach).**

## 1. ANTECEDENTES.

- El c**iberespacio** es un tema muy particular: de entrada, es transnacional, combina amenazas producidas por actores estatales y no estatales, afecta a vulnerabilidades civiles y militares, requiriendo de estas respuestas 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 modernas.

- Todos los países occidentales están en pleno desarrollo de definiciones de conceptos, adaptando o creando organizaciones: mandos y unidades militares a niveles estratégico, operacional y táctico, en relación con una visión y misión de políticas de ciberdefensa y ciberseguridad.



- La historia militar ha visto cómo, en menos de un siglo, se han incorporado a los ámbitos tradicionales de la tierra y el mar otros dominios físicos: el aire y el espacio y uno global y artificial (en realidad, físico también): el del ciberespacio. Hoy el vértigo de constatar que es cada vez más tarde para tomar ciertas decisiones **(tiempos digitales v/s tiempos analógicos)**, porque los acontecimientos muestran claramente la inmediatez de los eventos y que se marcha en una sola dirección.

- Se estima que 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.

- Aunque eso se ve aún muy lejos, efectivamente ese es el futuro, falta tan solo 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 (intervención a las redes ya se producen en instituciones del Estado).

- Si somos capaces de anticiparnos y reaccionar a tiempo, las consecuencias serán mínimas; si no nos organizamos antes, tarde o temprano habremos de sufrir las consecuencias a la imprevisión y falta de accionar en busca de una intervención y/o interrupción desconocida sin poder identificar.

## 2. CONCEPTOS CIBERDEFENSA Y CIBERSEGURIDAD.

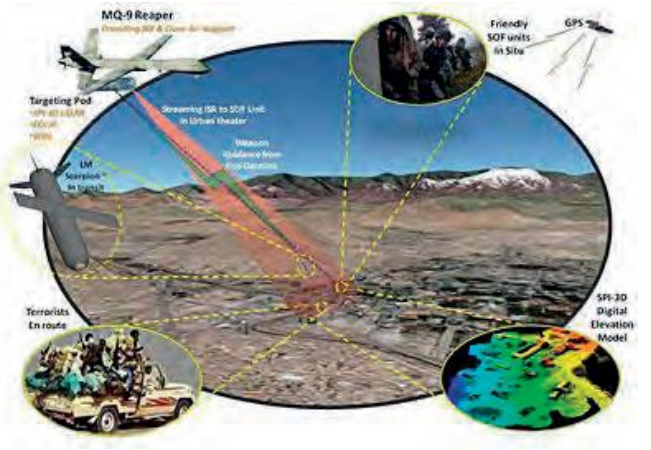
- Conviene que distingamos entre "c**iberseguridad y ciberdefensa**", porque entre ambos términos hay una frontera muy difusa, se entremezclan y es que, en ocasiones, son sinónimos. En relación con la "**ciberseguridad**", es más genérico, quien lo usa se refiere generalmente a la seguridad de la información de individuos concretos: usurpaciones de identidad, robos de propiedad intelectual; también denegaciones de servicios varios y ataques a infraestructuras no críticas (redundantes) o privadas.

- Con respecto 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 una amenaza, lo que es o no es 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" (Convención de Ginebra y Corte de la Haya),** si precisamos de leyes 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. 5 de la carta de Naciones Unidas sobre autodefensa y/o Art. V del **"Tratado de Washington de la OTAN",** la defensa individual y colectiva, como arbitrar reglas de enfrentamiento en el ciberespacio.

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

- En definitiva, cómo aplicar al ciberespacio el progreso logrado en el **"Ius ad Bellum"** (derecho internacional que regula el recurso a la fuerza por parte de los estados) y el **"Ius in Bello"** (derecho de la 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, las acciones relacionadas con la ciberguerra son ocultas.



## 3. MARCO JURÍDICO DEL CIBERESPACIO.

- Cuando se legisla es para regular la interacción social en cualquier ámbito en que esta se produzca, creando un marco que permita la convivencia y el respeto a los ciudadanos. 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 a medios informáticos en el mercado, etc.

- **En lo referido al ámbito internacional (legal) se define lo siguiente:**

• **Organización de las Naciones Unidas:**

Desde el año 2000 existen 4 resoluciones sobre aspectos concretos pero ningún acuerdo global; por ejemplo, en el año 2010 faltó consenso para aprobar una propuesta contra el cibercrimen.

• **Consejo de Europa:**

Concurre la existencia del Convenio sobre ciberdelincuencia (Budapest, 2001), aspectos de jurisdicción, extradición, coordinación, asistencia mutua.

• **Unión Europea:**
El año 2010, la Comisión Europea presentó un plan con iniciativas legislativas para ella misma y los estados miembros.

• **Parlamento Europeo:**
Se materializó la resolución general del año 2012.

• **España:**
▪ Hay artículos del Código Penal que son trasladables al ciberespacio.

▪ En el año 2010 se introdujeron dos nuevos delitos exclusivos (informáticos).

- **En lo referido a la OTAN:**

Cabe destacar el "**Manual jurídico 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, destacándose el Manual de Tallinn.

## 4. SÍNTESIS DEL MANUAL DE TALLINN

- Bajo los auspicios del "**Center of Excellence on Cyberdefense**", de Tallinn (Estonia), es un grupo internacional de expertos legales que 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 uno de los avances notables que se ha registrado a este respecto jurídico.

- El manual identifica cuánto les parece aplicable del derecho internacional, que no es poco, y establece hasta un total de 95 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.

- No hay un código de conducta internacionalmente aceptado 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. 5 de la UN Charter) requiere la existencia de un ataque armado, por lo que ya se precisa definir muy bien las características que deben reunir los ataques efectuados con medios cibernéticos para cumplir tal condición.

## 5. PRIORIDAD DE LA CIBERDEFENSA EN LA OTAN.

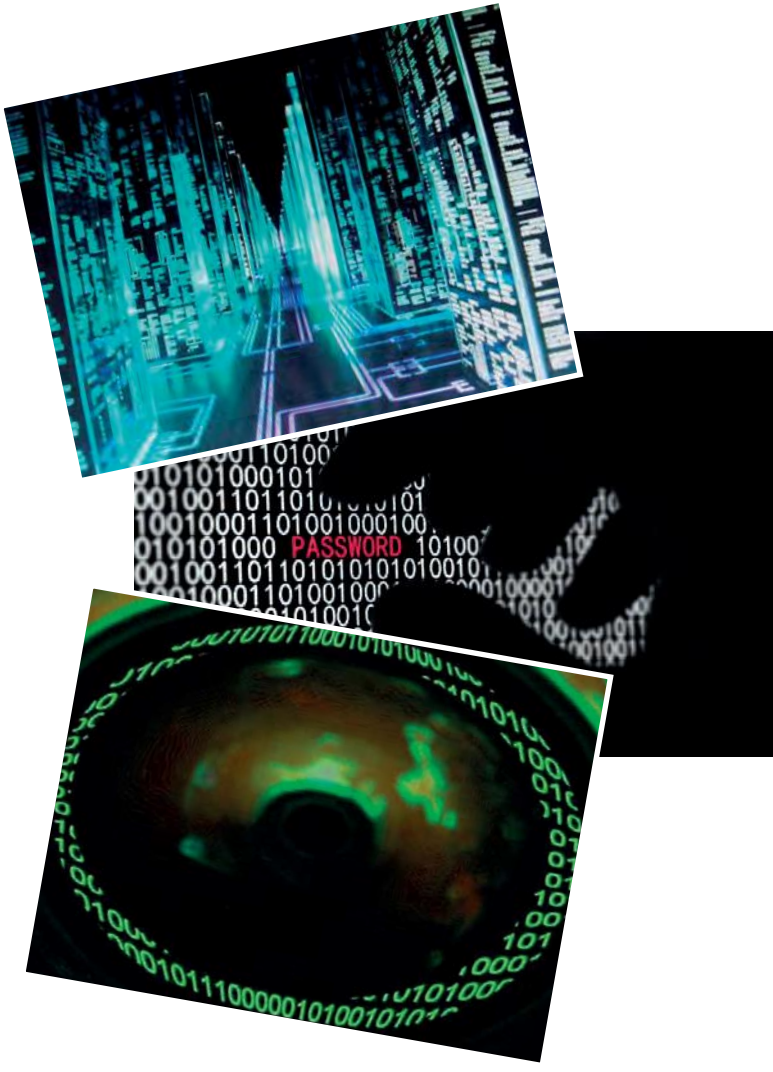
- La **ciberdefensa** está declarada como una de las primeras prioridades para **OTAN y UE**. También para **USA** (Comando de Ciberdefensa con 9.000 personas). En cuanto a otros países y ejércitos, como China, Irán y Corea del Norte, se cree que están preparando ciberejércitos.

- **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, política adoptada el mismo año por los Ministros de Defensa.

- **La UE** tiene una estrategia europea de seguridad, desde el año 2008, que identifica ya ciberamenazas, como posibles y probables, y establece la urgente necesidad de colaboración internacional en materia de ciberseguridad y ciberdefensa.

## 6. TÉCNICAS MILITARES Y OTRAS CONSIDERACIONES.

- La evolución de la guerra electrónica (consistente básicamente en impedir o perturbar las 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** por ejemplo (no digamos un grupo de ellos o un ejército de cibernautas), con un equipo portátil y cierto software solo necesita conocimiento de vulnerabilidades y ya puede atacar (dañar o tomar control de ordenadores y redes), de aquellos sistemas de información que él haya decidido convertir en sus objetivos críticos, como lo son: atacar la red eléctrica de un país, tránsito aéreo y urbano, embalses de agua, depósitos de ácidos de minerales, paralizar sistemas de información y comunicaciones de las FAs (Sistemas de Armas y Tecnologías, Sistemas de C4I y aviones UAVs).

- Cabe señalar que dentro del mundo de las **capacidades militares en materia de ciberdefensa,** se distinguen:

• **Defensa** (protección de las redes de información y comunicación y sistemas de armas propios).

• **Explotación** (inteligencia de adversarios y de sus medios e intenciones militares, etc.).

• **Respuesta** (ante un ataque cibernético o no con otro).

- Constituye una realidad que se está empezando a militarizar el ciberespacio, porque hay oportunidades para la acción estratégica que son mucho menos caras que las de las armas convencionales y nucleares, pero que pueden ser igual de efectivas que aquellas y, tal vez, que estas últimas.

- El ciberespionaje, que ya está ahí, y la militarización del ciberespacio que está por llegar, generará un nuevo paradigma de variables por considerar en el campo de batalla y las funciones de combate y para ello se necesita una respuesta común, porque los problemas y las amenazas serán comunes.

- 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…

- 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.

## 7. LA POLÍTICA DE CIBERDEFENSA EN 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.

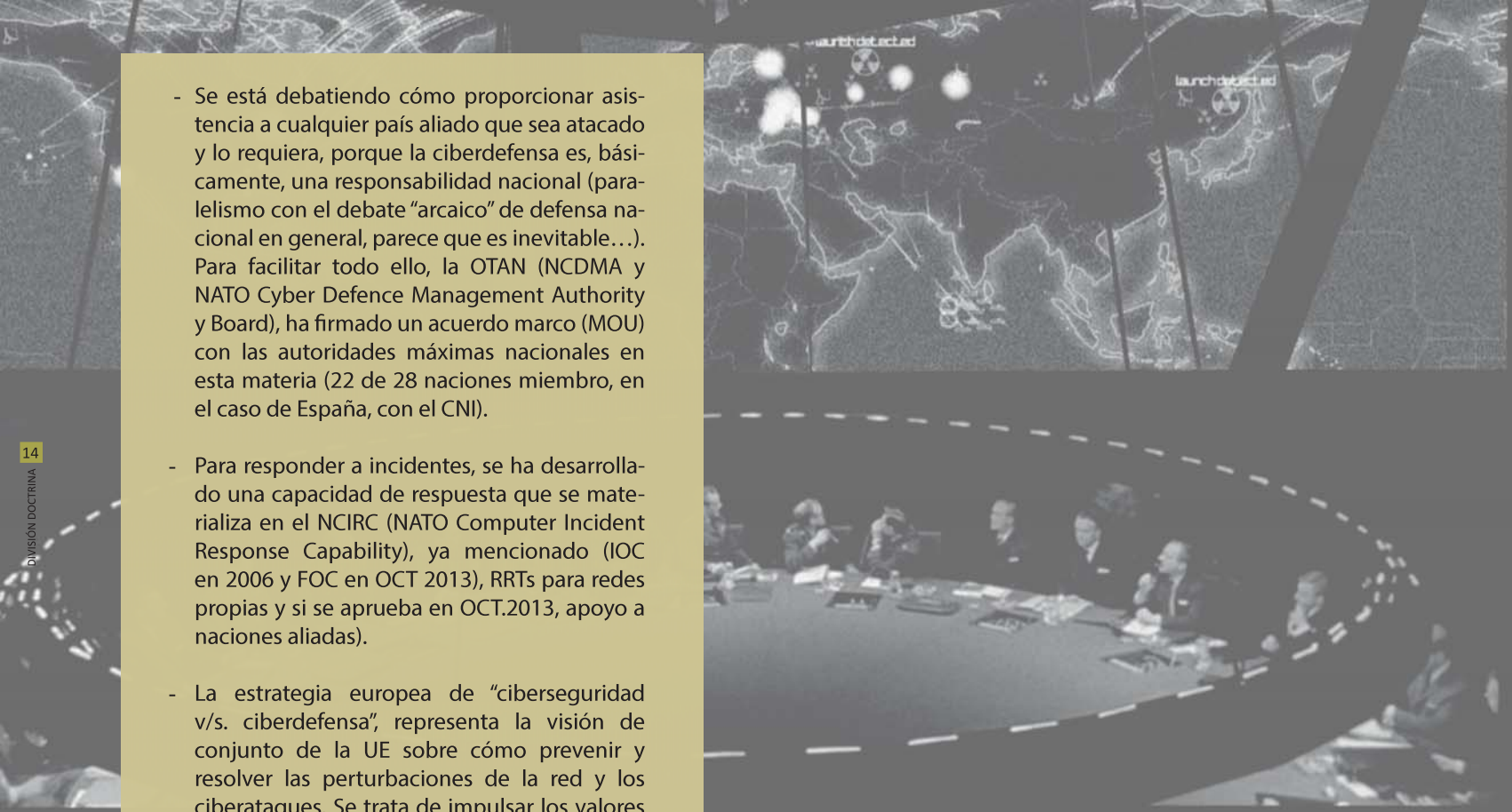
- Desarrollar capacidades y proteger las redes propias y nacionales conectadas, apoyando a los aliados en lo posible.

- 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 ante 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 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).

- Para responder a incidentes, se 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.2013, apoyo a naciones aliadas).

- La estrategia europea de "ciberseguridad v/s. 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 resistencia de los sistemas y reducir la delincuencia informática; además, desarrollar capacidades en el ámbito de la "Política Común de Seguridad y Defensa" (CSDP) y la colaboración en el establecimiento de una política internacional adecuada.

- Se han logrado importantes avances como crear un "Centro Europeo de Ciberdelincuencia".

  Pero también se preocupa la UE de la ciberdefensa como capacidad militar e integra su desarrollo en la "Planificación propia 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 las capacidades militares de la OTAN-UE.

## C. CONCLUSIONES.

- 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 sido 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 por hacer en este nuevo paradigma referido al ámbito del ciberespacio, para absorber adecuadamente los nuevos conceptos cibernéticos en el pensamiento estratégico y desarrollar las correspondientes nuevas capacidades, con el fin de estar en condiciones de defendernos de ciberataques y gestionar ciberemergencias.

- Las tecnologías de la información y comunicación hacen posible casi todo lo que nuestras FAs necesitan: apoyo logístico, mando y control, información de inteligencia en tiempo real etc. En menos de una generación, las TICs en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico.


## Bibliografía:

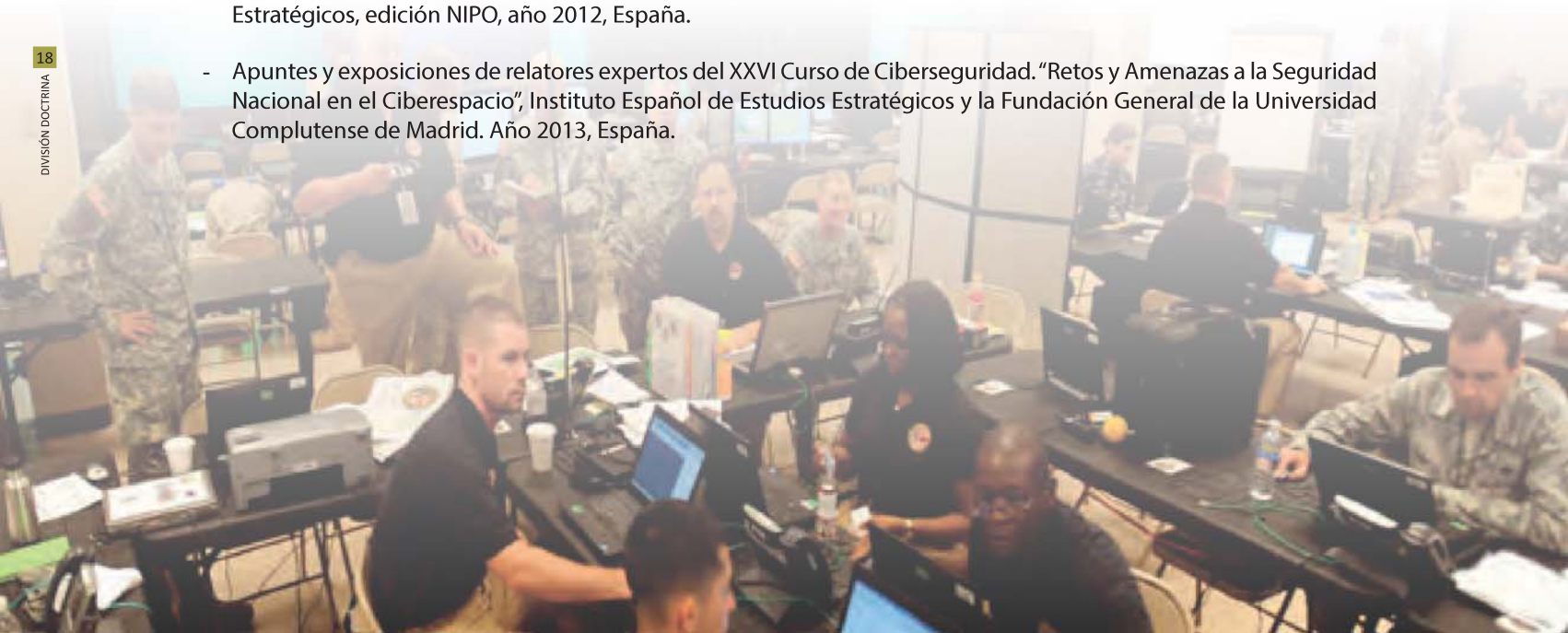

- Artiles Ganuza, Néstor, "La situación de ciberseguridad en el ámbito internacional y en la OTAN", Instituto Español de Estudios Estratégicos, edición NIPO, año 2011, España.

- Durán del Río, José Juan, "La ciberseguridad en el ámbito militar", Instituto Español de Estudios Estratégicos, edición NIPO, año 2011, España.

- Agreda de Gómez, Ángel, "El ciberespacio como entorno social y de conflicto", Instituto Español de Estudios Estratégicos, edición NIPO, año 2012, España.

- Apuntes y exposiciones de relatores expertos del XXVI Curso de Ciberseguridad. "Retos y Amenazas a la Seguridad Nacional en el Ciberespacio", Instituto Español de Estudios Estratégicos y la Fundación General de la Universidad Complutense de Madrid. Año 2013, España.



DIVDOC


DIVISIÓN
DOCTRINA