ARI | ARI 26/2013
4 de julio de 2013

Real Instituto Elcano

Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales

Thiber[1]

Tema

Las cibercélulas son una herramienta eficaz para que los países puedan operar, defenderse o atacar en un determinado ámbito cibernético y están llamadas a complementar las capacidades de ciberseguridad y ciberdefensa existentes.

Resumen

En la actualidad, y salvo países pioneros en la ciberseguridad y ciberdefensa como EEUU, China e Israel, la mayor parte de los países está desarrollando sus capacidades cibernéticas básicas, como sus tecnologías de información y comunicaciones y las organizaciones y procedimientos que las harán funcionar cuando alcancen su madurez. Cuando eso ocurra será necesario articular las organizaciones y procedimientos operativos –cibercélulas– que permitan operar desde esas capacidades previas. Este ARI describe el concepto de las cibercélulas, sus funciones, tareas y ámbitos de actuación, así como los habilitadores que permitirán su funcionamiento. Aunque se trata de una capacidad de siguiente generación y complementaria a las que se están instalando, los autores proponen la necesidad de que se vaya reflexionando en España sobre el tipo de cibercélulas que complementarían las capacidades de ciberseguridad y ciberdefensa que se están instalando para su empleo por las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado.

Análisis

Tras varias décadas marcadas por un espectacular desarrollo tecnológico, una notable despreocupación política y una excesiva confianza popular acerca del poder, impacto, penetración e influencia política, social y económica de las Tecnologías de la Información y las Comunicaciones (TIC), la mayoría de los gobiernos ha comenzado a constatar tanto las posibilidades como los riesgos que entraña el ciberespacio y proliferan las estrategias y organizaciones de ciberdefensa y ciberseguridad, de la que existen numerosos estudios recientes.[2]

1 Los autores forman parte del grupo de trabajo sobre "Cibercélulas" dirigido por THIBER, *The Cybersecurity Think Tank*, perteneciente al Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid. Por orden alfabético: Guillem Colom Piella, doctor en seguridad Internacional; José Ramón Coz Fernández, doctor en Informática y licenciado en Ciencias Físicas; Enrique Fojón Chamorro, ingeniero superior en informática y miembro del ISMS Forum Spain; y Adolfo Hernández Lorente, ingeniero superior en informática y gerente de seguridad en Ecix Group.

2 Applegate, Scott D. (2012), *Leveraging Cyber Militias as a Force Multiplier in Cyber Operations*, Center for Secure Information Systems, George Mason University, Fairfax.

Berman, Ilan (2012), *The Iranian Cyber Threat to the US Homeland*, comparecencia en el Comité de Seguridad Interior de la Cámara de Representantes, Washington DC, 26/IV/2012.

Cabinet Office (2012), *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World*, HMSO, Londres.

Defense Science Board (2013), *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, US Department of Defense, Washington DC.

Department of Defense (2013), *Defense Budget Priorities and Choices – Fiscal Year 2014*, US Government Printing Office, Washington DC.

Dev Gupta, Keshav, y Jitendra Josh (2012), "Methodological and Operational Deliberations in Cyber-attack and Cyber-exploitation", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, nr 11, pp. 385-389.

Liles, Samuel, y Marcus Rogers (2012), "Applying traditional military principles to cyber warfare", Cyber Conflict (CYCON), NATO CCD CoE Publications, Tallin, pp. 1-12.

Office of Public Affairs (2010), US Cyber Command Fact Sheet, Department of Defense, Washington DC.

Office of the Secretary of Defense (2013): Military and Security Developments Involving the People's Republic of China 2013, US Government Printing Office, Washington DC.

Aunque el ciberespacio se consideró inicialmente como un bien común global (*global common*) de toda la humanidad, en realidad dista mucho de ser un entorno neutro, libre e independiente. De hecho, la beligerancia en el ciberespacio es coetánea a su nacimiento y países como China, EEUU, Rusia, Israel e Irán están destinando ingentes recursos humanos, técnicos y económicos para el desarrollo de sus ciberfuerzas con un doble objetivo: por un lado, garantizar la seguridad y defensa de sus ciberespacios específicos y, por otro, ejercer poder e influencia entre sus ciudadanos, aliados y potenciales adversarios.

Igualmente, ante la imposibilidad de una regulación internacional y en ausencia de una gobernanza global de Internet, el ciberespacio ha visto un aumento de sus riesgos asociados a la seguridad de las sociedades avanzadas: el imparable incremento del cibercrimen, la utilización del ciberespacio por parte de grupos terroristas para ejecutar actividades de financiación, inteligencia, propaganda y captación, el ciberespionaje a gran escala entre Estados y/o empresas y el incremento de los delitos contra la privacidad de los usuarios en Internet son solo algunos de los retos a los que debe enfrentarse los responsables de las fuerzas de seguridad encargados de la ciberseguridad.

Del mismo modo, y en relación con la Defensa, las Fuerzas Armadas dependen de las TIC para comunicarse, ejercer el mando y control de las operaciones, obtener y distribuir información e inteligencia, realizar labores de vigilancia, reconocimiento o adquisición de objetivos o coordinar los fuegos, con lo que las TIC actúan como multiplicador de la fuerza y optimizan la concepción, planificación y ejecución de las operaciones, pudiendo condicionar el desarrollo y resultado de una contienda. Por lo tanto, la posesión de una infraestructura TIC robusta, segura y resiliente, la sistematización de las dimensiones que componen el ciberespacio y su integración en la planificación operativa o la capacidad para actuar en este dominio son algunos de los asuntos que más atención están recibiendo desde las Fuerzas Armadas.

Estado de riesgo del ciberespacio

El estado de riesgo del ciberespacio no es homogéneo. Ello se debe tanto a la existencia de distintos niveles de amenaza sobre los ciberespacios nacionales específicos como a que los sistemas y capacidades de ciberseguridad y ciberdefensa de los distintos países no son, en absoluto, homogéneos. Dependiendo del nivel de implantación y funcionalidad de sus sistemas nacionales de ciberseguridad y ciberdefensa, los países pueden agruparse en cuatro grandes grupos:

- Grupo 1, formado por aquellos países que disponen de un Sistema Nacional de Ciberseguridad y Ciberdefensa operativo, formalmente definido y en continúo proceso de evaluación, revisión y mejora. Este grupo estaría formado por países como EEUU, China e Israel.

• Grupo 2, formado por aquellos países que se encuentran en un proceso formal de construcción de sus sistemas nacionales de ciberseguridad y ciberdefensa. Este grupo estaría formado por países como Australia, Francia e Irán.
• Grupo 3, formado por aquellos países que se hallan en proceso de definición –formal o informal– de sus sistemas nacionales de ciberseguridad. Este grupo estaría formado por la gran mayoría de países, incluida España.
• Grupo 4, formado por aquellos países que todavía no han emprendido una definición –formal o informal– de su sistema nacional de ciberseguridad.

Recientemente, el gobierno de EEUU ha reconocido que el aumento exponencial en el volumen de recursos que sus adversarios –en especial China– destinan a la consolidación de sus ciberfuerzas, así como la evolución técnica de los ciberataques que éstos ejecutan, están dificultando enormemente las tareas de análisis e investigación de los mismos y, por tanto, una defensa nacional eficiente y efectiva en el ciberespacio.

Independientemente del origen y naturaleza de la amenaza, la ciberfuerza de una nación debe construirse sobre un conjunto de capacidades que le permitan alcanzar un estado de riesgo conocido y controlado. Este estado de riesgo solo podrá ser alcanzado por aquellos Estados cuyos ciberespacios específicos dispongan de unos niveles de madurez, resiliencia y seguridad suficientes que, en el corto plazo, sean capaces de absorber ataques de los niveles TIER I y TIER II, así como recuperarse de ataques TIER III y IV, que describe la Figura 1.

Figura 1. Niveles de amenazas cibernéticas

TIER	DESCRIPCIÓN	PERFIL DEL ATACANTE	CONSECUENCIAS POTENCIALES
I	Profesionales que hacen uso de exploits conocidos	Profesionales con una cualificación de nivel medio	Interrupción temporal de servicios TIC
II	Profesionales con gran experiencia y capacidad para desarrollar sus propias herramientas a partir de vulnerabilidades conocidas	Profesionales con una cualificación de nivel alto	Interrupción temporal de servicios TIC
III	Profesionales que se centran en el descubrimiento y el uso de códigos maliciosos desconocidos	Profesionales con una cualificación de nivel alto	Interrupción prolongada de servicios TIC
IV	Actores estatales o grupo criminales bien organizados y financiados con el objetivo de descubrir nuevas vulnerabilidades y desarrollar exploits	Actores estatales y grupos criminales	Sustracción de información clasificada y ataques a infraestructuras críticas
V	Actores estatales con la capacidad de crear vulnerabilidades a partir de la infiltracion en la cadena de produccion de productos y servicios comerciales con el objetivo de explotar redes y sistemas de interés	Actores estatales	Sustracción de información clasificada y ataques a infraestructuras críticas
VI	Actores estatales con la capacidad de ejecutar ataques de espectro completo, mediante el uso de capacidades cibernéticas y cineticas, con el objeto de lograr un resultado específico en los ámbitos político, militar, económico y/o social a gran escala	Actores estatales	Ataques a infraestructuras críticas y cambios geopolíticos

Las capacidades tradicionales –encuadradas dentro de los conceptos de seguridad de la información (*information security*) y aseguramiento de la información (*information assurance*)– son necesarias pero no suficientes para garantizar la ciberseguridad y la ciberdefensa nacional. En consecuencia, las principales potencias mundiales, así como organizaciones internacionales como la Alianza Atlántica y EUROPOL, están trabajando activamente en la redefinición de estas capacidades tradicionales y en la generación de nuevas capacidades cibernéticas tanto defensivas como ofensivas.

El aumento en el estado de riesgo del ciberespacio hace necesario que los gobiernos desarrollen capacidades específicas para mejorar su seguridad y defensa en él. Una de éstas son las cibercélulas, una capacidad avanzada que, susceptible de complementar a las capacidades tradicionales de ciberseguridad y ciberdefensa, puede emplearse tanto de forma defensiva como para realizar operaciones ofensivas en el ciberespacio. Preparadas para satisfacer todos aquellos problemas operativos que los medios cibernéticos existentes no pueden afrontar con suficiente agilidad y efectividad, las cibercélulas pueden ser integradas tanto en las fuerzas policiales como militares. Teniendo en cuenta estos elementos, a continuación se presentará el concepto de cibercélula y se expondrá su posible organización, funciones y cometidos.

Concepto de cibercélula

Una cibercélula se podría definir como una capacidad de alta especialización funcional y naturaleza dual –tanto defensiva como ofensiva– con la función de ejecutar una tarea encomendada con la finalidad de garantizar la seguridad y la defensa de un determinado ámbito cibernético. Dependiendo de las necesidades operativas y del ámbito en la que ésta actúe, una cibercélula puede tener asignadas tres grandes funciones:

- Ejecutar operaciones cibernéticas específicas o conjuntas con el resto de las dimensiones operativas (terrestre, naval, aérea y espacial).
- Apoyar la evaluación y mejora del nivel de madurez, resiliencia y seguridad de las capacidades cibernéticas nacionales, aliadas y multinacionales.
- Contribuir a la experimentación de nuevos conceptos operativos y capacidades cibernéticas.

Del mismo modo, y dependiendo de la función que desarrolle en cada momento, una cibercélula tendrá asignada una de las siguientes cuatro tareas: (1) aseguramiento; (2) experimentación; (3) ejercicios; y (4) operación. En las tres primeras tareas, la cibercélula asumirá el papel de "equipo rojo", por lo que simulará el comportamiento de un potencial adversario para intentar explotar las vulnerabilidades del ámbito evaluado. No obstante, cuando ésta se halle en modo operación, la cibercélula podrá realizar tanto acciones cibernéticas defensivas como ofensivas.

1. *Aseguramiento*: esta tarea permitirá analizar el estado de madurez, resiliencia y seguridad del ámbito en el que actúe la cibercélula.

2. *Experimentación*: durante la experimentación, la cibercélula podrá llevar a cabo actividades muy heterogéneas, como el estudio de nuevos conceptos operativos o la evaluación de la madurez, resiliencia y seguridad de nuevas capacidades cibernéticas que complementen a las ya existentes.

3. *Ejercicios*: durante los ejercicios, la cibercélula deberá poner a prueba su capacitación. Estos estarán diseñados y planificados con el objetivo de simular situaciones lo más cercanas a la realidad.

4. *Operación*: cuando las necesidades operativas lo demanden, la cibercélula deberá llevar a cabo actividades defensivas, ofensivas y/o de explotación en un ámbito determinado.

Cada una de las cuatro tareas encomendadas a la cibercélula se llevará a cabo en un determinado ámbito de los cinco que se identifican a continuación:

1. *Ámbito local*, circunscrito a un sistema TIC local.

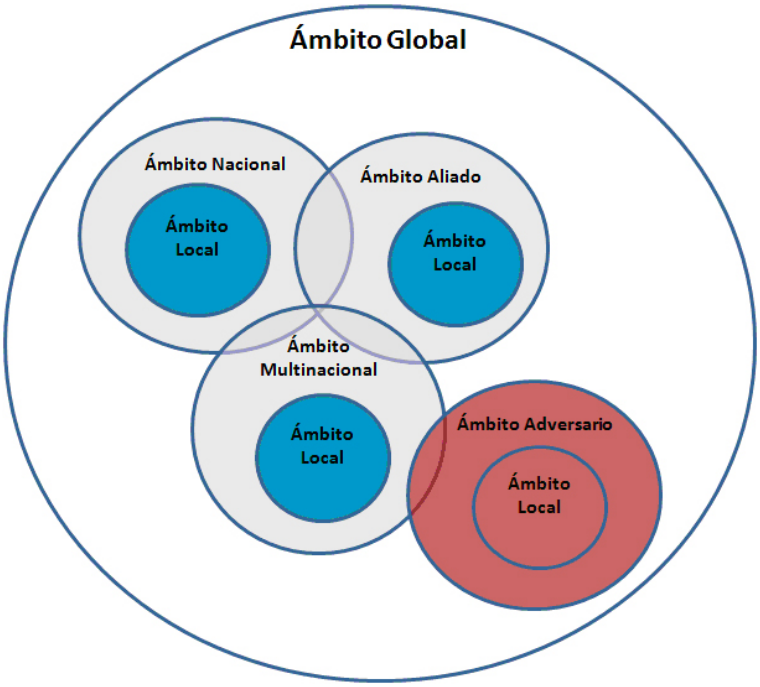
2. Ámbito nacional, circunscrito a un ámbito local o conjunto de ámbitos locales cuyo mando y control es ejercido por un organismo nacional.

3. *Ámbito aliado*, circunscrito a un ámbito local o conjunto de ámbitos locales cuyo mando y control es ejercido por un organismo propio de la Alianza Atlántica o Europol o por organismos pertenecientes a uno de sus Estados miembros.

4. *Ámbito de posibles adversarios*, circunscrito a un ámbito local o conjunto de ámbitos locales cuyo mando y control es ejercido por organismos pertenecientes a posibles adversarios. La naturaleza de los posibles adversarios es heterogénea, pudiendo tratarse de Estados o actores no-estatales, tales como grupos terroristas, ciber-bandas o grupos *hacktivistas*.

5. *Ámbito multinacional*, circunscrito a un ámbito local o conjunto de ámbitos locales cuyo mando y control es ejercido por un organismo multinacional o por un Estado perteneciente al organismo multinacional.

Figura 2. Ámbitos de actuación de una cibercélula



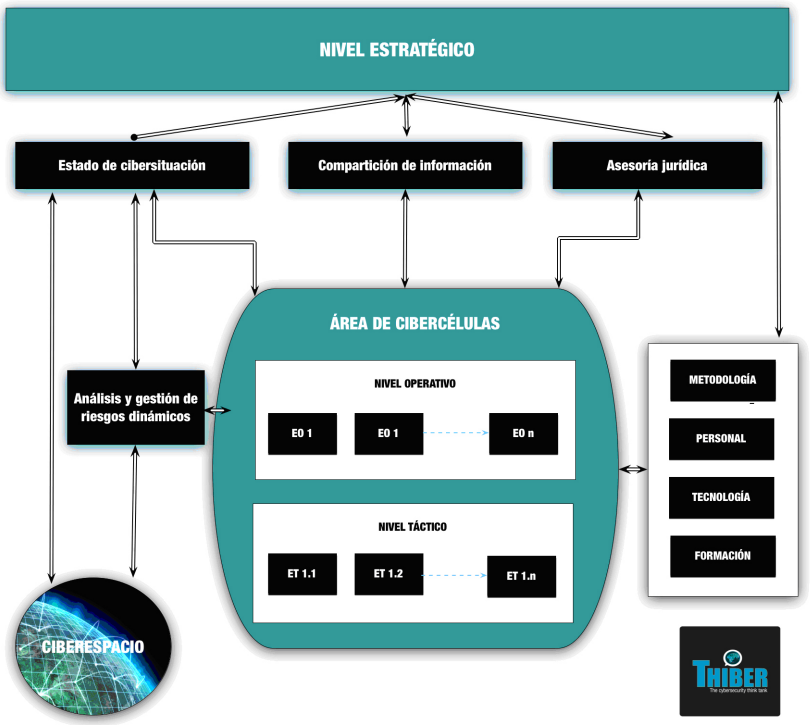
Habilitadores de las cibercélulas

Antes de la creación de las cibercélulas, los países deben contar con los habilitadores adecuados. Por habilitadores se entiende aquellos medios cibernéticos defensivos y ofensivos que cuenten con un nivel de madurez suficiente y que ya estén implantados en el país y a disposición tanto de las Fuerzas de Seguridad como de las Fuerzas Armadas. Su existencia en las condiciones descritas posibilitará que las cibercélulas puedan ejecutar con ciertas garantías de éxito las tareas asignadas.

Estos habilitadores son los siguientes: mando y control, organización, marco legislativo, metodología, conocimiento de la ciber-situación, análisis y gestión de riesgos, compartición de información, tecnología, personal y capacitación continua. El Mando y Control de las cibercélulas deberá ejercerse en los niveles estratégico, operacional y táctico y cada uno de estos niveles tendrá asignadas un conjunto de responsabilidades y acciones con el propósito de que las cibercélulas desempeñen su tarea con garantías. En el nivel estratégico se definirán los objetivos de alto nivel, las prioridades y los hitos que deben ser alcanzados por la cibercélula durante la tarea encomendada. Además, desde este nivel se deberá garantizar la viabilidad y evolución de la cibercélula, dotándola de todos los recursos humanos, económicos y tecnológicos necesarios. En el nivel operativo, se autorizarán y dirigirán todas las actuaciones pertenecientes a la tarea encomendada y cada una estará controlada por un equipo operativo (EO), de modo que durante la ejecución de una tarea habrá tantos equipos operativos como actividades que forman parte de cada tarea. Y la composición de estos equipos vendrá determinada

por la naturaleza de la tarea. Por último, y en el nivel táctico, los responsables de cada EO definirán los planes tácticos de las actividades. Para ello, desglosarán hasta el nivel más granular de definición posible cada una de las acciones que conforman una actividad con el asesoramiento de los responsables de los equipos tácticos asignados a cada acción (cada EO estará apoyado por tantos equipos tácticos como acciones formen parte de la actividad).

Figura 3. Contextos externo e interno de las cibercélulas



A pesar de la dificultad de localizar a los autores materiales de una agresión en el ciberespacio, así como a la ubicuidad, alto nivel de *interconectividad* y naturaleza transfronteriza del ciberespacio, es necesario que las tareas, actividades y acciones de las cibercélulas se mantengan dentro de los límites de la legalidad nacional e internacional. Para que el ordenamiento jurídico pueda servir de habilitador, debe estar al día en la regulación de aquellos aspectos sustantivos sobre ciberguerra y ciberdelincuencia, sus marcos normativos y su tipificación penal. También debe regular los aspectos procedimentales en materia de prueba electrónica, justicia penal y cooperación internacional. Finalmente, debe integrarse en la legislación nacional e internacional asociada con la prevención de los conflictos armados y el ejercicio de la autodefensa de la soberanía sobre el ciberespacio nacional.

Las cibercélulas deberán contar con una metodología de trabajo que proporcione un lenguaje común, unos fundamentos teóricos y tecnológicos homogeneizados y unos

procedimientos que normalicen su funcionamiento en los niveles estratégico, operacional y táctico. Además, se las deberá proporcionar el conocimiento inmediato del ciberespacio propio, del aliado, del multinacional, de los posibles adversarios y de cualquier otro grupo de interés, así como el conocimiento del estado y disponibilidad de las capacidades operativas que son necesarias para el planeamiento, dirección y gestión de las operaciones necesarias para la misión cibernética encomendada. El conocimiento del estado de la situación cibernética (ciber-situación) se obtendrá como resultado de la combinación de actividades de inteligencia y operativas en el ciberespacio junto con las realizadas en el espacio electromagnético y en cualquier otra de las dimensiones del entorno operativo (tierra, mar, aire y espacio). En consecuencia, la integración de la ciber-situación con el resto de capacidades es esencial para alcanzar los objetivos de la tarea encomendada. De esta manera, los procesos, procedimientos y capacidades del conocimiento de la ciber-situación deberán desarrollarse –siempre en línea con la metodología de trabajo vigente– de forma que los responsables de la cibercélula obtengan un conocimiento completo de la ciber-situación global y puedan progresar hacia los objetivos de las tareas encomendadas. Además, el conocimiento de la ciber-situación deberá proporcionar al responsable operativo de la cibercélula la visibilidad, en tiempo real, de las redes, sistemas y servicios locales y nacionales y de las acciones del posible adversario sobre las redes, sistemas y servicios propios, así como el posible impacto de estas acciones en la consecución de los objetivos operativos. La ciber-situación sobre la misión y el ciberespacio también ayudará a las cibercélulas a tomar decisiones si cuentan con la mejor información e inteligencia disponible y a actuar si conocen el efecto operativo de sus decisiones sobre el conjunto de la misión.

Cada tarea encomendada a una cibercélula llevará siempre asociado un conjunto de riesgos que dependerá de su naturaleza y del ámbito de ejecución, por lo que deberán desarrollar un proceso continuo de análisis y gestión de riesgos dinámicos en todas las fases de la tarea. En ellas se recopilará y analizará toda la información disponible y se distribuirá de manera pertinente al resto de actores involucrados en la tarea. Por lo tanto, será necesario articular un conjunto de mecanismos que distribuyan la información para tener un conocimiento fiable y actualizado de la ciber-situación, optimizar los resultados, mejorar la madurez, resiliencia y seguridad del ciberespacio nacional así como la gestión de las crisis cibernéticas.

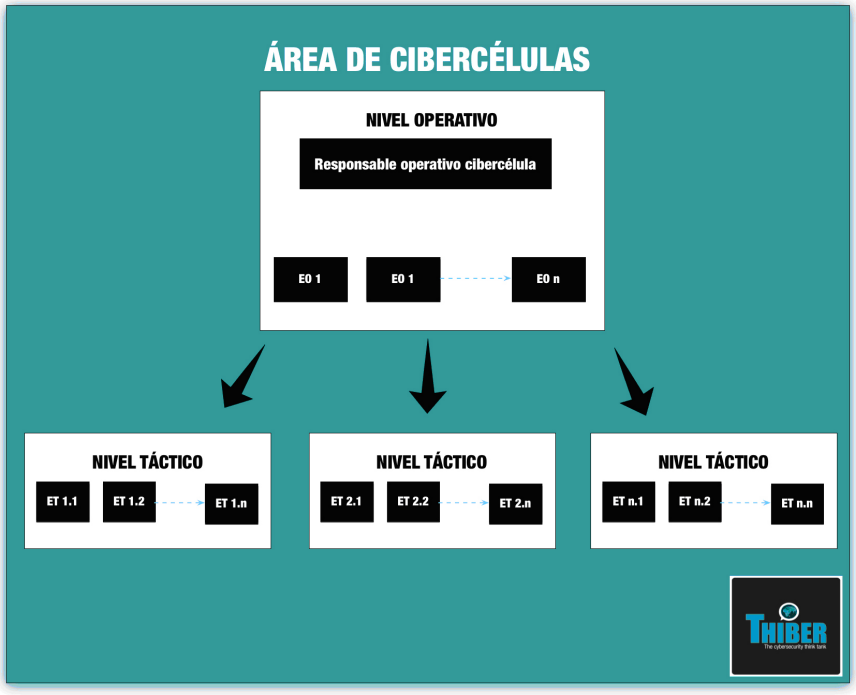
La tecnología es el componente central del ciberespacio. Por ello, las cibercélulas deberán estar dotadas de capacidades tecnológicas de primer nivel. También deberán estar formadas por un conjunto de profesionales altamente cualificados y especializados que cubran todas y cada una de las áreas de conocimiento de las actividades y acciones que forman parte de las tareas encomendadas. Además, será necesario disponer de un plan de formación continua y muy especializada en función de su papel específico dentro de la cibercélula y acorde con la continua transformación tecnológica y el

cambiante estado de riesgo del ciberespacio. En consecuencia, la capacitación será uno de los elementos clave para el éxito o fracaso de las cibercélulas.

Organización de una cibercélula

De la estructura de mando y control descrita en el apartado de habilitadores de la cibercélula del presente documento se deduce la organización de una cibercélula que aparece en la Figura 4. El responsable del área de la cibercélula es quien se encarga de traducir los objetivos estratégicos; planificar y supervisar la ejecución de las tareas encomendadas a las cibercélulas, proporcionar el conocimiento de la ciber-situación en cada momento, dirigir a los responsables operativos, planificar la formación, evaluar resultados, gestionar riesgos y habilitar los recursos técnicos y humanos necesarios. Debajo del anterior se encuentran los responsables operativos que informan al responsable del área de su cibercélula sobre el desarrollo operativo y táctico de las tareas encomendadas con unas responsabilidades similares a las de los responsables operativos de área pero a nivel inferior.

Figura 4. Organización de una cibercélula



Cada responsable operativo de un equipo se encargará de llevar a cabo cada una de las distintas actividades de la cibercélula. Ello incluirá informar al responsable operativo de la cibercélula sobre el desarrollo de la actividad encomendada, dividir las actividades en acciones, desglosar –hasta el mayor grado de granularidad posible– las acciones que serán encomendadas a los equipos tácticos, planificar y supervisar el trabajo de éstos, ejecutar el proceso continuo de análisis y gestión de las actividades encomendadas y

elaborar la información relevante de cada actividad. Finalmente, cada responsable de un equipo táctico se encargará de llevar a cabo una o más acciones, para lo que realizará las acciones encomendadas por el responsable del equipo de control operativo, informará al responsable del equipo de control operativo sobre el desarrollo de la acción encomendada, ejecutará el proceso continuo de análisis y gestión de las acciones encomendadas y elaborará la información relevante de cada acción.

Conclusiones

Tal y como ha expuesto el presente ARI, una cibercélula puede ser una eficaz herramienta para que tanto las Fuerzas de Seguridad como las Fuerzas Armadas de los Estados puedan mejorar la seguridad y la defensa de un determinado ámbito cibernético. Las cibercélulas estarían compuestas por equipos operacionales y tácticos actuando bajo el control de un mando estratégico cibernético y requieren que antes exista un conjunto de capacidades de ciberseguridad y ciberdefensa tradicionales ya maduras: una infraestructura TIC moderna, un conjunto de capacidades cibernéticas y un personal experimentado y habituado a operar en este entorno.

A partir de ahí, las cibercélulas podrían conducir operaciones cibernéticas de naturaleza defensiva y ofensiva, apoyarían la evaluación y mejora de las capacidades nacionales, multinacionales o aliadas, permitirían experimentar con nuevos conceptos operativos o adiestrar al personal destinado en esta organización. Su implementación puede mejorar sensiblemente la capacidad cibernética defensiva y ofensiva de una nación, contribuyendo así al control del ciberespacio y la creación de una ciberfuerza nacional moderna, efectiva y completamente interoperable con las ciberfuerzas aliadas. En el caso especifico de España, y al igual que el resto de sus aliados, los esfuerzos deberán concentrarse en madurar las capacidades cibernéticas de sus Fuerzas y Cuerpos de Seguridad y de sus Fuerzas Armadas a corto y medio plazo como paso previo a una implantación efectiva de una capacidad avanzada como son las cibercélulas. Sin embargo, y al igual que ya hacen los aliados, debería ir sopesando la conveniencia de implantarlas para que las capacidades cibernéticas en desarrollo puedan pasar a ser operativas a la mayor brevedad.

Real Instituto Elcano / Elcano Royal Institute
Príncipe de Vergara, 51
28006 Madrid - Spain
info[arroba]rielcano.org
www.realinstitutoelcano.org/wps/portal/
www.blog.rielcano.org/