ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

06/2014 13 enero de 2014

*José Luis Hernangómez de Mateo**

DILEMAS CIBERNÉTICOS Y LA ESTRATEGIA DE SEGURIDAD NACIONAL

DILEMAS CIBERNÉTICOS Y LA ESTRATEGIA DE SEGURIDAD NACIONAL

Resumen:

La Estrategia de Ciberseguridad Nacional española trata de dar respuesta al reto de preservar el ciberespacio, algo en realidad tan tangible como el terreno del boquete de Almansa o los teclados que manejamos a diario en nuestros sistemas. En alineación con la Estrategia de Seguridad Nacional, la recién nacida ciberestrategia evidencia la voluntad política de garantizar la seguridad de nuestros intereses. Más allá de las intenciones, principios que la rigen y objetivos a perseguir mediante unas líneas de acción y el diseño de una organización de alto nivel del Estado, ambas estrategias sugieren multitud de interrogantes acerca del carácter de nuestra ciberseguridad y de las consiguientes capacidades en desarrollo.

Abstract:

The Spanish National Cybersecurity Strategy seeks to address the challenge of preserving cyberspace, actually something as tangible as the terrain of the gap of Almansa or keyboards we use daily in our systems. In alignment with the national security strategy, the newly born Spanish cyberstrategy reflects the political will to ensure the security of our interests. Beyond intentions, principles that govern it and goals to pursue through a few lines of action and the design of a high-level of State Organization, both strategies suggest plenty of questions about the nature of our cybersecurity and the resulting capacities in development.

Palabras clave:

Seguridad, defensa, ciberseguridad, estrategia, vulnerabilidades, ofensiva, defensiva, capacidades, política, OTAN, UE.

Keywords: Security, defense, cybersecurity, strategy, vulnerabilities, offensive, defensive, skills, politics, NATO, EU.

DILEMAS CIBERNÉTICOS

"*La guerra actual puede desencadenarse desde un Starbuck*". La frase es de Steve Ewel, responsable del United States European Command (USEUCOM) para asuntos de ciberseguridad, durante un curso de verano de la Universidad Complutense de Madrid celebrado en El Escorial en julio de 2013. La ciberguerra es fragmentada y compleja, en algunos sentidos más que la convencional. Es así porque lo es el quinto terreno (el cibernético, junto a los ya tradicionales tierra, mar, aire y espacio). Aunque esa complejidad está recogida en la Estrategia de Seguridad Nacional (ESN) y en la recientemente aprobada Estrategia de Ciberseguridad Nacional (ECN), existen cuestiones de carácter estratégico que quizá no hayan quedado plasmadas en este nivel, quizá con la intención de esperar a un desarrollo posterior en un plano normativo inferior. En el caso de que hubieran sido obviadas de forma intencionada, la gravedad de las carencias detectadas sería aún mayor. La seguridad nacional debe proteger y corregir las vulnerabilidades de nuestros activos patrios, en este caso concreto, en lo que se refiere a la ciberseguridad. La pregunta que se plantea aquí y para la que deberíamos ser capaces de responder afirmativamente es si nuestras estrategias nos permiten estar preparados para detectar y reaccionar ante un ciber-Perejil, un ciber-11M o un ciber-apagón eléctrico, solos o en combinación de otro tipo de acciones más convencionales.

Ambas estrategias cumplen requisitos formales de toda estrategia -finalidad, alcance, análisis y propuestas de futuro-, pero presentan carencias que en sí mismas constituyen vulnerabilidades potenciadoras de otras vulnerabilidades. Las dos estrategias aprobadas deberían contribuir a subsanar puntos débiles que convierten a algunos activos nacionales en víctimas muy accesibles de agresiones potenciales. Y estas agresiones no siempre serán exclusivamente cibernéticas. Por ejemplo, una agresión militar convencional podría venir acompañada -en el antes, durante o el después- de un ciberataque. Y al revés: un ciberataque militar podría venir acompañado de acciones más convencionales. Ante toda agresión, cada vulnerabilidad es un talón de Aquiles del activo, es uno de sus puntos más débiles. No hay un activo sin vulnerabilidades, ni existe activo al que no se le pueda dañar.

Un análisis de riesgos realizado de modo tradicional, con independencia de las diferentes metodologías existentes, concluye con una relación priorizada de riesgos a minimizar mediante la aplicación de unas medidas de seguridad. Dos precisiones a este respecto. La primera es que puede ocurrir que exista un riesgo muy bajo de que sobre un activo muy importante se pueda llegar a materializar una amenaza sumamente improbable. Mientras la práctica habitual suele ser no tratar dicho riesgo, resulta innegable que es una práctica en sí misma sumamente peligrosa: ¿acaso debemos no preocuparnos de una denegación prolongada del suministro eléctrico en una gran parte del territorio nacional a causa de un ataque, ciber o no, por muy improbable que resulte y por muy costosa que parezcan las medidas a adoptar? La segunda precisión es que, para proteger los activos, habitualmente

podremos actuar solo sobre sus vulnerabilidades, no sobre las amenazas. Por ejemplo: ante el terrorismo, podremos proteger nuestras infraestructuras críticas corrigiendo debilidades "defensivas" propias, pero no suprimiendo a toda la amenaza, a todos los terroristas. Eliminar esa amenaza, además de ser tarea compleja o más bien imposible, implicaría probablemente actuaciones escasamente legales y éticas. Las dos estrategias nacionales han trazado el abanico de amenazas posibles, aunque en el caso de la ciberseguridad no es fácil encontrar menciones a las agresiones militares, y han señalado un catálogo de activos a proteger. Como la Seguridad Nacional trata, entre otras cosas, de corregir las vulnerabilidades nacionales para prevenir o mitigar riesgos, y hoy día eso es tarea de todos y no solo de los militares, es necesario que todos abramos los ojos y las mentes para combatir a los agresores y no a escenarios que se deben plantear aunque haya quienes piensen que serían cosas de ciencia ficción que solo ocurren a los demás.

La ESN dice de sí misma que es "*la articulación fundamental de la Seguridad Nacional como Política de Estado. Contiene directrices con el fin de reasignar todos los recursos disponibles del Estado de manera eficiente para la preservación de la Seguridad Nacional. En particular, hace un diagnóstico de nuestro entorno de seguridad, concreta los riesgos y amenazas a los que se enfrenta España en un mundo en constante transformación, define líneas de acción estratégica y configura un nuevo Sistema de Seguridad Nacional*". Básicamente, expone dos cosas: un análisis de riesgos y un sistema de gestión de la seguridad. La Seguridad Nacional es definida como "*la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos*". Aquí se marcan los grandes fines últimos de la Seguridad Nacional, directamente relacionados con activos concretos a proteger.

Un repaso no exhaustivo de los tres grandes fines de la Seguridad Nacional y de los activos vinculados, nos permite vislumbrar a grandes rasgos los activos a proteger y, por tanto, ir perfilando las vulnerabilidades de la ESN y de nuestro nuevo sistema de gestión. Nos referimos a la libertad y el bienestar de sus ciudadanos (estrechamente relacionados con las infraestructuras críticas), a la defensa de España y sus principios y valores constitucionales (estrechamente relacionados con el título preliminar y varios artículos de nuestra Constitución y de la Carta de Naciones Unidas), a la seguridad internacional en el cumplimiento de los compromisos asumidos (vinculados con las legalidades nacional e internacional), así como a los intereses económicos y financieros, básicamente, bajo el paraguas de las relaciones políticas en espacios internacionales y supranacionales diversos.

La Estrategia de ciberseguridad de la UE[1] también nos habla de los activos que, al parecer, son del interés de los europeos: las leyes y normas, la protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad, el acceso para todos, la gobernanza multilateral democrática y eficaz y la responsabilidad compartida a la hora de garantizar la seguridad. Para ello, la UE se marca cinco prioridades: lograr la ciberresiliencia (concepto últimamente de moda, sobre todo para quienes, como se dice coloquialmente, suelen tocar de oído); reducir drásticamente (interesante este énfasis) la ciberdelincuencia; desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD); desarrollar recursos industriales y tecnológicos de ciberseguridad; y establecer una política internacional coherente del ciberespacio para la UE y promover los valores esenciales de la UE. En ese discurso estratégico, destaca su sesgo preminentemente "civil" y reactivo-defensivo, frente al "militar" y al prácticamente inexistente proactivo-ofensivo. Este extremo se trata más adelante.

Los dilemas planteados tienen que ver con carencias e incertidumbres en algunos casos fácilmente explotables por amenazas potenciales. Algunas son muy ciertas y próximas, y no solo externas. Y todas están íntimamente relacionadas con la ciberseguridad y la ciberdefensa.

IDENTIFICACIÓN INSUFICIENTE DE VALORES. "¿EN QUÉ CREEMOS?"

En una Estrategia, ¿está de más hablar de valores, identificarlos, explicitarlos y consolidarlos? La ESN actual habla de valores constitucionales, de valores compartidos, de valores exclusivamente nacionales... pero no quedan recogidos como hacía la anterior Estrategia Española de Seguridad de 2011: "*los valores democráticos y del Estado de Derecho, junto a la defensa de la paz, la libertad, la tolerancia, la solidaridad, la sostenibilidad y el progreso global, y la preservación de unos modos de vida respaldados por el Estado del bienestar. Dichos valores son el reflejo de las convicciones de nuestra sociedad y están recogidos en la Constitución Española y en la Carta de Naciones Unidas*". ¿Está de más que sean citados expresamente, a pesar de que todos nos sepamos de memoria la Constitución?

[1] Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF). Acceso el 11.12.2013.

PERCEPCIÓN DÉBIL DE LA AMENAZA. "NO DESCUIDEMOS NINGÚN AGRESOR POTENCIAL"

No basta con que las elites de la sabiduría política y de seguridad elaboren documentos de alto nivel. Es preciso que la percepción de la amenaza esté firmemente arraigada a los tres niveles políticos, de la administración y de la sociedad. Sin paranoias. Algunas agresiones militares suelen sorprender. Como las acciones terroristas. Como los tsunamis. Como los casos de ciberespionaje. ¿Realmente nos tomamos todos en serio el problema de la seguridad? Recordemos a Casandra y a Apolo: Casandra emitía oráculos presagiando desgracias, pero Apolo había conjurado al Olimpo para que nadie la creyera… ¿Estamos en ese estadio? Dicen que la mayor victoria del diablo es hacer creer a la gente que él no existe. ¿Nos creemos inmunes a los Stuxnet, Duqu o Flame? ¿a los *manning*, a los *snowden* o a quienes ponen en evidencia? Para hablar de nosotros, los españoles, ¿ninguna empresa o institución ha sido, será o ya está siendo objeto de robos de información o de caída o de descontrol de algunos sistemas? ¿Tenemos claro qué clase de ciberataques pueden desencadenar qué tipo de respuesta? La necesidad de fomentar la cultura de seguridad es una necesidad real y primaria a todos los niveles. En casa, en el colegio, en la universidad, en la empresa, en los medios de comunicación… El informe Mandiant no es ciencia ficción. Todos tenemos una piedra en mitad del camino.

COMPARTIMENTACIÓN EXCESIVA DE AMENAZAS. "EL MAL TAMBIÉN ES GLOBAL"

La ESN define como un ámbito de actuación la lucha contra el terrorismo, y como otro diferente la ciberseguridad. La ECN habla del ciberterrorismo y de la ciberdelincuencia en la misma línea de acción. Son ámbitos distintos, pero no estancos, porque nos pueden golpear amenazas "ciber" procedentes, no de un *hacker friki*, juguetón solitario o a sueldo de otros, sino perteneciente a una organización terrorista, al crimen organizado o a la inteligencia enemiga (el enemigo existe, aunque sea un término quizá demasiado en desuso). Recordemos el caso Stuxnet. La seguridad energética propia y ajena está íntimamente relacionada con la ciberseguridad y los ciberataques contra los sistemas SCADA que controlan nuestras centrales energéticas de generación o distribución. Aunque las dos estrategias traten escenarios y activos distintos, la ciberseguridad es global y no debemos olvidar que un ciberataque puede ser desencadenado contra casi todos los "ámbitos de actuación", y que en dichos ámbitos pueden combinarse ciberarmas en su operativa. De igual modo, hay agresiones muy "físicas" (tradicionalmente contra la seguridad física) realizadas desde, por ejemplo, ámbitos militares, terroristas o de algunos servicios de inteligencia encaminados a destruir, dañar o penetrar sistemas de información. Los conceptos manejados son muy mejorables.

EQUÍVOCOS CON "NUBE" Y "CIBER". "NI TODO ES NUBE, NI TODO ESTÁ PROTEGIDO"

Este asunto está íntimamente relacionado con el anterior y resultaría muy peligroso que estuviéramos confundiendo el concepto del campo de batalla, del terreno por y sobre el que combatimos. De hecho, es muy peligroso, porque es una creencia errónea muy extendida. La nube no es algo etéreo, gaseoso, sideral. Este campo de batalla de hoy, tan "*cloud*", sin embargo es muy visible y muy tangible: es nuestro tablet, nuestro portátil y nuestro *smartphone* personal conectados a nuestra red corporativa; es el computador de sobremesa de nuestra casa desde el que nuestros hijos chatean no sabemos muy bien de qué ni con quién; son nuestros *routers*, el de casa y el de la oficina, quizá de una marca afamada estadounidense pero fabricado en un país asiático muy agresivo; es el edificio donde está mi empresa y su intranet; es el edificio donde están los servidores de correo y los sistemas externalizados de mi compañía; son las destructoras de papel que copian y las impresoras de red que se pueden *hackear* e incendiar desde un Starbucks…; son los tendidos telefónico y de fibra óptica por donde circulan nuestros datos y el control de nuestras infraestructuras, que salen de aquellos edificios y que atraviesan nuestro territorio y se extienden bajo el mar, a una profundidad muy alcanzable en muchos puntos; son los sistemas SCADA de nuestras centrales de producción y distribución de energía eléctrica que, quizá, no estén desconectados de internet… En otras palabras, la nube es algo muy material y la seguridad de esa nube no es competencia y responsabilidad únicamente del jefe supremo de la seguridad, sino más bien del jefe supremo de la empresa llamada Estado o llamada negocio. La seguridad del territorio nacional y la de los edificios de nuestras empresas y domicilios, cosas claramente físicas y tangibles, es asunto de la infantería, de la policía y de los guardias civiles, pero también de los cibersoldados y ciberpolicías. Y, desde luego, asunto nuestro también como usuarios, empleados, ciudadanos…

TIMIDEZ ESTRATÉGICA (DE FUTURO). "LOS EXPERIMENTOS, CON GASEOSA"

Toda estrategia se refiere al posicionamiento y a los actos futuros propios. Un árbol cronológico de ideas podría ser el siguiente: decisión política, estrategia, organización, planes y recursos. Por ese orden. La voluntad política y la consiguiente decisión política -sin la primera, no hay segunda- son el primer elemento y la última garantía de que el sistema funcione. Y el sistema funciona en base a la disuasión, vocablo en el trastero terminológico como si tras la guerra fría careciera de sentido… pero que se lo digan, por ejemplo, a los jugadores de rugby o a los ajedrecistas, o a quienes compiten en el sector de las teleco o de las luchas políticas. Atención: la disuasión solo es efectiva bajo tres condiciones: que estemos dispuestos a enseñar parte de nuestras capacidades agresoras; que el agresor potencial nos preste atención; y que ese agresor está convencido de que estamos en condiciones de localizarle, causarle daños relevantes y exigirle responsabilidades

posteriores. En el cibermundo, esto no es trivial. La mejor acción disuasoria es la que consigue que los agresores -voluntarios o involuntarios- entiendan nuestra determinación a protegernos y, en su caso, responder. En el cibermundo actual, la disuasión es compleja de manejar, porque ninguno de los contendientes está dispuesto a mostrar todas sus cartas, al contrario de lo ocurrido en la era de los misiles balísticos de la Guerra Fría. Como primero es la voluntad y luego la decisión, y dándolas por ciertas tras la aprobación de las dos Estrategias, deberíamos detenernos en las demás ideas. La organización de la ciberseguridad, de la ciberdefensa… ¿está siendo la adecuada? Las políticas y planes que se estén desarrollando, ¿son los adecuados? Los recursos, humanos y materiales que dedicar de forma gradual y modulados por las dificultades económicas actuales… ¿son los que conviene? ¿Podríamos estar confundiéndonos en las definiciones y objetivos estratégicos si solo hubiéramos iniciado desarrollos organizativos en los niveles operacionales? Y a nivel estratégico, ¿qué decir?, ¿qué se desea con la ESN y con la ECN?, ¿hay en marcha un nuevo Libro Blanco de la Defensa, una nueva Revisión Estratégica de la Defensa, una nueva Estrategia Militar?, ¿estamos en plazos –diciembre de 2013- para que el Consejo de Seguridad Nacional elabore su propuesta de anteproyecto de Ley Orgánica de Seguridad Nacional, de creación de la arquitectura institucional del sistema de seguridad integral y coherente con la política de seguridad y defensa del Estado? Por otro lado, la defensa de intereses exige libertad de acción, y esta se consigue con algo que en términos geopolíticos -y, por ende, militares- se denomina superioridad estratégica. Para lograr esa superioridad estratégica, España, sola o en alianza, ¿debería ser capaz de realizar acciones ofensivas (atacar) para “ganar” y mantener esa iniciativa? Si nos moviéramos solo en supuestos defensivos (reactivos), ¿estaríamos dando alas a quienes estuvieran dispuestos a dañar nuestra libertad de acción y todo aquello que deseamos proteger?

OBJETIVOS Y CAPACIDADES CIBERDEFENSA INDETERMINADOS. “LO PRIMERO ES LO PRIMERO”

Este punto está vinculado al anterior y muy relacionado con la Directiva de Defensa Nacional. Hagámonos preguntas simples, aunque las respuestas sean complejas. ¿Debemos bombardear las instalaciones o la infraestructura cibernética o de otro tipo de un agresor potencial o real para disuadirle de realizar o como respuesta de haber desencadenado un ciberataque contra nosotros? Otra pregunta: ¿debemos ciberinutilizar su red de mando y control estratégico, o el operacional, o ambos, en evitación o respuesta de un ataque con armas digamos convencionales? Una estrategia de seguridad nacional debe disuadir -inducir contención- en el adversario. Otra pregunta: la ECN aprobada en España, ¿tiene carácter ofensivo o defensivo?, ¿define el alcance de los roles del Estado y del mundo privado, de las empresas y de los ciudadanos?, ¿distingue lo suficiente entre conflicto físico y conflicto cibernético, o es lo suficientemente sinérgica porque todo son distintas formas de acción?

En caso de ciberagresión, el texto no induce a pensar en una eventual obligación de intervenir en solitario o de cooperar con socios y aliados, a modo de artº 5 del Tratado del Atlántico Norte o de la cláusula de solidaridad del artº 222 del Tratado de la UE. Quizá esta cuestión, si se plantea, quede para otros documentos de rango inferior. Siendo como somos dependientes energéticamente, ¿cuál es nuestra intención y el tratamiento dado por la ECN en caso de agresión sobre una tercera parte proveedora o distribuidora de energía?, ¿y si esa tercera parte fuera el agresor? Por otro lado, nuestra estrategia de ciberseguridad… ¿permite crear la necesaria capacidad ofensiva?, ¿tenemos voluntad y decisión de hacer lo que parecen haber hecho los países punteros en esta materia, entendiendo como punteros los que ya llevan años combatiendo realmente en este tipo de guerra real?, ¿crearemos grupos de *hackers* civiles y militares?, ¿posibilita el desencadenamiento de operaciones de ciberinteligencia contra el software y el hardware del adversario?, ¿permitirá la adopción de medidas "ciber" o no de protección ofensiva y defensiva de nuestro ciberespacio? En otro orden de cosas, ¿se están sentando las bases de una cooperación verdaderamente práctica para que las empresas trabajen codo con codo con el Estado y puedan socorrerse mutuamente? Parece que estamos dando pasos para crear unidades militares preparadas para la ciberguerra, pero… ¿solo para detectar, parar o mitigar ataques?, ¿o también con capacidad para, por ejemplo, plantar con antelación suficiente bombas lógicas en las infraestructuras críticas, civiles o militares, de un adversario potencial y activarlas cuando sea necesario?

PLANIFICACIÓN Y ARTICULACIÓN COMPLEJA. "CREÍ QUE ESTO LO HARÍAS TÚ"

Evitemos desarrollar un avatar con más músculo que cerebro. No lo hagamos de forma tardía, ni precipitada ni insuficiente. ¿Qué desarrollo tiene el Sistema de Seguridad Nacional, con su Consejo de Seguridad Nacional y los Comités Especializados en esta materia?, ¿en qué medida la seguridad nacional la hace suya, de verdad, cualquier departamento ministerial, alguno con mayor intensidad que otros?, ¿se avanza en el plan estratégico de I+D+i en Ciberseguridad (industrial) y se hace en tiempo (límite 2016)? Hemos creado organismos de ciberdefensa -el Mando Conjunto de Ciberdefensa (MCCD) de las Fuerzas Armadas- antes de definir la Estrategia de Ciberseguridad Nacional. ¿Cuánto de alineado está el objetivo y la tarea del MCCD ya creado con la estrategia surgida con posterioridad? ¿Qué seguridad presta este cibermando? En teoría, su ámbito de actuación es de los medios de las Fuerzas Armadas (es de suponer que también, en su caso, a los cibermedios externalizados), no respondiendo en primera instancia de la protección última de nuestras infraestructuras críticas, en manos privadas en un muy alto porcentaje. Si el MCCD no lo hace, ¿quién y en qué medida lo hará?, ¿los propios operadores críticos? Una cosa es cierta operación compartida y otra muy distinta la responsabilidad última y la operativa global del "sistema" llamado España. Como ha escrito Richard Clarke, en la época de la Guerra Fría no hubiera

sido aceptable que el gobierno estadounidense hubiera dicho a la General Motors "*cómprese misiles tierra aire para protegerse de los misiles balísticos rusos, que yo no lo voy a hacer*" por el hecho de que esa compañía fuera estratégica para los intereses del país. Hoy día no sería aceptable que le dijera "*cómprese el hard y el soft necesario para protegerse de los ciberataques chinos, que yo no lo haré*". Y nosotros, en España… ¿qué estamos haciendo y qué haremos? Sabemos bien que cuanto más desarrollo tengamos en nuestro país, también seremos más dependientes de los sistemas de información y de telecomunicaciones. ¿Cuánto de dependientes somos y seremos de las ciberinfraestructuras? No solo nos preguntamos cuánto de dependientes de la red son nuestras empresas, sino cuánto de dependientes lo son hoy día nuestras Fuerzas Armadas. ¿En qué porcentaje el "verdadero" cibersistema de Fuerzas Armadas y, en general, de seguridad nacional es… internet? A nivel estratégico, quizá debería modificarse la doctrina militar incorporando la ciberguerra. A nivel operacional, además del mando creado, ¿se prevé la adopción de un "reglamento de empleo táctico de las ciberarmas" por el que se regirán las ciberunidades? La OTAN, convertida desde hace años en una organización de seguridad y no tanto de defensa, ha integrado la ciberdefensa en su proceso de planeamiento...pero solo protege sus propias redes y las asociadas, no el resto. Solo es un esquema defensivo preventivo, y la respuesta operativa está en manos del Consejo del Atlántico Norte... y eso que es la OTAN. En última instancia, la planificación y articulación de nuestra ciberseguridad… ¿está contribuyendo eficazmente a disuadir a nuestros adversarios o enemigos potenciales en el orden político, económico, militar…?, ¿presenta indefiniciones, voluntarias o involuntarias?, ¿nos deja encantados de habernos conocido y de evitar situaciones incómodas?

POSICIÓN MUY DEFENSIVO-REACTIVA. "¿DE NUEVO *GUERRA, DE ENTRADA, NO*?"

En la *POTUS 21 Executive Order Improving Critical Infrastructure Cybersecurity de 12 febrero de 2013*[2] se establece que, entre líneas de acción del Departamento de Defensa, está la de responder a los ciberataques como a cualquier otra agresión. En la estrategia europea, el discurso es preminentemente "civil" y reactivo-defensivo frente al limitado "militar" y al inexistente proactivo-ofensivo. La PCSD habla poco de defensa y más de seguridad. El Parlamento Europeo ha adoptado varias resoluciones dirigidas a la seguridad y defensa, incluyendo su Estrategia de Ciberseguridad[3], también con un acento no muy marcado en las cuestiones de defensa[4]. El Consejo de Europa aprobó un convenio sobre ciberdelincuencia

[2] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (acceso el 11 de diciembre de 2013).
[3] Ver http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667 (acceso el 17.12.2013)
[4] La UE creó en 2004 la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), elaboró su

(2001) y otro sobre Prevención del Terrorismo (2005). El marco más global (ONU) es muy generalista: solo hay cuatro resoluciones de escasa aplicación al tema que nos ocupa. La UE y España hablan de prevenir (que está muy bien) y de resolver su seguridad ante la ciberdelincuencia, lo que puede producir cierta sensación de desarme a los propios y de poderío a "los otros". Sirva como ejemplo la creación del Centro Europeo contra la Ciberdelincuencia… En España y en la Unión Europea nos movemos en un entorno "*soft*". Aunque con matices, los europeos hemos apostado por la terminología y la diplomacia de "misión humanitaria" antes que de "guerra" o de "conflicto de alta intensidad". La palabra "guerra" no aparece en la Estrategia de Seguridad Nacional ni en la Estrategia de Ciberseguridad Nacional. Tampoco en la ciberestrategia europea, aunque sí se puede leer la expresión "conflictos armados". Entonces, en el marco de la ECN española, ¿suscribirá España una definición de ciberguerra, más allá de la ciberseguridad, en la que de alguna forma se afirme que la ciberguerra es el conjunto de actividades encaminadas a alterar la información, los sistemas enemigos y otros recursos, y a proteger los propios de las acciones enemigas? Mientras, la OTAN se ha orientado de forma diferente, aunque parcialmente complementaria. La OTAN se preocupa especialmente de la *hard security*, de la ciberguerra, del combate contra los enemigos; ha elaborado su Nuevo Concepto Estratégico y en materia "ciber" el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (NATO CCD COE) elaboró el conocido como "Manual de Tallin" (*Tallinn Manual on the International Law Applicable to CyberWarfare*), una especie de manual legal –descargable de internet- aunque no aprobado aún como doctrina (aunque es el esfuerzo más relevante en esta materia) que puede fundamentar la elaboración de los procedimientos de actuación en caso de guerra cibernética. Es claro que la UE -y España- apuestan más por la *soft security*, la ciberseguridad y la lucha contra la delincuencia que por otros ámbitos de actuación. El Primer Ministro David Cameron, en la Conferencia de Londres sobre el Ciberespacio (enero 2013), dijo que "*no podemos avanzar por la vía de la mano dura. Si lo hacemos destruiremos todo lo que de bueno tiene internet*". Se refería a la protección de intimidad de ciudadanos, a la seguridad. ¿Aplicaremos la misma receta a todas las cuestiones de la seguridad?, ¿con la defensa también? España aprobó su estrategia nacional en 2011 y la modificó de forma continuista en 2013. La Directiva de Defensa Nacional (10 páginas aprobadas en 2012) hace una única mención a lo "ciber": "*Se participará en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establezcan al efecto en la Estrategia de Ciberseguridad Nacional*". En seguridad y defensa… ¿no hay mucho ruido y pocas nueces? La propia ESN, en cuanto al objetivo de la "Defensa nacional", dice: "*Objetivo: Hacer frente a los conflictos armados que se puedan producir como consecuencia tanto de la defensa de los*

Estrategia en 2008 y la Agencia Europea de Defensa desarrolla algunos proyectos de ciberseguridad; también adoptó la comunicación "Seguridad de las redes y de la información: propuesta para un enfoque político europeo [COM(2001)298], adoptó una Estrategia para una sociedad de la información segura [COM(2006)251]; y adoptó un plan de acción y una comunicación sobre protección de infraestructuras críticas de información [COM(2009)149 y COM(2011)163], entre otras.

intereses o valores exclusivamente nacionales -en los que se intervendría de manera individual-, como de la defensa de intereses y valores compartidos en virtud de nuestra pertenencia a organizaciones internacionales tales como la ONU, la OTAN o la UE, en los que se intervendría conforme a sus tratados constitutivos junto con otros aliados o socios". Y como objetivo de la ciberseguridad se puede leer: "*Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques*". Es verdad que se habla de respuesta, pero ¿solo de respuestas?, ¿no de acciones anticipadas o de acompañamiento?, ¿seguimos pensando en el fondo que la defensa de verdad (la defensa militar, la guerra) es cosa de otros?

LEGISLACIÓN CLARA INSUFICIENTE. "¿HABLAMOS DE PROLIFERACIÓN DE CIBERARMAS DE DESTRUCCIÓN MASIVA?"

La actualidad ha puesto de moda este tema. Posiblemente tengamos una carencia de legislación clara sobre ciberseguridad y ciberdefensa. Serán precisos cambios éticos en nuestra mente y en nuestra legislación, bajo el eterno debate entre libertad y seguridad, de modo que el Estado de Derecho tenga la potencia necesaria para protegernos y también para que esté sometido a control para evitar abusos de poder. Como ocurre ahora con cualquier otra censura de comunicaciones (correo, teléfono…). Al tratarse de armas ofensivas que pueden recortar derechos fundamentales, las ciberarmas en manos del Estado necesitan controles que otorguen garantías a los ciudadanos. Los noticiarios están salpicados de noticias relacionadas con SITEL, PRISM, etc., y de propuestas de uso de malware para que, bajo control judicial, las fuerzas de seguridad puedan investigar delitos. Si hemos aceptado la expresión "bajo control judicial" para la intervención telefónica o la interceptación de correspondencia postal, de igual modo deberíamos modularla para el mundo ciber. A otra escala, ¿haría falta nueva legislación internacional que regule el uso de ciberarmas? La propia estrategia europea de ciberseguridad establece que "*la UE no defiende la creación de nuevos instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el ciberespacio*". ¿Sería necesario y abordable un tratado de proliferación de ciberarmas de destrucción masiva?, ¿necesitamos y podemos hablar de medidas de confianza, aun con una verificación difícil por no decir imposible? Regular la capacidad de defensa y de explotación quizá sea relativamente fácil de explicar y de asimilar, pero no lo parece en absoluto regular la capacidad de respuesta "ciber", combinada o no con la convencional. No es sencillo definir en qué consiste un ciberataque. La necesaria adaptación del art. 5 de Tratado Atlántico Norte y de Lisboa plantea cuestiones de legitimidad a ´respuestas complicadas… Otro vacío al que nos enfrentamos es el de las

responsabilidades nacionales. ¿Cuáles son las responsabilidades de los Estados ante los ataques desencadenados desde sus territorios, aunque ellos no hayan tenido conocimiento o no hayan participado voluntariamente? En todo caso, la capacidad "ciber" es hoy, sin duda, un instrumento real de poder militar y político y que debería reglarse en lo posible.

Como colofón, formulo dos preguntas añadidas a la reflexión. ¿Creemos que podemos vernos envueltos en una ciberguerra?, ¿qué queremos lograr, qué queremos hacer, cómo lo queremos hacer? En una escala de cero a diez… ¿vamos en la buena dirección?, ¿cuánto hemos avanzado?, ¿qué acciones habría que tomar?, ¿con qué prioridad?

CONCLUSIONES

Afirmar que internet y que nuestros sistemas de información no son algo etéreo sería una obviedad, como lo sería sostener que el ciberespacio es un nuevo terreno donde se desarrollan las guerras financieras, energéticas, empresariales, mediáticas, políticas... Dejémoslo en que la ciberguerra no es la única forma de combate y no tiene por qué darse en solitario. Nuestras estrategias así lo muestran.

La Defensa con mayúscula es defensiva, pero también ofensiva. La iniciativa, la libertad de acción son principios de la máxima vigencia. En el cibermundo ocurre igual. Las posiciones equívocas pueden no restar votos, pero no servirán para evitar guerras o para ganarlas. La voluntad política de seguridad y la decisión política son algo esencial. La Estrategia de Seguridad Nacional y la Estrategia de Ciberseguridad Nacional son prueba de ello. Los documentos de alto nivel contienen premisas de ese mismo rango. Aunque acabe de adoptarse nuestra ciberestrategia, su carácter revisable debe permitir su adaptación más conveniente para su mejor desarrollo. La finalidad última es la protección activa y pasiva de los activos nacionales; las indefiniciones estratégicas pueden conducir a indefiniciones operacionales, con implicaciones que pueden ser muy relevantes en términos económicos y en términos de derechos básicos.

Que la ciberguerra ha llegado a ser una forma complementaria o sustitutiva de la guerra convencional es evidente en escenarios no muy lejanos y protagonizada o sufrida por países de nuestro entorno. El proceso de la seguridad implica la asunción de responsabilidades públicas y privadas, civiles y militares. No caben desarrollos intermedios. Es necesaria una decisión acerca del modelo -ofensivo, defensivo- y de las capacidades necesarias. Es necesario un trabajo estratégico para establecer definiciones estratégicas, porque estrategia equivale al mañana para cuando el hoy peligre. La ciberseguridad debe ostentar categoría principal en la realidad de la seguridad nacional y no ser un simple temario de moda en los foros al uso. Y no será tan principal mientras no hayamos determinado si los ciberataques

deberían tener respuesta como cualquier otra agresión, entendiendo como respuesta algo más contundente y disuasorio que una nota de prensa o incluso una queja diplomática.

La cooperación público-privada no es cuestión solo de compartir infraestructuras, sino de compartir preocupaciones porque muchos de los riesgos son compartidos. Es necesario materializar el intercambio de flujo informativo y de inteligencia en ambos sentidos. No bastan planes y leyes que apliquen al sector privado, porque, aunque necesarios, forman parte de una seguridad que no es transferible desde el Estado. Deberemos caminar hacia una mayor concreción en puntos de contacto; en intercambio de información sensible; en alianzas entre la Administración, las empresas y las instituciones académicas; en la monitorización pública y privada de la amenaza; y en el aseguramiento de la cadena de suministro, tarea en la actualidad compleja por la globalidad de nuestras actividades y recursos. ¿Queremos disponer de un buen equipo que vigile y detecte *zero days*?, ¿estamos dispuestos a conceder menos oportunidades a los agresores voluntarios e involuntarios?

Las cibermaniobras son una realidad, tanto a nivel nacional e internacional. Seamos capaces de crear entornos virtuales realistas. En los ámbitos de infraestructuras críticas hagamos posible actuaciones preventivas y operativas. Las estadísticas de riesgos cibernéticos parecen proliferar en el mundo sajón, mientras que en otras partes del mundo, quizá España entre ellas, es algo inusual que las empresas y en general organizaciones reconozcan incidentes de seguridad y proporcionen datos de gran utilidad para corregir vulnerabilidades sistémicas. Hablo de ejercicios de capacidades, de pasar de las musas al teatro ya.

La seguridad es un tema demasiado serio como para que sucumbamos bajo complejos. La implicación de las Fuerzas Armadas en la seguridad nacional es nítida y determinante en cuanto a todo tipo de amenazas, “ciber o no”, externas o internas, que puedan afectar a los tres activos bien definidos en el artículo 8 de nuestra Carta Magna y desarrollados por la restante legislación vigente. La ciberdefensa y el ciberataque no son ajenos a lo militar, claramente, puesto que la seguridad es cosa de todos.

La formación y la cultura son caldo de cultivo esencial para una nación. En seguridad también. Acabemos con el desconocimiento y la falta de percepción de los riesgos con los que convivimos. Los líderes públicos y privados, y los ciudadanos en general, sabemos cómo prevenir algunas enfermedades, accidentes o situaciones no deseadas… pero actuamos como si creyéramos que jamás nos afectará un ciberataque severo al sistema de producción y distribución de energía eléctrica. Utilicemos bien el lenguaje, que para eso está, porque el lenguaje es propaganda, y la propaganda un arma. No huyamos hablar de guerra, de igual modo que no lo hacemos al hablar de delincuencia. No infravaloremos la posibilidad de ser ciberatacados en esto que denominamos tiempo de paz. Sin obsesión, pero sin complejos.

Y tengamos presente que quien defiende todo no defiende nada. Atención a nuestras infraestructuras críticas. Algunas son más vitales que otras. Habrá activos a proteger en cualquier caso, con independencia de su probabilidad, porque no nos podemos permitir el lujo de que ocurran. Según la ESN, el bien último y prioritario son las personas, su bienestar y sus derechos. Sin dirección (algunas parcelas de gobierno a distintos niveles), sin energía (al menos, eléctrica) y sin alimentación y salud, nuestra debilidad como cuerpo social sería mayúscula.

[i]

*José Luis Hernangómez de Mateo**
Coronel de Artillería (R)
Doctor en Ciencias Políticas y Sociología
Gerente de Ciberinteligencia en N+1 Research & Intelligence