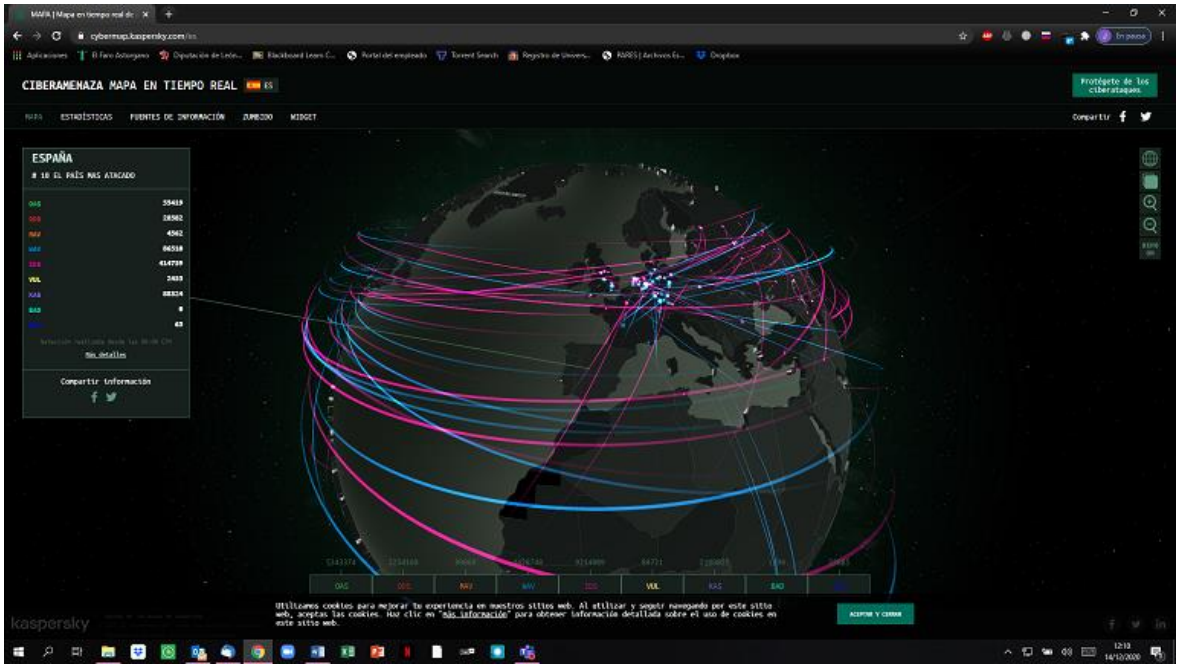
La protección de infraestructuras criticas frente a ciberataques: retos de su conceptualización



Juan Cayón Peña
Academia de las Ciencias y las Artes Militares
Sección de Futuro de las Operaciones Militares

21 de diciembre de 2020

El problema de partida

El 11 de septiembre de 2011 fue sin duda una fecha clave para Occidente y el mundo entero, pues supuso no el primero, pero si el más importante ataque exitoso a la potencia dominante, los Estados Unidos de Norteamérica, teniendo además el mismo en el centro neurálgico de su territorio. Tras el fin de la modernidad con la caída del muro de Berlín, que por más de cuarenta años puso una imagen gráfica al vergonzoso espectáculo de la política internacional de los aliados vencedores de la Segunda Guerra Mundial, por primera vez los Estados Unidos veían golpeada su integridad sobre su propio territorio.

La metodología utilizada por los terroristas fue una auténtica novedad histórica, sólo imaginable hasta la citada fecha por alguna superproducción cinematográfica. Pero lo más relevante es fundamentalmente el cambio de mentalidad en la estrategia de defensa que los ataques produjeron, la amarga sensación de vulnerabilidad frente a un enemigo poliédrico, irregular, amorfo y cambiante, que puede golpear de manera efectiva en cualquier parte del mundo con efectos devastadores tanto en la moral como en los efectos materiales de sus acciones.

Así la postmodernidad ha arrancado con un ambiente bélico radicalmente novedoso que se extiende a nivel planetario, pues el enemigo de Occidente se disemina por todos los continentes de manera eficaz, martilleando machaconamente los intereses económicos y políticos de las potencias occidentales y causando terror auténtico en la población. Ante dicha cruda realidad, una verdadera psicosis defensiva se ha apoderado, probablemente con razón, de los gobiernos y las sociedades occidentales. Las imágenes del derrumbe de las torres gemelas en el bajo Manhattan, los cadáveres desperdigados en las estaciones de tren de Madrid o los tradicionales autobuses londinenses reventados por los explosivos están en el imaginario colectivo grabadas de forma indeleble, de modo que la sociedad transige e incluso a veces demanda mayores medidas de seguridad, mayores capacidades de respuesta, mejor coordinación de las fuerzas y autoridades responsables de la seguridad.

Los errores patentes en los sistemas preventivos, defensivos y de respuesta occidental ante estas nuevas amenazas y riesgos reales, optando por la menos malintencionada de las interpretaciones posibles, demostraron ser netamente insuficientes, descoordinados y escasamente operativos frente al nuevo enemigo y su forma de hacer la guerra irregular. Por ello, los estados han adoptado muy distintas medidas desde entonces, nuevas estrategias y tácticas con las que enfrentar el nuevo panorama bélico del siglo XXI. En el seno de dichos cambios estratégicos, la preocupación por garantizar la supervivencia e intangibilidad de las infraestructuras consideradas esenciales, han dado lugar a uno y otro lado del Atlántico a sendas orientaciones estratégicas plasmadas en abundantes disposiciones de rango normativo. Es precisamente al análisis de estas últimas a las que habrá de centrarse especialmente en sólo uno de los frentes de combate, siendo a nuestro juicio el más interesante el de los ataques provenientes del mundo virtual, es decir, el ámbito cibernético. El interés de dicho campo de actuación reside en la alta incidencia que en los últimos años está tomando en las estrategias defensivas occidentales, principalmente con las primeras operaciones de esta naturaleza que son conocidas por la opinión pública y la enorme cantidad de recursos materiales y humanos que las potencias están empezando a consagrar a través de sus ciber-comandos.

Principales hitos para la definición, identificación y protección de infraestructuras críticas en el sistema estratégico occidental

El primer problema con el que se encuentra cualquier gobierno que desea avanzar en el camino de la organización de un sistema coherente y efectivo de protección de infraestructuras vitales es, precisamente, el de su adecuada conceptualización. Antes de pasar a una identificación de las infraestructuras cuyo uso deba ser protegido y el diseño de esta o aquella estrategia de protección, debe asegurarse una adecuada y precisa conceptualización de las mismas, lo que desde luego no es cuestión baladí y tampoco sencilla. El debate sobre las peligrosas implicaciones de una definición ambigua o poco precisa, ha estado encima de la mesa de quienes han debido asumir la responsabilidad sobre las citadas estrategias a uno y otro lado del Atlántico, y de hecho, puede fácilmente rastrearse en los distintos documentos legales y organizativos una cierta evolución conceptual que ha ido ampliando el contenido de lo que debe entenderse por infraestructura crítica y consecuentemente digna de protección tanto en el nivel estratégico como en el operativo.

Y es lógico que la cuestión sea debatida, pues son distintos, variados y siempre importantes los riesgos que se asumen optando por una extensión u otra del concepto, tanto por la posibilidad de hacer ineficiente el uso de los siempre escasos recursos económicos que se destinan a las cuestiones de seguridad nacional (si se hiciera una lista demasiado extensa que obligara a proteger infraestructuras que realmente no son críticas despilfarrando recursos necesarios en otros frentes), como por la contraria, política en la que, por ser demasiado estricto y limitativo en la conceptualización, obtendríamos como resultado el dejar fuera del ámbito de protección algunas infraestructuras cuya verdadera criticidad no hubiera sido adecuadamente prevista, con las nefastas consecuencias que acarrearía un ataque certero y eficaz frente a las mismas.

De ahí que, por ejemplo, el *Congressional Research Service* norteamericano, en su reporte del 1 de octubre de 2004 señalara con acierto que los riesgos a los que se enfrenta la conceptualización de infraestructuras críticas dignas de protección es proteger demasiadas, proteger las que no son, o ambas cosas a la vez, a lo que nosotros añadimos el de no proteger las que son.

Así, como primera aproximación, podríamos coincidir con una definición de infraestructura esencial o crítica que la conceptualiza como aquella facilidad básica, servicio o instalación necesaria para el funcionamiento de una comunidad o sociedad. La cuestión clave es que dicha aproximación resulta obviamente insuficiente sin la identificación concreta de las mismas, pues por si sola, la definición precisa de interpretación que permita concretar qué es «básico» y/o

«necesario», así como qué debemos entender por «funcionamiento». Este es el debate, por tanto, no la conceptualización en si de lo que debemos proteger, esto es, aquello que consideramos esencial para nuestra sociedad, sino qué cosas concretas consideramos esenciales. Y en esto la sociedad postmoderna sólo ha avanzado incluyendo cada vez más cosas tenidas por esenciales para su propia supervivencia, lo que inevitablemente nos trae el recuerdo del viejo adagio que considera más rico no al que más tiene sino al que menos necesita. Esta es una de las primeras reflexiones que debería hacer nuestra civilización, mirándonos en el espejo de aquellas otras que coinciden con nosotros en el tiempo y que pugnan con nosotros por la supremacía. Si algo tienen en común las potencias civilizacionales emergentes (pensamos a título de ejemplo en la cosmovisión del mundo musulmán o la propia del sistema comunista de mercado característica de China) que de una forma u otra nos disputan no sólo el mercado sino la influencia y hasta el concepto de la existencia es, precisamente, el que en su cosmovisión, hay muchas cosas, estructuras y prácticas que, siendo aparentemente insustituibles en Occidente, son sin embargo perfectamente prescindibles en sus respectivos entornos. Por más que resulta apasionante, no hablamos en este caso de la conceptualización de la política, democráticamente idólatra en nuestro caso, frente a la sencillez tribal o la organización por clanes propia de otras culturas, sino de las cuestiones materiales que han acompañado a Occidente como civilización de referencia en la modernidad. El punto hasta el que nos ha llevado el planteamiento hedonista y característico de la riqueza y sobreabundancia de la que hemos disfrutado, principalmente desde la Segunda Guerra Mundial y hasta nuestros días, bien pareciera un punto de no retorno, un punto que nos hace extremadamente sensibles a cualquier alteración del *status quo* alcanzado, que bien puede ejemplificarse con el hecho de nuestros jóvenes llegan realmente a frustrarse por no calzar las deportivas de una determinada marca o nuestros sistemas económicos se tambalean ante una evidente insostenibilidad del crecimiento constante de burbujas especulativas en el ámbito de las empresas tecnológicas o el sector inmobiliario.

Es precisamente en este contexto, en el que, durante toda la Modernidad, nuestros gobernantes y nuestra sociedad han estado más preocupados por la dotación de infraestructuras, por su adecuación a las exigencias de la economía de mercado capitalista, que por el hecho de su protección y la adopción de medidas que alivien su posible neutralización. E igualmente ocurre con aquellas otras infraestructuras relativas a las tecnologías de la información y las comunicaciones. La espiral tecnodependiente es muy reveladora de este fenómeno que apuntamos. Todos los esfuerzos políticos y sociales se han centrado en los últimos cien años en aplicar a nivel general las mejoras de infraestructuras y aquellos países que hoy se consideran plenamente industrializados, los del llamado primer mundo, si en algo

se distinguen del resto es precisamente en la calidad y abundancia de sus infraestructuras.

Por ello, precisamente porque en el siglo XXI una sociedad avanzada es inconcebible sin un enorme número de servicios e infraestructuras, es por lo que hoy como nunca somos especialmente vulnerables a cualquier adversidad de las mismas, máxime cuando hasta la fecha nuestras sociedades han estado mucho más pendientes de construirlas y mantenerlas, todo lo más, de asegurarlas frente a los desastres naturales más propios de cada entorno, mas no a defenderlas de ataques deliberados de grupos que quieren comprometer nuestra forma de vida y aspiran a golpear con el mayor impacto posible.

En lo que se refiere a la protección de infraestructuras consideradas críticas en la postmoderna sociedad norteamericana, golpeada en su orgullo y en su población como ninguna otra por el terrorismo, puede afirmarse que el primer avance concreto en esta materia provino del Presidente Clinton, quien cinco años antes de los atentados de 2001, dictó la *Executive Order* 13.010 (EO 13010) de 15 de julio sobre el tema de referencia, estableciendo por primera vez un organismo específicamente destinado a la protección de dichos activos nacionales, ya que por la referida orden ejecutiva, ve la luz la *President´s Comission on Critical Infrastructure Protection* que aspirará a tomar un papel relevante en nuestra temática. Por su parte, la Unión Europea hace ahora doce años dicta por primera vez una Directiva sobre la materia, el 8 de diciembre de 2008, la 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, fruto de la petición del Consejo Europeo que solicitó la elaboración de una estrategia global para mejorar la protección de infraestructuras críticas. En respuesta a esa solicitud, el 20 de octubre de 2004 la Comisión adoptó la Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, en la que se formulan propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que afecten a infraestructuras críticas y posteriormente como precedentes en 2005 adoptó el Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas, en el que se exponían las posibilidades de actuación para el establecimiento del Programa y de la Red de información sobre alertas en infraestructuras críticas (CIWIN). Las respuestas al Libro Verde destacaron el valor añadido de un marco comunitario para la protección de las infraestructuras críticas. En dicho texto se reconocía la necesidad de aumentar la capacidad de protección de estas infraestructuras en Europa y de contribuir a reducir sus vulnerabilidades y se hacía hincapié en la importancia de los principios claves de subsidiariedad, proporcionalidad y complementariedad, así como en el diálogo con los agentes interesados. Así, en Europa se define como infraestructura crítica, el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el

mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

El sector de las TIC y su incidencia social en la postmodernidad

Pero un análisis de la normativa aplicable, sus características y crítica intelectual quedaría incompleto sin un marco filosófico-práctico que juzgamos imprescindible, esto es, el que permita explicar el auge y papel fundamental de las llamadas tecnologías de la información y las comunicaciones (TIC) en nuestras vidas. Intentaremos siquiera aproximarnos a dicho marco.

El sector de las TIC es fundamental para la economía y la sociedad de la UE y el mundo avanzado. Incluso para aquellos países que aún se encuentran en vía de desarrollo, las TIC suponen una pieza clave de crecimiento, no sólo del sector económico en sí (telefonía, redes, equipos de hardware y empresas de software, etc…) sino para cualquier otro del conjunto nacional. No parece excesivo considerar por tanto que las tecnologías de la información y la comunicación se han convertido en el sistema nervioso central de la economía, y como más adelante veremos, incluso de la sociedad postmoderna en su conjunto, pues dicho sector es esencial para todos los segmentos de la sociedad. Las empresas y negocios, así como las instituciones oficiales, educativas, sanitarias, etc., dependen de él tanto para las ventas o actividades directas frente a terceros como para la eficiencia y eficacia de los procesos internos.

El mundo empresarial fue el primero en tecnificarse y enseguida descubrió como la utilización de estas tecnologías permitía acrecentar la eficiencia y mantener la productividad de cada empleado en cotas máximas, incluso por encima de lo previsto al penetrar en dicho entorno las tecnologías móviles que hacen que el personal trabaje incluso desde los entornos más insospechados o en tiempos que antes permanecían improductivos para la empresa aunque servían para el descanso y relajación de los trabajadores. Así, desde la más grande empresa multinacional hasta el pequeño colmado de la esquina, todos los negocios y empresas están en mayor o menor medida tecnificados, siendo a veces la tecnología incluso imprescindible para la operativa diaria de modo que cuando falla, el negocio debe cerrar sus puertas.

Por su parte, las TIC son imprescindibles en el funcionamiento de los gobiernos y las administraciones públicas: la utilización de la administración electrónica a todos los niveles, si bien garantiza en teoría unos procedimientos teóricamente más eficientes, rápidos y a veces hasta más sencillos (aunque no siempre por

desgracia), hace que el sector público dependa en gran medida de las TIC para muchas de sus relaciones con los administrados. Pero, además, es que dichas tecnologías resultan imprescindibles en sus procesos internos y aseguran el funcionamiento corriente del Estado (o lo que queda de él en la postmodernidad). Como preconizaba el famoso discurso sobre la dictadura de Donoso Cortés, los Estados modernos demandan constantemente nuevos medios de control social para imponer su concepción total de la vida comunitaria; en las TIC encontraron una herramienta de la máxima utilidad a tales fines, no sólo para el control y la vigilancia (fiscalidad, seguridad, censo, manejo de información de los ciudadanos, …) sino también para el entretenimiento, información y manipulación de los mismos.

Por último, aunque en consonancia con lo precedente, los ciudadanos dependen cada vez más en su vida diaria de los servicios de la sociedad de la información y utilizan las TIC constantemente, incluso cuando su uso no es impuesto por el empleador o el Estado. El indudable éxito de las redes sociales, la difusión de los grandes medios de comunicación en digital o el auge de la telefonía móvil para uso privado y de ocio, son buenos ejemplos de la extensión de la tecnodependencia a la esfera privada, de la postmoderna esclavitud del nuevo hombre que no es nada sin su virtualidad electrónica.

No cabe duda por todo ello que el futuro de las operaciones militares en materia de protección de infraestructuras críticas frente a ciberataques dará que hablar en el presente siglo, probablemente, más que ningún otro frente.