Ciberseguridad y seguridad integral en el sector energético

Félix Arteaga | Investigador principal de Seguridad y Defensa del Real Instituto Elcano y coordinador del Grupo de Trabajo sobre Ciberpolítica

Tema

Pese al razonable éxito de la ciberseguridad para hacer frente a los riesgos y amenazas del ciberespacio del sector energético, el crecimiento de éstos y la irrupción de otros nuevos obliga al sector a revisar el contexto estratégico de su seguridad.

Resumen

La ciberseguridad ha progresado de forma eficiente en el sector energético debido a la trascendencia de las infraestructuras críticas para los servicios públicos, el alto valor de los activos empresariales a proteger y, desafortunadamente, por la necesidad de defenderse ante los ciberataques que tienen al sector en su punto de mira.

Este ARI analiza el estado y expectativas de la ciberseguridad en un sector como el energético, sobre el que se van acumulando nuevos riesgos, tanto los relacionados con la ciberseguridad como los relacionados con los procesos más amplios de regulación y digitalización, así como los derivados de la creciente competencia geoeconómica entre las grandes potencias[1].

Análisis

El ciberespacio es el nuevo espacio donde se desarrollan la economía, la cultura, el consumo, la producción y el ocio de la sociedad de nuestro tiempo: la sociedad informacional o digital. Una sociedad en la que se producen cambios muy rápidos en los aspectos sociales, económicos y políticos y cambios disruptivos en lo tecnológico, lo geopolítico o lo geoeconómico, y esos cambios afectan al sector de la energía en general y muy especialmente al de su seguridad.

Son cambios que tienen que ver con la expansión del sector en el ciberespacio, su inmersión en la economía digital, su exposición a las nuevas reglas —o la falta de ellas— y, últimamente, al enfrentamiento geopolítico, geotecnológico y geoeconómico por el poder mundial entre las potencias al que se asiste. El sector energético, como tantos otros, no puede sustraerse a estos cambios, que van a tener —y ya tienen— un impacto funcional, orgánico y cultural en el sector de la energía.

[1] El contenido de este ARI se expuso previamente en la reunión anual de Sedigas de 26 de junio de 2019 en Madrid y va a servir de base a un análisis más detallado del Real Instituto Elcano en colaboración con el sector energético para evaluar conjuntamente el impacto funcional, orgánico y cultural de las tendencias de cambio en la seguridad que se incluyen en el texto.

La ciberseguridad en el sector energético

El sector cuenta con grandes compañías de petróleo, gas, electricidad, nucleares y renovables que controlan infraestructuras críticas para los servicios públicos esenciales y cuya perturbación puede generar un grave efecto dominó sobre el conjunto de la economía y el modo de vida de las sociedades avanzadas[2]. Las inversiones en ciberseguridad y el trabajo de los CISO y sus equipos han conseguido limitar razonablemente los daños en el sector de la energía y aumentar notoriamente su capacidad de resiliencia para reponerse tras los ciberataques.

A pesar de ello, el sector sigue atrayendo los ciberataques según todas las estimaciones de riesgo y algunos han conseguido su propósito, como muestra la siguiente selección de ciberincidentes[3]:

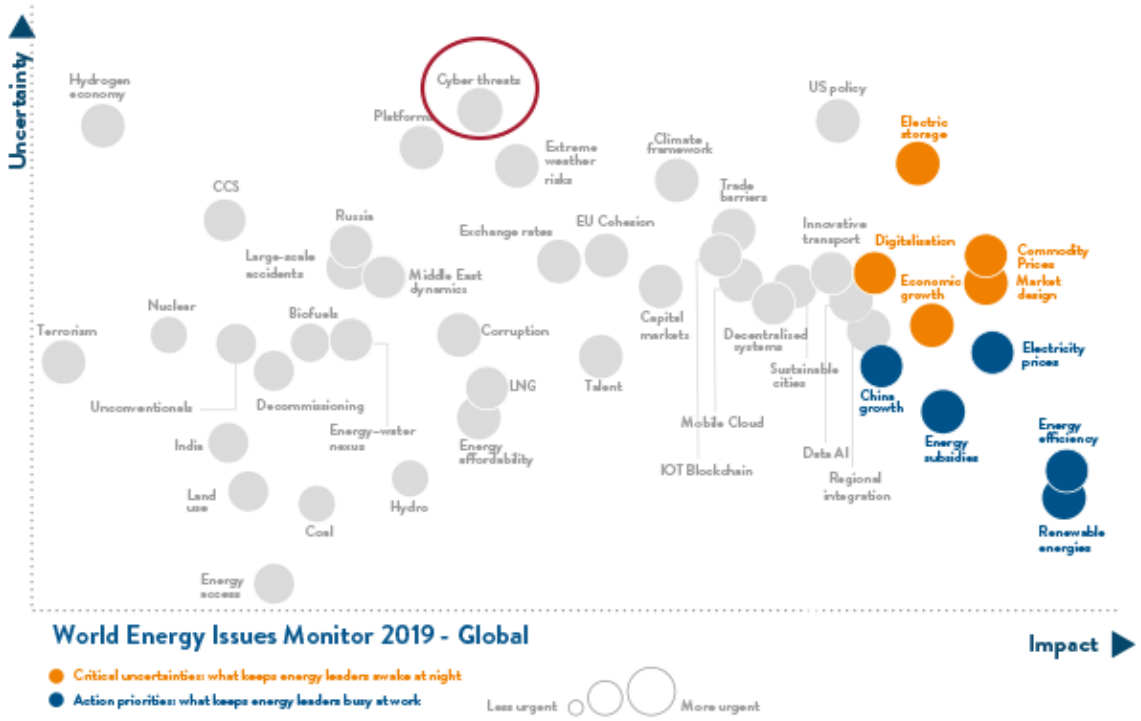
- USA, 2003, nuclear power plant, malware slammer;
- Iran, 2008, nuclear facilities, stuxnest worm;
- USA, 2012, power generation, human error, virus mariposa; Saudi Arabia, oil company, virus shamoon; The Netherlands, telecommunications, hacking;
- USA, 2013, non-energy infrastructure, malware slammer;
- USA and Canada, 2013-2015, power generation, human error, hacking;
- Germany, 2014, manufacturing, hacking;
- South Korea, 2015, nuclear power plant, hacking; Australia, public sector, hacking, virus;
- Israel, 2016, public sector; power grid, malware, human error;
- Saudi Arabia, 2017, oil safety instrumented systems, malware;
- USA, 2019, Los Angeles and Salt Lake electrical systems, DDoS.

Sin embargo, y quizás por la razonable satisfacción de lo logrado, la ciberseguridad no figura entre las preocupaciones más urgentes del sector, según los resultados de la última encuesta del World Energy Council a unos 2.300 directivos de 50 empresas y 6 continentes. Tal y como refleja la Figura 1, la encuesta revela que existe entre los directivos una preocupación moderada por el impacto de los ciberataques (figura en la zona media del indicador) aunque su probabilidad de que ocurra es de las más elevadas (figura en la parte alta del indicador). Lo que más tiempo les ocupa son asuntos como la situación en China, los subsidios a la energía, la eficiencia energética, los precios y las renovables (en color azul), pero lo que parece quitarles el sueño son los precios de las mercancías, los mercados, la digitalización, el crecimiento económico o el almacenamiento de la energía (en color naranja).

[2] Para una simulación del impacto de un apagón sobre la red eléctrica de Estados Unidos, ver "Bussines Blackout", Lloyd's, 2015, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout. En el mismo sentido, el encargo de la Comisión Europea a ECOFYS, "Study on the Evaluation of Risks of Cyber Incidents in the Energy Sector", https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf.

[3] Fuente: World Energy Council, Marsh & McLennan Companies, Swiss Re Corporate Solutions.

Figura 1. Preocupaciones principales entre los directivos del sector

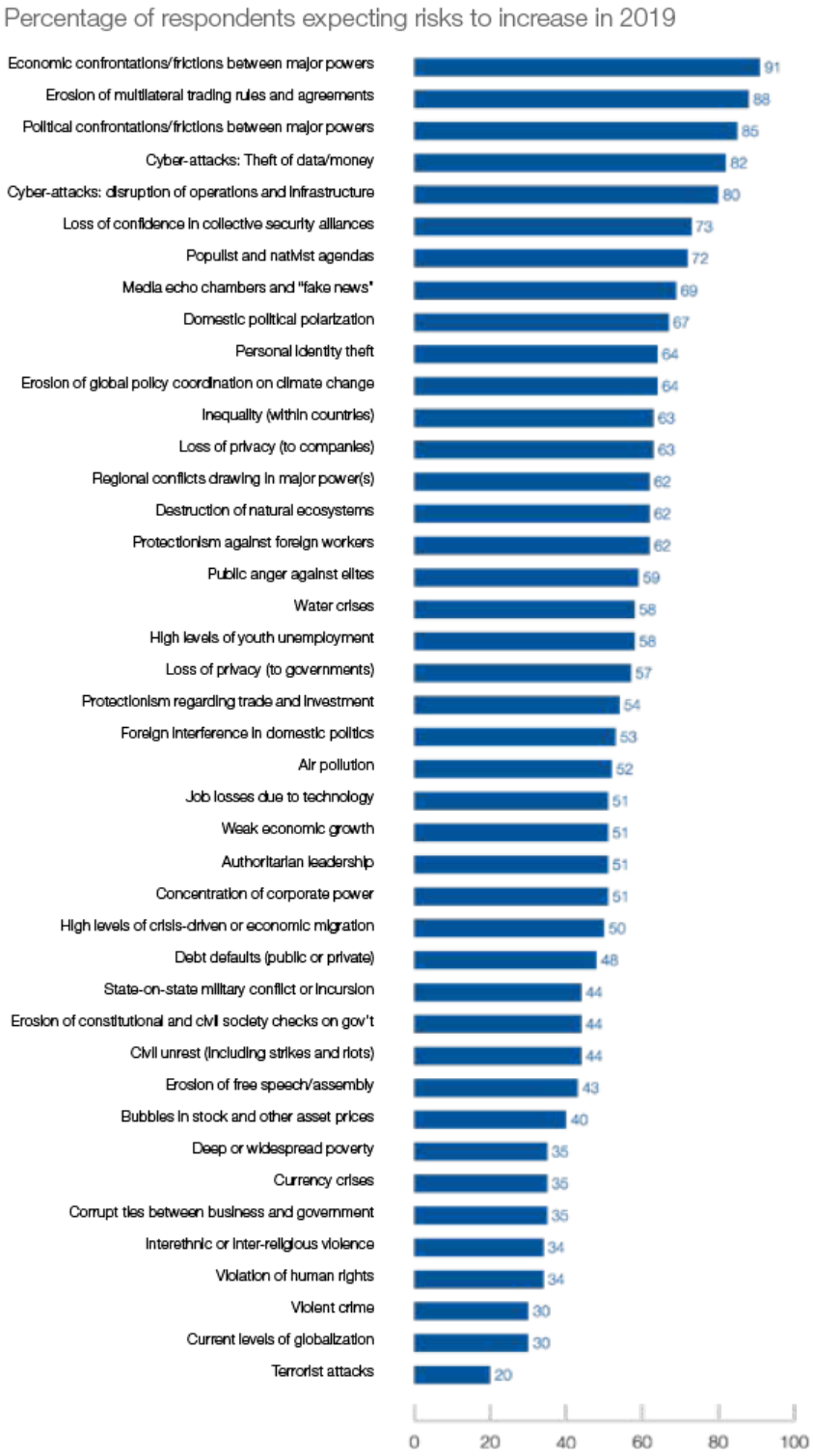


Fuente: World Energy Issues Monitor 2019, World Energy Council, p. 6, https://www.worldenergy.org/wp-content/uploads/2019/02/1.-World-Energy-Issues-Monitor-2019-Interactive-Full-Report.pdf.

Esa percepción del sector es más benigna que la que tienen otros directivos, como las recogidas por el World Economic Forum de Davos, que ven crecer en los últimos años la ciberseguridad y la tecnología como factores de riesgo empresarial[4]. En particular, como refleja la Figura 2, los directivos consultados incluyen entre los riesgos de

[4] Entre otros, "The Evolving Risk Report 2009-2019", World Economic Council, pp. 5-8.

Figura 2. Riesgos principales a corto plazo para los directivos empresariales



Fuente: The Evolving Risk Report 2009-2019, World Economic Council, p. 18, https://www.weforum.org/reports/the-global-risks-report-2019.

mayor crecimiento a corto plazo (en 2019) algunos de los que parece que van a afectar al sector de la energía en el futuro inmediato: el enfrentamiento político y económico entre las grandes potencias, la erosión de la gobernanza, los ciberataques para interrumpir los servicios, robar los datos o pedir rescates, el proteccionismo nacional y la desinformación.

Para hacer frente a estos riesgos, la ciberseguridad ha ido creciendo desde que atendía los riesgos de información y de los sistemas informáticos (TIC) a los aparecidos tras la conexión de los anteriores con otros a través de Internet, la protección de las infraestructuras críticas (PIC) como parte de la seguridad nacional, la obligación de salvaguardar los datos y la privacidad de los clientes y la prestación de servicios esenciales para la economía digital.

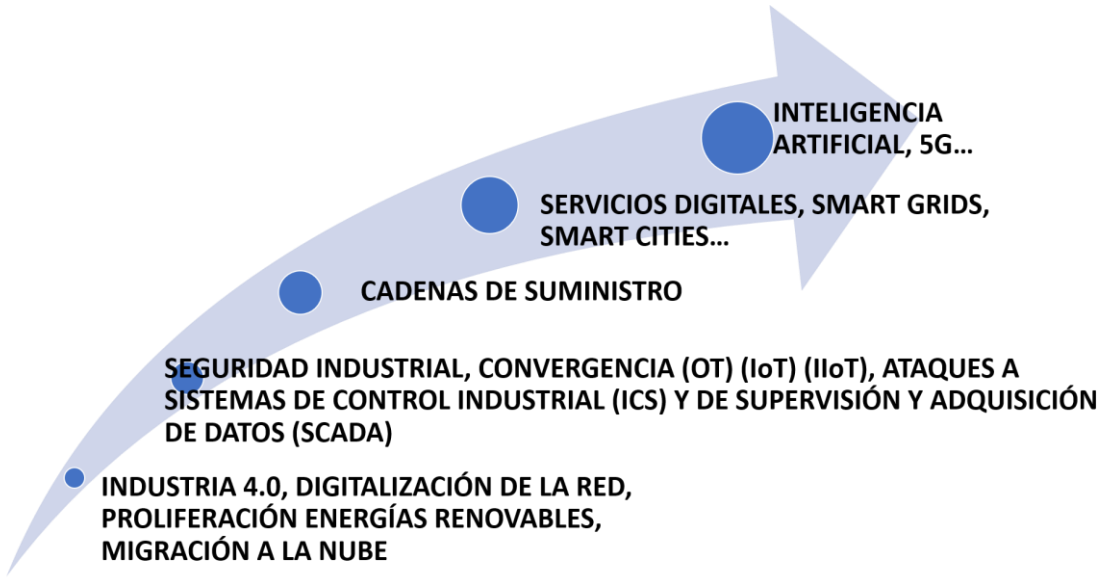
A mayor digitalización, más riesgos de seguridad

La digitalización, a la que la ciberseguridad debe proteger, está abriendo nuevos riesgos para la seguridad del sector de la energía. Las infraestructuras se digitalizan y las energías renovables traen nuevos actores al sector, como las centrales solares, los aerogeneradores, las electrolineras o los sistemas dedicados al almacenamiento de energía. Los datos y las operaciones de las compañías se suben a la nube y eso complica la gestión de la ciberseguridad (seguir protegiendo lo que se sube o delegar su protección al gestor de la nube).

Siguiendo la evolución de la Figura 3, la conectividad trae nuevos problemas de seguridad industrial a equipos industriales que antes estaban al margen de las redes y no tenían que protegerse de los riesgos del ciberespacio. Su exposición pone en peligro las tecnologías de las operaciones (OT) —conocidas como 'tecnologías de la información en la sombra' (*IT shadow*)— y, con ello, la generación, distribución y consumo de la energía. Un riesgo para el que la Comisión Europea acaba de pedir a los Estados miembros que presionen a los miembros del sector energético para que refuercen las medidas de concienciación y formación y, si es necesario, que se incluyan estas obligaciones en el ordenamiento del sector[5].

[5] Comisión Europea, Recomendación C(2019) 240 sobre ciberseguridad en el sector energético, de 3 de abril de 2019, https://ec.europa.eu/energy/en/topics/energy-security/critical-infrastructure-and-cybersecurity.

Figura 3. La evolución de la digitalización en el sector energético



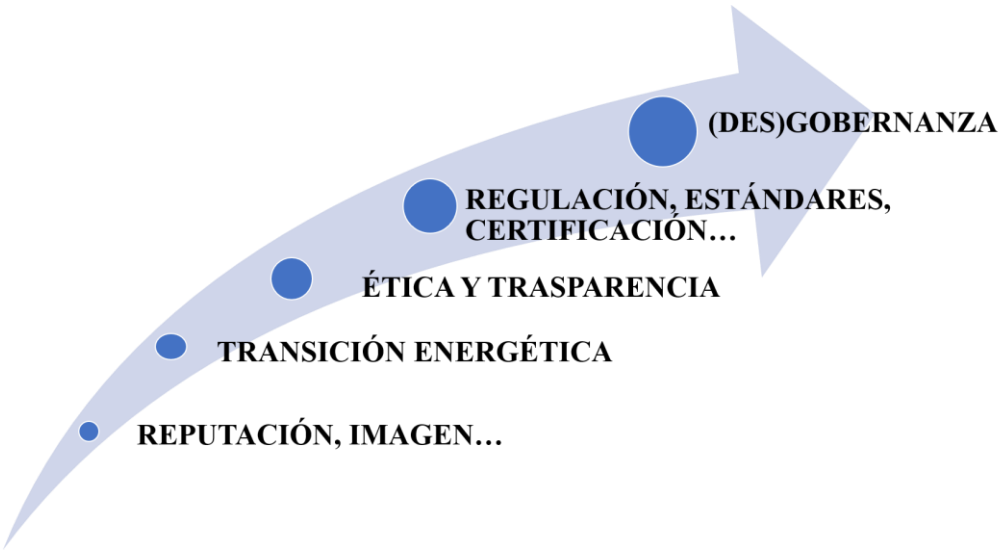
Fuente: Elaboración propia.

El crecimiento de la variedad y longitud de las cadenas de suministro aumenta también la vulnerabilidad del sector al eslabón más débil de la cadena. Aparecen nuevos servicios y productos digitales necesarios para los servicios, redes y ciudades inteligentes, como contadores o las cámaras y drones de vigilancia, entre otros, lo que acerca los riesgos del Internet de las cosas (IoT) al sector de la energía. Y, por si lo anterior no bastara para complicar la gestión de la seguridad, la inteligencia artificial irrumpe ahora como un multiplicador de los todos los factores de riesgos señalado debido a su capacidad para potenciarles y subirlos la seguridad a un nuevo nivel disruptivo para el sector.

Los riesgos de cumplimiento se disparan

El cumplimiento ha dejado de ser una obligación autoimpuesta para preservar la reputación y la imagen corporativa de las compañías mediante directrices y códigos internos. Estos siguen existiendo, pero se ven cada vez más desbordados por normas de obligado cumplimiento que emanan de las distintas autoridades regulatorias —nacionales e internacionales— a la que deben someterse las compañías del sector. A las obligaciones impuestas a los operadores críticos por el Plan Estratégico Sectorial de la Energía (electricidad, gas y petróleo) siguieron las derivadas del Reglamento General de Protección de Datos (RGPD) o de la trasposición de la Directiva para la seguridad de las redes y sistemas de información (Directiva NIS). A la regulación de naturaleza administrativa hay que añadir la derivada de los estándares técnicos a los que adaptarse o a los mecanismos de certificación que se deben reunir para operar.

Figura 4. Evolución de las obligaciones de cumplimiento



Fuente: Elaboración propia.

En la Figura 4 aparecen dos nuevos capítulos en el horizonte de la expansión del cumplimiento. Por un lado, la inmersión del sector en la transición energética aumenta las obligaciones —asumidas o impuestas— que las compañías deben cumplir para responder a las expectativas creadas desde el punto de vista de la eficiencia, la reducción de emisiones, la descarbonización y la sostenibilidad climática. Por otro, las grandes compañías comienzan a tener en cuenta nuevas obligaciones relacionadas con los aspectos éticos y de transparencia que los consumidores o los movimientos sociales espera de la responsabilidad social corporativa. La presión y el escrutinio social obliga al sector a crear códigos de conducta, centros y campañas de información para anticiparse a las dudas, quejas o campañas de desinformación que puedan afectar a la continuidad de su negocio.

Por último, pero no menos importante, la rivalidad entre las grandes potencias

La geografía ha vuelto[6] y las grandes potencias se enfrentan por el poder, arrastrando a todos los demás sin hacer prisioneros[7]. Esa competición se desarrolla también en el ciberespacio: los Estados desarrollan *software* malicioso que usan o ceden a sus grupos afines para que ataquen o espíen a sus países rivales, pero ese *know how* ha ido pasando a grupos criminales, individuos y compañías que lo utilizan ahora en su interés particular y lo ofrecen como servicio. Otras tácticas de enfrentamiento, como la desinformación o las operaciones de influencias, creadas también por los Estados para desacreditar o desmoralizar a sus rivales, seguirán probablemente el mismo camino y lo que ahora es un instrumento en la competición geopolítica entre Estados no tardará en ser un instrumento más de competición entre particulares y empresas.

[6] Robert D. Kaplan, *The revenge of geography*, Random House, Nueva York, 2012.

[7] Kristina Kauch, “Cheap Havoc: How Cyber-Geopolitics will Desestabilize the Middle East”, German Marshal Fund, noviembre de 2017, http://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east.

El trasvase se produce porque hay una combinación —una hibridación— de distintos actores y herramientas de agresión. Los actores públicos y privados (amenazas) cooperan para dificultar la atribución de sus ataques y combinan sus distintas capacidades cibernéticas (ciberataques, desinformación, sabotaje, espionaje, *fake news*, propaganda e influencia, entre otros). Pero también pueden combinarlas con ataques convencionales. Así, el enfrentamiento entre Irán y Estados Unidos durante junio de 2019 se tradujo en ataque sobre buques petroleros en las inmediaciones del estrecho de Ormuz, ataques con drones sobre oleoductos de Emiratos y un misil contra una planta saudí de electricidad. Como resultado, algunos gobiernos como Estados Unidos, el Reino Unido, Francia, o la propia Unión Europea, comienzan a adoptar medidas de defensa activa para evitar el crecimiento impune de los ciberataques al sector privado y disuadir a los rivales de amenazar las infraestructuras críticas.

Además, el proteccionismo y la rivalidad fragmentan los mercados, las regulaciones y las oportunidades de negocio en función de la geografía, lo que dificulta la gobernanza de un sector tan globalizado como el de la energía. La composición accionarial, los clientes o la ubicación de las instalaciones de las compañías del sector pueden crear problemas de identificación con alguno de los bandos en conflicto y exponerse a presiones, sanciones o exclusiones que deben, desde ahora, tenerse en cuenta en el análisis de riesgos. Además, la superioridad de Estados o empresas en tecnologías disruptivas como la inteligencia artificial o la computación cuántica pueden facilitar el desplazamiento de las empresas que lleguen tarde a ellas (*the winner takes it all*), por lo que la innovación tecnológica representa un reto adicional para la geopolítica de la energía[8].

Conclusiones (provisionales)

Como resultado de todos estos cambios, y si la investigación pendiente lo confirma, el sector energético podría colocarse en una situación de seguridad parecida a la siguiente:

- El sector es muy sensible a los cambios y deberá tomar conciencia de la acumulación y magnitud de los riesgos y adoptar medidas al respecto (la inacción o la minusvaloración de riesgos hace que la sensibilidad se convierta en vulnerabilidad).

- El análisis de riesgos y de respuestas se convierte en un elemento central en el diseño y conducción del negocio energético. Se debe pasar de la inteligencia táctica (ejecución) y operativa (respuestas a incidentes) a la inteligencia estratégica (conocer las amenazas, anticiparse a los riesgos y asistir a las decisiones).

[8] Severin Fischer, “Technology Innovation and the Geopolitics of Energy”, en *Strategic Trends 2018*, Center for Security Studies, Zúrich, 2018.

- Para limitar daños, se debe pasar de la concienciación voluntaria a la formación y exigencia coactiva de empleados y cadenas de suministro (formación obligatoria y responsabilidad contractual).

- La seguridad multiplica sus dimensiones y pasa de lo físico, lógico, reputacional, industrial, cumplimiento o una seguridad de seguridades (seguridad integral). Las dimensiones de seguridad se combinan y suben por la cadena orgánica (centralizar la gestión).

- La seguridad se convierte en un activo —o un pasivo— empresarial, porque los consejos de administración, las juntas de accionistas o los fondos de inversión valoran la madurez de las empresas (rendición de cuentas).

- El paso del ocultamiento de incidentes a la trasparencia obliga a desarrollar políticas y estructuras de comunicación estratégica, pasando de la nota de prensa única a los mensajes segmentados por los distintos públicos y redes sociales y de la reacción a la anticipación (ética y explicabilidad).

- Para limitar los daños y reforzar la resiliencia, el sector tendrá que articular su cooperación con el resto del sector para buscar sinergias (cooperación sectorial) y mejorar su capacidad de interlocución e influencia con el sector público para buscar una redistribución equilibrada de las responsabilidades (cooperación privada-pública).