Cod. 8882 | Tecnología de las telecomunicaciones | 3325.99-2 Seguridad informática

El reto de la ciber-seguridad en la industria conectada

The cyber-security challenge at the connected industry

Pablo García-Bringas, Ignacio Angulo, Aitor Goti-Elordi e Iker Pastor
Universidad de Deusto (España)

DOI: http://dx.doi.org/10.6036/8882

1. INTRODUCCIÓN

La seguridad informática, también conocida como Ciber-seguridad o seguridad de tecnologías de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras[1]. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La Ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El presente artículo tiene como objetivo ofrecer una reflexión abierta sobre los retos de Ciber-Seguridad en la Industria Conectada. La Industria Conectada es ya una realidad. La acelerada evolución de las diferentes corrientes tecnológicas confluye en esta última década en un efecto sinérgico que está llamado en nuestros días a constituir por sí mismo lo que algunos gurús ya denominan la Cuarta Revolución Industrial [2].

Después de la máquina de vapor y la mecanización (primera revolución industrial, segunda mitad del siglo XVIII), después del desarrollo de la electricidad aplicada a la industria (segunda revolución, finales del siglo XIX), y después de la automatización sistemática de los procesos industriales (tercera revolución, siglo XX), todo apunta a que el inmenso salto cualitativo aportado por las Tecnologías de la Información y las Comunicaciones (las denominadas TIC) constituye, está constituyendo, una transformación industrial de otra escala, de otro orden de magnitud, que apunta hacia una visión última de lo que es la denominada Fábrica Inteligente, o Smart Industry [3].

En esta carrera por conquistar el futuro, dos enfoques se han revelado significativamente por encima de los demás: por un lado, el nuevo paradigma de Smart Manufacturing del proyecto SMLC estadounidense, [4], [5], y por otro lado el concepto de Industria 4.0 europeo de la Academia Nacional de Ciencia e Ingeniería Alemana [6].

En el primero de los casos, la transformación industrial aparece sustentada sobre tres pilares fundamentales, intrínsecos de la cultura de innovación americana: (1) la interconexión de máquinas y procesos entre sí y con los centros de operación y decisión, (2) la integración de sistemas TIC en el propio emplazamiento productivo como parte consustancial de los nuevos enfoques, y (3) el inherente y permanente intercambio de información con el exterior de la fábrica (con clientes, proveedores, inversores, competidores, con otras fábricas inteligentes, etcétera). Dado este singular impacto que las comunicaciones introducen en el proceso de Transformación Digital de la Industria [7], una acepción especialmente acertada es la de Peter C. Evans y Marco Annunziata de General Electric [8][9] respecto a la Industria Conectada; Industria Conectada en la que todo pasa a girar en torno a esos tres ejes principales: Internet of Things, Datos y Servicios.

Por su parte, el segundo ejercicio de sustanciación de ese concepto de transformación digital, aportado por el gobierno alemán en su denominada Estrategia de Competitividad Industria 4.0, introduce un marco estratégico general de especial relevancia en el ámbito Europeo. Aunque los primeros pasos en esta materia se remontan a 2006, con la definición de la High-Tech Strategy, no fue hasta la feria de Hannover de 2011 cuando se sentaron las bases del nuevo enfoque. Un poco después, en la edición de 2013 de dicha feria, un singular grupo de trabajo en el que participaban entidades como BOSCH, SIEMENES, SAP, BMW, DAIMLER, ABB, THYSSENKRUPP, FRAUNHOFER o DEUTSCHE TELEKOM, entre otras, publicó su informe final de implementación de dicha estrategia [6]). De todo lo relacionado con la digitalización de su industria, el gobierno alemán esperaba un incremento de entre un 15% y un 25% de la productividad, un crecimiento del 1% del PIB y un crecimiento del empleo de un 6%.

Si bien es cierto que la industria en general, y la europea en particular, no ha dejado en ningún momento de transformarse y actualizarse, al menos durante las últimas tres décadas, sin duda este ejercicio de consolidación del concepto

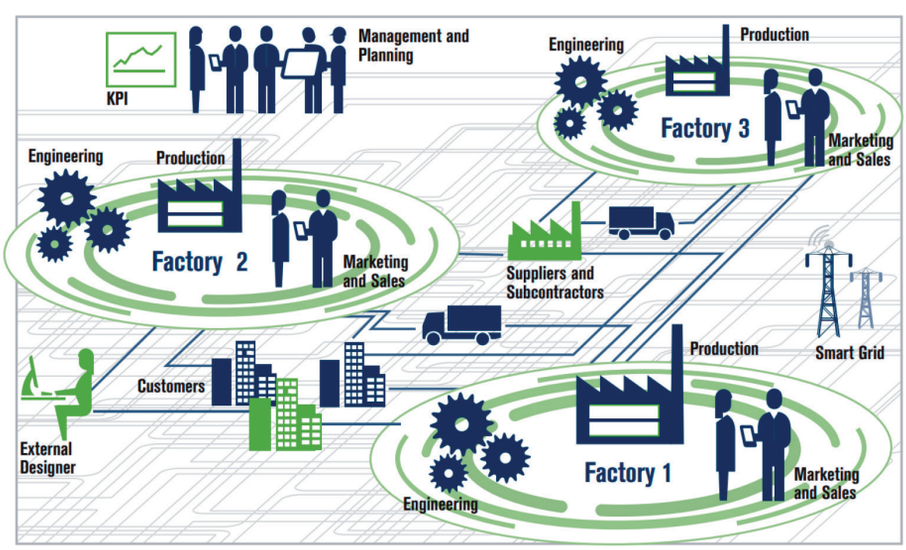

Figura 1: Red de valor horizontal (basado en HEWLETT-PACKARD 2013)

Industria 4.0 ha sido determinante a la hora de divulgar y concienciar en todo lo relativo a las oportunidades que la tecnología pone al servicio de la actualización industrial. También ha sido clave a la hora de consolidar los retos a los que se enfrenta la industria europea, en el objetivo de mantener su competitividad. Si bien es cierto que la mejora continua siempre ha estado en marcha, optando por actualizaciones incrementales, prudentes y de corto plazo, la consolidación del concepto 4.0 apunta claramente a que es el momento de aprovechar la actual ola de sinergias, a que es el momento de apostar por las innovaciones rupturistas, explosivas en términos de creación de valor. En particular, esta estrategia se desarrolla a lo largo de tres vectores transversales: (1) integración horizontal a través de redes de valor y de nuevos modelos de negocio (Figura 1), (2) ingeniería extremo a extremo, a lo largo de la cadena de valor (Figura 2); y (3) integración vertical y sistemas de producción industrial interconectados. Como puede observarse es una aproximación que presenta importantes analogías y paralelismos con el modelo americano.

En cualquier caso, ambos paradigmas vienen a coincidir en que no representan sino la transición de los tradicionales enfoques centralizados a un modelo de producción descentralizada. Una transición en la que se pasa de un proceso de producción convencional en el que la maquinaria genera un producto, a un nuevo enfoque en el que es el producto el que se comunica con la maquinaria a lo largo del proceso productivo para indicar en cada momento qué se tiene que hacer exactamente. Cada ejemplar de producto es quien indica sus especificaciones de fabricación, a lo largo y ancho de un sistema de producción Ciber-Físico o CPS [11] que lo conecta todo: máquinas, sistemas, procesos, productos y servicios, y negocio. La Figura 3 ilustra un caso de ejemplo de arquitectura de referencia para un sistema Ciber-Físico modelo.

2. MOMENTO DE CONFLUENCIA DE TECNOLOGÍAS

Se da el caso de que en los últimos tiempos han aparecido diversas tecnologías, muy basadas en Tecnologías de la Información y las Comunicaciones, que están alcanzando niveles de elevada madurez, no sólo tecnológica, sino también en lo relativo a su aplicabilidad a diferentes modelos y procesos de negocio. Así, dichas tecnologías se convierten en auténticos habilitadores clave frente a retos más ambiciosos, como es el caso del de la Industria Conectada. De hecho, la Comisión Europea habla precisamente de Key Enabling Technologies, o KETs [12], [13]. Dichas tecnologías están en el origen de los retos de la industria, y al mismo tiempo son también herramientas para afrontar dichos retos. Y es que la introducción de tecnología resuelve ciertos desafíos, y por lo general presenta otros nuevos.

Uno de los elementos tecnológicos que más relevancia ha adquirido y está adquiriendo es el denominado Internet of Things, o Internet de las Cosas, que conecta el mundo físico de los dispositivos (dispositivos de consumo o dispositivos industriales) con el mundo de los sistemas de información, con la misión de proveer al usuario o al consumidor de servicios cada vez más inteligentes [14]. No obstante, este elemento representa una idea más abstracta que una tecnología en sí misma, por lo que su participación en el concepto Ciber-Físico es estructural; es más bien un paradigma de conexión y representación, que depende de tecnologías específicas.

Existen diferentes perspectivas a la hora de aproximarse a la identificación de tecnologías habilitadoras clave. Una aproximación sencilla y directa es la realizada por el Departamento de Desarrollo Económico y Competitividad del Gobierno Vasco, a través de su Sociedad para la Promoción y Reconversión Industrial - SPRI [15]. No en vano precisamente el País Vasco constituye una región privilegiada a nivel europeo en materia de aportación industrial al PIB, y también en materia de porcentaje de dedicación del PIB a Investigación, Desarrollo de Tecnologías e Innovación. En ella, se han desarrollado diversas iniciativas público-privadas en las que han participados los principales agentes industriales y empresariales vascos, y también empresas industriales de primer nivel mundial, como es el caso de CAF, ABB, CIE, IBERDROLA, ITP, MERCEDES-BENZ, MICHELIN, MICROSOFT, REPSOL, SIEMENS O EUSKALTEL, entre otros, y en las que se ha venido consolidando el conjunto de tecnologías que resultan más relevantes por su proyección de futuro y su impacto estimado en el negocio [15]. En particular, la Fabricación Aditiva, la Robótica Colaborativa, los Sistemas Ciber-Físicos en sí mismos, la Realidad Aumentada, la Computación Cloud (en la nube), el Big Data, la Visión Artificial, y la Ciber-Seguridad, son las ocho principales herramientas que se han identificado.

Por otro lado, habitualmente se considera que estas tecnologías aportan su valor al concepto de Industria Conectada

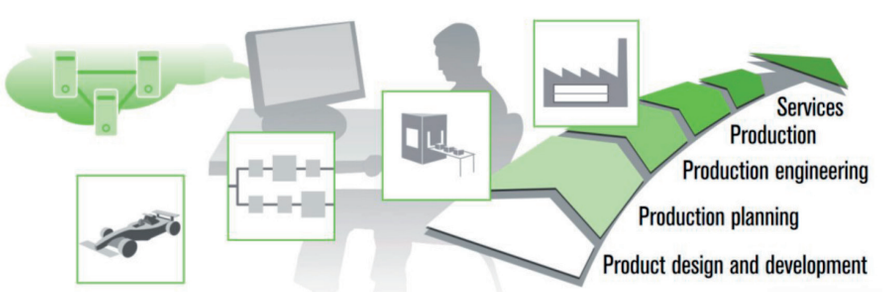

Figura 2: Ingeniería extremo a extremo. (Fuente: ACATECH 2013, SIEMENS, 2012)

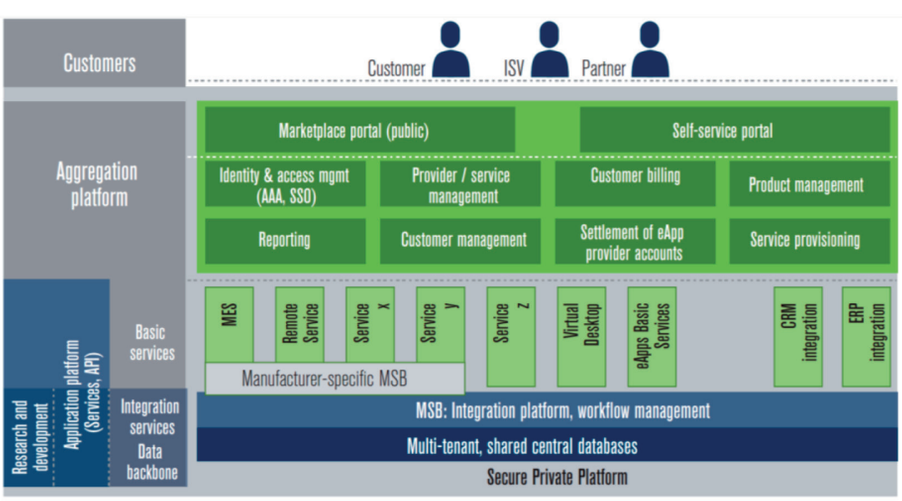

Figura 3: Arquitectura de referencia de un Sistema Ciber-Físico de ejemplo. (Fuente: ACATECH 2013, HP 2013).

Figura 4: Marco conceptual de tecnologías habilitadoras. (Fuente: Ministerio de Industria, Energía y Turismo, 2015).

desde diferentes niveles de abstracción, con un primer nivel cercano a la concreción de las máquinas y los sistemas; con un segundo nivel centrado en materia de representación y tratamiento de datos; y con un tercer nivel más abstracto, más cerca de la parte de negocio. El enfoque desarrollado por la iniciativa Industria Conectada 4.0 del Ministerio de Industria, Energía y Turismo Español proporciona un esquema general muy clarificador, estructurado precisamente en estos tres niveles de abstracción [7]. Éste es un enfoque que mantiene un cierto paralelismo con el esquema general de trabajo de la iniciativa americana. Así, se han señalado tres diferentes niveles, de (1) hibridación del mundo físico y el mundo digital, de (2) habilitación de comunicaciones y tratamiento de datos, y de (3) aplicaciones de gestión intraempresa e interempresas. La Figura 4 ilustra este esquema general.

En particular, de todo el espectro de corrientes tecnológicas presentado, existe un concepto especialmente habilitador, especialmente vinculado con la sostenibilidad y por tanto la competitividad de los enfoques, precisamente en un entorno de omni-conectividad: la Ciber-Seguridad.

3. EL RETO DE LA CIBER-SEGURIDAD EN LA INDUSTRIA CONECTADA

Desde luego, la Ciber-Seguridad constituye la tecnología habilitadora por excelencia. Incluso puede decirse que la carencia de unas medidas de seguridad adecuadas inhabilita, de partida, modelos de producción y de negocio que pueden ser prometedores en el resto de parámetros, pero que no tienen viabilidad en el caso de que por cualquier motivo no sea posible activar las diferentes funciones de seguridad. Ser o no ser. Efectivamente, la seguridad ha cobrado una dimensión determinante en cualquier proceso industrial, debido sobre todo a los nuevos niveles de conexión global, que introducen -además de las ventajas- importantes riesgos (Morrie, 2015). Y es que la descentralización de la información ha generado una ruptura en el paradigma de seguridad que se ha venido aplicando al menos en las dos últimas décadas. Tradicionalmente se han venido aplicando medidas de seguridad dirigidas a defender el perímetro tecnológico de las organizaciones, y estas medidas ya no son eficaces cuando el perímetro simplemente -gracias a las nuevas necesidades de conexión permanente y móvil, y especialmente a la Computación en la Nube- deja de existir [16]. Así, la seguridad termina afectando a todos los procesos e incluso al propio producto. Un ejemplo de esto puede ser el del fabricante de automóviles Land Rover, que ha tenido que retirar del mercado 65.000 vehículos, porque un problema de seguridad permitía fácilmente robar los automóviles [18]. Afortunadamente estos casos sirven como inmejorable impulso para redoblar los esfuerzos en materia de Ciber-Seguridad.

En definitiva, todo apunta a que estas tecnologías habilitadoras clave van a seguir experimentando sus propios procesos de evolución, y en ellos la aplicación al mundo industrial constituye un elemento catalizador de transformación digital de primer orden. Algunas de ellas se orientarán hacia aplicaciones más bien verticales, circunscritas a determinados espacios de los modelos productivos y de negocio, y algunas otras -como es precisamente el caso de la Ciber-Seguridad- mantendrán un carácter más bien transversal y más habilitador incluso, ya que de ellas dependerá la posibilidad de disponer (o no) de auténticas Industrias Conectadas.

La tecnología avanza a un ritmo muy rápido y desconocemos realmente cómo funciona. Cuando queremos conectar todas nuestras máquinas o la producción completa, en sí misma, surgen los problemas. En general ello sucede porque hay una clara falta de autocrítica. Muchas empresas e industrias contratan un filtro de tráfico de comunicaciones, un firewall, y un antivirus como máximos exponentes de su inversión en materia de seguridad de la información, y no optan por dar el paso delante de trabajar con expertos que verdaderamente aseguren la explotación de su negocio. ¿Realmente sabemos si la Ciber-Seguridad funciona en nuestra empresa? ¿Hacemos simulacros de ataques externos para comprobarlo? Muchas veces incluso ni siquiera sabemos si nuestra empresa está conectada. Creemos que no lo está y que podemos sentirnos seguros por ello, pero, en realidad, desconocemos si verdaderamente nuestros servicios internos tienen contacto directo con el exterior, o no. En los próximos años la práctica totalidad de aspectos de la industria se encontrarán hiper-conectados (televisión, Internet, móviles, etcétera), y el problema de las brechas de seguridad se incrementará de un modo todavía más explosivo que el actual. Un claro ejemplo de esto es el reciente Ciber-ataque a grandes empresas de Estados Unidos como Amazon, que se considera el primer ataque informático que ha utilizado masivamente la Internet de las Cosas, en lo que algunos expertos del sector consideran el primer caso de ataque IoT DoS (o de denegación de servicio *basado en la Internet de las Cosas*) [20]. En este caso las afectadas han sido grandes corporaciones, pero no podemos pensar que esos asaltos o intrusiones se centran exclusivamente en las grandes compañías; las pequeñas y medianas empresas también están expuestas y son mucho más indefensas, ya que por lo general adolecen de las capacidades de inversión en seguridad de las grandes. Hay que tener en cuenta que los ataques pueden provenir de cualquier lugar y afectar a cualquiera, sabiendo que, además se tardan unos 200 días por término medio en detectar una brecha en el sistema de seguridad [21]. En la propia experiencia de los autores se han llegado a observar un caso extremo en el que máquinas críticas en la producción de una empresa industrial, que habían sido infectadas, han estado intentando conectar con el creador del virus durante nada menos que 11 años. Todo ese tiempo estuvieron con el intruso en el interior y los responsables de la compañía no tenían conocimiento alguno. Esas intromisiones pueden identificar -y filtrar- los movimientos estratégicos de la empresa, o acceder

a información transmitida en reuniones secretas. Una pequeña y mediana empresa, por un único compromiso de seguridad, puede llegar a quebrar. La Ciber-delincuencia se extiende cada vez más y detrás de ella existen auténticos profesionales de la ingeniería e incluso grandes asociaciones -subversivas- muy estructuradas y organizadas, dedicadas por entero a esa actividad criminal. Afortunadamente, en la actualidad existen herramientas y conocimientos de expertos que permiten retrasar o impedir los ataques, si bien es cierto que solamente esto no es suficiente. La clave de la seguridad reside en el compromiso por parte de las compañías, y la visión estratégica y directiva más allá de los resultados de este trimestre. El principal reto al que se enfrenta la Industria Conectada en materia de seguridad no es sino de concienciación, de superación de esa falta tradicional falta de preocupación ante los riesgos de la información. Por eso es fundamental considerar la inversión en seguridad desde un planteamiento general de seguridad activa, que combine el despliegue de sistemas internos con servicios especializados, que detecten las brechas, respondan rápidamente, y ayuden a convertir la empresa en una fortaleza.

4. LA CONEXIÓN LEGAL

La Industria Conectada y, en general toda la tecnología (realidad aumentada, la Internet de las Cosas, la impresión 3D, la Ciber-Seguridad, etcétera), contienen una vertiente legal que las empresas no deben obviar. Internet es una realidad digital, un mundo en el que se echa en falta una mayor regulación propia (se hereda la regulación y legislación existente, que en general responde despacio a las nuevas realidades que la tecnología propicia rápidamente), y constituye en sí mismo un territorio infinito en manos privadas. Una muestra de esto puede ser el hecho de que el 95% de los delitos que se cometen en Internet quedan impunes, simplemente porque los ataques provienen de lugares donde es imposible detener a los culpables [22]. Cada vez más voces hablan de la necesidad de crear una especie de Ciber-Derecho, en el que se mezclara lo técnico con lo legal [23]. La industria tiene que protegerse desde el punto de vista técnico, pero también desde el legal. En diversas ocasiones, y pese a que se han desarrollado cantidad de leyes y reglamentos sobre seguridad y protección de datos (LOPD, LSSICE, ley de propiedad intelectual, Esquema Nacional de Seguridad, Reglamento Europeo de Protección de datos, etc.), más esquemas organizativos de estándares sobre seguridad (por ejemplo, ISO/IEC 27001), las incidencias relacionadas con la Ciber-seguridad han requerido de acciones correctivas, preventivas y paliativas de diversa índole. Ante un robo de secreto industrial o de cualquier otro tipo de información sensible, o ante un ataque informático contra nuestra propiedad intelectual o contra la disponibilidad de nuestros servicios, no existe respuesta o defensa posible si previamente no hemos protegido legalmente esos aspectos del negocio. Por eso es necesario contar con un protocolo de actuación que sirva para proteger los datos y los procesos de la industria. Disponer de pólizas de seguros frente a esos ataques también es una buena práctica. Otras medidas útiles son la regulación efectiva de los contratos en relación a los datos obtenidos de la sensorización de las máquinas. Así pues, es muy relevante que los aspectos jurídicos sean tenidos en cuenta en la Industria Conectada. El principal problema es que el legislador suele necesitar jurisprudencia para ir construyendo las adaptaciones de la regulación que necesita, y esto le implica ir por detrás de la realidad de los problemas. Además, en la actualidad los problemas que pueden derivarse de la tecnología son globales y su resolución está sujeta a una pluralidad de ordenamientos jurídicos. Por eso es especialmente necesario impulsar al máximo los diferentes procesos parciales de innovación legal.

5. CONCLUSIONES Y LÍNEAS FUTURAS

El presente artículo ofrece una reflexión abierta sobre los retos de Ciber-Seguridad en la Industria Conectada, partiendo de un análisis de la oportunidad del momento derivada de la confluencia de nuevas tecnologías interconectadas, concluyendo que más allá de la incertidumbre propia de la acelerada evolución tecnológica que vivimos, nos encontramos sobre todo en un momento de grandes retos, de prometedoras oportunidades. Conectividad, Ciber-seguridad, analítica de datos, más conversación de la tecnología con el cliente, nuevos perfiles y capacitaciones profesionales, implicaciones legales de los nuevos modelos de negocio, parecen ser las principales tendencias que están confluyendo en estos últimos tiempos, y sobre las que la empresa, la Sociedad, está llamada a construir buena parte del futuro. La Ciber-Seguridad en particular es una componente sin la que no es posible concebir mínimamente sostenibilidad y competitividad. ¿A qué esperamos?

REFERENCIAS

[1] M. Bishop, "What is computer security?," IEEE Secur. Priv. Mag., vol. 1, no. 1, pp. 67–69, Jan. 2003.

[2] K. Schwab, "The Fourth Industrial Revolution, by Klaus Schwab | World Economic Forum," 2016. [Online]. Available: https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab. [Accessed: 21-Jul-2018].

[3] Tecnalia Corp., "29 BIEMH BIENAL ESPAÑOLA DE MÁQUINA HERRAMIENTA," 2018. [Online]. Available: https://www.tecnalia.com/es/industria-transporte/eventos/29-biemh-bienal-espanola-de-maquina-herramienta.htm. [Accessed: 21-Jul-2018].

[4] Smart Manufacturing Leadership Coalition, "SMLC Forum Report: Priorities, Infrastructure and Collaboration for Implementation of Smart Manufacturing," 2012.

[5] "SMLC Project (2008): Smart Process Manufacturing: an Operations and Technology Roadmap. Smart Manufacturing Leadership Coalition, 2008."

[6] H. Kagermann et al., "Editorial staff Copy editing English translation Layout and typesetting Graphics beim Stifterverband für die Deutsche Wissenschaft - Recommendations for implementing the strategic initiative INDUSTRIE 4.0," 2013.

[7] "MINETUR (2015): La transformación digital de la industria española. Ministerio de Industria, Energía y Turismo. Gobierno de España, 2015."

[8] Morrie, G. (2015): Building a Secure Computer System. Ed. Van Nostrand Reinhold, 2015.

[9] "Industrial Internet Insights Report for 2015, General Electric and Accenture," 2015.

[10] P. C. Evans and M. Annunziata, "Pushing the Boundaries of Minds and Machines," 2012.

[11] i-scoop, "Industry 4.0: the fourth industrial revolution - guide to Industrie 4.0," 2018. [Online]. Available: https://www.i-scoop.eu/industry-4-0/. [Accessed: 22-Jul-2018].

[12] "NSF (2008): Cyber-Physical Systems (CPS). Program Announcements and Information. National Science Foundation - NFS, 2008." .

[13] European Commision, "EUR-Lex - 52009DC0512 - EN - EUR-Lex. - Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - «Preparar nuestro futuro: desarrollo de una estrategia común en la UE para las tecnologías facilitadoras esenciales» {SEC(2009) 1257}," 2009.

[14] European Commission, "Cross-sectoral analysis of the impact of international industrial policy on key enabling technologies - EU Law and Publications," 2011.

[15] Dave Evans, "White paper: The Internet of Things How the Next Evolution of the Internet Is Changing Everything," 2011.

[16] SPRI, "6 de noviembre 2016 Palacio Kursaal Donostia-San Sebastián DOSSIER DE PRENSA," 2016.

[17] M. B. Kelley, "Stuxnet Was Far More Dangerous Than Previous Thought - Business Insider," Business Insider, 2013. [Online]. Available: http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T. [Accessed: 22-Jul-2018].

[18] BBC, "Software bug prompts Range Rover recall - BBC News," BBC News, 13-Jul-2015.

[19] B. C. Nirmal and R. K. Singh, Contemporary Issues in International Law : Environment, International Trade, Information Technology and Legal Education.

[20] The Guardian, "DDoS attack that disrupted internet was largest of its kind in history, experts say", 26-Oct-2016.

[21] IT Governance, "How long does it take to detect a cyber attack?", Luke Irwin, 21-Feb-2018.

[22] El País, "El 95% de los ciberdelitos cometidos quedan impunes", Jesús Duva, 4-May-2014.

[23] Noticias jurídicas, "Ciberespacio, ciberderecho y ciberabogados", Álvaro Écija, 8-Mar-2017.