Panorama institucional de la gobernanza de la ciberseguridad en España

The institutional landscape of cybersecurity governance in Spain

CRISTINA DEL-REAL
Assistant Professor
Universidad de Leiden (Paises Bajos)

c.del.real@fgga.leidenuniv.nl

https://orcid.org/0000-0003-3069-4974

Resumen: Mantener seguro el ciberespacio es una tarea compleja que supone un reto constante para las instituciones públicas. A la primera oleada de desinterés político por la ciberseguridad le ha seguido una renovada preocupación por la soberanía digital, la defensa de la ciberseguridad nacional y, más recientemente, la protección de la ciudadanía en el ciberespacio. Para cumplir estos objetivos, los Estados han desarrollado normativas, instituciones y prácticas basadas en diferentes narrativas. Este estudio analiza las instituciones involucradas en la gobernanza de la ciberseguridad en España a través de cuatro prácticas: cultura de ciberseguridad, respuesta a ciber incidentes y ciber crisis, protección de infrastructuras críticas e investigación criminal. El artículo aporta evidencias coincidentes con la conclusión de que España ha adoptado la narrativa de la gobernanza multi-stakeholder a través de competencias distribuidas entre diferentes actores. Este enfoque se ha materializado en fragmentación institucional y a la falta de claridad sobre el sistema de ciberseguridad en España. El artículo finaliza con propuestas de políticas públicas que podrían contribuir a una mayor unidad, coordinación y claridad del sistema de gobernanza de la ciberseguridad.

***Abstract**: Securing cyberspace is a complex task and an ongoing challenge for public institutions. The first wave of political disinterest in cybersecurity has been followed by a renewed concern for digital sovereignty, the defence of national cybersecurity and, more recently, the protection of citizens in cyberspace. States have developed regulations, institutions and practices based on*

Recepción: 13/04/2022

Aceptación: 12/12/2022

Cómo citar este trabajo: DEL-REAL, Cristina. "Panorama institucional de la gobernanza de la seguridad en España", *Revista de Estudios Jurídicos y Criminológicos*, n.º 6, Universidad de Cádiz, 2022, pp. 15-51, DOI: https://doi.org/10.25267/REJUCRIM.2022.i6.03

different narratives to meet these objectives. This study analyses the institutions involved in the governance of cybersecurity in Spain through four practices: cybersecurity culture, cyber incident and cyber crisis response, critical infrastructure protection and criminal investigation. The article provides evidence that coincides with the conclusion that Spain has adopted the narrative of multi-stakeholder governance through distributed competences among different actors. This approach contributes to institutional fragmentation and a lack of clarity about the cybersecurity system in Spain. The article ends with proposals for public policies that could contribute to greater unity, coordination and clarity in the cybersecurity governance system.

Palabras claves: actores, gobernanza en red, cultura de ciberseguridad, respuesta a incidentes, protección de infraestructuras críticas.

Keywords*: actors, networked governance, cybersecurity culture, cyber incidents response, critical infrastructure protection.*

Sumario: 1. INTRODUCCIÓN. 2. GOBERNANZA DE LA CIBERSEGURIDAD. 2.1. Antecedentes históricos. 2.2. Marcos conceptuales. 3. RIESGOS VS AMENAZAS. 4. ANTECEDENTES EUROPEOS. 5. ESTRUCTURA DE LA GOBERNANZA DE LA CIBERSEGURIDAD EN ESPAÑA. 6. PRÁCTICAS DE CIBERSEGURIDAD. 6.1. Promoción de la sociedad digital y cultura de ciberseguridad. 6.2. Respuesta a incidentes de ciberseguridad y gestión de ciber crisis. 6.3. Protección de infrastructuras críticas. 6.4. Investigación criminal. 7. CONCLUSIONES. 8. REFERENCIAS.

1. INTRODUCCIÓN

En los últimos años, el ciberespacio se ha convertido en uno de los lugares preferidos por los criminales para llevar a cabo sus acciones ilícitas. Las investigaciones criminológicas realizadas hasta la fecha evidencian que, mientras el crimen tradicional está disminuyendo, el cibercrimen[1] aumenta[2]. Las oportunidades que ofrecen el anonimato, la inmediatez o la ausencia de fronteras que caracterizan al ciberespacio son a la vez una ventaja para los cibercriminales y organizaciones cibercriminales y un reto para la ciberseguridad. Entre otras cuestiones, la aparición de las ciberamenazas ha desafiado los tradicionales instrumentos del Estado para controlar la delincuencia y garantizar la seguridad nacional, al no encontrarse estos alineados con las necesidades del ciberespacio.

[1] Para consultar definiciones sobre "cibercrimen", ver por ejemplo MAIMON, D.; LOUDERBACK, E. R., "Cyber-Dependent Crimes: An Interdisciplinary Review", *Annual Review of Criminology*, vol. 2, 1, 2019; MCGUIRE, M.; DOWLING, S., *Chapter 2: Cyber-enabled crimes -fraud and theft*, Home Office, 2013, fecha de consulta 7 abril 2020; PAYNE, B. K. "Defining Cybercrime", en *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer International Publishing, Cham, 2019.

[2] Ver, p. ej., BUIL-GIL, D.; MIRÓ-LLINARES, F.; MONEVA, A.; KEMP, S.; DÍAZ-CASTAÑO, N., "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK", *European Societies*, 2020; MIRÓ-LLINARES, F.; MONEVA, A., "What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks 'Did cybercrime cause the crime drop?'", *Crime Science*, vol. 8, 1, 2019.

La literatura ha señalado algunas de las razones por las cuales las acciones maliciosas en el ciberespacio[3] han supuesto un reto para los instrumentos del Estado. En primer lugar, porque su lucha requiere de herramientas y técnicas diferentes a las tradicionales[4]. Como veremos más adelante en el artículo, esta necesidad de adaptación a las herramientas y técnicas utilizadas por las ciberamenazas ha producido que España desarrolle nuevos organismos –o secciones dentro de organismos tradicionales– con el objetivo de adaptar las capacidades del Estado a las amenazas a la ciberseguridad. En segundo lugar, existe una confusión terminológica sobre los problemas de ciberseguridad, que se traslada en confusiones en la regulación. Conceptos como ciberamenazas, ciber-riesgos, cibercrimen, ciber crisis o el propio concepto de ciberseguridad son utilizados desde distintas definiciones. Por ejemplo, el propio concepto de "ciberamenaza" no se utiliza de forma consistente ni por la literatura académica ni por la industria. Atendiendo a la RAE, la (ciber)amenaza sería la "acción de (ciber) amenazar"; es decir, supone la existencia de indicios de una voluntad de producir un mal o de la inminencia de este. Se pueden encontrar ejemplos en los que la "ciberamenaza" se utiliza como sinónimo de actores maliciosos en el ciberespacio (e.g., cibercriminales, grupos de hackers patrocinado por un Estado)[5]. Sin embargo, también existen autores que utilizan "ciberamenaza" como sinónimo de vulnerabilidad en un sistema informático[6], o incluso como sinónimo de "acción maliciosa en el ciberespacio", como se puede observar en el último Informe sobre la Cibercriminalidad en España del Ministerio del Interior[7].

En tercer lugar, si bien estas imprecisiones terminológicas son comprensibles en un contexto en constante evolución, pueden producir confusiones jurídicas y jurisdiccionales que hacen difícil su abordaje desde las políticas públicas. Así, las acciones maliciosas en el ciberespacio no respetan las tradicionales delimitaciones jurídicas, lo que puede

[3] Como se argumenta en este párrafo, los conceptos relacionados con la ciberseguridad son objeto de amplio debate. Por ello, en este artículo se ha optado por utilizar el génerico "acciones maliciosas en el ciberespacio", utilizado en la Estrategia Nacional de Ciberseguridad 2019, para incluir así tanto el cibercrimen tipificado en los instrumentos penales, el hacktivismo, así como actuaciones localizadas en la zona gris, como las ciber-operaciones relacionadas con el comportamiento de los Estados en un contexto geo-político.

[4] Al respecto BURNS, R. G.; WHITWORTH, K. H.; THOMPSON, C. Y., "Assessing law enforcement preparedness to address Internet fraud", *Journal of Criminal Justice*, vol. 32, 5, 2004; HINDUJA, S., "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", *Policing: An International Journal of Police Strategies & Management*, vol. 27, 3, 2004.

[5] MAVROEIDIS, V.; HOHIMER, R.; CASEY, T.; JESANG, T., "Threat Actor Type Inference and Characterization within Cyber Threat Intelligence", en *2021 13th International Conference on Cyber Conflict (CyCon)*, IEEE, Tallinn, Estonia, 2021, fecha de consulta 2 noviembre 2022, en https://ieeexplore.ieee.org/document/9468305/.

[6] MALINA, L.; SRIVASTAVA, G.; DZURENDA, P.; HAJNY, J.; RICCI, S., "A Privacy-Enhancing Framework for Internet of Things Services", en *Network and System Security. 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings*, vol. 11928, Springer Cham, 2019 (Lecture Notes in Computer Science).

[7] LÓPEZ GUTIÉRREZ, J.; SÁNCHEZ JIMÉNEZ, F.; HERRERA SÁNCHEZ, D.; MARTÍNEZ MORENO, F.; RUBIO GARCÍA, M.; GIL PÉREZ, V.; SANTIAGO OROZCO, A. M.; y GÓMEZ MARTÍN, M. A.; *Informe sobre la Cibercriminalidad en España*, Dirección General de Coordinación y Estudios y Secretaría de Estado de Seguridad. Ministerio del Interior. Gobierno de España, Madrid, España, 2022, fecha de consulta 11 enero 2022.

producir conflictos. Como ejemplo de esta falta de homogeneidad, se encuentra la regulación de la conducta de robo de secretos comerciales, una acción relacionada con el ciberespionaje industrial. El robo de secretos comerciales está recogido en el Título 18, Parte I, párrafo 1832[8], del Código de los EEUU[9]. Este Título tiene carácter penal. En cambio, en Reino Unido la regulación del robo de secretos comerciales se encuentra recogida en las *Trade Secrets (Enforcement, etc.) Regulations 2018*, aprobadas para implementar la Directiva 2016/943 del Parlamento Europeo y del Consejo, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. Previamente a la aprobación de las *Trade Secrets (Enforcement, etc.) Regulations 2018*, no existía legislación en Reino Unido que regulara el robo de secretos comerciales[10]. Esta norma, a diferencia de la estadounidense, tiene carácter civil. El problema deriva de que el robo de secretos comerciales, en un mercado globalizado, se producirá probablemente en escala igualmente global[11]. Este mercado globalizado abriría interrogantes o ampliaría la casuística a abordar en caso de que, por ejemplo, fuera un ciudadano británico el autor. Instrumentos como el Convenio sobre ciberdelincuencia (conocido también como el Convenio de Budapest) o Eurojust, la agencia europea de cooperación entre los organismos judiciales de los Estados miembros, han allanado el camino hacia una mejor respuesta frente al cibercrimen, aunque no terminan de ser suficientes ante un fenómeno tan mutable, dispersado y plural[12].

Finalmente, la capacidad de responder a las acciones maliciosas en el ciberespacio se ve afectada por la falta de denuncias y la cifra negra[13]; es decir, todos los ciber incidentes que no son reportados a las autoridades competentes. Si tenemos en cuenta que la eficacia de las medidas de prevención de estas acciones depende, en gran medida, de cuánto conozcamos el fenómeno a prevenir, conseguir que las víctimas notifiquen el delito a la policía, o a la autoridad competente es prioritario. Esta denuncia incrementará el conocimiento de los organismos públicos sobre el fenómeno y, podrá iniciar un proceso penal con el objetivo de establecer las causas y características del incidente.

---

[8] Obtenido de: https://www.law.cornell.edu/uscode/text/18/1832. [Recuperado el 16 de abril de 2022].

[9] El Código de los EEUU (llamado en inglés *Code of Laws of the United States, United States of American Code, US Code, o USC*), recoge las leyes federales que tienen vocación de permanencia de EEUU. Contiene 52 títulos, de los cuales el Título 18 regula el Derecho penal y procesal penal (llamado *Title 18. Crimes and criminal procedure*). A su vez, el Título 18 está dividido en cinco partes: (1) Parte I – Delitos (§§ 1-2725); (2) Parte II - Procedimiento penal (§§ 3001-3772); (3) Parte III - Prisiones y prisioneros (§§ 4001-4353); (4) Parte IV – Corrección de delincuentes juveniles; y (5) Parte V – Inmunidad de los testigos (§§ 6001-5005).

[10] APLIN, T. F.; ARNOLD, R., "UK implementation of the Trade Secrets Directive", *SSRN Electronic Journal*, 2019.

[11] En el año 2019, el comercio con Reino Unido supuso para EEUU el 3,2% del total de su comercio anual US CENSUS BUREAU FOREIGN TRADE DIVISION, "Foreign Trade: Data", 2020, fecha de consulta 16 abril 2021, en https://www.census.gov/foreign-trade/statistics/highlights/top/top1912yr.html.

[12] CHRISTOU, G., *Cybersecurity in the European Union*, Palgrave Macmillan UK, London, 2016.

[13] COLEMAN, C.; MOYNIHAN, J., *Understanding crime data: haunted by the dark figure*, Open University Press, Buckingham ; Philadelphia, 1996.

El cibercrimen sufre especialmente de una elevada cifra negra porque ni individuos ni empresas suelen denunciar[14]. En este sentido, las investigaciones empíricas realizadas hasta la fecha estiman que solo se denuncia una proporción reducida de todos los cibercrímenes que se cometen. En el estudio de DOMENIE *et al*.[15] sobre victimización por cibercrimen realizado en Países Bajos con una muestra 9163 usuarios de Internet, encontraron que sólo el 13,4% de las víctimas por cibercrimen había denunciado el hecho a la policía. Por tipo de delincuencia, encontraron que solo el 4,1% de las víctimas de *hacking* había denunciado el hecho a la policía, mientras que el delito más denunciado fue el *stalking* (30,4%).

Los estudios cualitativos han obtenido resultados similares. Las víctimas de cibercrímenes no suelen denunciar y, cuando están dispuestas a ello, no saben dónde deben presentar la denuncia[16]. Un estudio más reciente con una muestra de 97186 víctimas de delitos[17] encontró un resultado similar: mientras que los delitos tradicionales como el robo de coches o de otros vehículos a motor o la tentativa de allanamiento de morada se denunciaban en más del setenta porciento de los casos, la denuncia por cibercrímenes se encontraba por debajo del treinta porciento. Específicamente, el robo de identidad se denunció un 26,3% de las veces, el ciberfraude un 24%, y el *hacking* un 7,1%. Tras la pandemia por COVID-19, estas cifras han aumentado[18]. Con unas cifras tan bajas de denuncias, es muy complicado para la policía y otros actores implicados en la ciberseguridad diseñar medidas de prevención del cibercrimen adecuadas a la realidad del fenómeno[19].

Pero ni el Estado ni la sociedad han permanecido inmóviles a esta realidad. Como resultado, han aparecido nuevos organismos públicos y actores privados a distintos niveles territoriales que han asumido las funciones de prevenir, detectar, y responder ante las acciones maliciosas en el ciberespacio. La literatura anglosajona[20], ha estudiado este fenómeno como un proceso de fragmentación de las funciones de seguridad nacional y

[14] Ver, por ejemplo, KEMP, S., "Fraud reporting in Catalonia in the Internet era: Determinants and motives", *European Journal of Criminology*, 2020; KEMP, S.; MIRÓ-LLINARES, F.; MONEVA, A., "The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain", *European Journal on Criminal Policy and Research*, 2020.

[15] DOMENIE, M. M. L.; LEUKFELDT, R.; VAN WILSEM, J.; JANSEN, J.; STOL, W., *Victimisation in a digitised society: a survey among members of the public concerning e-fraud, hacking and other high volume crimes*, Eleven International Publishing, The Hague, 2013.

[16] Véase p.ej., BIDGOLI, M., *A mixed methods approach to understanding undergraduate students' victimization, perceptions, and reporting of cybercrimes*, University of California, Irvine, 2015.

[17] VAN DE WEIJER, S. G. A.; LEUKFELDT, R.; BERNASCO, W., "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking", *European Journal of Criminology*, vol. 16, 4, 2019.

[18] BUIL-GIL, D.; MIRÓ-LLINARES, F.; MONEVA, A.; KEMP, S.; DÍAZ-CASTAÑO, N., "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK", op. cit.

[19] BUIL-GIL, D.; LORD, N.; BARRETT, E., "The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention", *Victims & Offenders*, vol. 16, 2, 2021.

[20] JOHNSTON, L.; SHEARING, C., *Governing security: explorations in policing and justice*, Routledge, London; New York, 2003; LOADER, I., "Plural Policing and Democratic Governance", *Social & Legal Studies*, vol. 9, 3, 2000.

públicas que se ha materializado en distintos modelos de "seguridad plural" (del inglés, *plural policing*).

Los modelos de seguridad plural ofrecen una visión alejada del monopolio de un único actor proveedor de seguridad –tradicionalmente, la policía– y centra el estudio científico en las estructuras de complejas redes de proveedores de seguridad. Estos modelos entienden que la seguridad solo puede ser comprendida a partir de la asunción de la existencia de redes de colaboración interconectadas. Estos modelos de seguridad plural se relacionaron con el concepto de gobernanza de la seguridad[21], donde encontramos reflejada la idea de que la seguridad debe entenderse como el resultado de los procesos de interacción entre diferentes proveedores. Dichos proveedores basan sus actuaciones en lógicas de seguridad; es decir, narrativas y marcos conceptuales utilizados para definir y comprender un problema que determinan las prácticas de seguridad.

Este estudio contribuye a la comprensión de la gobernanza de la ciberseguridad en España a través de la descripción de la lógica de la gobernanza basada en un modelo multi-stakeholder; por otro. Para ello, se describirán las instituciones estatales y las prácticas de ciberseguridad identificadas en España. Este estudio contribuye así a comprender cómo la ciberseguridad se ha definido como problema en las políticas públicas en el contexto español. Algunos estudios previos han explorado parcialmente esta cuestión[22], si bien en contextos y con el empleo de enfoques distintos a los de este artículo.

Los resultados de este estudio se basan en el análisis de documentos publicados por organismos e instituciones. Esta es una técnica de recopilación de datos que considera a los documentos como una fuente de datos en bruto, no manipulada por los investigadores. En concreto, en este estudio se han incluido informes, estrategias nacionales de ciberseguridad, normativas y guías producidas por organismos públicos y privados. Entre ellos, se encuentran las Estrategias Nacionales de Ciberseguridad de 2013 y 2019, los informes sobre cibercriminalidad publicados por el Ministerio del Interior del Gobierno de España (2013-2019), los informes publicados por el Centro Criptológico Nacional (CCN) de acceso público sobre cibercriminalidad y ciberseguridad, y normativa específica relativa a las organizaciones públicas tanto nacional como europeas e internacionales.

El artículo se estructura como sigue. La sección 2 realiza un repaso de los antecedentes históricos de la gobernanza de la seguridad y presenta los modelos de gobernanza descritos en la literatura. En el centro de la discusión de la gobernanza de la ciberseguridad se sitúa la pregunta sobre el rol del Estado en esta. En la sección 3, el artículo ofrece una breve descripción del enfoque centrado en riesgos vs amenazas. En la sección 4, se describen los antecendentes europeos. La sección 5 se expone la estructura del sistema de gobernanza de ciberseguridad. En la sección 6 se describen las cuatro

[21] JOHNSTON, L.; SHEARING, C., *Governing security*, op. cit.

[22] Por ejemplo, ARCOS, R., "Securing the Kingdom's cyberspace: cybersecurity and cyber intelligence in Spain", en *Routledge Companion to Global Cyber-Security Strategy* (eds. Romaniuk, S. M., y Manjikian, M.), 2021; FOJÓN CHAMORRO, E.; SANZ VILLALBA, Á. F., "Ciberseguridad en España: una propuesta para su gestión", *Análisis del Real Instituto Elcano*, vol. 101, 2010.

prácticas de ciberseguridad seleccionadas. Finalmente, la sección 7 expone las conclusiones y las futuras líneas de investigación.

2. GOBERNANZA DE LA SEGURIDAD

2.1 Antecedentes históricos

El primer autor que puso en cuestión el modelo de gestión de la seguridad pública basado en el monopolio de las policías y de las estrategias reactivas frente al delito fue BAYLEY[23]. Este autor, a partir de un análisis comparado de los modelos policiales de Australia, Canadá, Reino Unido, Japón y Estados Unidos, abrió la espita de la discusión del modelo policial tradicional. La discusión de BAYLEY[24] se basaba esencialmente en tres argumentos. El primero era que el modelo monopolístico no había conseguido los objetivos de diminución de la delincuencia. El segundo, que las estrategias policiales basadas en el incremento del número de patrullas policiales en las calles no habían tenido un efecto directo y proporcional en la disminución de la violencia durante los años posteriores a la Segunda Guerra Mundial. Y, el tercero, que las estrategias policiales eran reactivas, puesto que dependían de que se produjera un delito para que la policía pudiera actuar; en consecuencia, la actuación policial quedaba condicionada a la interposición de una denuncia previa por parte de una víctima[25] o de un testigo[26].

Los argumentos sobre las limitaciones del modelo de gestión de la seguridad basado en el monopolio de la policía pronto se acompañaron de una pérdida fáctica de poder. En los Estados Unidos, las empresas de seguridad privada aparecieron como un nuevo actor de la seguridad a mediados de los años 70 y principios de los 80. Su auge estuvo auspiciado por la aparición de espacios de uso público, pero de propiedad privada, como fueron los centros comerciales, los parques temáticos, o bien los barrios residenciales privados[27], en un proceso de modificación de la trama urbana y social que pronto tuvo su traslado a muchos países de diversos continentes.

Este análisis apunta a que no se puede comprender el auge de la lógica de la gobernanza de la seguridad únicamente desde un estudio de la seguridad. Como cualquier otro proceso social, la provisión de seguridad está fuertemente anclada en los cambios económicos y políticos. En este sentido, el fracaso del keynesianismo en la gestión de la crisis del petróleo de 1973 aumentó la popularidad de las ideas neoliberales basadas en los trabajos de la escuela de Friburgo, con exponentes como HAYEK y FRIEDMAN en la escuela de Chicago[28]. Para solventar esta dura crisis económica, el pensamiento

[23] BAYLEY, D. H., *Police for the future*, First, Oxford University Press, New York, 1994.

[24] *Ibid.*

[25] ZAUBERMAN, R., "Les Attitudes des Victimes individuelles", en *Crime et Sécurité. L'État des Savoirs* (eds. Robert, P., y Muccheilli, L.), La Découverte, Paris, 2002.

[26] BAYLEY, D. H.; SHEARING, C., "The Future of Policing", *Law & Society Review*, vol. 30, 3, 1996.

[27] JOHNSTON, L.; SHEARING, C., *Governing security*, op. cit.

[28] BOAS, T. C.; GANS-MORSE, J., "Neoliberalism: From New Liberal Philosophy to Anti-Liberal Slogan", *Studies in Comparative International Development*, vol. 44, 2, 2009; FRIEDMAN, M., *Capitalism*

neoliberal recomendaba eliminar el recurso a la política fiscal defendida por el keynesianismo y reducir los gastos del Estado. Como consecuencia del éxito de estas ideas neoliberales, a partir de la década de los 70 se produjeron en las economías occidentales dos procesos rupturistas con el modelo del bienestar en lo que respecta al rol del Estado como proveedor de servicios públicos. Por un lado, algunos de estos servicios se redujeron o bien fueron suprimidos y, por otro lado, la provisión de los servicios fue transferida a empresas privadas[29], abandonándose a cierta velocidad el rol central que el Estado había jugado hasta entonces en la sociedad.

Una de las principales diferencias entre el modelo keynesiano y el neoliberal es la concepción que cada uno tiene del ciudadano. Si para el Estado de bienestar el ciudadano es un usuario-consumidor de servicios públicos, en el modelo neoliberal el ciudadano es un cliente. Desde estos postulados, el Estado comienza entonces a aplicar toda una serie de métodos de gestión empresarial, enlazando su actividad con el sector privado y terciarizando servicios en este. De esta forma, se empezaron a borrar las fronteras entre los servicios públicos y los privados. El cambio de modelo de provisión de la seguridad estaba ya en marcha.

El neoliberalismo se tradujo en un incremento de la oferta de servicios de seguridad privada, que pasarían a regirse por las reglas del mercado[30], identificándosele como un bien o servicio más de la economía capitalista. Las estrategias de provisión de la seguridad basadas en la contratación de servicios privados comienzan entonces a ser percibidas como más legítimas que las estrategias públicas de las policías bajo la promesa de una mayor eficiencia y eficacia en la gestión[31].

En el triunfante modelo neoliberal no se hablaría ya de gobierno, un término que sería desplazado por el de "gobernanza". Para RHODES[32], el neoliberalismo representa una nueva forma de hacer política en la que servicios que antes eran prestados de forma exclusiva por el Estado pasan a ser provistos a través de lo que él denomina "redes inter-organizativas auto-organizadas". Sería precisamente la participación de una multiplicidad de actores públicos y del mercado en estas redes inter-organizativas lo que desplazaría de facto al gobierno como único actor, sustituyéndolo por la "gobernanza" de las redes. A partir de entonces, la gobernanza en general, y la gobernanza de la seguridad en particular, pasarán a identificarse como una extensión del pensamiento neoliberal que da coherencia a las relaciones entre el Estado y el mercado[33].

---

and freedom, 40th anniversary ed, University of Chicago Press, Chicago, 2002; VON HAYEK, F. A., *The road to serfdom*, 50th anniversary ed. / with a new introd. by Milton Friedman, University of Chicago Press, Chicago, 1994; JONES, D. S., *Masters of the universe: Hayek, Friedman, and the birth of neoliberal politics*, Fith printing, and first paperback printing, Princeton University Press, Princeton Oxford, 2014.

[29] BAYLEY, D. H.; SHEARING, C., "The Future of Policing", op. cit.

[30] *Ibid.*

[31] RHODES, R. A. W., "The New Governance: Governing without Government", *Political Studies*, vol. 44, 4, 1996.

[32] *Ibid.*

[33] WOOD, J.; SHEARING, C., *Imagining security*, Willan, Cullompton, 2007.

Pero la gobernanza de los servicios públicos, y la gobernanza de la seguridad en particular, no surge a resultas de la ciega aplicación del pensamiento neoliberal, sino por el reconocimiento de la complejidad de solucionar los problemas sociales y la aparición de múltiples centros de poder. Efectivamente, la complejidad del crimen ha aumentado debido a la adopción intensa y amplia de las nuevas tecnologías y, aun cuando las tasas de crimen tradicional están disminuyendo[34], el cibercrimen aumenta[35].

La razón, en palabras de OSTROM[36], se encontraría en que los sistemas de gobierno verticales caracterizados por una clara diferenciación entre el sector público y el privado, pertenecen ya a una etapa pasada de "sistemas simples", en la que ambos sectores se equilibraban en una visión dicotómica del mundo. Las actuales condiciones sociales y económicas, y en particular las necesidades de seguridad –argumentan los defensores del neoliberalismo– no podrían ser ya solucionadas ni resueltas ni mediante la intervención única estatal ni mediante la actuación descoordinada y anárquica del mercado[37]. En este nuevo contexto social y económico, se impone entonces la necesidad de alcanzar una interacción entre ambas para dar solución a los problemas.

La aparición de las empresas de seguridad privada y los subsiguientes cambios en la gestión de la seguridad pública producidos por la modificación del espacio urbano y social eclosionaron en la década de los años 90 en un cambio de paradigma caracterizado por alejar el objeto de estudio de la policía y estudiar cómo la provisión de seguridad es un producto del trabajo de varios actores públicos y privados. Dicho cambio de paradigma se materializó en la gobernanza de la seguridad. La explosiva expansión de Internet, la globalización de la criminalidad –como el terrorismo global, el crimen organizado o el cibercrimen– y la configuración de la sociedad actual en red –como describiría de forma pionera Castells en su ya clásica obra *La sociedad red*[38] – terminaron de impulsar la pluralización de roles en la provisión de seguridad.

En el ámbito de los estudios de la seguridad, aquellos estudios que han explorado la gobernanza de la ciberseguridad se han centrado de manera principal en las instituciones y acuerdos público-privados desarrollados por diversos países para reestructurar las responsabilidades de ciberseguridad[39]. Más específicamente, la literatura ha buscado

[34] Ver, por ejemplo, BLUMSTEIN, A.; WALLMAN, J. (EDS.), *The Crime Drop in America*, 2, Cambridge University Press, 2005; FARRELL, G.; TSELONI, A.; MAILLEY, J.; TILLEY, N., "The Crime Drop and the Security Hypothesis", *Journal of Research in Crime and Delinquency*, vol. 48, 2, 2011 sobre el fenómeno conocido como "crime drop".

[35] LEUKFELDT, E. R.; HOLT, T. J. (eds.), *The human factor of cybercrime*, Routledge, Abingdon, Oxon ; New York, NY, 2020; MIRÓ-LLINARES, F.; MONEVA, A., "What about cyberspace (and cybercrime alongside it)?", op. cit.

[36] OSTROM, E., "Beyond Markets and States: Polycentric Governance of Complex Economic Systems", *American Economic Review*, vol. 100, 3, 2010.

[37] *Ibid.*; ROCHÉ, S., "Vers la démonopolisation des fonctions régaliennes : contractualisation, territorialisation et européanisation de la sécurité intérieure", *Revue française de science politique*, vol. 54, 1, 2004.

[38] CASTELLS, M.; *La sociedad red*, 3. ed, Alianza Ed, Madrid, 2005.

[39] P.ej., ELDEM,T.; "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security", *International Journal of Public Administration*, vol. 43, 5, 2020; KUERBIS, B; y BADIEI, F.,

comprender cuál es el rol y la estructura de los organismos públicos encargados de la ciberseguridad y cómo estos establecen acuerdos de colaboración con el sector privado y las redes internacionales[40]. No obstante, la literatura sobre gobernanza de ciberseguridad aún está en la infancia[41] y, en muy excepcionales ocasiones, han abordado casos fuera del mundo anglosajón o de los ciber "grandes poderes" (Estados Unidos, Rusia, China o Irán)[42].

2.2 Marcos conceptuales

La literatura sobre estudios de la seguridad distingue tres aproximaciones a la gobernanza de la seguridad principales según el rol del Estado: la gobernanza nodal, el pluralismo anclado y el capitalismo regulatorio. En primer lugar, la *gobernanza nodal* fue desarrollada por los trabajos teóricos de SHEARING, JOHNSTON y WOOD[43], que fueron complementados y actualizados por otros autores[44]. Para estos autores, en la provisión de seguridad intervienen múltiples actores –que los autores denominan "nodos"– de naturaleza pública, privada o híbrida. Esta provisión se realiza a partir de redes de nodos, que deben estudiarse como una pregunta "empíricamente abierta", sin una disposición ni idea preconcebida sobre los roles de los nodos públicos y privados[45]. Es decir, la gobernanza nodal rechaza la asunción de que las instituciones del Estado tienen, de partida, una posición jerárquicamente superior a otras en las redes de gobernanza. Estudios posteriores conceptualizan la idea de *nodos superestructurales*, que son redes de nodos que "unen a representantes de diferentes organizaciones de nodos […]

"Mapping the cybersecurity institutional landscape", *Digital Policy, Regulation and Governance*, vol. 19, 6, 2017; VAN PUYVELDE, D; BRANTLY, A. F., *Cybersecurity: politics, governance and conflict in cyberspace*, Polity Press, Cambridge, UK; Medford, MA, USA, 2019.

[40] ADAMS, S. A.; BROKX, M.; GALIČ, M.; KALA, K.; KOOPS, B.-J.; LEENES, R.; SCHELLEKENS, M.; E SILVA, K.; y ŠKORVÁNEK, I., *The governance of cybersecurity. A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK*, Tilburg Institute for Law, Technology, and Society, Tilburg, 2015; CALCARA, A.; y MARCHETTI, R., "State-industry relations and cybersecurity governance in Europe", *Review of International Political Economy*, 2021; KUERBIS, B.; y BADIEI, F., "Mapping the cybersecurity institutional landscape", *cit*.

[41] KUERBIS, B.; y BADIEI, F., "Mapping the cybersecurity institutional landscape", *cit.*

[42] P.ej., ELDEM, T., "The Governance of Turkey's Cyberspace», cit.; E. SUTHERLAND, «Governance of Cybersecurity – The Case of South Africa", *The African Journal of Information and Communication*, 20, 2017.

[43] Ver JOHNSTON, L.; SHEARING, C., *Governing security*, op. cit.; C. SHEARING, "Reinventing Policing: Policing as Governance", en Otwin Marenin (ed.) *Policing Change, Changing Policing*, Routledge, New York, 1996; SHEARING, C., "Reflections on the Refusal to Acknowledge Private Governments", en *Democracy, Society and the Governance of Security* (eds., Wood, J., y Dupont, B.), Cambridge University Press, 2006; SHEARING, C.; WOOD, J., "Nodal Governance, Democracy, and the New "Denizens"", *Journal of Law and Society*, vol. 30, 3, 2003; WOOD, J.; SHEARING, C., *Imagining security*, op. cit.

[44] Ver, por ejemplo, DUPONT, B., "Security in the Age of Networks", *Policing and Society*, vol. 14, 1, 2004; KEMPA, M.; SINGH, A.-M., "Private security, political economy and the policing of race: Probing global hypotheses through the case of South Africa", *Theoretical Criminology*, vol. 12, 3, 2008; MARKS, M.; WOOD, J., "South African policing at a crossroads: The case for a 'minimal' and 'minimalist' public police", *Theoretical Criminology*, vol. 14, 3, 2010.

[45] SHEARING, C.; WOOD, J., "Nodal Governance, Democracy, and the New "Denizens"", op. cit., p. 418.

para concentran los recursos y tecnologías de los miembros para un objetivo común"[46]. Como veremos abajo en el artículo, en España también es posible identificar nodos superestructurales en la gobernanza de la ciberseguridad.

En segundo lugar, el *pluralismo anclado* surgió como alternativa al modelo de gobernanza nodal para interpretar los cambios que ocurren en el ámbito de la provisión de la seguridad. Para LOADER Y WALKER[47], los autores que propusieron este modelo, el Estado debe actuar como "ancla" de la pluralidad de actores de seguridad para que estos actúen en beneficio del interés público. En otras palabras, LOADER Y WALKER consideran que la era de los modelos "westfalianos" de prestación de seguridad centrados en el Estado siguen aún influyendo en el sector de la seguridad nacional al promover que todos los actores involucrados, incluyendo los privados, identifiquen la seguridad como un bien público.

Aunque sus autores fundacionales argumentan que es un modelo normativo que explora el rol que el Estado *debería* de tener en la provisión de la seguridad colectiva –en oposición a los modelos explicativos–[48] CRAWFORD[49] defiende que este modelo también sirve para describir los diferentes atributos del Estado en el proceso regulatorio y la gobernanza de la seguridad. Para este autor, existen cuatro mecanismos por los cuales el Estado, a través de diferentes procesos, "ancla" la provisión de la seguridad en la lógica del interés público utilizando para ello: (i) su poder simbólico y autoridad cultural, (ii) su legitimidad, tanto la autoproclamada como la percibida por los ciudadanos, (iii) su posición táctica como recurso distintivo y como fuente de información, y (iv) su posición como actor de *ultima ratio* con respecto a formas más intrusivas de control social[50]. El Estado, a través de estos cuatro mecanismos, se encargaría de asegurarse de que los proveedores de seguridad privados no impongan una lógica pura de mercado que termine favoreciendo a las clases más altas y desprotegiendo a aquellos ciudadanos con menos recursos.

Estos dos marcos conceptuales coinciden al considerar la gobernanza a través de redes de actores. En ellos identificamos la preocupación de los autores por describir cuáles son los actores, su rol dentro de la gobernanza y la naturaleza de las relaciones entre ellos; es decir, las relaciones de poder. Así, con independencia de la conceptualización concreta que realicemos de los modelos de gobernanza, todos ellos suelen conceptualizarse en

---

[46] BURRIS, S.; DRAHOS, P.; SHEARING, C., "Nodal governance", *Australian Journal of Legal Philosophy*, 30, 2005, p. 38.

[47] LOADER, I.; WALKER, N., "Necessary Virtues: The Legitimate Place of the State in the Production of Security", en *Democracy, Society and the Governance of Security*, (eds., Wood, J., y Dupont, B.), Cambridge University Press, 2006; LOADER, I.; WALKER, N., *Civilizing security*, Cambridge University Press, Cambridge ; New York, 2007.

[48] Ver LOADER, I.; WALKER, N., "Policing as a Public Good:: Reconstituting the Connections between Policing and the State", *Theoretical Criminology*, vol. 5, 1, 2001; "Necessary Virtues: The Legitimate Place of the State in the Production of Security", op. cit.; *Civilizing security*, op. cit.

[49] CRAWFORD, A., "Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security", *Theoretical Criminology*, vol. 10, 4, 2006.

[50] *Ibid.*

mayor o menor medida alrededor de estos tres ejes[51], con los siguientes extremos: sobre los actores, la diferencia es si son de naturaleza *pública* o *privada*; sobre el rol, el foco se encuentra bien en la *producción* de políticas o en su *ejecución*; finalmente, sobre la naturaleza de las relaciones entre los actores, si esta es *horizontal* o *jerárquica*. Este estudio se centra en los actores de naturaleza pública involucrados en la gobernanza de la ciberseguridad.

3. RIESGOS VS AMENAZAS

Este artículo adopta la noción de la Escuela de Copenhague de que la comprensión de la seguridad que realiza el agente y la narrativa que le acompañe se traduce en prácticas de seguridad[52]. Entre estas narrativas, la literatura diferencia aquellas centradas en los riesgos en contraposición a las centradas en las amenazas[53]. Por un lado, la narrativa de la seguridad basada en el riesgo se centra en el discurso de las vulnerabilidades sistémicas y en el aumento de la resiliencia del objeto que puede sufrir un ataque[54]. El foco de análisis e intervención es el propio objeto –o víctima potencial– cuyas características *internas* o comportamiento le exponen a sufrir un ataque. Las prácticas de ciberseguridad basadas en una narrativa de riesgo se centran en abordar la ingeniería de la sociedad y en la gestión de las causas internas del daño a largo plazo sin que estas estén basadas en amenazas concretas[55].

Por el contrario, en la narrativa de la seguridad basada en la amenaza encontramos que discurso se centra en los sujetos que pueden causar un daño y en la intención de las partes en conflicto. Las acciones entonces se centran en la defensa contra las causas *externas* del daño (los antagonistas). El énfasis en las amenazas está relacionado con prácticas de seguridad enfocadas a amenazas concretas e identificables y en la militarización del ciberespacio[56]. Este estudio profundiza en los actores públicos de la gobernanza que

[51] DUPONT, B., "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime", *Crime, Law and Social Change*, vol. 67, 1, 2017; VAN EETEN, M., "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity", *Digital Policy, Regulation and Governance*, vol. 19, 6, 2017; KUERBIS, B.; y BADIEI, F., "Mapping the cybersecurity institutional landscape", *cit.*; RONDELEZ, R., "Governing Cyber Security Through Networks: An Analysis Of Cyber Security Coordination In Belgium", 2018, Zenodo, fecha de consulta 28 mayo 2020; STERLINI, P.; MASSACCI, F.; KADENKO, K.; FIEBIG, T.; VAN EETEN, M., "Governance Challenges for European Cybersecurity Policies: Stakeholder Views", *IEEE Security & Privacy*, vol. 18, 1, 2020.

[52] BUZAN, B.; WÆVER, O.; y DE WILDE, J., *Security: a new framework for analysis*, Lynne Rienner Pub, Boulder, Colo, 1998.

[53] CORRY, O., "Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change", *Millennium: Journal of International Studies*, vol. 40, 2, 2012.

[54] BENGTSSON, L.; BORG, S.; RHINARD, M., "European security and early warning systems: from risks to threats in the European Union's health security sector", *European Security*, vol. 27, 1, 2018; CORRY O.,, "Securitisation and 'Riskification'", *cit*.

[55] CORRY, O., "Securitisation and 'Riskification'", *cit*., p. 245.

[56] BACKMAN, S., "Risk vs. threat-based cybersecurity: the case of the EU", *European Security*, 2022; CORRY, O., "Securitisation and 'Riskification'", *cit*.

ejecutan las políticas de ciberseguridad. El estudio diferencia cuatro líneas de ejecución en torno a las cuales se ha estructurado la provisión de ciberseguridad en España: (i) cultura de ciberseguridad; (ii), respuesta a ciber-incidentes; (iii) protección de infrastructuras críticas; y (iv) investigación criminal. A través de estas cuatro prácticas y las instituciones responsables, este estudio desentraña las dos líneas narrativas en torno a las cuales se ha configurado la gobernanza de la ciberseguridad en España.

4. ANTECEDENTES EUROPEOS

En los últimos diez años, la Unión Europea (UE) ha llevado a cabo una ingente producción normativa y documental con el objetivo de regular la gobernanza de la ciberseguridad a nivel europeo en respuesta al aumento de las acciones maliciosas en el ciberespacio. La política de la UE para el combate contra el cibercrimen tiene como origen la Convención de Budapest (*Convention on Cybercrime*, 2001), impulsada por el Programa de Estocolmo (*The Stockholm Programme: An open and secure Europe serving and protecting citizens*, 2010), que establece las prioridades de la UE para el desarrollo de un espacio de libertad, seguridad y justicia (2010-2014), e indica que los Estados miembros de la UE deben, lo antes posible, "ratificar el Convenio sobre la Ciberdelincuencia del Consejo de Europa de 2001" considerándolo como "el marco jurídico central de referencia para la lucha contra la ciberdelincuencia a nivel mundial" (p. 22).

Las políticas de ciberseguridad de España han estado marcadas por la UE, como se puede observar en la Figura 1 donde se observa que algunas de las decisiones tomadas por España son precedidas por instrumentos y normativas europeos. En concreto, la aprobación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS, que incentivó a los Estados miembro a adoptar medidas para reforzar la seguridad de las redes y sistemas de información. Entre otras medidas, la Directiva NIS introdujo la obligatoriedad en los Estados miembro de contar con una autoridad nacional, designar centros de respuesta a emergencias informáticas (en adelante, CERT)[57], aprobar una estrategia nacional de ciberseguridad, establecer mecanismos de cooperación entre Estados, y mejorar el compromiso y la preparación del sector privado obligándoles a informar de los principales incidentes en redes y sistemas de información a las autoridades

[57] En este sentido, es necesario aclarar la confusión que existe en torno a las diferencias entre los CERT y los CSIRT. La confusión deriva de que el concepto CERT es en realidad la marca registrada de este nuevo tipo organización: los CSIRT, por lo que a menudo se utilizan como términos intercambiables. Sin embargo, con el tiempo y el uso de ambos conceptos, los CERT han terminado identificándose más con la producción de inteligencia y la respuesta a incidentes a escala nacional, mientras que los CSIRT se asociarían con equipos de respuesta dentro de las empresas. Para más información, ver: WEST-BROWN, M. J.; STIKVOORT, D.; KOSSAKOWSKI, K.-P.; KILCRECE, G.; RUEFLE, R.; ZAJICEK, M, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University, Pittsburgh, 2003.

nacionales competentes. No obstante, la presente directiva está siendo actualizada por la NIS2[58].

Además, la UE cuenta con agencias con misiones expresas asignadas para la ciberseguridad, la ciberdefensa y la lucha contra el cibercrimen. Particularmente, la Agencia de la Unión Europea para la Ciberseguridad (en adelante, ENISA), que promueve el establecimiento de un ecosistema de ciberseguridad europeo a través de actuaciones de *soft law*[59] que buscan la armonización de las políticas de ciberseguridad entre los Estados; la Agencia Europea de Defensa (en adelante, EDA), que trabaja para desarrollar la política de ciberdefensa europea; y Europol, específicamente el Centro Europeo de Cibercrimen (EC3), que actúa como unidad de apoyo técnico a operaciones de lucha contra el cibercrimen en Europa. Recientemente, se fundó el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad[60], cuyo objetivo es contribuir a aumentar las capacidades y la competitividad de Europa en investigación, tecnología y desarrollo industrial de la ciberseguridad. En el ámbito de la respuesta a incidentes de ciberseguridad, la UE cuenta con el CERT-UE, encargado de responder a los ciberincidentes que afecten a las instituciones, cuerpos y agencias de la UE.

[58] La propuesta se puede consultar en: https://www.nis-2-directive.com/NIS_2_Directive_Articles_(Proposal _16.12.2020).html

[59] El término "*soft law*" hace referencia a todos los instrumentos normativos (recomendaciones, comunicaciones, noticias, guías, códigos de conducta, declaraciones, etc.) que no tienen fuerza vinculante o cuya fuerza vinculante es más débil que la del Derecho tradicional, pero que albergan efectos legales indirectos cuyo objetivo es producir efectos prácticos.

[60] Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

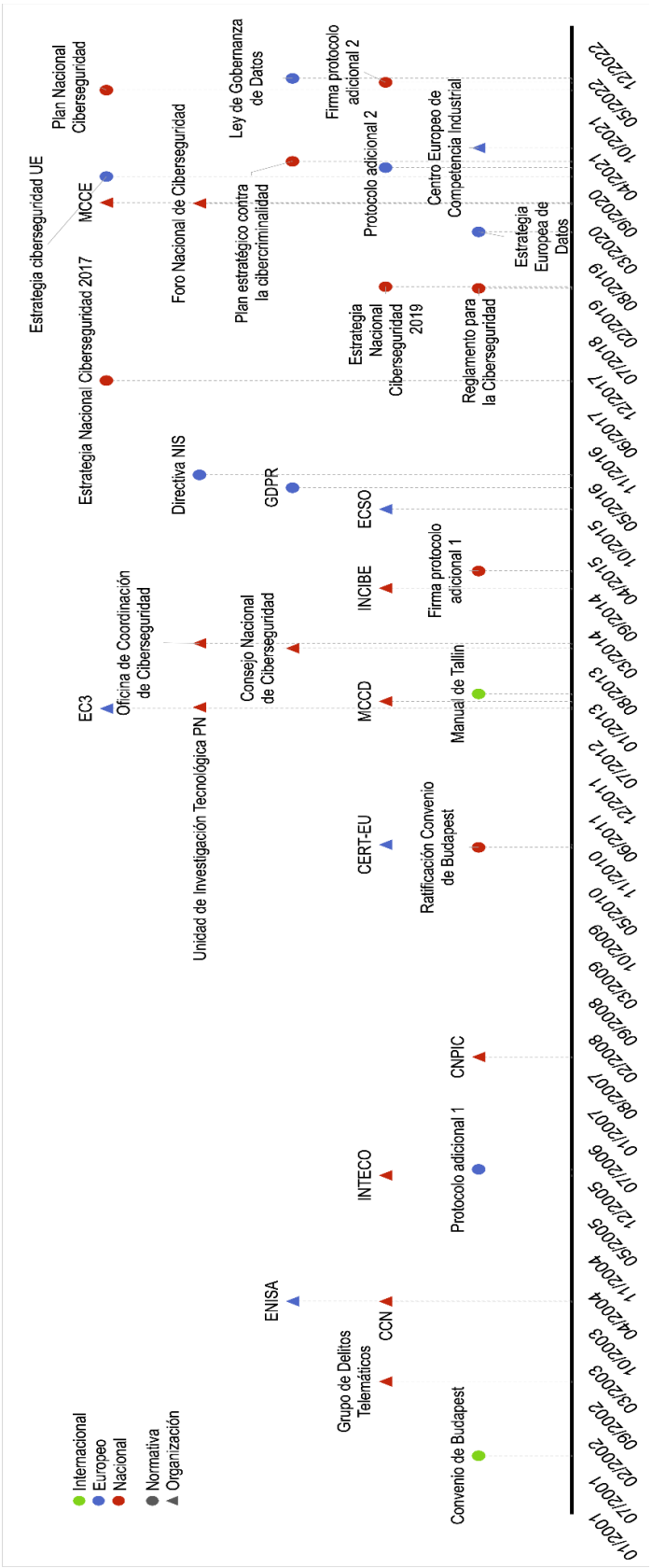

***Figura 1**. Evolución de políticas y organizaciones de ciberseguridad a nivel internacional, europeo y estatal.*

[61] Las abreviaturas se refieren a lo siguiente (de izquierda a derecha): Centro Criptológico Nacional (CCN), *European Union Agency for Cybersecurity* (ENISA), Instituto Nacional de Tecnologías de la Comunicación (INTECO), Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), *Computer Emergency Response Team for the EU institutions, bodies and agencies* (CERT-EU), *European Cybercrime Centre* (EC3), Mando Conjunto de Ciberdefensa (MCCD), Instituto Nacional de

5. ESTRUCTURA DE LA GOBERNANZA DE LA CIBERSEGURIDAD EN ESPAÑA

En el sistema nacional de ciberseguridad español se diferencian a los actores según estos sean órganos políticos, técnicos u operativos. Para asignar a cada actor una u otra categoría se ha utilizado la definición incluida en las normas de creación de cada uno de los órganos. Los órganos políticos son aquellos que están compuestos por cargos electos y cuya función principal es la elaboración de políticas, planes y estrategias. Los órganos técnicos serían aquellos compuestos por personal especialista en alguna materia y cuyo objetivo principal sería asesorar a los órganos políticos. Los órganos operativos serían aquellos que ejecutan de manera instrumental los planes, programas y políticas, y prestan los servicios conforme a las políticas diseñadas desde arriba. En el esquema de la Figura 2 también podemos identificar órganos de coordinación política, cuyo objetivo es coordinar la elaboración de políticas y estrategias, y órganos de coordinación operativa, que tienen como objetivo coordinar las actuaciones de los diferentes órganos operativos.

Ciberseguridad (INCIBE), *European Cyber Security Organisation* (ECSO), *General Data Protection Regulation* (GDPR), y Mando Conjunto del Ciberespacio (MCCE).

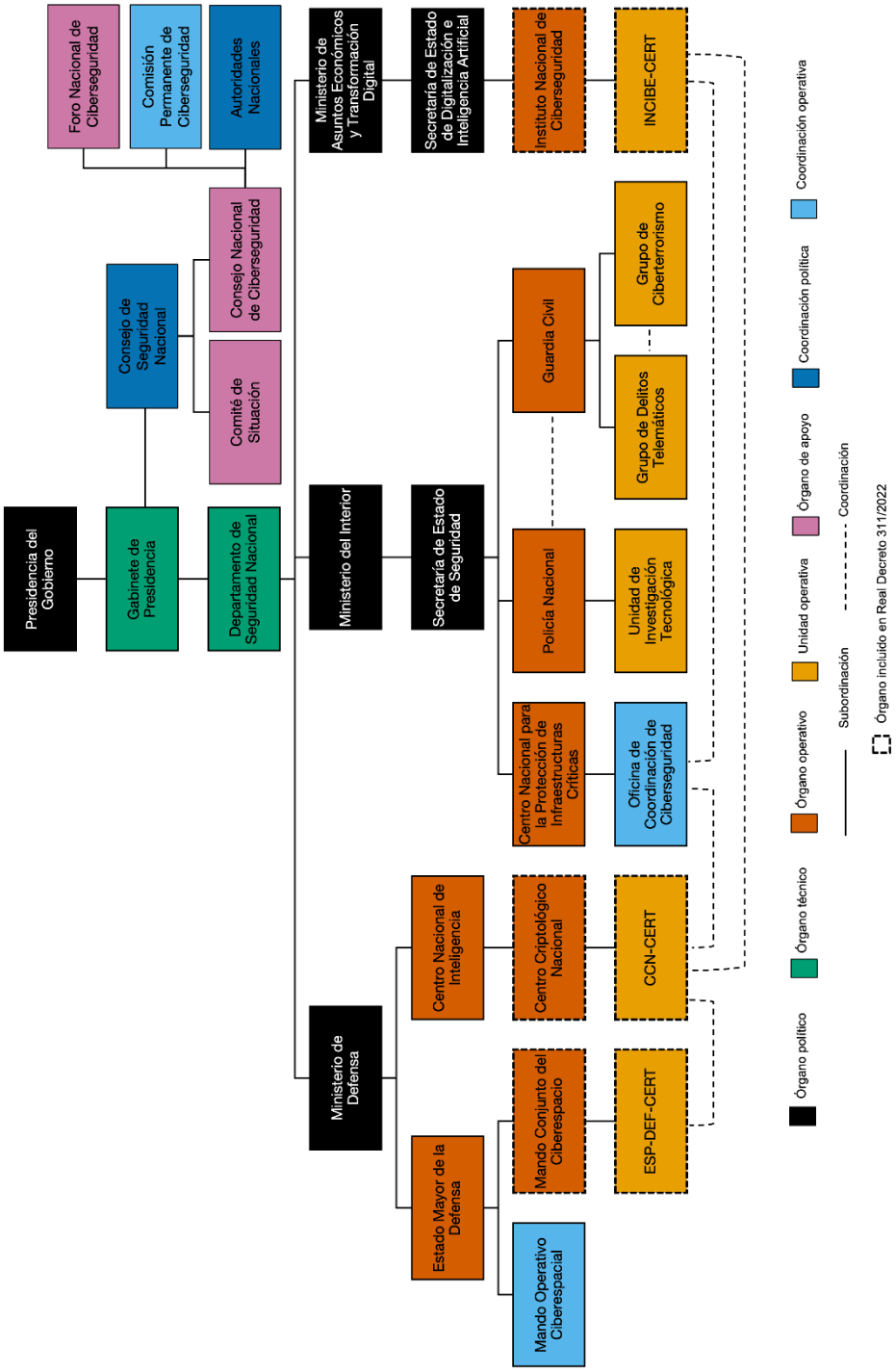

Figura 2. Esquema simplificado de las organizaciones involucradas en la provisión de ciberseguridad en España (2022). Elaboración propia.

[1] Los colores de la figura 2 no siguen ningún criterio ideológico. Se han escogido de una paleta de colores apta para personas con daltonismo.

En las páginas siguientes se definirán las principales funciones y roles asignados a estos organismos según la normativa española en vigor. Se han incluido todos aquellos órganos que tienen atribuidas funciones de carácter directo sobre la ciberseguridad en España, si bien el análisis normativo muestra cómo prácticamente todos los órganos de la administración central ejercen alguna función relacionada con la protección del ciberespacio. La exposición de los diferentes organismos seguirá, siguiendo un orden jerárquico, la clasificación de la Figura 2; esto es, empezando por los órganos adjuntos a la Presidencia del Gobierno y finalizando con las unidades operativas.

Como cualquier otra estructura de la administración pública –y conforme al artículo 97 de la Constitución Española– el nodo de inicio del que emanan todos los demás órganos es la Presidencia del Gobierno. De esta depende el Gabinete de Presidencia, un órgano técnico cuya principal función es asesorar al Presidente del Gobierno en diferentes asuntos de interés y, específicamente, según recoge el artículo 2.1 e) del Real Decreto 136/2020, de 27 de enero, por el que se reestructura la Presidencia del Gobierno, "en materia de Seguridad Nacional". Del Gabinete de Presidencia depende el Departamento de Seguridad Nacional (en adelante, DSN), creado por el Real Decreto 1119/2012 de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, y actualmente regulado por el Real Decreto 136/2020, de 27 de enero. Este es el órgano técnico que tiene como función asesorar a la Presidencia del Gobierno de España en materia de seguridad nacional.

El DSN se estructura en siete unidades, entre las cuales se encuentra la Unidad de Ciberseguridad y Desinformación[62]. Esta Unidad se encarga de coordinar las actuaciones de los diferentes Ministerios y otros organismos de ciberseguridad dado que, como podemos observar en la Figura 2, en el sistema nacional de ciberseguridad de España existen múltiples organismos con competencias en ciberseguridad, lo que hace necesaria esta coordinación. La preponderancia de este departamento se refleja en el hecho de que el DSN ocupa tanto la vicepresidencia como la secretaría del Consejo Nacional de Ciberseguridad (en adelante, CNC).

El principal organismo de coordinación política en materia de ciberseguridad es el CNC, creado por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013 y constituido formalmente el 24 de febrero de 2014. El CNC es un órgano colegiado de apoyo al Consejo de Seguridad Nacional cuya misión es, según el artículo 21 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, la de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad. Desde su creación, el Consejo ha tenido como labor la formulación de las estrategias nacionales de ciberseguridad, que tuvieron lugar en los años 2013 y 2019. El CNC es la agencia competente en España en materia

[62] El resto de unidades pueden ser consultadas en la página oficial del Departamento de Seguridad Nacional, y son: (i) unidad de seguimiento y alerta, (ii) unidad de planteamiento político-estratégico, (iii) unidad de sistemas e infraestructura, (iv) unidad de gestión de crisis y ejercicios, (v) unidad de análisis de seguridad nacional, y (vi) unidad de apoyo.

de ciberseguridad y tiene la estructura y composición que se puede consultar en la Figura 3.

Ministerio de Agricultura, Pesca y Alimentación	Secretario de Estado - Directora del Centro Nacional de Inteligencia (Presidenta)	Presidencia del Gob. Director del Departamento de Seguridad Nacional (Vicepresidente)	Presidencia del Gob. Departamento de Seguridad Nacional (Secretario)	Ministerio de Asuntos Exteriores, Unión Europea y Cooperación
Ministerio de Ciencia e Innovación	Ministerio de Cultura y Deporte	Ministerio de Defensa	Ministerio de Asuntos Económicos y Transformación	Ministerio de Educación y Formación Profesional
Ministerio de Transportes, Movilidad y Agenda Urbana	Ministerio de Hacienda	Ministerio de Industria, Comercio y Turismo	Ministerio de Interior	Ministerio de Justicia
Ministerio de Política Territorial y Función Pública	Ministerio de Presidencia, Relaciones con las Cortes y Memoria Democrática	Ministerio de Sanidad	Ministerio de Trabajo y Economía Social	Ministerio de Transición Ecológica y Reto Demográfico
Ministerio ded Derechos Sociales y Agenda 2030	Ministerio de Inclusión, Seguridad Social y Migraciones	Ministerio de Igualdad	Ministerio de Consumo	Ministerio de Universidades

Figura 2. *Composición del Consejo Nacional de Ciberseguridad español según la Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional. Elaboración propia.*

Dependientes de la Presidencia del Gobierno y coordinados por el DSN y el CNC, se encuentran tres Ministerios de los cuales dependen los principales órganos operativos de ciberseguridad en España: (i) el Ministerio de Defensa, (ii) el Ministerio del Interior, y (iii) el Ministerio de Asuntos Económicos y Transformación Digital[63]. Estos tres Ministerios engloban los órganos encargados de las cuatro prácticas de ciberseguridad que describiremos en este estudio: (i) cultura de ciberseguridad; (ii), respuesta a ciber-incidentes; (iii) protección de infrastructuras críticas; y (iv) investigación criminal.

6. PRÁCTICAS DE CIBERSEGURIDAD

6.1. Promoción de la sociedad digital y cultura de ciberseguridad

La expansión de las tecnologías de la información y la comunicación y la aparición del ciberespacio supusieron, a comienzos del siglo XXI, un reto para los Estados. Por primera vez, debían desarrollar instrumentos para regular el comportamiento de sus ciudadanos en un ámbito que no seguía las reglas precedentes establecidas por límites territoriales. El Estado se enfrentaba a un doble reto: por un lado, asegurar que sus ciudadanos no se quedaban atrás en la adopción de las nuevas tecnologías; por otro, que dicha adopción se realizara de forma responsable y sin exponer en exceso a la población y a las instituciones estatales a las nuevas amenazas que se extendían en el ciberespacio. Para afrontar este reto, España fundó en 2006 el Instituto Nacional de Tecnologías de la Comunicación

[63] A fecha 22 de marzo de 2022.

(INTECO) como un instrumento de la Secretaría de Estado de Comunicación y Sociedad de la Información, dependiente entonces del Ministerio de Industria, como parte del *Plan Avanza.* El objetivo de este plan fue el de impulsar el uso de las TIC en la ciudadanía y las empresas. Un año antes de su creación, únicamente el 28,5% de los hogares españoles tenía acceso a Internet. Hoy esa cifra asciende al 87,3%[64], por lo que existen evidencias de que los objetivos del plan se cumplieron.

En aquel entonces se decidió crear INTECO en formato de Instituto con el objetivo de contar con un organismo con capacidad de implementar los programas del *Plan Avanza*; es decir, no se pretendía poner el foco en la creación de políticas sino en asegurar que dichas políticas –y sus correspondientes programas– terminaran llegando a la ciudadanía y a las empresas. INTECO se creó con tres ejes principales de trabajo: (i) la seguridad de la información desde un punto de vista de la concienciación de utilizar las redes de forma segura, impulsando un comportamiento seguro sin llegar a disuadir a los ciudadanos y empresas de su uso mediante mensajes sobre los riesgos y problemas que conllevaba el uso de Internet; (ii) calidad del software, para lo cual se encargaba de ayudar a las empresas a crear programas con calidad y de diseño seguro[65]. Por último, (iii) la accesibilidad web, cuyo objetivo era que las webs que se creaban fueran accesibles, de forma que sus contenidos pudieran llegar a toda la ciudadanía con independencia de minusvalías o discapacidades, temporales o permanentes.

En el año 2013 el INTECO se desprende de los dos últimos ejes de trabajo para centrarse en la ciberseguridad. Fruto de la priorización de este eje –con un mayor potencial de desarrollo y el que más necesidades presentaba– este Instituto se renombra como Instituto Nacional de Ciberseguridad (INCIBE), actualmente dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Este Instituto es el principal organismo dentro de España encargado de la concienciación en ciberseguridad a empresas y ciudadanos.

Actualmente, INCIBE es una sociedad mercantil estatal –*i.e*., una empresa pública– cuya principal función es la de proveer servicios públicos a la ciudadanía, empresas y operadores de servicios esenciales privados. En la actualidad, INCIBE continúa representando la misma visión de la ciberseguridad con la que nació INTECO. Sus líneas de trabajo aúnan concienciación y reconocimiento de los problemas de ciberseguridad y de la necesidad de abordarlos al tiempo que promueve la digitalización. Sin embargo, en los últimos años este enfoque inicial ha virado, como consecuencia de la alta penetración de Internet en la sociedad y el aumento de las ciberamenazas, hacia la *cultura de ciberseguridad*. La cultura de ciberseguridad es definida como "el conocimiento y la sensibilidad de la sociedad en general y de cada persona en particular, de los riesgos y amenazas susceptibles a comprmeterla, del esfuerzo de los actores y organismos implicados en su salvaguarda y la corresponsabilidad de todos en las medidas de

[64] FERNÁNDEZ, R., *Porcentaje de hogares con acceso a Internet España 2005-2021*, Statista, 2022, fecha de consulta 11 noviembre 2022.

[65] Esta línea de trabajo del INTECO, sin embargo, pronto se agotó tras la producción de numerosas normas, consejos y procedimientos.

anticipación, prevención, deteccnión, protección, resistencia, colaboración y recuperación respecto a dichos riesgos y amenazas"[66]. La necesidad de desarrollar una cultura de ciberseguridad es una de las misiones del Gobierno contempladas en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y ha sido incluida en las dos Estrategias de Ciberseguridad Nacional (2017 and 2019) y en la Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021, por el que se aprueba el Plan Integral de Cultura de Seguridad Nacional.

En este sentido, INCIBE se ha convertido en uno de los principales instrumentos del Estado para promover la cultura de ciberseguridad. Entre ellos, podemos encontrar en INCIBE iniciativas como la *Academia Hacker*, que busca mejorar, de manera gratuita, las competencias de la ciudadanía en ciberseguridad, o la iniciativa "*protege tu empresa*", que incluye políticas de seguridad para la pyme, el kit de concienciación en ciberseguridad para PYMES, que ofrece recursos para que estas puedan entrenar a sus empleados en conocimientos de ciberseguridad, y formación sectorial[67]. También tiene una línea de concienciación a las familias y menores a través de *Internet Segura for Kids* (IS4K) y el programa de *cibercooperantes*, un voluntariado en el que expertos en ciberseguridad realizar sesiones formativas en centros educativos.

Recientemente, INCIBE, en colaboración con el Observatorio Nacional de Tecnología y Sociedad (ONTSI[68]) adscrito a Red.es[69], creó el *ObservaCIBER*, un observatorio público cuyo objetivo, según su web, es "aumentar la cultura de la ciberseguridad facilitando el acceso a la información y fomentando su calidad"[70]. Hasta la fecha, tiene dos líneas principales de informes publicados. Por un lado, informes semestrales (dos hasta la fecha[71]) sobre hábitos, incidencias y percepción en materia de ciberseguridad de los usuarios de tecnologías e Internet en España. Por otro, un informe sobre el talento en ciberseguridad en España.

A la cultura de la ciberseguridad también contribuye activamente el Centro Criptológico Nacional (en adelante, CCN), un organismo adscrito al Centro Nacional de Inteligencia

[66] FORO NACIONAL DE CIBERSEGURIDAD, *Informe sobre la cultura de ciberseguridad en España*, Foro Nacional de Ciberseguridad, 2021, p. 14, fecha de consulta 11 noviembre 2022.

[67] Todos ellos se pueden consultar en su web: https://www.incibe.es/

[68] ONTSI es un observatorio adscrito a la Secretaría de Estado de Digitalización e Inteligencia Artificial (Ministerio de Asuntos Económicos y Transformación Digital) encargado de generar conocimiento para las políticas públicas en torno al desarrollo tecnológico y su impacto en la economía, el empleo, los servicios públicos, los derechos, la seguridad, la calidad de vida y la igualdad entre las personas, información disponible en: https://www.ontsi.es/index.php/es/Que-hacemos, fecha de consulta 11 noviembre 2022.

[69] Red.es es una entidad española encargada de impulsar la Agenda Digital. Creada en 2002, Red.es "desarrolla iniciativas y proyectos de digitalización y desarrollo tecnológico en el ámbito de la economía, los servicios públicos, la ciudadanía, las infraestructuras y la internacionalización de empresas", información disponible en: https://red.es/es/sobre-nosotros/que-hacemos, fecha de consulta 11 noviembre 2022.

[70] Información disponible en https://www.observaciber.es/, fecha de consulta 11 noviembre 2022.

[71] Noviembre de 2022.

(CNI) que a su vez depende orgánicamente del Ministerio de Defensa[72]. Sus funciones y estructura se encuentran reguladas en el Real Decreto 421/2004, de 12 de marzo, en base a la Ley 11/2002, de 6 de mayo. El Real Decreto encomienda al CNI el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información (artículo 4.e), y de protección de la información clasificada (artículo 4.f). Desde entonces, el CCN ha tenido un papel muy relevante en el desarrollo de la ciberseguridad en España[73]. Entre las funciones asignadas al CCN, se encontraba la de "constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, de aplicación a productos y sistemas en su ámbito"[74]. Esta función se materializó por Orden PRE/2740/2007, de 19 de septiembre en su Organismo de Certificación.

El CCN contribuye a la cultura de la ciberseguridad en España a través de numerosas iniciativas. Entre ellas, destacan la labor de generación de conocimiento, formación, y difusión de la cultura de ciberseguridad. Como generación de conocimiento, el CCN publica periódicamente guías CCN-STIC[75], que son normas, instrucciones, guías y recomendaciones orientadas a mejorar el grado de ciberseguridad en organizaciones[76], divididas en diez series[77]. En el apartado de formación, el CCN desarrolló Ángeles, un programa sobre formación, capacitación y talento en ciberseguridad que incluye cursos formativos presenciales y online, pruebas de destrezas y capacidades a través de la plataforma Atenea, y ciberconsejos[78]. También cuenta con ELENA, un simulador de técnicas de civervigilancia que permite a los usuarios adquirir el rol de analista de ciberamenazas en un entorno simulado. Finalmente, en el apartado de difusión de cultura de ciberseguridad, el CCN organiza cuatro grandes eventos anuales: las Jornadas de Seguridad TIC, las Jornadas del SAT[79], el Encuentro del Esquema Nacional de Seguridad

[72] Si bien funcionalmente de la Presidencia del Gobierno, lo que hace en ocasiones discutido su engarce administrativo.

[73] Entre otros hitos, se pueden señalar la integración de las capacidades de inteligencia, defensa de las redes y SIGINT (inteligencia de señales), el desarrollo de diferentes herramientas como SARA (Sistema de Aplicaciones y Redes para las Administraciones), INES (Informe Nacional de Estado de Seguridad), LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas), CARMEN (Centro de Análisis de Registros y Minería de Eventos), entre otras; o la publicación de normas, procedimientos, instrucciones técnicas y guías en abierto en su página web: https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es [Accedido el 22/03/2022].

[74] Real Decreto 421/2004.

[75] STIC es el acrónimo de "Seguridad de ñas Tecnologías de la Información y la Comunicación"

[76] Aunque las guías están dirigidas principalmente al personal de Administraciones Públicas, el CCN las comparte también entre empresas y organizaciones de interés estratégico.

[77] Estas series incluyen: políticas (000), procedimientos (100), normas (200), instrucciones técnicas (300), guías generales (400), entornos Windows (500), otros entornos (600), Esquema Nacional de Seguridad (700), informes técnicos (900), procedimientos de empleo seguro (1000), y organismos de certificación (2000).

[78] Se puede consultar todos sus servicios en https://angeles.ccn-cert.cni.es/index.php/es/, fecha de consulta 11 noviembre 2022.

[79] SAT es el acrónimo de "Sistema de Alerta Temprana".

(ENS), y las Jornadas STIC-Capítulo Colombia, además de estar constantemente presente en redes sociales[80] y otros eventos de ciberseguridad.

Existen otras iniciativas por parte de otros actores, como el proyecto C1b3rWall de la Escuela Nacional de Policía (Policía Nacional) –que incluye el Congreso C1b3rwall de Seguridad Digital y Ciberinteligencia, C1b3rwall Academy, orientada a la formación gratuita en ciberseguridad, y el C1b3rwall Challenge, una plataforma de retos de ciberseguridad[81]– o la Liga de Retos en el Ciberespacio –también conocida como "National CyberLeague GC"– de la Guardia Civil, una competición para jóvenes universitarios y de formación profesional[82].

Recientemente, España ha creado un instrumento dentro de la estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional específicamente dirigido a fomentar la cultura de ciberseguridad, el Foro Nacional de Ciberseguridad (en adelante, FNC). El FNC fue contemplado como medida número 9 en la Estrategia Nacional de Ciberseguridad 2019, Acción 4 –"Impulsar la ciberseguridad de ciudadanos y empresas". El Foro se constituyó en julio de 2020, y se estructura en una Presidencia (DSN), una Vicepresidencia Primera (INCIBE), una Vicepresidencia Segunda (CCN), una Secretaría (DSN), vocalías permanentes (representantes de cada uno de los miembros de la Comisión Permanente de Ciberseguridad) y vocalías de diferentes organizaciones. Entre los cinco grupos de trabajo que lo componen, uno de ellos es la de "cultura de ciberseguridad"[83] con el objetivo de "evolucionar de la concienciación al compromiso", y liderado por el DSN, ISMS Forum[84] y la Fundación Borredá[85]. Entre sus primeros entregables se encuentra el "Informe sobre la cultura de ciberseguridad en España", publicado en 2021, donde el FNC realiza un análisis de las actuaciones encaminadas a mejorar la cultura de ciberseguridad y propone ocho acciones futuras.

[80] Por ejemplo, a fecha 11 noviembre de 2022 su CERT –que se explica abajo– cuenta con 28,9 mil seguidores en Twitter,

[81] Los detalles de los tres servicios se pueden consultar en https://c1b3rwall.policia.es/.

[82] Información sobre la iniciativa disponible en https://www.nationalcyberleague.es/#.

[83] Los otros cuatro grupos incluyen: (i) *impulso a la industria y a la I+D+i* (liderado por INCIBE y Cámara de España), (ii) *formación, capacitación y talento* (liderado por CCN, CRUE-Universidades y operadores de servicios esenciales y críticos), (iii) *análisis e impulso a la industria de ciberdefensa* (liderado por el Mando Conjunto del Ciberespacio y la Asociación Española de Empresas Tecnolóigicas de Defensa, Seguridad, Aeronáutica y Espacio-TEDAE, con el apoyo de la Confederación Española de Organizaciones Empresariales-CEOE y la Dirección General e Armamento y Material-DGAM del Miinisterio de Defensa), y (iv) *regulación* (liderado por Real Instituto Elcano y la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior). Más información en la página web del Foro Nacional de Ciberseguridad: https://foronacionalciberseguridad.es/, fecha de consulta 12 de noviembre 2022.

[84] ISMS Forum (2007) es una organización sin ánimo de lucro encargada de promover el desarrollo, conocimiento y cultura de la seguridad de la información en España. Más información en https://www.ismsforum.es/quien/index.php. Fecha de consulta 12 noviembre 2022.

[85] La Fundación Borredá es una organización de naturaleza fundacional privada, sin ánimo de lucro, dedicada a la difusión, promoción, defensa, estudio y fomento de la seguridad en todos sus ámbitos. Más información sobre sus fines en https://www.fundacionborreda.org/qui%C3%A9nes-somos/fines/. Fecha de consulta 12 noviembre 2022.

6.2. Respuesta a incidentes de ciberseguridad y gestión de ciber crisis

Mientras que las actuaciones arribas descritas se encuadran en estrategias de prevención de ciberincidentes, no todos los ciberincidentes pueden prevenirse. Un área en la que España ha prestado especial atención es en la respuesta a incidentes de ciberseguridad y la gestión de ciber crisis. Un ciber incidente se diferencia de una ciber crisis en que esta última en que su gestión sobrepasa los mecanismos habituales de gestión de ciber incidentes. Así, las ciber crisis se han definido como:

> Una ciber crisis es una situación durante la cual el daño o la explotación de un "ciber activo vital" puede causar un daño grave o una interrupción de las funciones críticas de la sociedad, afectando a la infraestructura crítica, las operaciones rutinarias, la reputación y la economía, y amenazar los valores fundamentales de la sociedad o, en casos extremos, poner en peligro vidas humanas. Una ciber crisis es demasiado extensa para que los mecanismos ordinarios de gestión de incidentes puedan manejarla o, en ocasiones, para que un solo Estado pueda hacerlo. Al iniciarse a partir de una vulnerabilidad en el ciberespacio, pasa desapercibida, trasciende las fronteras territoriales, sectoriales o temporales, activa simultáneamente crisis en otros ámbitos y estalla inesperadamente en la agenda política, lo que a su vez provoca una crisis de confianza hacia las instituciones públicas. Por lo tanto, requiere una oportuna adaptación y coordinación institucional[86].

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad contempla en su Artículo 33 sobre capacidad de respuesta a incidentes de seguridad tres CERT con competencias sobre operadores de servicios que afecten al sector público. En primer lugar, el CCN-CERT –el Centro de Respuesta a incidentes de Seguridad de la Información del CCN– fue creado en 2006 como CERT gubernamental. Sus funciones están recogidas en el artículo 37 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, que fue modificado por el Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Estas funciones son:

(i) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad

[86] PREVEZIANOU, M. F., "Beyond Ones and Zeros: Conceptualizing Cyber Crises", *Risk, Hazards & Crisis in Public Policy*, vol. 12, 1, 2021, p. 65 Traducción propia del original en inglés: *A cyber crisis is a situation during which damage to or exploitation of a "vital cyber asset" can cause serious damage or disruption to critical societal functions, such as critical infrastructure, routine operations, reputational damage and economic damage, threaten fundamental societal values, or, in extreme cases, endanger human lives. A cyber crisis is too extensive for ordinary incident management mechanisms to handle or even for one nation to manage. Initiating from a vulnerability in cyberspace, it goes unnoticed, transcends across territorial, sectoral or temporal boundaries, simultaneously activates crises in other domains, and unexpectedly explodes on the political agenda, which in turn leads to a crisis of trust towards public institutions. It, therefore, requires timely institutional adaptation and coordination.*

jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas, ya sean o no operadores de servicios esenciales.

(ii) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas.

(iii) Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

(iv) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

Dentro del CCN-CERT destacan los Sistemas de Alerta Temprana (SAT), desarrollados por el CCN en 2008 para detectar incidentes que afecten a las administraciones públicas. Estos sistemas actúan mediante sondas; unos servidores de alto rendimiento que monitorizan y gestionan el tráfico de Internet. Los SAT están incluidos en los SOC, que son los encargados de vigilar y detectar las amenazas en las operaciones diarias de los sistemas de información y comunicaciones de las administraciones públicas[87]. Aunque en principio nació con la vocación de ser el único CERT nacional, en la actualidad comparte la categoría de CERT nacional con el ESPDEF-CERT y el INCIBE-CERT, que veremos a continuación. El CCN-CERT es, de acuerdo con los artículos 33 y 34 del Real Decreto 311/2022, el CERT responsable de prestar servicios de respuesta a incidentes a las entidades del sector público. Además, el CCN-CERT impulsó en 2022 la Red Nacional de SOC, que integra y coordina a los SOC del sector público[88].

Por su parte, el el ESPDEF-CERT se encuentra en el Mando Conjunto del Ciberespacio (MCCE), dentro de las Fuerzas Armadas (en adelante, FAS), dependientes del Estado Mayor de la Defensa. El MCCE es de reciente creación. En concreto, son fruto del Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. Este Real Decreto reconocía en su Preámbulo la importancia que el ámbito ciberespacial tiene en la defensa nacional y supuso un paso adelante en la consolidación de un ejército del ciberespacio que garantice las actuaciones de las FAS en este ámbito.

Dentro de la estructura del Estado Mayor de la Defensa, el órgano especializado en la defensa del ciberespacio es el MCCE, que se define, según el artículo 13.1 de este Real Decreto 521/2020, como "el órgano responsable de la dirección, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial", así como el encargado, también, de responder a las ciberamenazas a la seguridad nacional provenientes del exterior. Este organismo viene a

[87] Dentro del CCN-CERT encontramos tres tipos. SAT-INET se refiere a la intranet de la administración. SAT-ICT, para los sistemas de control industriales, y SAT SARA, para los sistemas de aplicaciones y redes para las administraciones.

[88] Más información disponible en: https://rns.ccn-cert.cni.es/es/, fecha de consulta 15 noviembre 2022.

sustituir al anterior Mando Conjunto de Ciberdefensa, creado en 2013 y a la Jefatura de Sistemas de Información y Telecomunicaciones. El ESPDEF-CERT es el Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa. Según el Artículo 33.4 del Real Decreto 311/2022, el ESPDEF-CERT deberá ser informado "*Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas*".

El INCIBE-CERT es, junto con el CCN-CERT y el ESPDEF-CERT, uno de los tres CERT nacionales y el más grande con el que cuenta España. Es un servicio que opera 24/7 y en el cual se reciben las notificaciones de incidentes de ciudadanos, empresas y operadores críticos. Según el Artículo 33.7 del Real Decreto 311/2022, el INCIBE-CERT deberá ser informado cuando el incidente afecte a las "*organizaciones del sector privado que presten servicios a las entidades públicas*". Su objetivo es analizar estos incidentes, mitigarlos y aportar soluciones para que las víctimas puedan recuperarse. El INCIBE ha creado una línea telefónica de marcación rápida y unificada, el 017, cuyo objetivo es canalizar todas las consultas y notificaciones por parte de los usuarios. En caso de cibercrisis, estos organismos deberán coordinarse con el Comité de Situación del DSN.

El "Plan de Choque de Ciberseguridad", aprobado el 25 de mayo de 2021, incrementa aún más las competencias de gestión de ciber incidentes del CCN. Este Plan nace con el objetivo de reforzar las capacidades de ciberseguridad en España, en parte como reacción al incremento del cibercrimen sufrido durante la pandemia de Covid-19 y los dos ciberataques que afectaron al Ministerio de Trabajo y al Servicio Estatal de Empleo en marzo y junio de 2021[89]. Dentro del Plan de Choque se incluye la creación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (en adelante COCS). El COCS "reforzará las capacidades de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad, asesoramiento y apoyo a la gestión de la ciberseguridad de un modo centralizado". El COCS, cuya fundación se prevé que se produzca en el plazo de dos años, estará operado por el CCN y dirigido por la Secretaría de Administración Digital de la Secretaría de Estado de Digitalización e Inteligencia Artificial, en un paso más que refuerza la posición del servicio de inteligencia como actor central de la ciberseguridad en España.

6.3. Protección de infrastructuras críticas

Si hay un ámbito que preocupa especialmente a los Estados es el de la protección de sus infraestructuras críticas, aquellas que se definen como las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre los que descansa el

[89] JIMÉNEZ, M., "El Ministerio de Trabajo sufre un ciberataque, tres meses después de ser "hackeado" el SEPE", *El País*, 2021, Cinco Días, Madrid.

funcionamiento de los servicios esenciales[90]. Estas infraestructuras son las que dan soporte a los servicios esenciales de España, entre los que podemos incluir a los servicios de comunicaciones, la gestión de aguas y residuos, o las instalaciones energéticas y nucleares. Se caracterizan porque un incidente en alguna de estas infraestructuras tendría un impacto disruptivo muy elevado, como ya pudo comprobar Estonia fruto de los ciberataques sufridos en el año 2007. Por su necesidad de especial protección, tanto la UE a través de la Directiva 2008/114/CE, como España con la llamada Ley PIC han desarrollado normativas y creado organismos destinados a protegerlas.

El organismo de protección de infraestructuras críticas creado en España es el CNPIC que vio la luz con la Ley 8/2011, de 28 de abril, y por la que se establecen medidas para la protección de las infraestructuras críticas[91]. El CNPIC depende de forma directa del Secretario de Estado de Seguridad, dentro del Ministerio del Interior. Su función consiste en impulsar, supervisar y coordinar todas aquellas políticas y actividades relacionadas con la protección de infraestructuras críticas en España. Para ello, cuenta con la Oficina de Coordinación de Ciberseguridad (OCC) –anteriormente, Oficina de Coordinación Cibernética– que es el órgano que se encarga de coordinar las actuaciones entre el INCIBE-CERT y el CCN-CERT, y que está regulado por el Real Decreto 734/2020, de 4 de agosto.

6.4. Investigación criminal

La última práctica de ciberseguridad corresponde al proceso de atribución, materializado en la investigación judicial de cibercrímenes. Este último proceso no está incluido dentro del Esquema Nacional de Seguridad, pero se ha decido incluirlo en este artículo por su relevancia y porque también aporta importante información acerca del discurso sobre fragmentación institucional y distribución de competencias sobre el cual se ha estructurado la gobernanza de la ciberseguridad en España. Además, estudios recientes discuten que su exclusión del marco de gobernanza español debería ser solucionado[92]. Aunque España se caracteriza por contar con un sistema policial mixto, con policías de ámbito nacional, autonómico y local, en este apartado solo analizaremos aquellas estructuras que forman parte de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), esto es, la Guardia Civil y el Cuerpo Nacional de Policía. Estos dos cuerpos de ámbito estatal son los dos principales organismos policiales con competencia en materia de cibercrimen en España. Junto a estas, y dependiente también del Ministerio del Interior, se encuentra el CNPIC que vimos arriba.

[90] En España estas se agrupan en 12 sectores de más a menos prioritario: energía, tributario y financiero, agua, transporte, TIC, químico, nuclear, espacio, alimentación, administración pública, salud e investigación.

[91] La Ley 8/2011 fue elaborada sobre la base de normativa europea. En concreto, la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

[92] DEL-REAL, C.; y DÍAZ-FERNÁNDEZ, A. M., "Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange", *International Cybersecurity Law Review*, vol. 3, 2, 2022.

La Guardia Civil cuenta con dos grupos dedicados a combatir la ciberdelincuencia. En primer lugar, el Grupo de Delitos Telemáticos (GDT), que depende de la Unidad Central Operativa de la Guardia Civil y fue creado en 1996 con el objetivo de investigar todos aquellos delitos cometidos en (y a través) de Internet. Por su parte, el Grupo de Ciberterrorismo fue creado en 2003 dependiente de su Servicio de Información. Su objetivo es combatir la amenaza terrorista a través del ciberespacio y prestar apoyo en todo lo relativo a las Tecnologías de la Información a los demás grupos que integran el Servicio de Información.

Por su parte, el Cuerpo Nacional de Policía, cuenta con la Unidad de Investigación Tecnológica (UIT) dentro de la estructura de la Comisaría General de Policía Judicial, que es la encargada, según la Orden INT/28/2013, de 18 de enero, de "la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica". La UIT se compone de dos brigadas: la Brigada Central de Investigación Tecnológica (BIT) y la Brigada Central de Seguridad Informática (BSI). La BIT se encarga de investigar "las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones", mientras que la BSI tiene competencias en la "investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes".

7. CONCLUSIONES

Desde el año 2013, con la aprobación de la primera Estrategia Nacional de Ciberseguridad, la ciberseguridad se ha consolidado como un elemento central de las políticas de seguridad nacional en España. Esto ha motivado, además de la aprobación de numerosas leyes de protección del ciberespacio, la creación y consolidación de nuevas agencias encargadas de garantizar la ciberseguridad nacional. Este estudio analiza las intituciones públicas involucradas en la gobernanza de la ciberseguridad en España a través de cuatro prácticas de seguridad: cultura de ciberseguridad, respuesta a ciber incidentes y ciber crisis, protección de infraestructuras críticas, e investigación criminal. El análisis de las instituciones involucradas en estas cuatro prácticas aporta evidencias para concluir que España ha adoptado una narrativa de la ciberseguridad basada en la fragmentación institucional y la distribución de competencias, y donde se identifican tanto prácticas orientadas a riesgos como a amenazas.

La fragmentación institucional, consecuencia parcial del modelo multi-stakeholders adoptado por la UE, se observa en el número de diferentes instituciones involucradas en cada una de las prácticas de ciberseguridad descritas en este artículo. Estudios recientes ya han resaltado que el modelo de gobernanza se ha estructurado en torno a dos actores principales, el CCN y el INCIBE, a los que rodean una enorme variedad de otros actores

públicos y privados[93]. La fragmentación política y narrativa de la gobernanza de la ciberseguridad ha sido descrita por otros estudios[94], consecuencia de complejidad tecnológica, la carencia de modelos de gobernanza del ciberespacio consolidados. A través del estudio normativo y documental de las prácticas de ciberseguridad observamos que, en algunas de estas, cada uno de los actores despliega diferentes iniciativas, a menudo desconectadas unas de otras. Este proceso se observa especialmente en la promoción de la cultura de la ciberseguridad, donde cada uno de los actores ha desarrollado sus propios proyectos y bajo su propia narrativa. Por ejemplo, mientras el INCIBE fomenta una cultura de ciberseguridad basada en la gestión de riesgos y la adopción de buenas prácticas de ciber-higiene, siguiendo una narrativa coincidente con la de la salud pública, el CCN o las FCSE siguen un enfoque basado en las ciber-amenazas, más propio de la narrativa centrada en la defensa de seguridad nacional y el cibercrimen[95].

No obstante, la comparación de estos resultados con estudios previos en otros contextos, arroja que el modelo español de provisión de ciberseguridad es distinto del modelo que siguen los países anglosajones. De esta manera, los resultados de este estudio contrastan con los estudios revisados en la sección 2, que describen cómo la pluralización de la seguridad en los países anglosajones se comprende por la adopción del discurso neoliberal. Recordemos que este discurso defiende la idoneidad de reducir la intervención estatal y estructurar la provisión de seguridad en torno a las leyes del mercado –la competencia, el emprendimiento y la contratación de servicios[96]. Los resultados de este estudio sugieren que España no ha asumido el discurso neoliberal en la misma medida que los países anglosajones, pues ha desarrollado prácticas de ciberseguridad e instituciones públicas con un rol creciente en la provisión de ciberseguridad. Los resultados de este estudio apuntan a que España ha desarrollado más bien un modelo de pluralismo anclado, más parecido a aquellos existentes en países con una fuerte presencia del Estado como Francia[97] y Noruega[98], y distinto del modelo de gobernanza nodal de los países anglosajones.

---

[93] DEL-REAL, C.; y DÍAZ-FERNÁNDEZ, A. M., "Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange", op. cit.

[94] DUNN CAVELTY, M. D.; WENGER, A., *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1, Routledge, London, 2022; DUNN CAVELTY, M.; WENGER, A., "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, vol. 41, 1, 2020.

[95] MULVENON, J. C.; RATTRAY, G. J. (EDS.), *Addressing cyber instability*, Cyber Conflict Studies Association, Vienna, VA, 2012.

[96] LOADER, I., "Consumer Culture and the Commodification of Policing and Security", *Sociology*, vol. 33, 2, 1999; LOADER, I.; WALKER, N., *Civilizing security*, op. cit.; VAN STOKKOM, B.; TERPSTRA, J., "Plural policing, the public good, and the constitutional state: an international comparison of Austria and Canada – Ontario", *Policing and Society*, vol. 28, 4, 2018.

[97] QUÉRO, Y.-C.; DUPONT, B., "Nodal governance: toward a better understanding of node relationships in local security governance", *Policing and Society*, vol. 29, 3, 2019.

[98] NØKLEBERG, M., "Examining the how of Plural Policing: Moving from Normative Debate to Empirical Enquiry", *The British Journal of Criminology*, vol. 60, 3, 2020.

España parece estar siguiendo así la estela europea al producir instituciones y prácticas que le permitan retomar el control sobre la soberanía digital[99]. A este respecto, el indicador más reciente del compromiso de España con la ciberseguridad es que, en febrero de 2022, la Mesa del Congreso de los Diputados seleccionó la ciberseguridad como uno de los primeros cuatro temas sobre los que la recientemente creada Oficina de Ciencia y Tecnología del Congreso de los Diputados debía centrar sus primeros informes, hecho que se produjo en noviembre de 2022[100]. Este informe es el primer paso para producir políticas públicas de ciberseguridad basadas en evidencias científicas. Este estudio contribuye a ellas al identificar dos posibles áreas de mejora.

Por un lado, sería conveniente reducir –o, en su defecto, coordinar– la fragmentación institucional. Esta recomendación será apoyada por normativas europeas. Por ejemplo, ya la propuesta de Directiva NIS2 propone la creación de una "ventanilla única" para canalizar todas las notificaciones de ciberincidentes[101]. La gran variedad de organismos públicos creados puede producir confusión en la ciudadanía. Por ello, sería conveniente crear una *Agencia Nacional de Ciberseguridad* transversal a todos los organismos competentes, encargada de coordinar las actuaciones entre estos, de desarrollar una narrativa nacional coherente sobre la ciberseguridad, y de realizar un uso eficiente de los recursos a través de la canalización de las normativas, certificación y supervisión de la interoperabilidad de los servicios.

En este sentido, la gobernanza de la ciberseguridad en España se beneficiaría de una mayor integración en la difusión de la inteligencia sobre ciberseguridad, en la línea del nuevo SOC de las Administraciones Públicas. En concreto, sería conveniente crear un *Centro de Inteligencia contra el Cibercrimen y las Amenazas a la Ciberseguridad,* quizás integrado en esta nueva Agencia. Al igual que ocurre con otros tipos de delincuencia compleja como el terrorismo y el crimen organizado, la lucha efectiva contra el cibercrimen requiere de una alta inversión en inteligencia. Los cibercriminales utilizan complejas herramientas y procesos para llevar a cabo sus actuaciones. Al mismo tiempo, el ciberespacio se ha convertido en un ámbito más de la defensa de la seguridad nacional, y donde las ciberamenazas tienen el potencial de afectar al adecuado funcionamiento de la democracia y al desarrollo económico y social del país, a un nivel comparable al del terrorismo o el crimen organizado.

Con estos argumentos como justificación, se propone la creación de un Centro de Inteligencia contra el Cibercrimen y las Amenazas a la Ciberseguridad. Siguiendo el ejemplo del actual Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), este nuevo centro coordinaría el intercambio de información entre todos los

[99] FARRAND, B.; CARRAPICO, H., "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity", *European Security*, vol. 31, 3, 2022.

[100] OFICINA DE CIENCIA Y TECNOLOGÍA DEL CONGRESO DE LOS DIPUTADOS (OFICINA C), *Ciberseguridad: España en un ecosistema tecnológico y social en constante evolución*, Oficina C, 2022, fecha de consulta 15 noviembre 2022.

[101] ALONSO LECUIT, J., *Directiva NIS2: valoraciones y posiciones desde el sector privado*, Real Instituto Elcano, 2021, p. 19, fecha de consulta 17 noviembre 2022.

miembros de la comunidad de ciberseguridad, incluyendo la Policía Nacional, la Guardia Civil, el CNI, el CCN, el INCIBE, el CNPIC y las FAS. Un centro de estas características integraría la información de la que disponen todos estos actores para elaborar inteligencia estratégica, consiguiendo a partir de ella y de las relaciones de cooperación que se generarían a nivel internacional una mejora en la actuación y coordinación operativa frente al cibercrimen y las ciberamenazas. En este sentido, podría tomar como ejemplo la plataforma recientemente creada Cyber Intel/Info Cel (CIIC) en Países Bajos para compartir información sobre ciberamenazas y ciberincidentes y en el que participan todos los organismos con competencias en ciberseguridad del país[102].

Finalmente, este estudio tiene limitaciones que deben ser mencionadas. Primero, se basa fundamentalmente en material documental. Por tanto, sus resultados pueden estar sesgados por la principal fuente de información, que a menudo no incluye la práctica real de la gobernanza de la ciberseguridad. Segundo, el análisis de cada una de las prácticas descritas en este artículo daría para un artículo completo. Este estudio supone una primera aproximación que, no obstante, deberá ser complementada por otros estudios. En tercer y último lugar, la ciberseguridad es profundamente amplia y especializada. Este estudio no entra a analizar áreas concretas de la ciberseguridad. Por ejemplo, la cultura de ciberseguridad puede enfocarse desde una perspectiva económica –p.ej., centrada en el ciber-fraude– a una más geopolítica – p.ej., centrada en las ciber-operaciones llevadas a cabo por grupos patrocinados por Estados. Futuros estudios deberán analizar las prácticas aplicadas a ámbitos concretos de la ciberseguridad.

8. REFERENCIAS

ADAMS, S. A.; BROKX, M.; GALIČ, M.; KALA, K.; KOOPS, B.-J.; LEENES, R.; SCHELLEKENS, M.; E SILVA, K.; ŠKORVÁNEK, I., *The governance of cybersecurity. A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK*, Tilburg Institute for Law, Technology, and Society, Tilburg, 2015.

ALONSO LECUIT, J., "Directiva NIS2: valoraciones y posiciones desde el sector privado", *Real Instituto Elcano*, 2021.

APLIN, T. F.; y ARNOLD, R., "UK implementation of the Trade Secrets Directive", *SSRN Electronic Journal*, 2019.

ARCOS, R., "Securing the Kingdom's cyberspace: cybersecurity and cyber intelligence in Spain", en Scott N. Romaniuk, Mary Manjikian (eds.) *Routledge Companion to Global Cyber-Security Strategy*, 2021.

BACKMAN, S., "Risk vs. threat-based cybersecurity: the case of the EU", *European Security*, 2022, pp. 1-19.

[102] Más información sobre la plataforma de intecambio de información en "Convenant tussen AIVD, MIVD, Politie, NCSC, OM en NCTV inzake de samenwerking in de Cyber Intel/Info Cel (Convenant samenwerking CIIC)".

BAYLEY, D. H., *Police for the future*, First, Oxford University Press, New York, 1994.

BAYLEY, D. H.; y SHEARING, C., "The Future of Policing", *Law & Society Review*, vol. 30, n.º 3, 1996.

BENGTSSON, L.; BORG, S.; y RHINARD, M., "European security and early warning systems: from risks to threats in the European Union's health security sector", *European Security*, vol. 27, n.º 1, 2018, pp. 20-40.

BIDGOLI, M., *A mixed methods approach to understanding undergraduate students' victimization, perceptions, and reporting of cybercrimes*, Universidad de California, Irvine, 2015.

BLUMSTEIN, A.; y WALLMAN, J. (eds.), *The Crime Drop in America*, 2, Cambridge University Press, 2005.

BOAS, T. C.; y GANS-MORSE, J., "Neoliberalism: From New Liberal Philosophy to Anti-Liberal Slogan", *Studies in Comparative International Development*, vol. 44, n.º 2, 2009, pp. 137-161.

BRAITHWAITE, J. B., "Neoliberalism or Regulatory Capitalism", *SSRN Electronic Journal*, 2006.

– *Regulatory capitalism: how it works, ideas for making it work better*, Edward Elgar, Cheltenham, UK; Northampton, MA, 2008.

– "The New Regulatory State and the Transformation of Criminology", *British Journal of Criminology*, vol. 40, n.º 2, 2000, pp. 222-238.

BUIL-GIL, D.; LORD, N.; y BARRETT, E., "The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention", *Victims & Offenders*, vol. 16, n.º 2, 2021, pp. 286-315.

BUIL-GIL, D.; MIRÓ-LLINARES, F.; MONEVA, A.; KEMP, S.; y DÍAZ-CASTAÑO, N., "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK", *European Societies*, 2020.

BURNS, R. G.; WHITWORTH, K. H.; y THOMPSON, C. Y., "Assessing law enforcement preparedness to address Internet fraud", *Journal of Criminal Justice*, vol. 32, n.º 5, 2004, pp. 477-493.

BURRIS, S.; DRAHOS, P.; y SHEARING, C., "Nodal governance", *Australian Journal of Legal Philosophy*, n.º 30, 2005.

BUZAN, B.; WÆVER, O.; y DE WILDE, J., *Security: a new framework for analysis*, Lynne Rienner Pub, Boulder, Colo, 1998.

CALCARA, A.; y MARCHETTI, R., "State-industry relations and cybersecurity governance in Europe", *Review of International Political Economy*, 2021, pp. 1-26.

CASTELLS, M., *La sociedad red*, 3. ed, Alianza Ed, Madrid, 2005.

DUNN CAVELTY, M.; y WENGER, A., *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1, Routledge, Londres, 2022.

CHRISTOU, G., *Cybersecurity in the European Union*, Palgrave Macmillan UK, London, 2016, DOI: 10.1057/9781137400529.

COLEMAN, C.; y MOYNIHAN, J., *Understanding crime data: haunted by the dark figure*, Open University Press, Buckingham; Philadelphia, 1996.

CORRY, O., "Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change", *Millennium: Journal of International Studies*, vol. 40, n.º 2, 2012, pp. 235-258.

CRAWFORD, A., "Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security", *Theoretical Criminology*, vol. 10, n.º 4, 2006, pp. 449-479.

DEL-REAL, C.; y DÍAZ-FERNÁNDEZ, A. M., "Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange", *International Cybersecurity Law Review*, vol. 3, n.º 2, 2022, pp. 313-343.

DOMENIE, M. M. L.; LEUKFELDT, R.; VAN WILSEM, J.; JANSEN, J.; y STOL, W., *Victimisation in a digitised society: a survey among members of the public concerning e-fraud, hacking and other high volume crimes*, Eleven International Publishing, The Hague, 2013.

DUNN CAVELTY, M.; y WENGER, A., *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1, Routledge, Londres, 2022.

– "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, vol. 41, n.º 1, 2020, pp. 5-32.

DUPONT, B., "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime", *Crime, Law and Social Change*, vol. 67, n.º 1, 2017, pp. 97-116.

DUPONT, B., "Security in the Age of Networks", *Policing and Society*, vol. 14, n.º 1, 2004, pp. 76-91.

VAN EETEN, M., "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity", *Digital Policy, Regulation and Governance*, vol. 19, n.º 6, 2017, pp. 429-448.

ELDEM, T., "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security", *International Journal of Public Administration*, vol. 43, n.º 5, 2020, pp. 452-465.

FARRAND, B.; y CARRAPICO, H., "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity", *European Security*, vol. 31, n.º 3, 2022, pp. 435-453.

FARRELL, G.; TSELONI, A.; MAILLEY, J.; y TILLEY, N., "The Crime Drop and the Security Hypothesis", *Journal of Research in Crime and Delinquency*, vol. 48, n.º 2, 2011, pp. 147-175.

FERNÁNDEZ, R., *Porcentaje de hogares con acceso a Internet España 2005-2021*, Statista, 2022.

FOJÓN CHAMORRO, E.; y SANZ VILLALBA, Á. F., "Ciberseguridad en España: una propuesta para su gestión", *Análisis del Real Instituto Elcano*, vol. 101, 2010, pp. 1-8.

FORO NACIONAL DE CIBERSEGURIDAD, *Informe sobre la cultura de ciberseguridad en España*, Foro Nacional de Ciberseguridad, 2021, pp. 1-52.

FRIEDMAN, M., *Capitalism and freedom*, 40th anniversary ed., University of Chicago Press, Chicago, 2002.

HAAS, E. B., *Uniting Of Europe: Political, Social, and Economic Forces, 1950-1957*, University of Notre Dame Press, 2004.

HAYEK, F. A. VON, *The road to serfdom*, 50th anniversary ed. / with a new introd. by Milton Friedman, University of Chicago Press, Chicago, 1994.

HINDUJA, S., "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", *Policing: An International Journal of Police Strategies & Management*, vol. 27, n.º 3, 2004, pp. 341-357.

JIMÉNEZ, M., "El Ministerio de Trabajo sufre un ciberataque, tres meses después de ser "hackeado" el SEPE", Cinco Días, Madrid, *El País*, 2021.

JOHNSTON, L.; y SHEARING, C., *Governing security: explorations in policing and justice*, Routledge, London; New York, 2003.

JONES, D. S., *Masters of the universe: Hayek, Friedman, and the birth of neoliberal politics*, Fith printing, and first paperback printing, Princeton University Press, Princeton Oxford, 2014.

KEMP, S., "Fraud reporting in Catalonia in the Internet era: Determinants and motives", *European Journal of Criminology*, 2020, p. 147737082094140.

KEMP, S.; MIRÓ-LLINARES, F.; MONEVA, A., "The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain", *European Journal on Criminal Policy and Research*, 2020, DOI: 10.1007/s10610-020-09439-2.

KEMPA, M.; y SINGH, A.-M., "Private security, political economy and the policing of race: Probing global hypotheses through the case of South Africa", *Theoretical Criminology*, vol. 12, n.º 3, 2008, pp. 333-354.

KUERBIS, B.; BADIEI, F., "Mapping the cybersecurity institutional landscape", *Digital Policy, Regulation and Governance*, vol. 19, n.º 6, 2017, pp. 466-492.

LEUKFELDT, E. R.; y HOLT, T. J. (eds.), *The human factor of cybercrime*, Routledge, Abingdon, Oxon; New York, NY, 2020.

LEVI-FAUR, D., "The Rise of Regulatory Capitalism: The Global Diffusion of a New Order", *The ANNALS of the American Academy of Political and Social Science*, vol. 598, n.º 1, 2005, pp. 200-217.

LEVI-FAUR, D.; y JORDANA, J., "Globalizing Regulatory Capitalism", *The ANNALS of the American Academy of Political and Social Science*, vol. 598, n.º 1, 2005, pp. 6-9.

LOADER, I., "Consumer Culture and the Commodification of Policing and Security", *Sociology*, vol. 33, n.º 2, 1999, pp. 373-392.

– "Plural Policing and Democratic Governance", *Social & Legal Studies*, vol. 9, n.º 3, 2000, pp. 323-345.

LOADER, I.; y WALKER, N., *Civilizing security*, Cambridge University Press, Cambridge; New York, 2007.

– "Necessary Virtues: The Legitimate Place of the State in the Production of Security", en Wood, J., y Dupont, B., (eds.) *Democracy, Society and the Governance of Security*, Cambridge University Press, 2006, pp. 165-195.

– "Policing as a Public Good: Reconstituting the Connections between Policing and the State", *Theoretical Criminology*, vol. 5, n.º 1, 2001, pp. 9-35.

LÓPEZ GUTIÉRREZ, J.; SÁNCHEZ JIMÉNEZ, F.; HERRERA SÁNCHEZ, D.; MARTÍNEZ MORENO, F.; RUBIO GARCÍA, M.; GIL PÉREZ, V.; SANTIAGO OROZCO, A. M.; y GÓMEZ MARTÍN, M. A.; *Informe sobre la Cibercriminalidad en España*, Dirección General de Coordinación y Estudios y Secretaría de Estado de Seguridad. Ministerio del Interior. Gobierno de España, Madrid, España, 2022, pp. 1-65.

MAIMON, D.; y LOUDERBACK, E. R., "Cyber-Dependent Crimes: An Interdisciplinary Review", *Annual Review of Criminology*, vol. 2, n.º 1, 2019, pp. 191-216.

MALINA, L.; SRIVASTAVA, G.; DZURENDA, P.; HAJNY, J.; RICCI, S., "A Privacy-Enhancing Framework for Internet of Things Services", en Joseph K. Liu, Xinyi Huang (eds.) *Network and System Security. 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings*, vol. 11928, Springer Cham, 2019 (Lecture Notes in Computer Science), pp. 77-97.

MARKS, M.; y WOOD, J., "South African policing at a crossroads: The case for a 'minimal' and 'minimalist' public police", *Theoretical Criminology*, vol. 14, n.º 3, 2010, pp. 311-329.

MAVROEIDIS, V.; HOHIMER, R.; CASEY, T.; JESANG, A., "Threat Actor Type Inference and Characterization within Cyber Threat Intelligence", en *2021 13th International Conference on Cyber Conflict (CyCon)*, IEEE, Tallinn, Estonia, 2021, pp. 327-352.

MCGUIRE, M.; y DOWLING, S., *Chapter 2: Cyber-enabled crimes -fraud and theft*, Home Office, 2013.

MIRÓ-LLINARES, F.; y MONEVA, A., "What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?", *Crime Science*, vol. 8, n.º 1, 2019.

MULVENON, J. C.; RATTRAY, G. J. (eds.), *Addressing cyber instability*, Cyber Conflict Studies Association, Vienna, VA, 2012.

NØKLEBERG, M., "Examining the how of Plural Policing: Moving from Normative Debate to Empirical Enquiry", *The British Journal of Criminology*, vol. 60, n.º 3, 2020, pp. 681-702.

OFICINA DE CIENCIA Y TECNOLOGÍA DEL CONGRESO DE LOS DIPUTADOS (OFICINA C), *Ciberseguridad: España en un ecosistema tecnológico y social en constante evolución*, Oficina C, 2022.

OSTROM, E., "Beyond Markets and States: Polycentric Governance of Complex Economic Systems", *American Economic Review*, vol. 100, n.º 3, 2010, pp. 641-672.

PAYNE, B. K., "Defining Cybercrime", en *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer International Publishing, Cham, 2019, pp. 1-24, DOI: 10.1007/978-3-319-90307-1_1-1.

PONTE, S.; GIBBON, P.; y VESTERGAARD, J. (eds.), *Governing through standards: origins, drivers and limitations*, Palgrave Macmillan, Houndmills, Basingstoke, Hampshire; New York, 2011.

PREVEZIANOU, M. F., "Beyond Ones and Zeros: Conceptualizing Cyber Crises", *Risk, Hazards & Crisis in Public Policy*, vol. 12, n.º 1, 2021, pp. 51-72.

QUÉRO, Y.-C.; y DUPONT, B., "Nodal governance: toward a better understanding of node relationships in local security governance", *Policing and Society*, vol. 29, n.º 3, 2019, pp. 283-301.

RHODES, R. A. W., "The New Governance: Governing without Government", *Political Studies*, vol. 44, n.º 4, 1996, pp. 652-667.

ROCHÉ, S., "Vers la démonopolisation des fonctions régaliennes: contractualisation, territorialisation et européanisation de la sécurité intérieure", *Revue française de science politique*, vol. 54, n.º 1, 2004, p. 43.

RONDELEZ, R., "Governing Cyber Security Through Networks: An Analysis Of Cyber Security Coordination In Belgium", 2018.

SAATSCOURANT, "Convenant tussen AIVD, MIVD, Politie, NCSC, OM en NCTV inzake de samenwerking in de Cyber Intel/Info Cel (Convenant samenwerking CIIC)".

SHEARING, C., "Reflections on the Refusal to Acknowledge Private Governments", en Wood, J., y Dupont, B., (eds.) *Democracy, Society and the Governance of Security*, Cambridge University Press, 2006, pp. 11-32.

– "Reinventing Policing: Policing as Governance", en Otwin Marenin (ed.) *Policing Change, Changing Policing*, Routledge, New York, 1996, pp. 285-307.

SHEARING, C.; y WOOD, J., "Nodal Governance, Democracy, and the New "Denizens"", *Journal of Law and Society*, vol. 30, n.º 3, 2003, pp. 400-419.

STERLINI, P.; MASSACCI, F.; KADENKO, N.; FIEBIG, T.; VAN EETEN, M., "Governance Challenges for European Cybersecurity Policies: Stakeholder Views", *IEEE Security & Privacy*, vol. 18, n.º 1, 2020, pp. 46-54.

VAN STOKKOM, B.; y TERPSTRA, J., "Plural policing, the public good, and the constitutional state: an international comparison of Austria and Canada – Ontario", *Policing and Society*, vol. 28, n.º 4, 2018, pp. 415-430.

SUTHERLAND, E., "Governance of Cybersecurity – The Case of South Africa", *The African Journal of Information and Communication*, n.º 20, 2017, pp. 83-112.

US CENSUS BUREAU FOREIGN TRADE DIVISION, "Foreign Trade: Data", 2020.

VAN PUYVELDE, D.; BRANTLY, A. F., *Cybersecurity: politics, governance and conflict in cyberspace*, Polity Press, Cambridge, UK ; Medford, MA, USA, 2019.

VAN DE WEIJER, S. G. A.; LEUKFELDT, R.; y BERNASCO, W., "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking", *European Journal of Criminology*, vol. 16, n.º 4, 2019, pp. 486-508.

WEST-BROWN, M. J.; STIKVOORT, D.; KOSSAKOWSKI, K.-P.; KILCRECE, G.; RUEFLE, R.; ZAJICEK, M., *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University, Pittsburgh, 2003.

WOOD, J.; y SHEARING, C., *Imagining security*, Willan, Cullompton, 2007.

ZAUBERMAN, R., "Les Attitudes des Victimes individuelles", en Robert, P., y Muccheilli, L. (eds.) *Crime et Sécurité. L'État des Savoirs*, La Découverte, Paris, 2002, pp. 309-319.