El espionaje del Siglo XXI: Ciberespionaje

PROYECTO INTELIGENCIA VISUAL ANALÍTICA
GRUPO 4

Máster Interuniversitario en Analista de Inteligencia
XII Edición

Universidad Rey Juan Carlos

uc3m | Universidad Carlos III de Madrid

SISD | CÁTEDRA SERVICIOS DE INTELIGENCIA Y SISTEMAS DEMOCRÁTICOS

1. Introducción

El espionaje entre Estados es un fenómeno que se ha dado históricamente, pero en las últimas décadas el mundo se ha movido a un nuevo ámbito de esta práctica: el ciberespionaje.

En 2013 se publicó el denominado Manual de Tallin, resultado de una conferencia organizada por el Centro de Excelencia de la Ciberdefensa Cooperativa de la OTAN en Tallin, Estonia, que intenta proporcionar definiciones, procedimientos y reglas que rigen las operaciones cibernéticas internacionales. Este manual define el ciberespionaje como «un acto emprendido clandestinamente o bajo falsas pretensiones que utiliza capacidades cibernéticas para recopilar (o intentar recopilar) información con la intención de comunicar a la parte contraria».

Otra definición aceptada es:
- Actividades de espionaje llevadas a cabo en el ciberespacio o utilizando el ciberespacio como medio. El ciberespionaje roba datos clasificados y sensibles o propiedad intelectual para obtener una ventaja sobre una empresa o entidad gubernamental de la competencia.

Esta nueva forma de espionaje está afectando las relaciones económicas y políticas entre Estados y está cambiando la forma de la guerra moderna, siendo uno de los problemas internacionales más importantes en el mundo actual.

La característica definitoria del ciberespionaje es que ocurre en secreto, por lo que hay una gran falta de conocimiento sobre el tema. Algunos factores que influyen en cómo se percibe son, por ejemplo:

- la extensión y la naturaleza del daño causado por el ataque
- la identidad de los atacantes
- cómo se usa la información robada

Los términos ciberespionaje y ciberguerra son similares, pero no son lo mismo. La mayor diferencia es que el objetivo principal de un ataque de ciberguerra es interrumpir las actividades de un Estado-nación, mientras que el objetivo principal de un ataque de ciberespionaje es que el atacante permanezca oculto el mayor tiempo posible para reunir información. Aunque el ciberespionaje y la ciberguerra son dos conceptos distintos, a menudo se utilizan juntos. Por ejemplo, el ciberespionaje puede utilizarse para obtener información que ayude a un Estado a prepararse para declarar una guerra física o cibernética.

2. Marco teórico

2.1. Definiciones

A continuación, se presentan las definiciones de diferentes conceptos que resultan de interés para entender el contexto en el que se dan las actividades de ciberespionaje.

- **AMENAZAS HÍBRIDAS:** Fenómenos que combinan ataques convencionales y no convencionales para desestabilizar un país, en muchas ocasiones combinando ciberataques y ciberespionaje, lo que implica acciones de mayor alcance, coordinadas y sincronizadas gracias a la tecnología.

- **CIBERATAQUE:** Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan. El atacante busca acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios.

- **CIBERCRIMEN:** Delito muy grave cometido mediante el uso de métodos informáticos o a través de Internet o las redes virtuales.

- **CIBERDEFENSA:** Concepto que engloba todas las actividades ofensivas y defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC (redes de ordenadores, ordenadores, programas informáticos, etc.), y cuyo campo de batalla es el ciberespacio. Las actividades de desarrollo de la ciberdefensa van encaminadas hacia la capacitación de los gobiernos y naciones en la denominada Ciberguerra y el objetivo es reducir el riesgo para la seguridad a un nivel aceptable. La Ciberdefensa consta de las siguientes funciones: Proteger, Detectar, Responder y Recuperar. Se puede dividir en:

    - **CIBERDEFENSA ACTIVA:** Medidas proactivas para detectar u obtener información sobre una ciberintrusión, un ciberataque o una ciberoperación inminente, o para determinar el origen de una operación que implique el lanzamiento de una operación preventiva, preventiva o de cibercontraataque contra el origen.

    - **CIBERDEFENSA PASIVA:** Medidas establecidas para detectar y mitigar las ciberintrusiones y los efectos de los ciberataques que no implican el lanzamiento

de una operación preventiva o de contraataque contra la fuente. Ejemplos de medidas de ciberdefensa pasiva son los cortafuegos, los parches, los programas antivirus y las herramientas forenses digitales.

- CIBERINTELIGENCIA: Actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciberamenazas y se analizan las intenciones y oportunidades de los ciberadversarios con el fin de identificar, localizar y atribuir fuentes de ciberataques.

- **CIBERSEGURIDAD:** Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. Sinónimo del término Ciberdefensa. Normalmente el término Ciberdefensa se suele utilizar en el ámbito militar, y el término Ciberseguridad en el ámbito civil.

- HACKER: Término asociado a todo aquel experto de las tecnologías de comunicación e información que utiliza sus conocimientos técnicos en computación y programación para superar un problema, normalmente asociado a la seguridad. Habitualmente son técnicos e ingenieros informáticos con conocimientos en seguridad y con la capacidad de detectar errores o fallos en sistemas informáticos para luego informar de los fallos a los desarrolladores del *software* encontrado vulnerable o a todo el público. Este concepto debe diferenciarse del concepto de *cracker* ya que, si bien ambos son expertos en descubrir vulnerabilidades en sistemas, el segundo lo hace con propósitos ilícitos.

2.2. Justificación de estudio

La situación geopolítica actual marca una tendencia creciente al ciberespionaje y en los últimos años ha aumentado exponencialmente el número de países que han adquirido la capacidad de extraer inteligencia del ciberespacio, por lo que es prioritario el estudio y respuesta a esta amenaza.

El ciberespionaje es un método relativamente económico, rápido, que conlleva menos riesgos que el espionaje tradicional y facilita el anonimato, dada la dificultad de atribución de la autoría. En los últimos años, muchos gobiernos, incluyendo España, han sido víctimas de ataques persistentes a gran escala, originados en terceros países, incluidos algunos que no habían sido previamente identificados como una amenaza para las redes de los gobiernos atacados.

No solo los gobiernos son susceptibles de sufrir ciberespionaje. Las infraestructuras críticas, las empresas estratégicas y otras organizaciones relevantes componen el blanco principal, por ser objetivos cruciales de alto impacto y valor, pero también individuos particulares en posiciones de relevancia para los intereses de los atacantes.

El alcance y la magnitud de los ataques no siempre se conoce con certeza, a lo que ha de sumarse una amplia tipología de actores involucrados y ataques que continuamente adoptan nuevas formas.

Dentro del contexto del ciberespionaje debe tenerse en cuenta el desarrollo de las amenazas híbridas, que se han visto potenciadas por el avance tecnológico y el proceso de digitalización, que han favorecido la accesibilidad y la exposición de las vulnerabilidades, generando un complejo escenario para la guerra cibernética.

3. Análisis

3.1. Amenazas

En la actualidad más de cien países tienen la capacidad de desarrollar ataques de ciberespionaje y su especialización sigue creciendo, de la misma manera que lo hace la amenaza que representan. Esta amenaza, utilizada principalmente por servicios de inteligencia, está dirigida tanto al sector público como al privado y suele provenir de países que desean posicionarse de manera más favorable desde los puntos de vista político, estratégico o económico. Todo ello sin olvidar las mafias organizadas que obtienen enormes beneficios de la información que logran sustraer.

El resultado es el incremento de las campañas detectadas de ciberespionaje, tanto de motivación económica, como política. Importantes datos de investigaciones avanzadas en materia de tecnologías de la información, marítima, energética o de defensa se han exfiltrado junto con datos personales. Tales ataques son una amenaza para el desarrollo económico y la capacidad de defensa militar y confirman el interés de los atacantes en la información sensible de las empresas e instituciones.

Los servicios de inteligencia occidentales han identificado que muchos países están invirtiendo en la creación de capacidades digitales ofensivas (esencialmente: ciberguerra o guerra híbrida).

El objetivo parece claro: influir en las operaciones de información. Así, se atacan cuentas de usuario para recabar información confidencial que más tarde publica un tercero (aparentemente) independiente, al objeto de sembrar confusión y división en los oponentes. Además de ello, se ha evidenciado que muchos países están invirtiendo notablemente en la creación de capacidades digitales destinadas a un eventual o futuro sabotaje de procesos críticos.

La ocultación de los atacantes también se ha profesionalizado. Los servicios de inteligencia han observado que varios actores estatales están utilizando estructuralmente compañías privadas de TI como tapaderas para disfrazar sus actividades de espionaje. Además de ello, es sabido que las empresas de TI y las instituciones académicas son utilizadas por muchos Estados para desarrollar código dañino, lo que incrementa el potencial de los actores estatales para perpetrar ciberataques.

El ciberespionaje se está volviendo más avanzado, efectivo y profesional, relacionado con la cada vez mayor dependencia de nuestro mundo de los ordenadores y se está convirtiendo en un medio de guerra aceptado e incluso preferido. Esto no quiere decir que el ciberespionaje reemplace los medios tradicionales de guerra, pero está afectando a la naturaleza del conflicto entre Estados. Este cambio comenzó con la Guerra Fría, cuando Estados Unidos y Rusia centraron sus esfuerzos en la recopilación de información encubierta sobre la guerra directa. Debido a que la guerra total entre las principales potencias mundiales se ha vuelto menos aceptable en el mundo moderno, tiene sentido que la preferencia por estrategias más furtivas haya continuado en el siglo XXI. Especialmente en las últimas décadas, a medida que la tecnología se ha vuelto más avanzada, las herramientas de ciberespionaje se han vuelto indispensables para las operaciones militares modernas.

Aunque muchos países están cometiendo espionaje cibernético, Estados Unidos, Rusia, Corea del Norte, Irán y China son considerados los países más avanzados y prolíficos en este sentido.

La mayoría de las acciones de ciberespionaje se aprovechan de vulnerabilidades de los sistemas informáticos, agujeros de seguridad que surgen de una deficiente programación que no tiene en cuenta la seguridad en el ciclo de vida del desarrollo del software y los diversos protocolos de comunicación.

Las tácticas de ciberespionaje son variadas. Incluyen, pero no se limitan a:

- Explotar vulnerabilidades en sitios web o navegadores

- Interceptar comunicaciones

- Ataques a la cadena de suministro dirigidos a los socios del objetivo principal

- Infectar las actualizaciones de las aplicaciones de software de terceros más utilizadas

Las herramientas y procedimientos para realizar ataques a redes se pueden obtener fácilmente, en Internet por ejemplo. El ciberespacio ofrece medios para realizar ataques organizados a distancia. Solamente es necesario disponer de la tecnología necesaria. Además, permite a los atacantes esconder sus identidades, localizaciones y rutas de entrada. En el ciberespacio, las fronteras nacionales pierden su significado, ya que la información fluye a través de las divisiones políticas, étnicas y religiosas. Incluso la infraestructura (tanto software como hardware) es global en su diseño e implantación. Además, cuando varias organizaciones colaboran, a menudo crean instituciones con procedimientos compartidos que, a su vez, pueden derivar en nuevas vulnerabilidades. Un ejemplo de esto son los estándares para interoperabilidad, que permiten que los problemas creados en un continente, tengan repercusiones potenciales en las redes de otro. Como consecuencia, las vulnerabilidades están abiertas en todo el mundo, disponibles para todo aquel que quiera explotarlas y tenga capacidad para hacerlo

Para llevar a cabo estas operaciones algunos de los tipos de ataques más conocidos son:

• Virus: Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.

• Ataques DDoS, que se utilizan principalmente para interrumpir los sistemas de comunicación de la nación-estado víctima. Se prefieren los ataques DDoS porque un atacante puede implementarlos con recursos muy limitados contra una víctima más grande y poderosa.

• Código dañino, también conocido como código malicioso, maligno o «malware» en su acepción inglesa: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.

• Bomba lógica: Segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre desencadenan alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal.

• Troyano: Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.

• Gusano: Programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

Además, la tecnología digital está influyendo en el ciberespionaje de formas inesperadas. Debido a los avances en la manipulación de fotos y vídeos, una vez que un atacante obtiene acceso a las redes de sus víctimas, puede manipular lo que la víctima está viendo en tiempo real, comprometiendo así la confiabilidad de la contrainteligencia de la otra nación. Por otro lado, las actividades de espionaje no se realizan sólo mediante acciones de forzamiento o programas especiales. La existencia de ordenadores desprotegidos, conectados a su vez a dispositivos ópticos, supone una fuente potencial de información y facilitan mucho las labores de espionaje

Los atacantes se pueden clasificar atendiendo a diferentes criterios:

- Motivación: búsqueda de un cambio social o político, beneficio económico, político o militar, o satisfacer el propio ego
- Objetivo: ya sean individuos, empresas, gobiernos, infraestructuras, sistemas y datos de tecnologías de la información, públicos o privados
- Método empleado: código dañino, virus, gusanos, troyanos, etc.

Atendiendo a su autoría se pueden clasificar en:

• Ataques patrocinados por Estados: los conflictos del mundo físico tienen su continuación en el mundo del ciberespacio. En los últimos años se han detectado ciberataques contra las

infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. El ejemplo más conocido es el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico o los ciberataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino. Aquí también puede incluirse el espionaje industrial.

• Servicios de inteligencia y contrainteligencia: empleados por los Estados para realizar operaciones de información. Suelen disponer de medios tecnológicos muy avanzados.

• Ataques de delincuencia organizada: las bandas de delincuencia organizada han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como objetivo la obtención de información sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos.

3.2. Objetivos e impactos del Ciberespionaje

El ciberespionaje, como normal general, persigue los siguientes objetivos:
- Obtener ventajas estratégicas
- Obtener conocimiento gratis
- Obtener información de alto nivel que influya mucho en el PIB. (Ej. Las medidas de un estado, inversiones, innovación).

Para entender los impactos y consecuencias que provoca el ciberespionaje, es imprescindible poner en perspectiva el alcance de esta actividad, teniendo en cuenta que no existen fronteras virtuales y las fronteras físicas no pueden impedir al tráfico de información, así como su violación. El oportunismo internacional es imprescindible y tanto para las organizaciones criminales, los crackers individuales y los Estados atacantes, encontrar el momento idóneo pasa por ver cuáles son las circunstancias de la potencial víctima y cómo usar esa ventana de oportunidad.

Los impactos pueden ser varios y de distinta naturaleza, siendo los más obvios aquellos que pueden afectar a la seguridad y a la economía de los Estados, empresas y particulares. El impacto puede variar significativamente, desde la pérdida monetaria hasta el daño de la infraestructura física y las bajas civiles, y el coste puede variar de insignificante a devastador. Las infraestructuras críticas, compuestas de instituciones públicas y privadas, constituyen el sistema nervioso de las naciones desarrolladas. El ciberespacio es fundamental para su

funcionamiento y, por ello, para la seguridad de la nación. La globalización de Internet hace que los centros de gravedad de un Estado sean más vulnerables a un ataque, al ser las fronteras de la red permeables. Un ataque contra el sistema informático de una infraestructura crítica puede generar muchos daños con un riesgo mínimo para el atacante. Sin embargo, para el atacante, los costes del ciberespionaje son considerablemente más bajos que otros tipos de ataques. En el mundo cibernético se considera más fácil ser el atacante que el defensor: el defensor debe protegerse contra todas las vulnerabilidades posibles, mientras que el atacante debe encontrar solo una. Por lo tanto, es menos costoso para una nación invertir su dinero, su ejército y su tecnología en operaciones ofensivas en lugar de invertir solo en defensa.

Como empresa objetivo, la amenaza de ciberataques siempre está presente. Seguir ciertas pautas de precaución o contratar los servicios de alguna empresa de ciberseguridad puede no ser suficiente permitiendo a los hackers conseguir sus objetivos: robar datos, secuestrar servidores, instalar malware… En este contexto, se está dando un fenómeno que ha llegado a normalizarse a pesar de que las autoridades gubernamentales lo desaconsejan de forma firme, el pago de rescate realizado por las empresas para recuperar la información robada. En otras palabras, pagan a quienes les han atacado para que dejen de hacerlo. El cobro se hace con criptomonedas, que no son rastreables y se da después de que empresa y secuestrador lleguen a un acuerdo ponderado. En este punto, las empresas y los hackers deben ser conscientes de hasta dónde pueden pedir y en qué cifras deben empezar a ceder. En muchas ocasiones, además, se produce una doble extorsión o doble pago cuando los atacantes piden un rescate por la información sustraída y otro a cambio de no vender los datos.

Otro ejemplo de los impactos que pueden tener los ciberataques son las guerras de dominio o las campañas de influencia. Según el Centro Criptológico Nacional, la red social Twitter tuvo que cancelar más de 97 millones de cuentas por presunta manipulación y desinformación, únicamente en los primeros 6 meses de 2019.

La difusión de desinformación es una táctica usada frecuentemente por actores no estatales que están financiados por gobiernos, aunque los propios gobiernos también utilizan estas tácticas. El objetivo es usar una información incorrecta o manipulada para generar inestabilidad en el país contra el que se use la información. Las informaciones y su seguridad son clave para evitar filtraciones. Las «fake news» o noticias falsas, sirven para crear confusión, distorsión informativa y estimular aquellas sensaciones ciudadanas de repulsión que conduzcan a acciones disruptivas o para hacer cambiar la opinión de los ciudadanos o las sociedades para

conseguir vulnerar la toma de decisiones a favor de ciertos intereses para la parte manipuladora. Los actores que hacen uso de campañas de desinformación no siempre proceden del extranjero, sino que también pueden ser actores nacionales con intereses económicos o de control de poder.

Algunos de los elementos clave de las campañas de desinformación y que inciden directamente en el ciberespionaje son el auge de las TIC y su gran alcance y poder de difusión, el uso de perfiles sociales falsos monitorizados por agentes extranjeros que aumentan el foco de las noticias falsas y crean opinión, los algoritmos que analizan nuestras opiniones y ofrecen una descripción actualizada de nuestro estatus y el propio crackeo, ya sea obteniendo información opaca, generando un perjuicio o incluso interviniendo la cuenta social de alguien influyente que pueda generar confusión y cambios de opinión.

Algunos ejemplos de cómo se usa el espacio cibernético para la guerra de dominio los encontramos en dos sucesos políticos de la última década: la victoria de Donald Trump y el Brexit. En ambas ocasiones se usó el espacio cibernético para, conjugado con mecanismos de ingeniería social, manipular la voluntad política mediante la difusión de noticias falsas en redes sociales.

Existen distintas formas de combatir las campañas de desinformación. Evidentemente existen métodos a nivel técnico relacionados con la verificación de la fuente o del origen del código, incluso de análisis de imágenes y de metadatos. Sin embargo, la mejor forma de prevenirse ante campañas de desinformación es crear una cultura de concienciación en la que los medios implicados adquieran un criterio unificado de cómo distinguir las noticias falsas de las reales para así no difundir información falsa. La misma cultura o criterio la debe adoptar el usuario final, pues debe ser lo bastante maduro como para no caer en confusiones, verificar la credibilidad de la fuente y no basar su toma de decisiones en informaciones vagas o que no hayan sido contrastadas.

A un nivel más geopolítico, el ciberespionaje y los ciberataques subsecuentes entre Estados se usan como arma de presión que ayuda a equiparar el equilibrio de poderes entre dos países. Evidentemente, la guerra también se ha trasladado al espacio cibernético. Un ejemplo es el presunto virus israelita que se instaló en la planta nuclear de Natanz en Irán o el espionaje de la NSA a mandatarios europeos.

Por otro lado, los impactos pueden ser tangibles y subyacentes. Los tangibles son los que ya han sido mencionados (económicos, de seguridad, geopolíticos); Los impactos subyacentes son aquellos que no son consecuencia directa del ciberespionaje o los ciberataques, pero su ocurrencia no se habría dado de no ser por esta actividad. Un ejemplo sería el desastre reputacional que puede suponer para un partido político el hecho de que un hacker acceda a información confidencial, o la desventaja estratégica que implica que tu adversario empresarial conozca tus intenciones debido a infiltraciones informáticas.

El rápido avance de la tecnología puede provocar impactos aún más graves en un futuro a medio o largo plazo. Actualmente, se están desarrollando dos tecnologías que reflejan esta tendencia. La que por ahora está más desarrollada, siendo más propia de las organizaciones criminales, es la aplicabilidad de la Inteligencia Artificial y el *Machine Learning*, que combina el aprendizaje de los sistemas informáticos con la ingeniería social para conseguir refinar sus ataques de phishing o de ransomware. Un atacante puede lanzar malware que recoja información para determinar por qué un ataque no ha tenido éxito y utilizar esta información para lanzar un segundo ataque mejor adaptado a la organización objetivo. En esta misma línea, gracias a la Inteligencia Artificial, se están desarrollando técnicas como el *Targeted Attack Analysis*, con la que se ponen a prueba las organizaciones objetivo, estudiando su respuesta ante determinados estímulos y definiendo un perfil de funcionamiento de la organización desde el punto de vista de su defensa frente a ataques, lo que permite adaptar y refinar esos ataques a las especificidades de la víctima.

La otra tecnología con importantes implicaciones para el futuro del ciberespionaje es la computación cuántica. Esta tecnología ha entrado en el terreno de la seguridad nacional y en la carrera geoestratégica para controlar dicha tecnología emergente, que se espera que se consolide en 2035. El enfoque de la computadora cuántica es resolver problemas de una manera fundamentalmente nueva. Los investigadores esperan que con este nuevo enfoque de la computación puedan comenzar a explorar algunos problemas que no podrían resolverse de otra manera en campos como la energía o la medicina, pero también en la seguridad, pues puede conseguir que cualquier comunicación sea segura o proteger bajo encriptación robusta e impenetrable cualquier información.

Evidentemente, controlar esta tecnología es clave para muchos países, claramente entre otros para las grandes potencias, que tienen personal trabajando en ello. De esta tecnología se desprenden numerosos riesgos para la ciberseguridad ya que podrían sintetizarse virus informáticos más complejos, precisos y letales. Ya en 2007 un grupo de hackers con apoyo de

Rusia paralizó Estonia durante tres semanas, y otros desde Corea del Norte y China le hicieron lo propio a Corea del Sur. Así, los futuros ciberataques de una potencia con capacidades cuánticas no solo podrían sabotear la actividad de un país, sino provocar disrupciones con pérdidas económicas y humanas. Los países sin acceso a esta tecnología casi no tendrán capacidad de ciberdefensa. Esta alta capacidad de disrupción de la computación cuántica se basa en su potencial de descifrar cualquier sistema informático por muy seguro que sea y de vulnerar, manipular y destruir cualquier sistema con un código que no esté preparado para el ataque.

Respecto a España, las competencias en materia de defensa contra ciberataques le corresponden al Centro Criptológico Nacional (CCN). Dicho Centro se creó por la Ley 11/2002, de 6 de mayo, que regula el Centro Nacional de Inteligencia, e incluye al CCN. Posteriormente, por Real Decreto 421/2004, de 12 de marzo, se regula y define el ámbito y funciones del CCN. En 2019, el CCN tuvo que gestionar 42.997 ciberataques, de los cuáles, un 7,5% fueron considerados críticos o muy graves.

Según la firma neozelandesa Emsisoft, en España en 2019 hubo 8.800 incidentes de ransomware con un coste mínimo de 100 millones de euros. El informe respectivo al 2020 indica que se produjeron menos de la mitad de los incidentes, aunque aumentó el daño económico. En este caso la cifra llegó hasta los 125 millones de euros. Estas cifras no contemplan las pérdidas ocasionadas por la reducción de la actividad empresarial, por tanto, no reflejan el alcance real del perjuicio económico[1].

3.3. Estrategias de Defensa

La frontera entre el ciberataque, el ciberespionaje y el cibercrimen se diluye, ya que, en la mayoría de los casos, uno es el paso previo del otro, y además comparten las técnicas necesarias para su desarrollo. El resultado es que en la lucha para contrarrestarlos no cabe distinción. Los métodos que se desarrollen para combatirlos servirán para la lucha contra todos ellos.

[1] Aguiar, Alberto R. 2021. Los rescates de 'ransomware' provocaron en 2020 pérdidas de mínimo 125 millones de euros a firmas españolas, y ahora las administraciones están en la diana. Business Insider. Recuperado de: https://www.businessinsider.es/perdidas-ransomware-espana-crecieron-24-2020-861021

Toda estrategia diseñada para la lucha contra este tipo de amenazas debe incluir la prevención de los ciberataques contra las infraestructuras críticas de la nación, un programa para la reducción de la vulnerabilidad ante este tipo de ataques, así como medidas para la reducción de daños que éstos puedan causar y del tiempo necesario para la recuperación de los sistemas e infraestructuras afectados.

Debido a que la guerra cibernética sigue siendo una forma relativamente nueva de conflicto todavía faltan las leyes sobre su uso, tanto en el plano defensivo como en el ofensivo. Las potencias mundiales apenas comienzan a definir qué constituye un ciberataque y qué contramedidas están legalmente permitidas.

El mencionado Manual de Tallin ofrece algunas reglas para determinar qué tipos de ataques constituyen la guerra cibernética y, por lo tanto, están sujetos a regulación y posibles contraataques en virtud del derecho internacional. Este Manual ayuda mucho a las naciones a actuar después de un ataque cibernético.

La primera regla en el Manual de Tallin establece que el ciberespacio de un Estado es territorio soberano, lo que abre la posibilidad de que los ciberataques sean tratados con la misma seriedad que los ataques en territorio físico. Sin embargo, este enfoque no siempre es efectivo.

Cuando se trata del derecho internacional, las actividades que no están explícitamente prohibidas están de hecho permitidas. Las represalias solo están permitidas a un Estado cuando otro Estado ejerce un «uso ilegal de la fuerza» en contra. Por lo tanto, la propaganda, la guerra psicológica y la coerción económica o política no se consideran ilegales, incluso en el ciberespacio. En estos casos, una nación víctima puede apelar a la comunidad internacional, pero no hay garantía de que reciba ningún apoyo.

La disuasión es una estrategia útil de contraespionaje para los Estados con la autoridad y los recursos para llevarla a cabo. Se produce cuando una nación convence a su enemigo de que está dispuesta y puede responder a las intrusiones cibernéticas utilizando la fuerza militar. El propósito es asustar a otros Estados para que no cometan ciberataques y así evitar la necesidad de represalias reales.

Por supuesto, cuando la simple disuasión no funciona, un Estado siempre puede recurrir a represalias con fuerza física, pero esta estrategia es muy poco común. A menudo es difícil determinar la identidad de un atacante, por lo que no sería práctico perder tiempo y recursos

en una operación militar si una nación no estuviera completamente segura del origen del ataque.
Una de las soluciones más efectivas que podrían implementarse en un futuro sería la cooperación internacional y los tratados. Similar a la carrera de armamentos nucleares, las grandes potencias mundiales pueden reconocer que la guerra cibernética es una carrera sin fin y pueden elegir simplemente detenerla pacíficamente.

Por lo general, las disputas cibernéticas en los últimos tiempos se resuelven a través de los tribunales. En el caso de la disputa entre Estados Unidos y China, por ejemplo, Estados Unidos ha estado capacitando a abogados para manejar casos de ciberataques internacionales como parte de su estrategia de contraespionaje.

Finalmente, siempre existe la opción de combatir un ataque cibernético respondiendo con otro. Esta no es siempre una opción disponible, ya que muchas naciones carecen de la tecnología para igualar a su atacante, pero una operación cibernética defensiva no necesita ser sofisticada para hacer daño.

3.3.1. Estrategias de defensa en la UE

- Cronología legislativa/Principales hitos en la lucha contra los ciberataques en la UE

La historia reciente de la UE en la lucha contra las actividades delictivas en el ciberespacio nos lleva a 2016. En este año, el Consejo realizó dos textos de conclusiones, instando a la mejora de la cooperación en la lucha contra este tipo de actividades y creando un calendario de actuaciones futuras. Dentro de estas conclusiones se instaba a una racionalización en los procedimientos de asistencia judicial y el desarrollo de una mejor cooperación con los proveedores de servicios online. En el mismo año se aprobó la Directiva de Seguridad de Redes y Sistemas de Información (directiva NIS).

El 24 de octubre de 2017, el Consejo de la UE a través del Consejo de Transporte, Telecomunicaciones y Energía, consiguió un acuerdo para la creación de un plan de acción para la reforma de la ciberseguridad. Dentro de este pacto, se debían incluir elementos para la defensa y disuasión de los ciberataques, una propuesta de ley de ciberseguridad, una actualización de la Agencia de la Unión para la Seguridad de las Redes y la Información (ENISA), la creación de un marco de certificación en la UE para productos TIC y una propuesta legislativa de directiva sobre la lucha contra el fraude. Sin embargo, el pacto más importante de 2017 en

materia de ciberseguridad fue el acuerdo interinstitucional a través del cual se creó un Equipo de Respuesta a Emergencias Informáticas (CERT-UE). Este equipo sería a partir de entonces el encargado de dar una respuesta coordinada a todas las instituciones en la lucha contra los ciberataques que estas pudieran sufrir. Este grupo ya existía previo al acuerdo de 2017, pero a través de éste se consolidó como un equipo de respuesta permanente.

Otro de los eventos de mayor importancia en materia de ciberseguridad de 2017 fue la creación de instrumentos conjuntos de ciberdiplomacia. Se adoptó un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas, tratando así de reducir las amenazas gracias a la cooperación entre los Estados de la UE.

En 2018 el Consejo manifestó su preocupación por la capacidad de agentes no estatales y Estados no pertenecientes a la unión, de realizar actividades informáticas «malintencionadas». Además, se reiteró la estrecha colaboración con otras organizaciones internacionales, en particular las Naciones Unidas, la OSCE y el Foro Regional de la ASEAN. Este mismo año, se actualizó el Marco político de ciberdefensa de la UE, estableciendo como prioridades el apoyo en el desarrollo de las capacidades de ciberdefensa de los Estados miembros, mejorar la protección de las redes de comunicación utilizados por entidades de la UE, el fomento de la cooperación cívico-militar, un fomento del desarrollo tecnológico y una mejora en las posibilidades educativas de los ciudadanos europeos.

La Ley de ciberseguridad permitió la introducción de una certificación de ciberseguridad, facilitando así la confianza de los usuarios en los productos tecnológicos y apoyando a las empresas en su desarrollo de actividades internacionales. Esta certificación es voluntaria y posee tres niveles diferentes basados en el nivel de riesgo asociado a la utilización prevista del producto.

En 2019 se estableció el marco legislativo que permite a la UE imponer medidas restrictivas específicas para disuadir y contrarrestar los ciberataques que representen una amenaza para la UE o sus Estados miembros, en particular los perpetrados por terceros Estados u organizaciones internacionales. Las sanciones son aplicables a personas o entidades responsables de ciberataques o tentativas de ciberataques, o que presten para ello apoyo financiero, técnico o material o estén implicadas de algún otro modo, así como a las personas y entidades asociadas con ellas.

Adentrados en la pandemia global de la COVID-19, en diciembre del 2020 el Consejo instó a reforzar la resiliencia y a luchar contra las amenazas híbridas, en particular contra la desinformación. Se creó entonces la Estrategia de Ciberseguridad de la UE, la cual permite a la UE intensificar el liderazgo internacional en la creación de normas sobre el ciberespacio, refuerza la resiliencia cibernética e insta a un aumento en la colaboración internacional. Además, se presentaron para el estudio de la Comisión una Directiva sobre medidas para un alto nivel común de ciberseguridad en toda la Unión y una nueva Directiva sobre resiliencia de entidades críticas.

El ultimo hito dentro de la legislación europea sobre ciberataques se ha producido en junio del 2021. La Comisión Europea realizó una recomendación para la creación de una Joint Cyber Unit. El objetivo de esta unidad sería la creación de una unidad informática única para enfrentar de forma unitaria y coordinada los ciberataques a empresas, ciudadanía y organismos públicos.

Existen tres documentos clave en la creación de la nueva estrategia en ciberdefensa de la UE:

- Horizonte Europa. Es un programa de financiación de la UE para la investigación e innovación, cuyos objetivos finales son los ODS, el aumento de la competitividad y el crecimiento de la unión.

- Europa Digital. Este marco trata de ampliar las capacidades e infraestructuras de la UE en materia de ciberseguridad.

- Plan de Recuperación. Ante la necesidad de dar una respuesta a la pandemia global de la COVID-19, este plan incluye fuertes inversiones ante el incremento de ciberataques durante la misma.

3.3.2. Organismos para ciberseguridad de la UE

La UE se ha dotado de organismos públicos para la lucha contra los ciberataques a lo largo de los años. Cada organismo posee unas competencias definidas, diferenciándose según los objetivos de las mismas. Los organismos con mayor importancia son:

- **Alto Representante de la UE para Asuntos Exteriores y Política de Seguridad.** El actual Alto Representante es el español Josep Borrell. Las funciones del cargo son la dirección de la política exterior y de seguridad común (PESC), la dirección de la Agencia Europea de Defensa y la

dirección del Consejo de Asuntos Exteriores. Bajo su mandato también se encuentran el Servicio Europeo de Acción Exterior (SEAE) y el Comité Político y de Seguridad (CPS).

- Agencia Europea de Defensa (AED). Este organismo constituye un foro de debate para los ministros de Defensa de los Estados miembros. Su función principal es el apoyo a proyectos de cooperación en defensa europea.

- **Agencia de la Unión para la Seguridad (ENISA).** Esta organización realiza un asesoramiento a los Estados miembros e instituciones europeas en cuestiones cibernéticas. Colabora con las políticas europeas de certificación de la ciberseguridad, organiza ejercicios periódicos y simulaciones y ha apoyado la creación de una red de funcionarios de enlace nacionales para una mayor facilidad en el intercambio de información entre los Estados miembros. ENISA ha creado un inventario de Equipos de respuesta ante emergencias informáticas (CERT), clasificándolos por países.

- **Centro Europeo Industrial, Tecnológico y de Investigación en Ciberseguridad.** La principal función de la organización es procurar un aumento en la seguridad de las redes y de los sistemas de información de la UE y reforzar la coordinación en investigación e innovación en ciberseguridad.

- **Red de Centros Nacionales de Coordinación (NCC).** Está constituida por un tejido de centros especializados en ciberseguridad, los cuales son designados por los Estados miembros.

- **Centro de Competencias en Ciberseguridad (ECCC).** La función principal del centro es un aumento en la competitividad de la ciberseguridad en Europa. Para cumplir dicho objetivo se encargará de la coordinación y toma de decisiones de las inversiones conjuntas en proyectos de ciberseguridad en la UE. El ECCC trabajará para la exitosa consecución del Programa Europa Digital y los programas Horizonte Europa.

- Centro Europeo de Ciberdelincuencia (EC3). El EC3 es uno de los órganos especializados que se integran en la EUROPOL, junto con el Centro Europeo de Lucha contra el Terrorismo (ECTC) y el Europeo Contra el Tráfico Ilícito de Migrantes (EMSC). El organismo se centra en tres tipologías de delitos: ataques contra actividades financieras, explotación sexual infantil online y delitos contra infraestructuras críticas de la UE.

- **Plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT).** Esta plataforma se creó por iniciativa de los Estados miembros de la UE con el objetivo de abordar las amenazas que representan la delincuencia internacional, por lo que la ciberdelincuencia se encuentra entre sus prioridades.

- **Asociaciones público-privadas:** Además de estas organizaciones públicas, existen algunas asociaciones financiadas por la Comisión Europea como la Organización Europea de Seguridad Cibernética (ECSO), EU Robotics, Big Data Value Association (BDV), Alliance for Internet of Things Innovation (AITI), European factories of the Future Research Association (EFFRA), 5G Infraestruture Association (5G IA), International Association for Trusted Blockchain Applications (INATBA), Sustainable Process Industry through Resource and Energy Efficiency (SPIRE), Shaping Digital Innovation (ECSEL), entre otras.

3.3.3. Publicación de datos/Transparencia

Dentro de la Unión Europea es obligatoria la notificación de vulneraciones de la ciberseguridad para las empresas. Esta responsabilidad se encuentra recogida en la Directiva de la UE sobre seguridad de redes y sistemas de información (Directiva NIS), la cual está en vigor desde 2018. La directiva introduce normas de notificación de incidentes en ciberseguridad para empresas de servicios esenciales en sectores críticos como la energía, transporte, finanzas y salud.

El encargado de la recopilación anual de los ciberataques dentro de la Unión Europea es ENISA, la cual realiza un informe anual. En dicho informe se elabora un análisis sobre los 15 ciberataques más frecuentes en el año en curso, una clasificación de los mismos por sectores y una recopilación de los principales incidentes a nivel mundial.

3.3.4. Elementos de ciberdisuasión dentro de la UE

La UE ha creado mecanismos que tratan de eliminar el estímulo o aliento para la realización de ciberataques a los organismos públicos de la organización. Los más importantes son la ciberdiplomacia, las sanciones económicas, la ciberresiliencia, el sistema de certificación, los sistemas de prevención y detección y la protección de infraestructuras críticas.

- **Ciberdiplomacia**. La diplomacia es conocida por ser el mecanismo que se encarga de la formulación y ejecución de la acción exterior de los Estados. Con la llegada de la globalización y el avance tecnológico, los Estados se han visto obligados a generar nuevas herramientas dentro de las tecnologías y la comunicación para continuar

desarrollando su influencia. Es un instrumento que incluye la cooperación y el diálogo diplomáticos, así como medidas preventivas contra los ciberataques y sanciones.

- **Sanciones económicas.** Gracias al nuevo marco legal creado en mayo de 2019 que permite las condenas monetarias, el 30 de julio del 2020 se realizó la primera sanción contra seis personas y tres entidades responsables de diversos ataques informáticos. Estas sanciones fueron realizadas contra los responsables del intento de ciberataque contra la OPAQ (Organización para la Prohibición de las Armas Químicas) y los conocidos como «WannaCry», «NotPetya» y «Operation Cloud Hopper».

- **Ciberresiliencia**. La resiliencia es la «capacidad de adaptación de un ser vivo frente a un agente perturbador». Por lo que la ciberresiliencia, según el INCIBE, es la «capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes». Esta herramienta fue uno de los pilares fundamentales dentro de la Estrategia de Ciberseguridad de la UE presentada en diciembre del 2020. El objetivo principal de la estrategia es «reforzar la resiliencia de Europa frente a las ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables». Además, en marzo del 2021 el Consejo aprobó unas Conclusiones sobre la Estrategia de Ciberseguridad en las que se resaltó que la ciberseguridad es esencial para construir una Europa resiliente, ecológica y digital.

- **Sistema de certificación.** Este consiste en un método de autentificación para lugares web, el cual asegura que estos cumplen con las reglas, requisitos técnicos y procedimientos establecidos por la UE. De este modo, los usuarios aumentarán su confianza y aumentará la seguridad en aquellas páginas web que posean la certificación europea.

- **Sistemas de prevención y detección.** Elementos como la protección de redes inalámbricas, cortafuegos, cifrados y herramientas para el control de tráfico de red son algunos de los más extendidos. Sin embargo, dentro de estos mecanismos no se encuentran los ataques preventivos. La realización de acciones preventivas de detección es posible gracias al aumento en la financiación de la investigación dentro de la unión.

4. Caso de estudio: SolarWinds

SolarWinds es la empresa que fabrica Orión, un software de gestión y administración que utilizan las empresas de la lista Fortune500[2] y las principales instituciones públicas de EE.UU, así como otras empresas internacionales. El código de actualización que utilizaba SolarWinds para este producto fue modificado por los atacantes que consiguieron infectar a los clientes de la empresa a través de una actualización oficial.

El incidente fue reconocido de forma pública el 13 de diciembre de 2020 por la firma de seguridad informática estadounidense FireEye, que detectó actividades inusuales en su red. Sin embargo, las operaciones habían comenzado meses antes.

FireEye descubrió que los hackers insertaron el código malicioso SurnBust en las versiones 2019.4 a 2020.2.1 de Orión, publicadas entre marzo de 2020 y junio de 2020. Lo que les permitió acceder de forma remota a los sistemas de más de 18.000 clientes de SolarWinds.

A medida que los clientes descargaban los paquetes de actualización de SolarWinds, los atacantes podían acceder a los sistemas de las empresas que ejecutaban estos productos. Los ataques pasaban inadvertidos por las víctimas ya que los intrusos aparentaban ser empleados al contar con certificados de confianza.

Una segunda oleada de ataques se registró el 19 de diciembre de 2020, bajo el nombre de SuperNova. El tercer incidente significativo fue dirigido a organizaciones no gubernamentales y tuvo lugar el 28 de mayo de 2021.

Para solucionar la vulnerabilidad de la seguridad, SolarWinds notificó el ataque a sus clientes, pidiéndoles que actualizaran inmediatamente a la nueva versión presentada, pero existe la posibilidad de que, aún en este momento, haya afectados que no sepan que han sido atacados.

Por su complejidad y nivel de sofisticación el ataque se atribuye a Rusia, aunque ante la falta de pruebas, este país ha exigido que, o se justifique su autoría o se deje de incriminarle. El 23 de febrero de 2021 se realizó la primera audiencia del congreso de los Estados Unidos por este asunto sin resultados determinantes.

[2] Lista anual de las corporaciones más grandes de los Estados Unidos, clasificada por ingresos para el año fiscal.

Los detalles del ataque a SolarWinds continúan saliendo a la luz y puede que pasen años antes de que se puedan contabilizar los daños finales. Este ataque no tiene precedentes por su capacidad de causar daños importantes, ya que impactó en los proveedores de infraestructuras críticas, afectando potencialmente a las capacidades energéticas y de fabricación y creó una intrusión continua que debe ser tratada como un evento serio con potencial de gran daño.

5. Ejercicio práctico de análisis de escenarios simples

En esta parte del informe nos planteamos la creación de un análisis de escenarios simples como ejercicio práctico. El objetivo no es predecir el futuro, sino poner sobre la mesa posibles escenarios a los que el Gobierno de España puede llegar a enfrentarse en relación con el ciberespionaje. Según Heuer y Pherson, en su libro «Técnicas analíticas estructuradas para el análisis de inteligencia», esta técnica se usa comúnmente cuando las estrategias nacionales se encuentran en fase de formulación en campos demasiado complejos como para confiar en una única predicción.

Desarrollo del ejercicio:

1.- Definimos el asunto esencial y los objetivos específicos

- Asunto esencial: establecer los posibles escenarios en los que España se puede encontrar en lo relativo al ciberespionaje y sus efectos

- Objetivos específicos:

1. Identificar impulsores que puedan influir en el escenario actual
2. Identificar indicadores que nos permitan predecir la ocurrencia o no ocurrencia de los escenarios en el futuro

2.- Lista de impulsores que pueden influir en el futuro del ciberespionaje.

- Impulsores no filtrados:
    - Innovación tecnológica de las instituciones orientada a la protección de información.
    - Separatismo.
    - Inestabilidad política.
    - Infrafinanciación.
    - Poder e influencia geoestratégica de España en el escenario mundial.
    - Poder e influencia de los países aliados de España.
    - Capacidad cibernética de Rusia.
    - Capacidad cibernética de China.

- Terrorismo contra España.
- Proliferación de cibercrimen/ Delincuencia organizada.
- Capacidad defensiva del CCN, CNI, Policía Nacional y Ministerio de Defensa.
- Conflictos ideológicos con otros países.
- Conflictos comerciales con otros países.
- Conflictos militares con otros países.

- Agrupamos los impulsores que tienen afinidad entre sí.

- Inestabilidad política interna
- Capacidades cibernéticas defensivas de las instituciones gubernamentales y empresas de España
- Capacidades cibernéticas de los adversarios de España
- Poder e influencia geoestratégica de España y sus aliados
- Terrorismo contra España
- Contexto favorable al cibercrimen y delincuencia organizada
- Conflicto con otros países

3.- Creamos una matriz con la lista de impulsores a la izquierda y los posibles escenarios en la parte superior.

- Posibles escenarios:

- Escenario favorable
- Escenario medio
- Escenario no favorable
- Escenario crítico.

- **Asignamos valor + o – por cada impulsor y en cada escenario.**

En este caso el símbolo + implica ocurrencia del impulsor, y el símbolo – implica no ocurrencia.

La ocurrencia o no de los impulsores es lo que influirá en cada uno de los escenarios.

	Escenario favorable	Escenario medio (contextualizado)	Escenario crítico	Escenario adicional
Inestabilidad política interna	-	-	+	-
Capacidades cibernéticas defensivas	+	+	-	+
Capacidades de los adversarios	-	+	+	+
Influencia geoestratégica de España	+	+	-	+
Terrorismo contra España	-	+	+	-
Cibercrimen y delincuencia organizada	-	-	+	-
Conflictos con otros países	-	+	+	+

4.- Hacemos una descripción escrita de cada escenario planteado y describimos las implicaciones que estos tendrían

El primer escenario, el favorable, es aquel en el que España se encuentra dentro de un contexto de estabilidad política interna, sin separatismos ni polarización que dificulte la gobernabilidad del país y el funcionamiento de las instituciones. Tampoco se da una situación de conflicto ideológico o militar con ninguna otra nación o grupo terrorista y los mecanismos cibernéticos defensivos no permiten a la delincuencia organizada operar en el país. Este escenario implicaría un cierto descenso de los ataques dirigidos a instituciones o empresas españolas y por tanto sus efectos.

El segundo escenario, es probablemente el escenario más real y actualizado de la situación a la que deberá enfrentarse España en cuanto al ciberespionaje. Un contexto en el que el sistema político y social se vea desestructurado por el auge de separatismos o de crisis económicas puede conllevar cierto nivel de inestabilidad política que ofrezca ventanas de oportunidad para

el ciberespionaje, por ejemplo, con campañas de desinformación que afecten la toma de decisiones de las personas. Sin embargo, las capacidades defensivas de los organismos encargados siguen siendo robustas y el tejido gubernamental y empresarial, a pesar de recibir ataques constantemente, consigue evitar que se produzcan daños mayores con pérdidas económicas demasiado grandes.

Evidentemente las capacidades de países como Irán, China, Rusia y Pakistán serían significativamente altas y España podría ser un objetivo de sus ataques o campañas de desinformación dada su posición estratégica, dentro de la UE y aliado del bloque occidental. En este escenario no estaríamos en conflicto directo con ninguna nación, ni mucho menos de tipo militar, pero la idiosincrasia ideológica y el conflicto de intereses podría provocar que España fuese el blanco de multitud de ataques cuyo origen serían naciones adversarias. A pesar de que la eficacia de los servicios de seguridad ante el terrorismo sea muy alta, en este escenario persistiría cierto nivel de amenaza en este sentido. Lo mismo pasaría con el cibercrimen, pues a pesar de los bien orientados esfuerzos de la policía, un país sin ciberdelincuencia sería irreal. Este escenario implicaría que las defensas españolas en este ámbito tendrían que mantenerse alerta a fin de evitar pasar a estadios más peligrosos para la ciberseguridad general del país.

El tercer escenario es aquel que se asemeja al primero en el sentido de que también es un escenario cuya probabilidad de ocurrencia es muy baja o incluso irreal. Estamos hablando de un escenario en el que existe una inestabilidad política imperante en el país y donde la fractura social ha desvirtualizado cualquier poder político de distensión. En este caso las defensas cibernéticas de los órganos encargados de la seguridad serían de nivel muy bajo y por lo tanto España sería vulnerable a cualquier ataque por parte de sus adversarios, grupos terroristas y cibercriminales. Las pérdidas de datos y económicas serían devastadoras para muchas empresas y para el Estado en sí. La sociedad sufriría los efectos de continuas campañas de desinformación por parte de Rusia y China. Nuestra influencia geoestratégica dentro de Europa y en el Mediterráneo se vería alterada por nuestra vulnerabilidad e inestabilidad. Las infraestructuras críticas del país como, por ejemplo, aeropuertos, centrales nucleares o centros de logística se verían bajo constante amenaza por los grupos terroristas.

El cuarto escenario, es un escenario que, en el libro de Técnicas Analíticas Estructuradas para el Análisis de Inteligencia, de Heuer y Pherson, se aconseja desarrollar a fin de plantear escenarios que no sean bipolares o que se orienten demasiado al centro. En este caso, el escenario implicaría que España no gozase de un alto nivel de estabilidad política, sin embargo,

las defensas cibernéticas serían lo bastante avanzadas como para detener los efectos adversos en la economía de los ciberataques y el ciberespionaje.

Evidentemente las capacidades ofensivas de los adversarios seguirían siendo fuertes y la posición geopolítica española, afín a los intereses de Europa, implicaría que fuésemos el blanco de campañas de desinformación y sabotaje por parte de países como Rusia.
Estos conflictos ideológicos con otros países serían los que añadirían vulnerabilidad en cuanto a las campañas de desinformación, que son más difíciles de detectar y contrarrestar. Por otro lado, las capacidades defensivas ayudarían a equilibrar de forma positiva la influencia del cibercrimen y los posibles ataques terroristas no sucederían.

5.- Hacemos una lista de aquellos indicadores que debemos observar para ver cómo se van desarrollando los acontecimientos en el futuro.

A continuación, creamos una lista de todos aquellos indicadores que, por su relevancia, pueden ayudarnos a entender si alguno de los impulsores que hemos mencionado se está desarrollando y, en consecuencia, lo hace el escenario correspondiente. Los indicadores son:

- Índices de ciberdelitos
- Evolución geopolítica de las amenazas provenientes de Rusia, China o cualquier otro país
- Detrimento o mejora de las capacidades defensivas de España
- Detrimento o mejora de las capacidades ofensivas de otros países
- Aparición de contextos de inestabilidad política que favorezcan la desinformación
- Nivel de terrorismo

6. Conclusiones

- En la actualidad, ante el gran desarrollo y difusión de los sistemas de información, y la dependencia de ellos de las sociedades modernas, el ciberespacio se presenta como un gran campo para el espionaje. Sin embargo, ésta no es la única oportunidad que brinda a los potenciales agresores, ya que puede ser empleado también como vehículo para todo tipo de actividades ilegítimas

- El ciberespionaje constituye uno de los problemas más importantes actualmente y, a medida que las sociedades se vuelvan más tecnológicas, será una práctica predominante, con impactos más graves en un futuro a medio o largo plazo.

- El uso global de las tecnologías de la información para la gestión de casi cualquier actividad ha creado nuevas amenazas a la discreción y seguridad de modo que con un ataque es posible acceder a mayor cantidad de información y en menos tiempo.

- El ciberespionaje puede ser utilizado tanto contra el sector público como contra el sector privado y afectar a diferentes campos, fomentado por los menores riesgos y la posibilidad de anonimato.

- No existe una legislación internacional concluyente en relación al ciberespionaje.

- Las nuevas tecnologías crean nuevas vulnerabilidades. Una mayor inversión en ciberseguridad es imprescindible para protegerse del ciberespionaje y los ciberataques.

- La cooperación internacional y los tratados serán piezas clave para la lucha contra el ciberespionaje. En este sentido, el intercambio de información sobre incidentes es fundamental.

- La Unión Europea ha desplegado una serie de iniciativas legislativas y organismos para combatir el ciberespionaje y los ciberataques y sus consecuencias.

7. Bibliografía

- Aguiar, Alberto R. 2021. **Business Insider**. https://www.businessinsider.es/perdidas-ransomware-espana-crecieron-24-2020-861021

- Ayerbe, Ana. 2020. **La ciberseguridad y su relación con la Inteligencia Artificial**. Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial

- Rodríguez, Andrea G. 2021. **La carrera por dominar la computación cuántica, la próxima revolución tecnológica.** El orden mundial. https://elordenmundial.com/carrera-dominar-computacion-cuantica-revolucion-tecnologica/

- Salvador, Antonio. 2021. **2020, año récord de ciberataques.** El independiente. https://www.elindependiente.com/espana/2021/01/01/2020-ano-record-en-ciberataques/

- Centro Criptológico Nacional. 2020. Ciberamenazas y tendencias. Edición 2020. CCN-CERT IA-13/20. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

- Seguritecnia, 2019. https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/3573-ciberespionaje-una-amenaza-al-desarrollo-economico-y-la-defensa/file.html

- Baker, Pam. 2021. CSO España. https://cso.computerworld.es/cibercrimen/cronologia-del-ciberataque-a-solarwinds

- Puime Maroto, Juan. 2009. La violencia del siglo XXI. Nuevas dimensiones de la guerra. https://dialnet.unirioja.es/servlet/articulo?codigo=4549946